# Diagnostic and Troubleshooting Guide for CBX 500

*Ascend Communications, Inc.*

Product Code: 80050
Revision 00
May 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

## 2 Monitoring Trunks and Circuits

# A Trap Alarm Condition Messages

# B Summary of Error Codes

# C Console Commands

## D Using Copy Database



## E Signalled QoS, BBC, and BEI Service Category Mappings

# List of Figures

# List of Tables

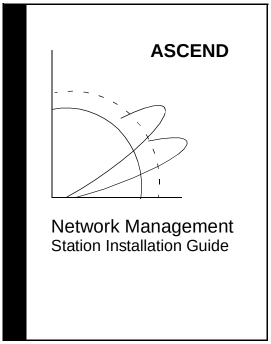
# About This Guide

The *Diagnostic and Troubleshooting Guide for CBX 500* describes how to monitor and troubleshoot activity and events on a Cascade-switch network. This guide describes the features supported in CascadeView/UX Release 2.4 and CBX 500 switch software, Release 2.0. For information on using HP OpenView functions, refer to the appropriate HP documentation.

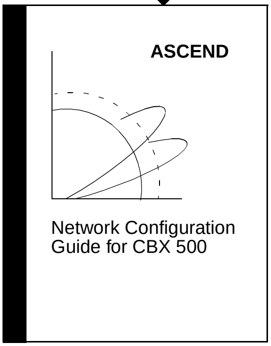
> *Read the CascadeView/UX and CBX 500 Software Release Notices for additional information about these products.*

# Documentation Reading Path

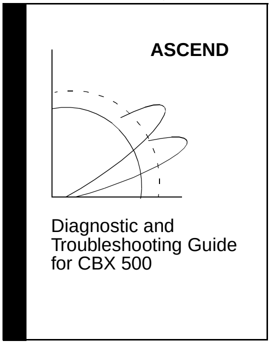
The following manuals provide the complete document set for NMS Release 2.4/CBX 500 Release 2.0:




This guide describes prerequisite tasks, hardware and software requirements, and Solaris, HP Openview, 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 in the back of this guide and return it to us.

# How to Use This Guide

This section highlights the chapters and contents in this guide.

| Read | To Learn About |
|---|---|
| Chapter 1 | Monitoring Cascade objects on the network. |
| Chapter 2 | Monitoring trunks and circuits. |
| Chapter 3 | Node-level diagnostic information for a selected switch, as well as physical and logical port-level diagnostic information. |
| Chapter 4 | Using loopback tests to troubleshoot physical and logical ports and circuits. |
| Chapter 5 | Generating real-time statistics to monitor and troubleshoot the Cascade network. CascadeView/UX generates statistics for a selected physical port, logical port, circuit, or trunk. This chapter also describes how to set the statistics polling interval. |
| Chapter 6 | Performance monitoring statistics for physical ports. |
| Chapter 7 | Using the Event Categories window to display or delete events, add event categories, and move events from one category to another. |
| Chapter 8 | Configuring and using Network Traffic Management (NTM) and Network Data Collection (NDC) on the CBX 500 switch. Cascade has based the functional requirements for NTM and NDC on the Bellcore GR-1248 specification [GR1248]. |
| Chapter 9 | Using the Management Information Base (MIB) browser to display information about specific CascadeView/UX MIB objects. |

| Read | To Learn About |
|---|---|
| Chapter 10 | Troubleshooting NMS software application problems. Unless otherwise noted, this guide addresses software problems and their solutions. If you suspect hardware problems, refer to the *CBX 500 Hardware Installation Guide.* |
| Appendix A | Trap alarm messages and descriptions. |
| Appendix B | Error codes and suggested resolutions. |
| Appendix C | Console commands that you can use to perform various switch tasks or to obtain switch information. |
| Appendix D | The Copy Database utility, which enables you to copy data into or out of any CascadeView/UX database. |
| Appendix E | Signalled QoS, BBC, and BEI Service Category Mappings. |
| Appendix F | Using SVC failure location information displayed in the failure location and failure cause fields on the Show Failed Call Attributes dialog box. |

# What’s New in This Guide?

Table 1 lists new product features in this release, as well as enhancements and changes made to this guide. Some of this information was previously available only in Technical Tips or Software Release Notices.

**Table 1. NMS Release 2.4 Features**

| New Features | Enables You to... | Described in... |
|---|---|---|
| SVC Route Tracing | View a hop-by-hop trace of active SVCs that traverse multiple switches using the Show All Active SVCs dialog box. Use this feature to determine which trunks in the network an SVC traverses. | Chapter 2 |
| Configurable SVC Trap Thresholds | Display a value for the number of SVC failures that can occur on a UNI port before a trap is issued. | Chapter 2 |
| SVC Release Call Function | Release individual SVCs on a UNI port without affecting other SVCs on the same port. | Chapter 2 |
| SVC OAM Support | Generate OAM loopback cells out the UNI endpoints. This release provides full support of ATM Layer OAM Fault Management functions for SVCs. | Chapter 4 |
| SVC Statistics | Display individual per VC cell count statistics for every SVC in the network. The format of SVC statistics is similar to PVC statistics. You can use SVC statistics to monitor and troubleshoot SVC usage. | Chapter 5 |
| Physical Layer Performance Monitoring | Detect performance degradation in network elements at the physical layer level. | Chapter 6 |

Table 1. NMS Release 2.4 Features (Continued)

| New Features | Enables You to... | Described in... |
|---|---|---|
| Trap Filtering | Filter traps that you do not want the switch to send to the Events Browser. The switch forwards *only* unfiltered traps to the NMS. You can filter specific traps or traps based on severity level. | Chapter 7 |
| GR 1248 Compliance (NTM/NDC) | The Bellcore GR1248 compliance implementation for Network Traffic Management (NTM) and Network Data Collection (NDC) is a component of the overall Bulk Statistics architecture. NTM reports traffic utilization such as the cell loss percentage and buffer usage. NDC reports network trends and shows violations of service subscription parameters on VCs. | Chapter 8 |
| IOA Type Mismatches | Use the “show card” console command to view information about the type of installed IOA. | Appendix C |

# Related Documents

This section lists the related Cascade and third-party documentation that you may find useful for reference.

## Cascade

- *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)
- *Cascade Enterprise MIB Definitions* (80015)
- *SYBASE 11 SQL Server Upgrade Guide* (80040)
- *Upgrading to Solaris 2.5.1 and HP OpenView 4.11* (80045)
- *Accounting System Administrator's Guide* (80046)
- *Bulk Statistics Collector for CBX 500 User's Guide* (80047)
- *ATM Flow-Control Processor User's Guide* (80048)
- *Network Configuration Guide for CBX 500* (80049)

## 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*

# 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`** |
| `Courier` | Screen or system output. | `Please wait...` |
| **[*bold italics*]** | Variable parameters to enter. | **[*your IP address*]** |
| `<Return>` | Press Return or Enter. | `<Return>` |
| **Boldface** | User input in text. | Type **cd install** and ... |
| Menu ⇒ Option | Select an option from the menu. | CascadeView ⇒ Logon |
| Gray boxes surrounding text | Notes and warnings. | See examples below. |
| *Italics* | Book titles, new terms, filenames, directories, and emphasized text. | *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.*

1

# Monitoring the Network

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

*You do not need to log on to display information through the Monitor menu. Monitoring functions do not require Operator passwords.*

# Accessing the Monitor Menu Functions

Table 1-1 references the section of the book that describes each of the functions you can access from the Monitor menu.

**Table 1-1. Monitor Menu Options**

| Select Monitor ⇒ Cascade Objects ⇒ | To view | Refer to |
|---|---|---|
| Show Detail. | Switch back panel. | "Viewing Switch Details" on page 1-11 |
| Show Detail. Double-click on the SP card slot and select Active at the prompt. | Attributes for the switch processor (SP) and system timing. | "Viewing Card Status for a Switch Processor Module" on page 1-17 |
| Show Detail. Double-click on the IOM card slot. | Attributes for the selected IOM. | "Viewing Card Status for an IOM" on page 1-25 |
| Show Detail. Double-click on the physical port. | Attributes and status messages for the selected physical port. | "Reviewing the Status of Physical Ports" on page 1-29 |
| Show Detail. Double-click on the physical port. Choose Logical Port. | Attributes and status messages for the selected logical port. | "Viewing Logical Port Status" on page 1-39 |
| Show All Subnets. | Subnets for this network map. | "Viewing Subnets" on page 1-59 |
| Show All Clusters. | Clusters for this network map. | "Viewing Clusters" on page 1-60 |
| Show All Switches. | Switch attributes. | "Viewing Switch Status" on page 1-61 |

# Monitoring the Network Map

After you download a network configuration, you can monitor the status of a network map using the color-coded status indicators described in Table 1-2.

**Table 1-2. Network Map Status Indicators**

| Object Color | Description |
|---|---|
| Yellow | An I/O module in the switch may be out of synch. Display the Show Switch Back Panel dialog box and review the status of each module. If necessary, synchronize PRAM. |
| Wheat | The switch object is not managed. You unmanage an object to prevent the NMS from polling the object while you configure it. To manage an object, from the Options menu, select Manage Object. |
| Red | The indicated object is in a failed state and cannot actively communicate with the NMS. |
| Green | The indicated objects/switches are actively communicating with the NMS. |

# Viewing an Object Description

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

- A selected object on the network map
- Map description for a selected object
- Submap description for a selected object

## Displaying an Object Description

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

1. Select the switch object on the network map.
2. From the Edit menu, select Describe/Modify Object. The following dialog box appears.

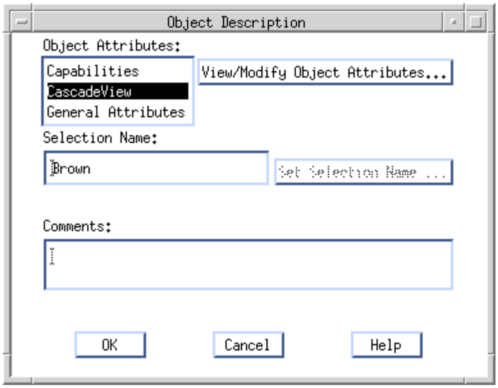



**Figure 1-1. Object Description Dialog Box**

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

*Refer to the* HP OpenView User's Guide *for information about modifying Object Capabilities and General Attributes.*

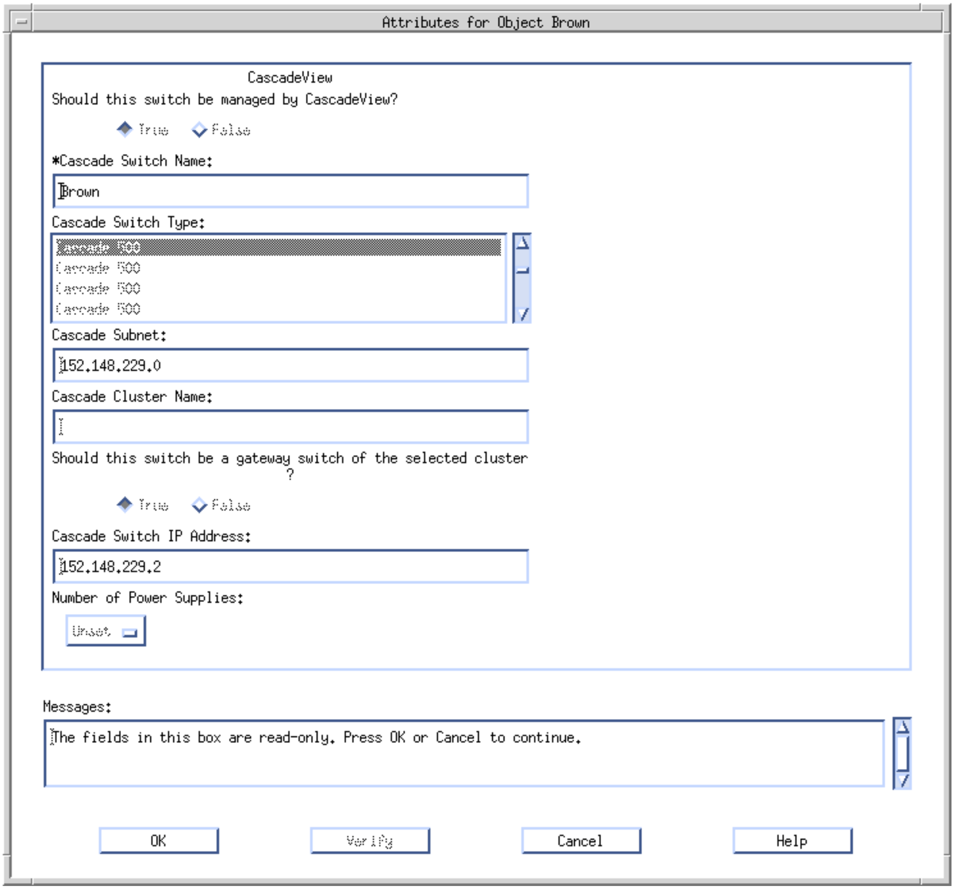



**Figure 1-2. Attributes for Object [Switch] Dialog Box**

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

**Table 1-3. Attributes for Object Fields**

| Field | Action/Description |
|---|---|
| Should this switch be managed by CascadeView? | Displays *True* if CascadeView manages the switch. |
| Cascade Switch Name | Displays the switch name. |
| Cascade Switch Type | Displays the switch type (CBX 500). |
| 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 CBX 500* 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. |
| Cascade Switch IP Address | Displays the IP Address for the selected switch. |
| Number of Power supplies | This field is disabled. |
| 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.

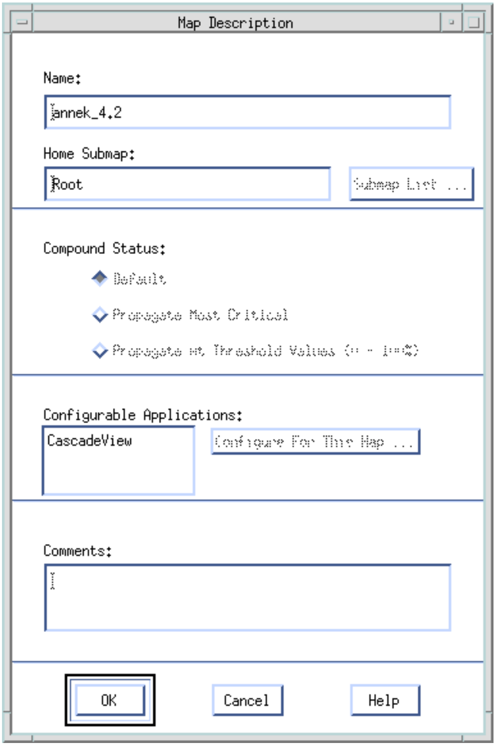



**Figure 1-3. Map Description Dialog Box**

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

**Table 1-4. 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 | Displays the desired status propagation:<br>*Default* – Causes HP OpenView to propagate status according to a predefined algorithm.<br>*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.<br>*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.<br>%warning 30<br>%minor 20<br>%major 10<br>%critical 5<br>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:

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.

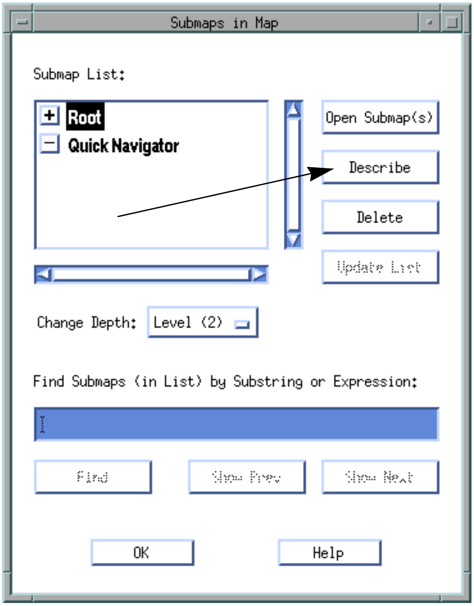



**Figure 1-4. Submaps in Map Dialog Box**

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

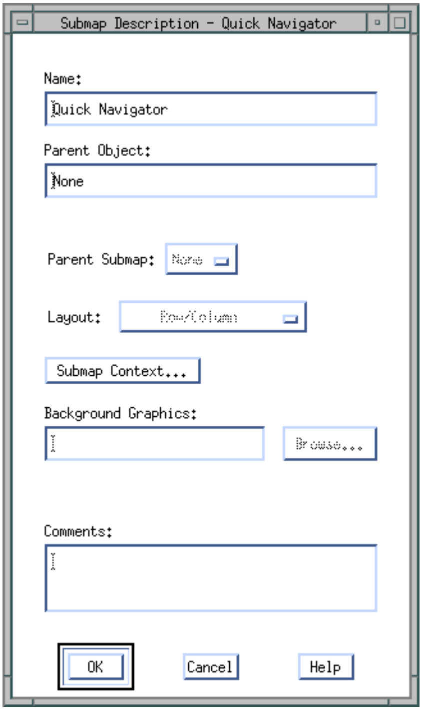



**Figure 1-5. Submap Description Dialog Box**

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

**Table 1-5. 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. |

**Table 1-5. Submap Description Fields (Continued)**

| Field | Action/Description |
|---|---|
| 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. |

# Viewing Switch Details

The Show Detail function polls the switch for the appropriate operational status of the power supplies, fan modules, and I/O modules.

To view details of a switch:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The following dialog box appears.

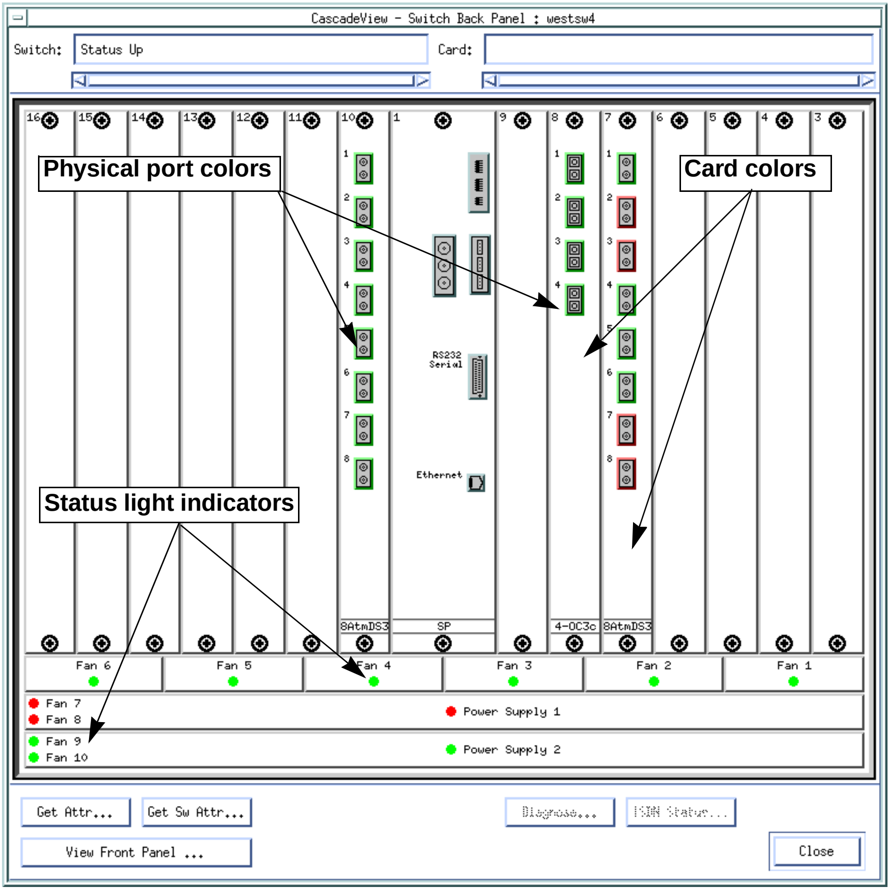



**Figure 1-6. Switch Back Panel Dialog Box**

Table 1-6 describes the command buttons on this dialog box.

**Table 1-6. Switch Back Panel Dialog Box Command Buttons**

| Choose | To |
|---|---|
| Get Attr | Display attributes for the selected item, either an input/output module (IOM), SP, or physical port. You can also select the item and double-click to display the corresponding Set Attributes dialog box. |
| Get Sw Attr | Display the configured switch attributes, including the local IP address of the switch. For more information about this command, refer to the *Network Configuration Guide for CBX 500*. |
| View Front Panel | Display the front panel of the switch. Refer to "Viewing the Front Panel" on page 1-15 for more information. |
| Diagnose | Access diagnostics for a selected module. |
| Close | Exit this dialog box. |

## 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.

## Physical 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 or a logical port is not defined.
- A green physical port indicates that the port is accurately configured and operational.
- A red physical port indicates that the port is configured but has an Admin Status of Down and/or an Operational Status of Down.

## Card Colors

CBX 500 cards also change color to indicate their operational status. They use the following color scheme:

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

## Viewing the Front Panel

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

To display the Show Switch Front Panel dialog box, choose View Front Panel from the Switch Back Panel dialog box. The Show Switch Front Panel dialog box appears as shown in Figure 1-7.

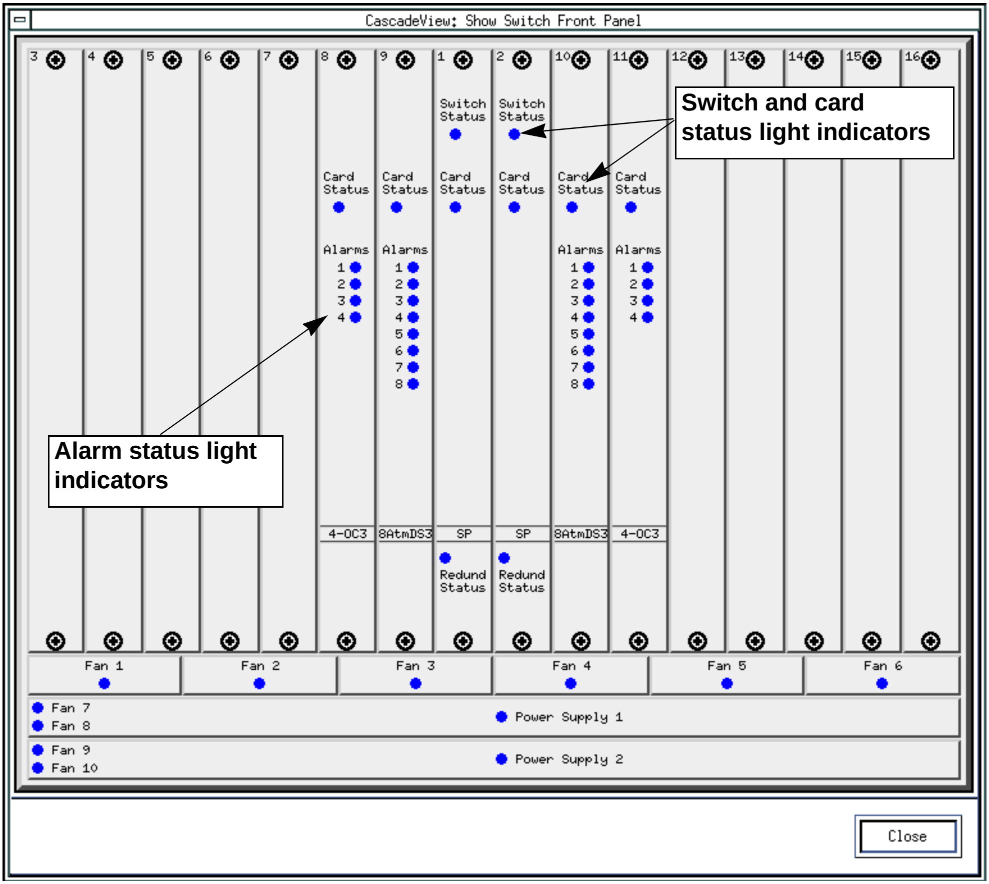



**Figure 1-7. Show Front Panel Dialog Box**

# 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 Switch Processor card and 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.
- Red LED indicates a red alarm condition.
- Yellow LED indicates a yellow alarm condition.

# Viewing Card Status for a Switch Processor Module

To display information for an SP:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The CascadeView Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).
3. Select the SP card slot and choose Get Attr. Select Active at the prompt. The following dialog box appears.

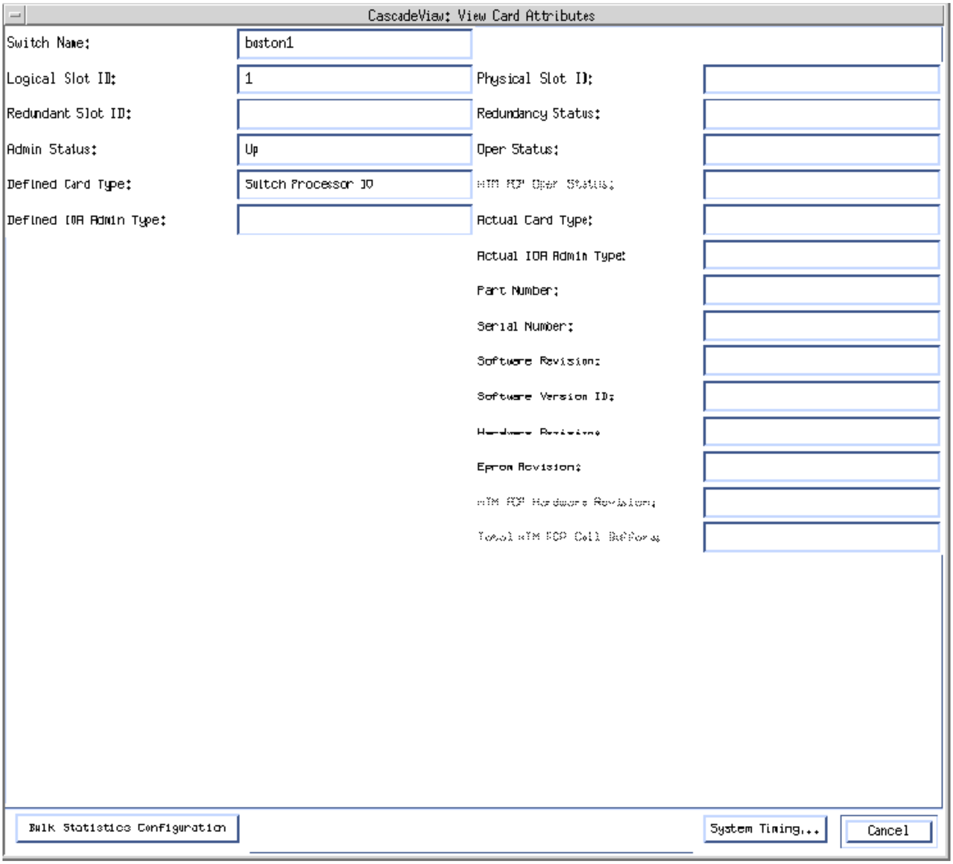



**Figure 1-8. View Card Attributes Dialog Box**

For information about ATM FCP fields, refer to the *ATM Flow-Control Processor User's Guide*. For information about the Bulk Statistics command and the dialog box it displays, refer to the *Bulk Statistics Collector for CBX 500 User's Guide*.

Table 1-7 describes the SP card attribute fields.

**Table 1-7. View Card Attributes**

| Field | Description |
|---|---|
| Switch Name | The name of the switch in which this SP resides. |
| Logical Slot ID | The slot ID for which this SP is configured. |
| Redundant Slot ID | The slot ID of the redundant SP (if applicable). |
| Admin Status | Displays one of the following:<br><br>*Up (Default)* – The SP becomes fully operational at switch start-up. To become operational, the module gets its application code from the PCMCIA hard drive card, which resides in the SPA module.<br><br>*Down* – The SP does not come on-line at switch start up. The configuration is saved in the switch configuration table, but is not downloaded to the switch. Use this option when running foreground diagnostics.<br><br>*Maintenance* – The SP does not receive the application code at switch start-up. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem. |
| Defined Card Type | The configured card type for this SP, either SP10 for a Model 10 or SP20 for a Model 20. |

**Table 1-7. View Card Attributes (Continued)**

| Field | Description |
|---|---|
| Defined IOA Type | Not applicable to the SP. |
| Physical Slot ID | The slot ID in which this SP resides. |
| Redundancy Status | The redundancy status, either active or standby. |
| Oper Status | The operational status of this SP. |
| Actual IOA Type | The actual card type as defined by the firmware. |
| Actual Interface | Not applicable to the SP. |
| Part Number | The part number of the SP. |
| Serial Number | The serial number of the SP. |
| Software Revision | The revision of switch code software. |
| Software Version ID | The build ID and date of the switch code software. |
| Hardware Revision | The hardware revision number. |
| Eprom Revision | The EPROM firmware revision number. |

4. Choose System Timing to display the configured timing options. The following dialog box appears.

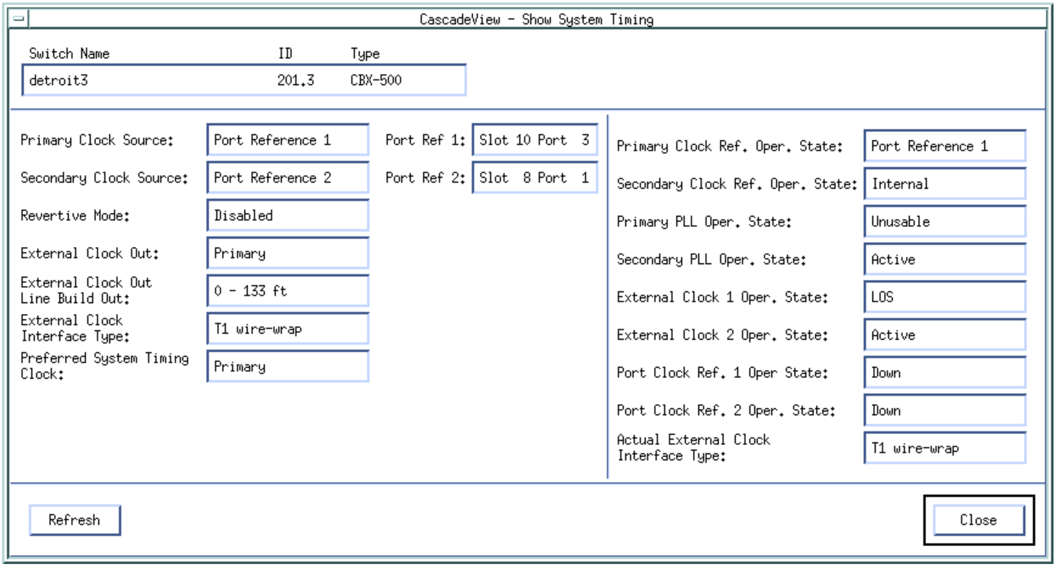



**Figure 1-9. Show System Timing Dialog Box**

The Show System Timing dialog box displays the configured timing settings and monitors the clock status. Table 1-8 on page 1-21 describes these fields.

5. Choose Refresh to update this information.

6. Choose Close to return to the View Card Attributes dialog box.

**Table 1-8. Show System Timing Fields**

| Field | Description |
|---|---|
| Primary and Secondary Clock Source | Displays the configured primary and secondary clock sources:<br>*Internal* – The switch uses the Stratum 3 clock on the SPA module as the primary (or secondary) clock source.<br>*External 1* – The switch uses the primary external clock connection on the SPA module to provide the primary (or secondary) clock source.<br>*External 2* – The switch uses the secondary external clock connection on the SPA module to provide the primary (or secondary) clock source.<br>*Port Reference 1* – This option appears only if you first configure one of the physical ports on the switch as the Primary System Clock Source. The switch uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source.<br>*Port Reference 2* – This option appears only if you first configure one of the physical ports on the switch as the Secondary System Clock Source. The switch uses an incoming clock signal on a selected physical port as the primary (or secondary) clock source. |

**Table 1-8. Show System Timing Fields (Continued)**

| Field | Description |
|---|---|
| Revertive Mode | Displays the configured revertive mode (if the primary clock source fails).<br><br>*Enabled* – If the switch loses the primary clock source, causing the secondary clock source to take over system timing, the system automatically reverts back to the primary clock source when it becomes available again.<br><br>*Disabled* – If the switch loses primary clock source, the secondary clock source takes over system timing. However, the system will not automatically revert back to the primary clock source once it is restored.<br><br>***Note:*** *If you disable Revertive Mode, use the Manual Restore button on the Set System Timing dialog box to revert back to the primary clock source.* |
| External Clock Out | Displays one of the following External Clock Out options:<br><br>*Primary* – The external clock output references the clock that the switch uses as the primary source.<br><br>*Secondary* – The external clock output references the clock that the switch uses as the secondary source.<br><br>*Loopback ext1* – The clock that is wired to the external clock input #1 on the SPA module is fed directly to the external clock output jack.<br><br>*Tx AIS* – In the event of system clock loss, the external clock output transmits an AIS signal. |

**Table 1-8. Show System Timing Fields (Continued)**

| Field | Description |
|---|---|
| External Clock Out Line Build Out | Displays the length of the external clock line connected to the external clock output on the SPA module. |
| External Clock Interface Type | Displays the configured external clock interface type. T1 wire-wrap (the default) specifies a North American SP. This option accepts T1 timing inputs and outputs. E1 BNC specifies an International SP for E1 inputs and outputs. |
| Preferred System Timing Clock | Displays one of the following Preferred System Timing Clock methods:<br>*Primary* – The switch uses the clock source specified in the Primary Clock Source field.<br>*Secondary* –The switch uses the clock source specified in the Secondary Clock Source field.<br>***Note:*** *If the primary clock source becomes unavailable, the system automatically provides the secondary clock source to the I/O modules.* |
| Primary Clock Ref. Oper. State | Displays the actual primary clock source: Internal, External, Port Ref. 1, or Port Ref. 2. |
| Secondary Clock Ref. Oper. State | Displays the actual secondary clock source: Internal, External, Port Ref. 1, or Port Ref. 2. |

**Table 1-8. Show System Timing Fields (Continued)**

| Field | Description |
|---|---|
| Primary PLL Oper. State | Displays the current state of the primary synchronization PLL.<br>*Active* – Clock source is active as a timing reference.<br>*Inactive* – Clock source is not active as a timing reference.<br>*Unusable* – Indicates that at the time the PLL state was sampled, the PLL output could not be used as a system timing reference (e.g., the PLL is configured to use an external reference and that reference is physically disconnected). |
| Secondary PLL Oper. State | Displays the current state of the secondary synchronization PLL. |
| External Clock 1 Oper. State | Displays the current state of external clock 1.<br>*Active* – Valid clock source.<br>*AIS* – Detected an AIS condition.<br>*LOS* – Detected loss of signal.<br>*LOF* – Detected loss of frame. |
| External Clock 2 Oper. State | Displays the current state of external clock 2. |
| Port Clock Ref. 1 Oper. State | Displays the current state (active or down) of the physical port configured as port reference 1. |
| Port Clock Ref. 2 Oper. State | Displays the current state (active or down) of the physical port configured as port reference 2. |
| Actual External Clock Interface Type | Displays the actual external clock interface: primary, secondary, loopback ext1, or TX AIS. |

# Viewing Card Status for an IOM

To display information for a switch IOM:

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

2. From the monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).

3. Double-click on a card slot. The View Card Attributes dialog box appears. (Figure 1-10 shows the attributes for an ATM E3 card.)

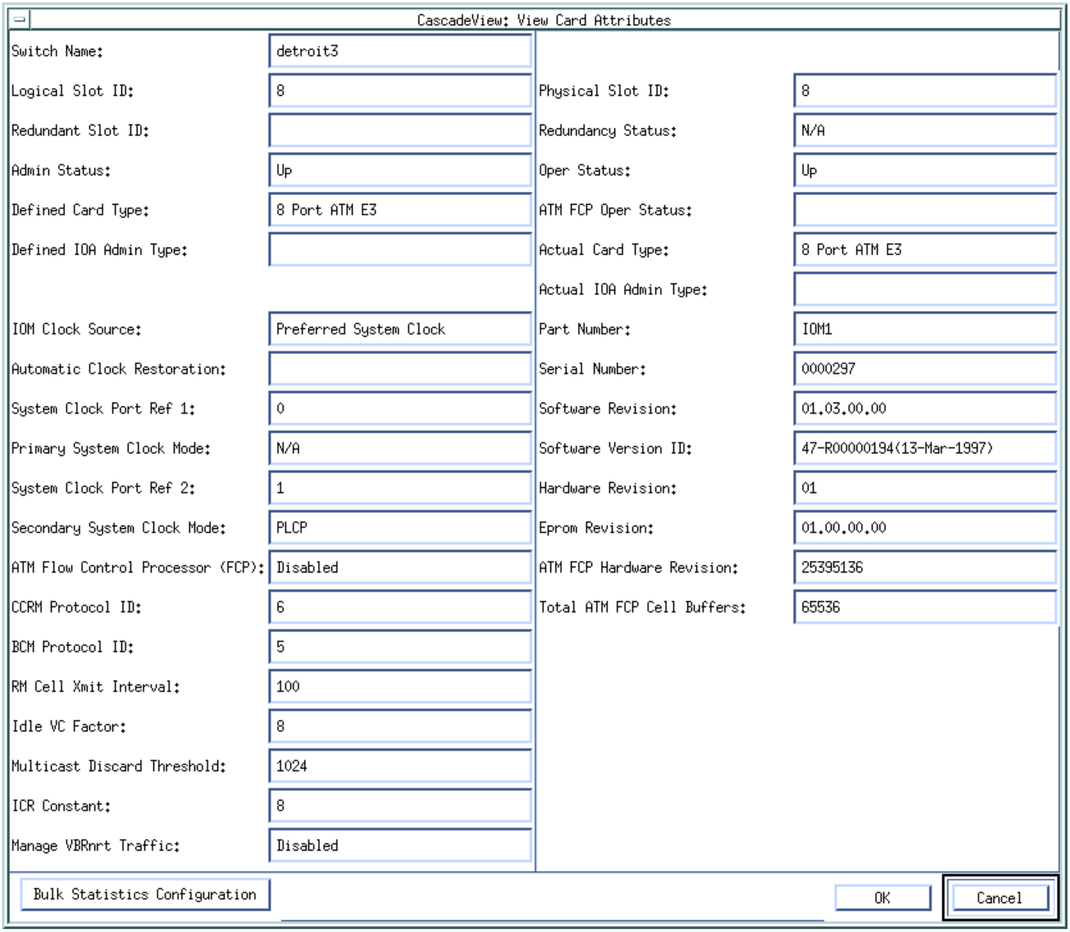



**Figure 1-10. View Card Attributes Dialog Box**

For information about ATM FCP fields, refer to the *ATM Flow-Control Processor User’s Guide*. For information about the Bulk Statistics Configuration command and the dialog box it displays, refer to the *Bulk Statistics Collector for CBX 500 User’s Guide*.

Table 1-9 describes the View Card Attributes dialog box fields.

:

**Table 1-9. View Card Attributes Fields**

| Field | Description |
|---|---|
| IOM Clock Source | Displays the internal timing source for the IOM. This setting applies only to those physical ports on the IOM whose Xmit Clock Source is set to *Internal*. It has no effect on physical ports where the Xmit Clock Source field is set to Loop-Timed, since the clock for these ports is derived from the non-external clock source coming into the port.<br><br>Options include:<br><br>*Preferred System Clock* – (Default) Indicates the preferred system clock provides the IOM clock source, which can be either the primary or secondary system clock (whichever of the two is currently up).<br><br>*Local Clock* – Indicates the local clock on the IOM provides the clock source.<br><br>*Primary System Clock Only* – Indicates the primary system clock source provides the IOM clock source.<br><br>*Secondary System Clock Only* – Indicates the secondary system clock source provides the IOM clock source. |
| System Clock Port Ref 1 | Indicates whether the IOM provides the primary system clock source to the SP module. Options include:<br><br>*No Physical Port* – (Default) Indicates the SP does not get its primary system clock source from a port on this IOM.<br><br>*Physical Port* – Indicates the physical port that provides the primary system clock source to the SP. The incoming clock signal on the selected port is provided to the SP as the primary system clock source. |

**Table 1-9. View Card Attributes Fields (Continued)**

| Field | Description |
|---|---|
| Primary System Clock Mode (*DS3/E3 only*) | This field is available only if you selected a physical port in the System Clock Port Ref 1 field. Refer to the *Network Configuration Guide for CBX 500* for more information. Options include:<br>*PLCP* – Indicates the module uses a PLCP frame, which transmits 12 ATM cells every 125 µs.<br>*Line Rate* – Indicates the module uses the DS3 line rate as the clock mode. The DS3 line rate is 44.5 Mbps. Line Rate is the only option for E3 modules. |
| System Clock Port Ref 2 | Indicates whether the IOM provides the secondary system clock source to the SP module. Options include:<br>*No Physical Port* – (Default) Indicates the SP does not get its secondary system clock source from a port on the IOM.<br>*Physical Port* n – Indicates the physical port that provides the secondary system clock source to the SP. The SP uses the incoming signal on the selected port as the secondary system clock source. |
| Secondary System Clock Mode (*DS3/E3 modules only*) | This field is available only if you selected a physical port in the Secondary System Clock Source field. Refer to the *Network Configuration Guide for CBX 500* for more information. Options include:<br>*PLCP* – Indicates the module uses a PLCP frame, which transmits 12 ATM cells every 125 µs.<br>*Line Rate* – Indicates the module uses the DS3 line rate as the clock mode. The DS3 line rate is 44.5 Mbps. Line Rate is the only option for E3 modules. |
| Physical Slot ID | The slot ID in which this IOM resides. |
| Redundancy Status | Not supported in this release. |

**Table 1-9. View Card Attributes Fields (Continued)**

| Field | Description |
|---|---|
| Oper Status | The operational status of this IOM. |
| Actual Card Type | The actual card type as defined by the firmware. |
| Part Number | The part number of the IOM. |
| Serial Number | The serial number of the IOM. |
| Software Revision | The revision of switch code software. |
| Software Version ID | The build ID and date of the switch code software. |
| Hardware Revision | The hardware revision number. |
| Eprom Revision | The EPROM firmware revision number. |

# 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:

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 1-11 shows an example of an ATM OC3 module Physical Port Attributes dialog box.

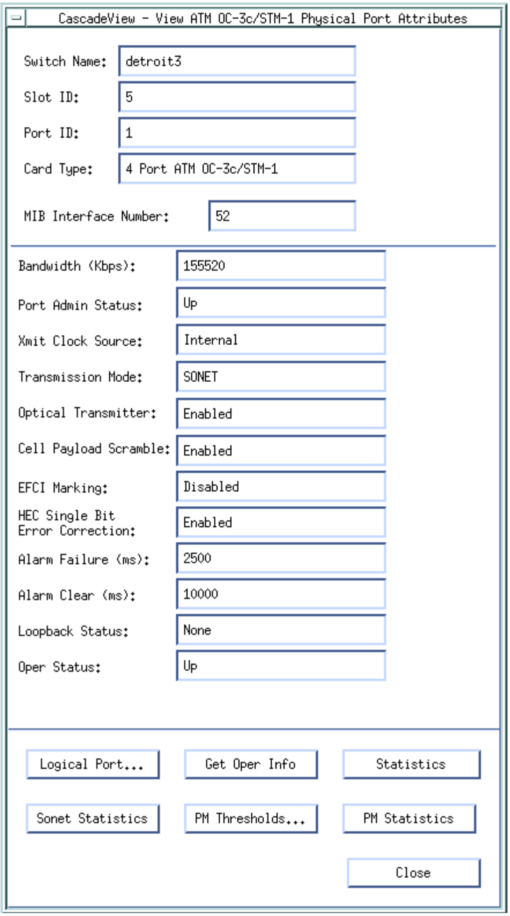



**Figure 1-11. View Physical Port Attributes Dialog Box (OC3c/STM-1)**

Table 1-10 describes the command buttons on the View Physical Port Attributes dialog box that enable you to obtain additional information about the physical port.

**Table 1-10. View Physical Port Attributes Dialog Box Command Buttons**

| 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. |
| Sonet Statistics | (*OC3, OC12, STM-1, and STM-4*) Access Sonet/SDH MIB statistics. |
| PM Threshold | (*OC3, STM-4, OC-12, STM-4, DS3, E3, and T1*) Display configured performance monitoring attributes. |
| PM Statistics | (*OC3, STM-4, and T1*) Access performance monitoring statistics. |
| FDL | (*T1 only*) Display facility data link (FDL) control information for Extended Superframe circuits. |
| 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. |
| Close | Exit the dialog box and return to the network map. |

Table 1-11 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 1-11. View (or Show) Physical Port Attributes Fields**

| Field | Action/Description |
|---|---|
| MIB Interface Number | Displays the MIB interface number for the physical port. The software assigns a unique number to each physical port on the switch. |
| Bandwidth (Kbps) | Displays the amount of available bandwidth (in Kbps) for this physical port. |
| Port Admin Status | Displays up or down to indicate the port admin status. |
| Xmit Clock Source | Displays the transmit clock source.<br>*Internal* – (Default) The IOM's internal timing source provides the clock source to this port.<br>*Loop-Timed* – The clock source is derived from the signal coming into this port. |
| Transmission Mode | Displays the configured individual ports on this IOM as either SONET (OC3/OC12) or SDH (STM-1/STM-4). |

**Table 1-11. View (or Show) Physical Port Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| Optical Transmitter | 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 LED for this port, and prevents the port from transmitting incoming traffic. You must set this option to On to transmit incoming traffic out of this port.<br><br>**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.<br><br>***Note:*** *When you disable the transmit laser, the CPE or switch at the other end of the connection reports a red port alarm to indicate signal loss.* |
| Line Build Out (*DS3 modules only*) | Displays 0– 225 feet (the default) for a short cable or 226 – 450 feet for a long cable. This measurement represents the length of the cable that connects the physical port to other network equipment. |
| Cell Payload Scramble | Displays enabled (the default) or disabled to indicate the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (that is, it prevents ATM cell header alienation). |
| C-Bit Parity (*DS3 modules only*) | Displays enabled (the default) or disabled to indicate the C-Bit Parity function. The C-Bit Parity function provides a way to monitor the end-to-end performance of T3 circuits.<br><br>***Note:*** *This feature requires C-bit parity-compatible customer premise equipment (CPE).* |

**Table 1-11. View (or Show) Physical Port Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| PLCP Options (*DS3/E3 only*) | Displays enabled or disabled to indicate the Physical Layer Convergence Protocol (PLCP) option. When Enabled (the default), the physical port uses a PLCP frame, which transmits 12 ATM cells every 125 µs. Note that when PLCP is enabled, available bandwidth is reduced. When PLCP is disabled, the port operates in a direct mapping (HEC) mode. |
| EFCI Marking | The Explicit Forward Congestion Indicator (EFCI) determines if congestion (or impending congestion) exists in a node. This option is disabled by default.<br><br>Enabled indicates the congested node modifies the EFCI bit in the ATM cell header to indicate congestion. If the equipment connected to the CBX 500 can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve the congestion. EFCI is only set in the UBR queue and affects all connections in this physical port queue. |
| HEC Single Bit Error Correction | Displays enabled (the default) or disabled to indicate the configured single bit header error correction (HEC) on a per port basis. |
| FEAC Loopback (*DS3 modules only*) | Displays enabled (the default) or disabled to indicate the switch's ability to respond to loopback commands on the Far-End Alarm and Control (FEAC) channel.<br><br>Enabled allows the switch to respond to FEAC loopback commands from far end equipment (loop up and loop down), that can put the port into remote loopback.<br><br>Disabled ignored loop up and loop down commands on the FEAC channel. |

**Table 1-11. View (or Show) Physical Port Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| Alarm Failure (ms) | Displays a value between 0 to 65535 ms to indicate how long the switch waits before declaring a physical layer problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch “soaks” the physical layer alarm for 2.5 seconds before declaring the physical port down.<br><br>A value of 0 ms means the physical port goes down immediately following any physical layer failure. |
| Alarm Clear (ms) | Displays a value between 0 to 65535 ms to indicate how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the physical port up.<br><br>A value of 0 ms means the physical port comes back up as soon as the physical layer failure alarm clears. |
| Loopback Status | Displays the port loopback status, if you enabled diagnostic loopback tests. The default is None. |
| Oper Status | Indicates the operational status of the physical port (Up or Down). If this field is blank, the IOM did not respond to a status request. |

# Viewing FDL Information for a T1 Port

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

To display the FDL information:

1. Select the appropriate switch object on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box appears (Figure 1-6 on page 1-12).
3. Select the T1 physical port for which you want to display FDL information. The Show Physical Port Attributes dialog box appears.
4. Choose FDL. The system displays the Show ATM T1 Physical Port FDL Parameters dialog box as shown in Figure 1-12.

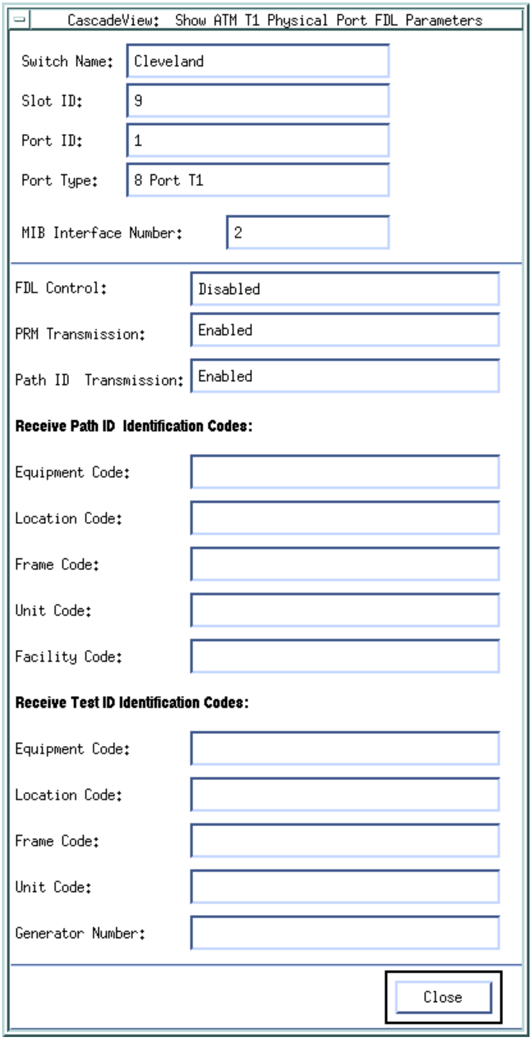



**Figure 1-12. Show ATM T1 Physical Port FDL Parameters Dialog Box**

Table 1-12 on page 1-38 describes these dialog box fields.

5. Choose Close to exit when you finish viewing this dialog box.

**Table 1-12. Show ATM T1 Physical Port FDL Parameters Fields**

| Field | Description |
|---|---|
| FDL Control | Displays enabled if this port uses the FDL control parameters; displays disabled if the carrier does not use them. |
| PRM Transmission | The T1 module processes incoming performance report messages (PRM) messages that provide error count information for far end equipment. This field displays enabled if this port transmits a PRM signal; it displays disabled if this port does not transmit this signal. (You can disable PRM transmission if the equipment connected to this port does not process PRM signals.) |
| Path ID Transmission | The T1 module processes path ID messages it receives from other equipment. This field displays enabled if this port transmits a Path ID signal; it displays disabled if this port does not transmit this signal. (You can disable path ID transmission if the equipment connected to this port does not process path ID information.) |
| Receive Path ID Identification Codes | Displays the following information describing the equipment connected to this T1 physical port:<br>*Equipment Code* – The type of hardware connected to this port.<br>*Location Code* – The location of this hardware.<br>*Frame Code* – The location (within a building) of this hardware.<br>*Unit Code* – The location of this equipment within a bay.<br>*Facility Code* – The specific DS1 path the signal uses. |

**Table 1-12. Show ATM T1 Physical Port FDL Parameters Fields (Continued)**

| Field | Description |
|---|---|
| Receive Test ID Identification Codes | Displays the following information describing the test signal generating equipment connected to this physical port.<br>*Equipment Code* – The type of test signal hardware connected to this port.<br>*Location Code* – The location of this hardware.<br>*Frame Code* – The location (within a building) of this hardware.<br>*Unit Code* – The location of this equipment within a bay.<br>*Generator Number* – Identifies the signal generator (for testing only). |

# Viewing Logical Port Status

To display logical port status and configuration information:

1. Select the appropriate switch icon on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Logical Ports. The Show All Logical Ports in Switch dialog box appears.
3. Select a logical port name from the list box on the left as shown in Figure 1-13.

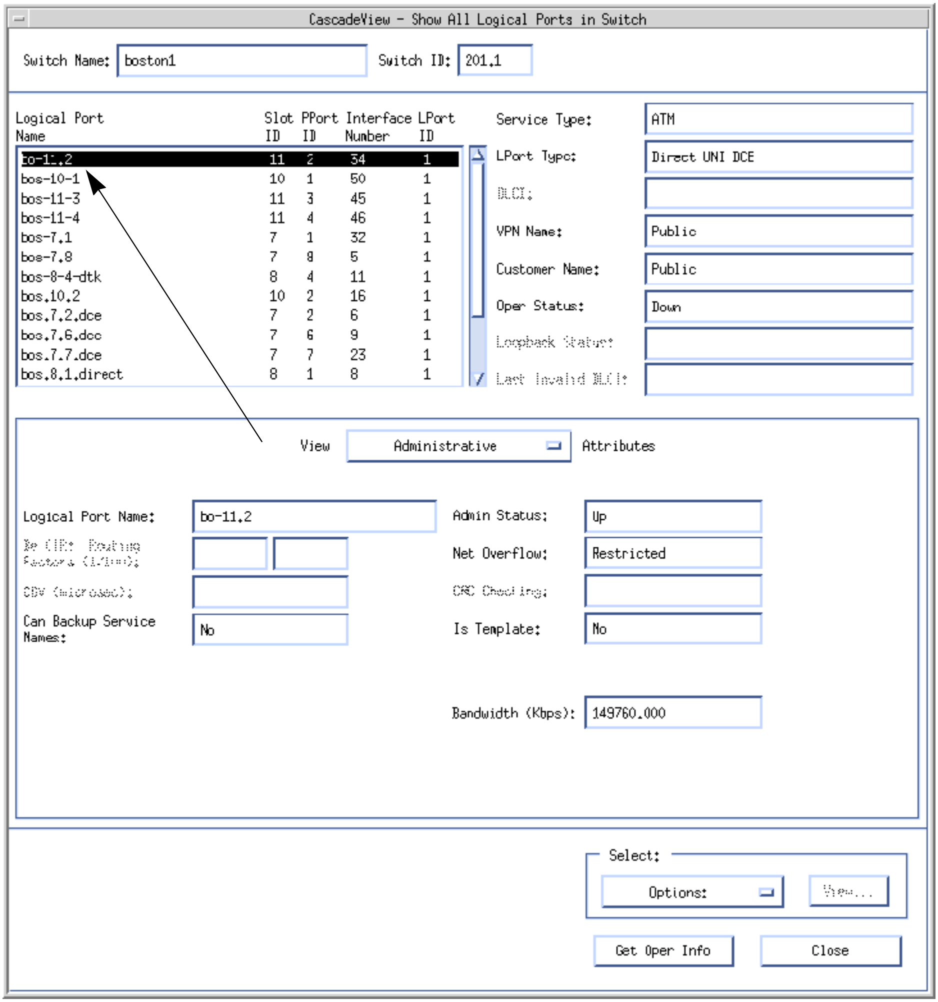



**Figure 1-13. Show All Logical Ports in Switch Dialog Box**

Table 1-13 describes the dialog box command buttons.

**Table 1-13. Show All Logical Ports Dialog Box Command Buttons**

| Choose | To |
|---|---|
| Get Oper Info | Update status information for the selected logical port. The Oper Status field indicates whether this port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status. |
| Use the Select: Options button to select the following logical port options. Once you select an option from this list, choose View to display the information.   | |
| Statistics | Displays the summary statistics for the selected logical port. For more information refer to Chapter 5, "Generating Statistics". |
| QoS Parameters | Displays the quality of service parameters (including bandwidth and routing metrics) for the selected logical port. Refer to page 1-51 for more information. |
| NTM Parameters | Displays the configured network traffic management (NTM) parameters for the selected logical port. For more information refer to Chapter 8, "NTM and NDC". |
| NTM Statistics | Displays the NTM statistics for the selected logical port. For more information refer to "Viewing NTM Logical Port Statistics" on page 8-10. |
| NDC Statistics | Displays the NDC statistics for the selected logical port. For more information refer to "Viewing NDC Logical Port Statistics" on page 8-12. |
| ATM Accounting | Accesses the ATM accounting functions for a logical port. For more information, refer to the *Accounting System Administrator's Guide*. |

**Table 1-13. Show All Logical Ports Dialog Box Command Buttons (Continued)**

| Choose | To |
|---|---|
| Screen Assignments | Displays the port security screen assignments for the selected logical port. For more information refer to "Viewing Port Security Screens" on page 2-44. |
| Close | Exit the Show All Logical Ports in Switch dialog box. |

## Show All Logical Ports in Switch Fields

Table 1-14 describes the switch identification 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 1-14. Show All Logical Ports in Switch Identification Fields**

| Field | Action/Description |
|---|---|
| Customer Name | Displays the name of the customer to which this logical port is dedicated. |
| Switch Name | Displays the name entered to identify the switch at the time of configuration. |
| Logical Port Name | Displays a unique alphanumeric name for this port. CascadeView/UX uses this name to reference the logical 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. |

**Table 1-14. Show All Logical Ports in Switch Identification Fields (Continued)**

| Field | Action/Description |
|---|---|
| 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*). |
| Loopback Status | Indicates whether loopback testing is enabled on this logical port. The default is None (no testing). |
| LPort ID | Displays the ID number that uniquely identifies each logical port. |
| 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 the *Network Configuration Guide for CBX 500* for more information. |

4. Choose the View Attributes option to display various attributes for the logical port. Table 1-15 identifies each of the different attribute types along with a reference to the table that describes the attribute fields.

5. When you finish reviewing the logical port information, choose Close to 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 PPort dialog box. The attribute information that the system displays differs depending on the attribute that you select from the View Attributes option.

Table 1-15 identifies each of the different attribute types along with a reference to the page that describes these attributes.

**Table 1-15. Logical Port Attribute Types**

| For Information About | See... |
|---|---|
| Administrative | "Administrative Attributes" on page 1-44. |
| ATM FCP | For more information about these parameters, refer to the *ATM Flow-Control Processor User's Guide*. |
| SVC VPI/VCI Range | "SVC VPI/VCI Range Attributes" on page 1-46. |
| ILMI/Signaling/OAM | "ILMI/Signaling/OAM Attributes" on page 1-47. |

## Administrative Attributes

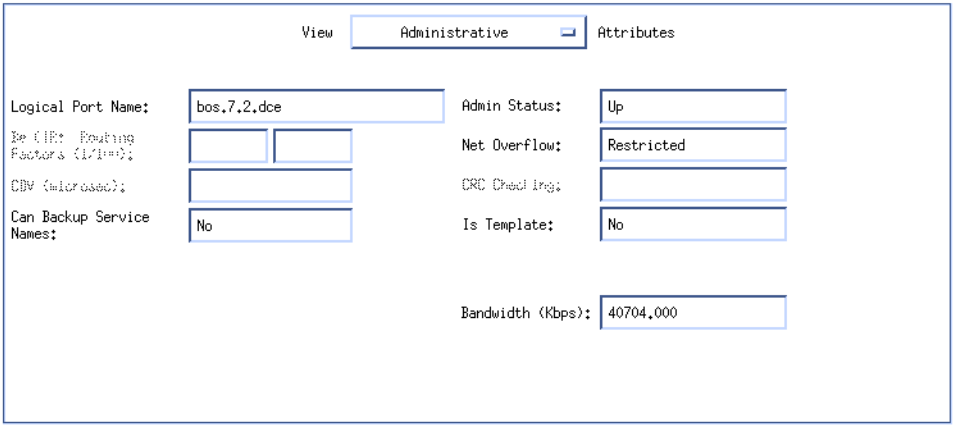



**Figure 1-14. Administrative Attributes**

Table 1-16 describes the administrative attribute fields.

**Table 1-16. 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 configured bandwidth for the selected logical port. |
| 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. |
| CDV (microsec) | *(ATM Optimum Cell Trunks only)* Displays the maximum cell delay variation (in microseconds) for this logical port.<br><br>The default value is 684 for DS3 ports, 45 for OC12 ports, 3331 for E1/T1 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. |
| 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.<br><br>***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 1-16. Administrative Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| VPI/VCI (*OPTimum trunk only*) | Displays the configured VPI/VCI value. |
| Logical Port Name | Displays the name assigned to this logical port. |

## SVC VPI/VCI Range Attributes

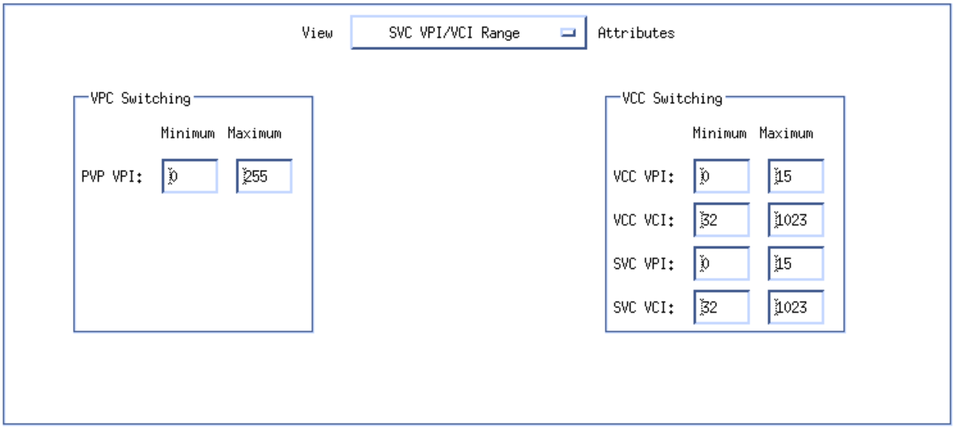



**Figure 1-15. SVC VPI/VCI Range Attributes**

Table 1-17 describes the SVC VPI/VCI Range Attributes fields.

**Table 1-17. SVC VPI/VCI Range Attributes Fields**

| Field | Description |
|---|---|
| PVC VPI | Displays the VPI range for a PVC. |
| PVC VCI | Displays the VCI range for a PVC. |
| SVC VPI | Enter values to represent the VPI range for an SVC. |
| SVC VCI | Enter values to represent the VCI range for an SVC. |

## ILMI/Signaling/OAM Attributes

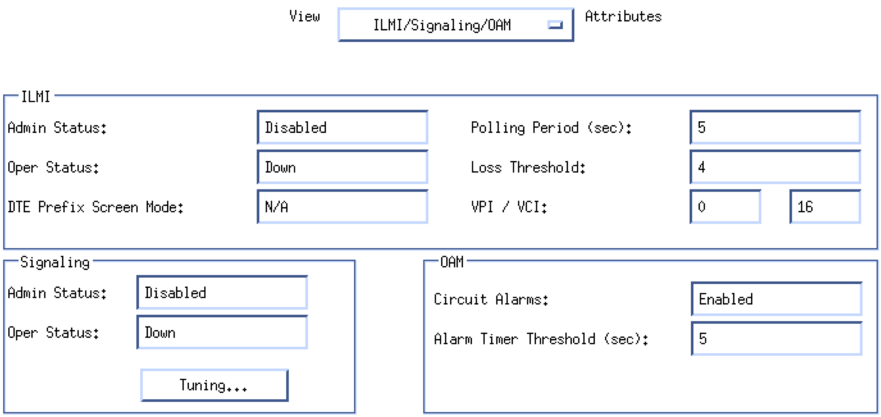



**Figure 1-16. ILMI/Signaling/OAM Attributes**

Table 1-18 describes the ILMI/Signaling/OAM Attributes fields.

**Table 1-18. ILMI/Signaling/OAM Attributes Fields**

| Field | Action/Description |
|---|---|
| **ILMI Attributes** | |
| Admin Status | Displays enabled or disabled. When ILMI is enabled, 1% of the bandwidth in the VBR-NRT QoS class is reserved for ILMI.<br><br>When ILMI is Disabled (the default), this bandwidth is not reserved. If the attached device does not support ILMI, leave ILMI disabled. For information about ILMI support, refer to the *Network Configuration Guide for CBX 500.* |
| DTE Prefix Screen Mode (DTE ports) | Displays the various DTE prefix screening modes. Options include:<br><br>*Accept All* – No screening occurs; accepts all prefixes.<br><br>*Node Prefix* – Accepts only network prefixes that partially or fully match a configured node prefix.<br><br>*Port Prefix* – Accepts only network prefixes that partially or fully match a configured port prefix.<br><br>*Node or Port Prefix* – Accepts only network prefixes that partially or fully match either a configured node prefix or a configured port prefix.<br><br>*Reject All* – Rejects all network prefixes received from an external network. |
| Polling Period | Displays the polling period (T) for an ILMI poll. The switch generates an ILMI poll every (T) seconds. The default is 5 seconds for a polling period and 4 seconds for a loss threshold. |

**Table 1-18. ILMI/Signaling/OAM Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| Loss Threshold | Displays the number of times (K) the logical port will issue an ILMI poll before the link is considered down. If no responses are seen in K x T seconds, the link is considered down. The default is 4. |
| VPI | Displays the ID of the virtual path for ILMI traffic. The default is 0. |
| VCI | Displays the ID of the virtual channel for ILMI traffic. The default is 16. |
| Oper Status | Displays the current operational status. |
| **Signalling Attributes** | |
| Admin Status | Displays enabled or disabled. Enabled supports the UNI signalling protocol. When UNI signalling is enabled, 2% of the bandwidth in the VBR-NRT QoS class is reserved for this purpose. The default setting, disabled, uses this logical port only for PVCs (that is, you will not create SVCs on the port). |
| Oper Status | Displays the current operational status. |
| Tuning | Displays the Set Logical Port Signalling Tuning Parameters dialog box. For information about Tuning parameters, refer to the *Network Configuration Guide for CBX 500.* |
| **OAM Attributes** | |

**Table 1-18. ILMI/Signaling/OAM Attributes Fields (Continued)**

| Field | Action/Description |
|---|---|
| Circuit Alarms | Displays enabled or disabled. Enabled (the default) allows this logical port to generate OAM AIS alarms. The switch uses these alarms to signal when the circuits have gone down. Disabled does not generate OAM AIS alarms on this logical port. |
| Alarm Timer Threshold | Before generating an OAM AIS alarm, the switch waits until the circuit has been down for the time period specified in this field. The default is 5 seconds. |

# Viewing the Quality of Service Parameters

This section describes how to display the QoS parameters for a logical port. These parameters enable you to display the bandwidth and routing metrics (if applicable) for the various traffic service classes. The Show Logical Port QoS Parameters dialog box fields are the same regardless of the logical port type. The fields display the Quality of Service information configured for the logical port, and enable you to monitor the actual bandwidth on the egress port.

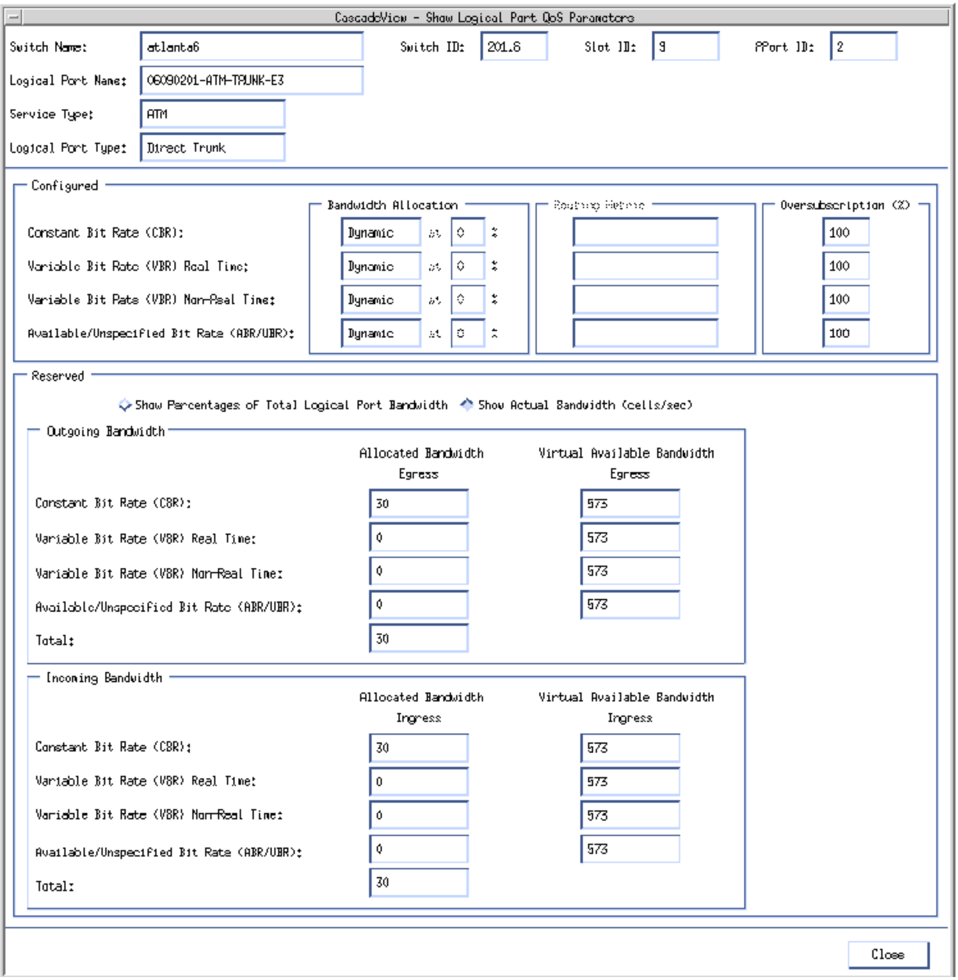
As you view this information, keep in mind the following:

- The CBX 500 implements a bandwidth reservation process for all types of DCE and DTE logical ports to accommodate ILMI and UNI signalling.
- If you enable signalling for a UNI logical port, 2% of the available bandwidth is reserved from the VBR-NRT QoS class.
- If you enable ILMI for a UNI logical port, the switch reserves 1% of the available logical port bandwidth for this purpose.
- If you are viewing a trunk logical port, the switch reserves 5% of the available logical port bandwidth in the CBR QoS class.

## Displaying QoS information

To display QoS parameters, use the following steps:

1. From the Show All Logical Ports in Switch dialog box (Figure 1-13 on page 1-40), select Options ⇒ QoS Parameters.
2. Choose View. The following dialog box appears.




## Figure 1-17. Show Logical Port QoS Parameters Dialog Box

The default view displays the percentages of allocated bandwidth and virtual available bandwidth.

Table 1-19 describes each of the fields on the Show Logical Port QoS Parameters dialog box.

**Table 1-19. Show Logical Port QoS Parameters Dialog Box**

| Field | Description |
|---|---|
| **Identification Fields** | |
| Switch Name | Displays the name of the switch. |
| Switch ID | Displays the switch ID number. |
| Slot ID | Displays the slot ID number of the module you are monitoring. |
| PPort ID | Displays the physical port ID number. |
| 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. |
| 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. CPE protocols adjust for any delay or loss incurred through the use of VBR non-real time. |
| Available/Unspecified Bit Rate (ABR/UBR) | Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic. |

**Table 1-19. Show Logical Port QoS Parameters Dialog Box (Continued)**

| Field | Description |
|---|---|
| Bandwidth Allocation | Displays *Dynamic* or *Fixed* for each service class.<br><br>*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.<br><br>*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.<br><br>Refer to the *Network Configuration Guide for CBX 500* 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.<br><br>***Note:*** *The Oversubscription value for CBR is always set at 100% and cannot be modified.*<br><br>Refer to the *Network Configuration Guide for CBX 500* for more information about oversubscription. |
| 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. |

**Table 1-19. Show Logical Port QoS Parameters Dialog Box (Continued)**

| Field | Description |
|---|---|
| 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. |

3. To view the actual bandwidth, use the *Show Actual Bandwidth (cells/sec)* option to display the percentages of allocated bandwidth and virtual available bandwidth.

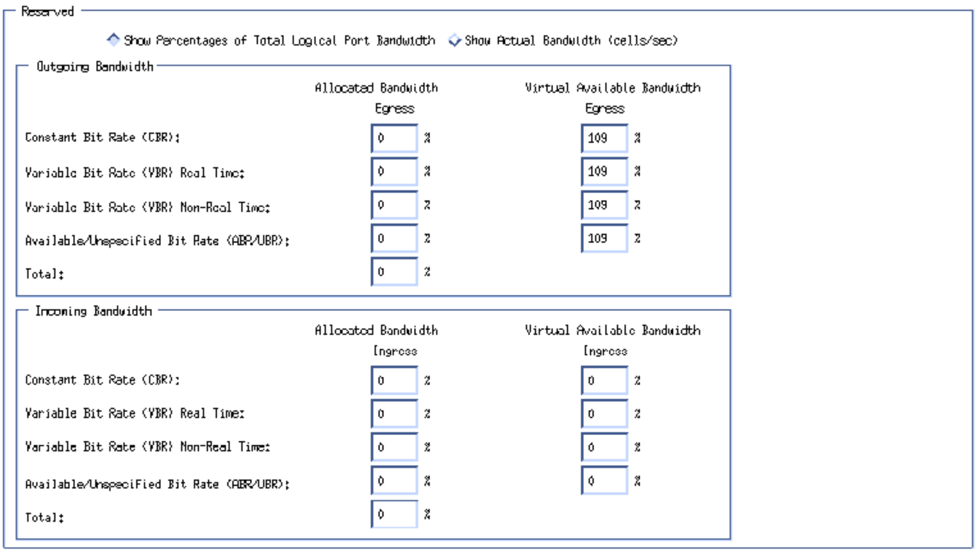



**Figure 1-18. Show Actual Bandwidth (for QoS)**

4. When you finish, choose Close to return to the Show All Logical Ports dialog box.

# Viewing Logical Port UNI Signalling Tuning Parameters

This section describes the Signalling Tuning Parameters for a logical port. In an ATM network, UNI signalling is responsible for establishing and releasing SVCs. Signalling is used only on ingress and egress ports, including user-to-network, network-to-user, and network-to-network ports.

To view signalling tuning parameters:

1. Choose View Attributes for UNI Signalling from the Show All Logical Ports in Switch dialog box (Figure 1-13 on page 1-40).
2. Choose the Tuning command. The following dialog box appears. (The fields are the same regardless of the type of logical port you are monitoring.)

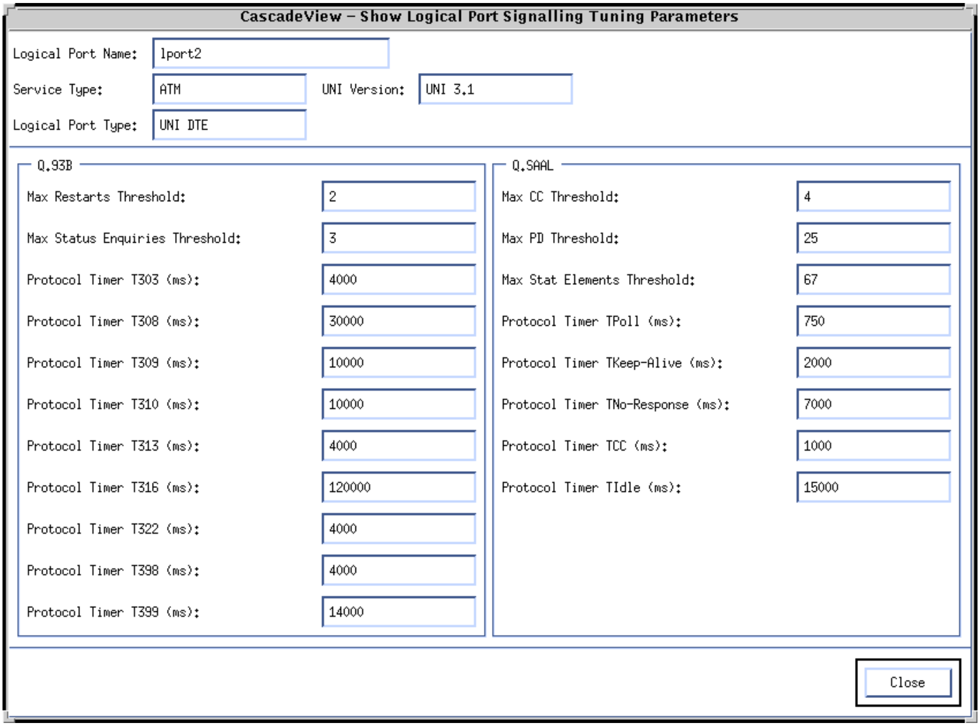



**Figure 1-19. Show Logical Port Signalling Tuning Parameters**

The Show Logical Port Signalling Tuning Parameters dialog box displays the Q.93B thresholds and timers, and the Q.SAAL protocol data unit (PDU) thresholds and timers. The displayed defaults are based on the selected UNI version (3.0 or 3.1 or IISP 3.1) for the logical port.

Table 1-20 describes the Show Logical Port Signaling Tuning Parameters fields.

**Table 1-20. Set Logical Port Signalling Tuning Parameters Fields**

| Field | Action/Description |
|---|---|
| **Q.93B Signalling** | |
| Max Restarts Threshold | Displays the maximum number of restarts to send without a response. The default is 2. |
| Max Status Enquiries Threshold | Displays the maximum number of status enquiries that can be unacknowledged before the call is dropped. The default is 1. |
| Protocol Timer T303 | Displays how long to wait for a response after a SETUP protocol data unit (PDU) has been sent. The default is 4000. |
| Protocol Timer T308 | Displays how long to wait for a response after a RELEASE PDU has been sent. The default is 30000. |
| Protocol Timer T309 | Displays how long to wait before calls are dropped. The default is 10000 for the UNI 3.1 ATM protocol and 90000 for UNI 3.0. |
| Protocol Timer T310 | Displays how long to wait for the next response after a CALL PROCEEDING PDU has been received. The default is 10000. |
| Protocol Timer T313 | Displays how long to wait for a response after a CONNECT PDU has been sent. This function defaults to 4000 for DTE logical ports; it is disabled for DCE logical ports. |
| Protocol Timer T316 | Displays how long to wait for a response after a RESTART PDU has been sent. The default is 120000. |
| Protocol Timer T322 | Displays how long to wait for a response after a STAT ENQUIRY PDU has been sent. The default is 4000. |
| Protocol Timer T398 | Displays how long to wait for a response after a DROP PTY PDU has been sent. The default is 4000. |

**Table 1-20. Set Logical Port Signalling Tuning Parameters Fields (Continued)**

| Field | Action/Description |
|---|---|
| Protocol Timer T399 | Displays how long to wait for a response after an ADD PTY PDU has been sent. The default is 14000. |
| **Q.SAAL Signalling** | |
| Max CC Threshold | Displays the maximum number of transaction retries for control PDUs. The default is 4. |
| Max PD Threshold | Displays the maximum number of data PDUs without a POLL. The default is 25. |
| Max STAT Elements Threshold | Displays the maximum number of missing elements in a STATUS PDU. The default is 67. |
| Protocol Timer TPoll (ms) | Displays how often a poll is sent when the Q.SAAL is active. The default is 100 if this port uses the UNI 3.0 ATM protocol; the default is 750 for UNI 3.1. |
| Protocol Timer TKeep-Alive (ms) | Displays how often a poll is sent when the Q.SAAL is in the transient state. The default is 2000. |
| Protocol Timer TNoResponse (ms) | Displays the maximum amount of time that can pass without a STATUS PDU being received. The default is 7000. |
| Protocol Timer TCC (ms) | Displays the retry time for control PDUs. The default is 1000. |
| Protocol Timer TIdle (ms) | Displays how often a poll is sent when Q.SAAL is idle. This parameter does not apply to UNI 3.0 connections. The default is 15000. |

3. When you finish, choose Close to return to the network map.

# Viewing Subnets

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

1. Select the switch on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show All Sub Nets. The following dialog box appears.

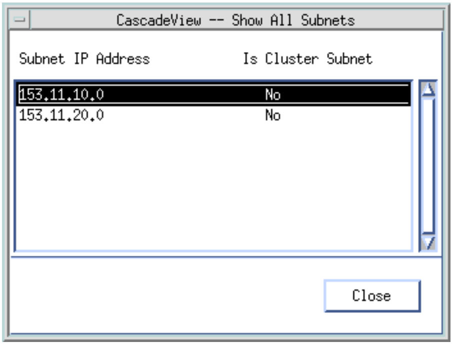



**Figure 1-20. Show All Subnets Dialog Box**

The Show All Subnets dialog box displays the following information:

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

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

For more information about subnets, refer to the *Network Configuration Guide for CBX 500*.

# Viewing Clusters

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

1. Select the switch on the network map.

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

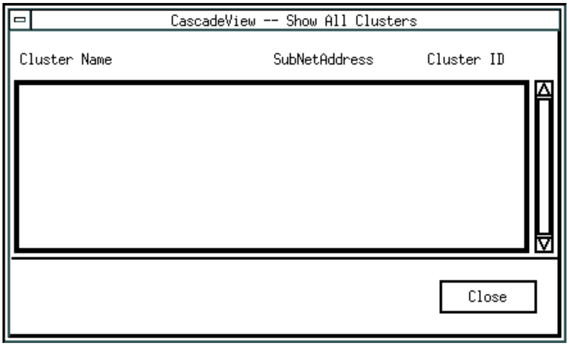



**Figure 1-21. Show All Clusters Dialog Box**

The Show All Clusters dialog box displays the following information:

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

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

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

For more information about subnets, refer to the *Network Configuration Guide for CBX 500.*

# Viewing Switch Status

To display status and configuration information for any switch on the network map:

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

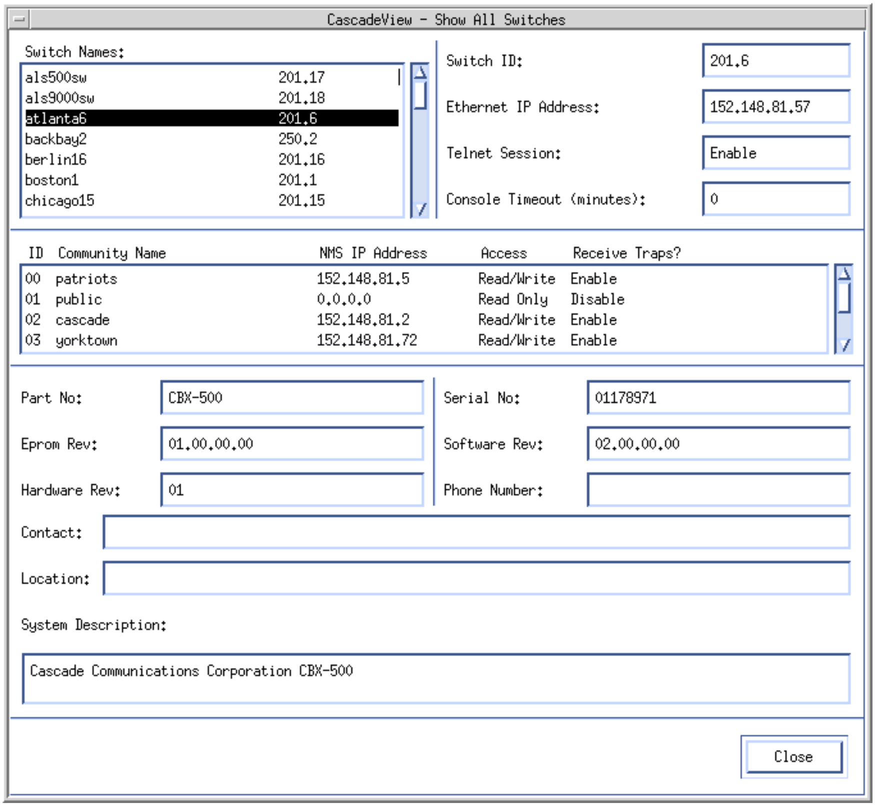



**Figure 1-22. Show All Switches Dialog Box**

2. Select the name of the switch from which you want to retrieve configuration information. Table 1-21 on page 1-62 describes the dialog box fields.

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

**Table 1-21. Show All Switches Fields**

| Field | Description |
|---|---|
| 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 connection. You assign this IP address to the Ethernet module in the switch during configuration. |
| Telnet Session | Displays whether Telnet access to the switch is enabled or disabled. |
| Console Timeout (minutes) | Displays how long (in minutes) the console can be inactive before it is logged off. |
| Community Name | Displays the name used to control access to the switch's configuration. The Community Name is used with the NMS IP address to identify whether the specified NMS has authority to send intrusive commands to the switch. The default name for the first NMS is *cascade* (case-sensitive). |
| NMS IP Address | Displays the address of the NMS configured to communicate with the selected switch. Traps generated from the selected switch are sent to this IP address. To send SNMP commands to the switch and to download switch software, the NMS IP address must match the switch IP address. |
| Access | Displays the access privileges between the NMS and the selected switch. The first NMS always has read/write access. An NMS with read-only access can receive traps but cannot send write commands to the switch. |
| Receive Traps | 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 switch processor (SP). |
| Eprom Rev | Displays the switch's EPROM revision level, 2.0 or greater. |

**Table 1-21. Show All Switches Fields (Continued)**

| Field | Description |
|---|---|
| Hardware Rev | Displays the revision level of the switch processor. |
| Serial No. | Displays the switch serial number, obtained from the switch's SPA module. |
| Software Rev | Displays the revision number for the firmware currently running on the switch. |
| Phone Number | Displays the telephone number for the contact person. |
| Contact | Displays the name of the contact person. |
| Location | Displays the physical location of the switch. |
| System Description | Displays the switch type. This parameter is taken directly from the switch and therefore is only displayed if the NMS is actively communicating with the selected switch. |

2

# Monitoring Trunks and Circuits

This chapter describes how to monitor trunks, circuits, and switched virtual circuits (SVCs) for a specified switch. Table 2-1 on page 2-2 lists the section that describes each of the Monitor functions.

> *You do not need to log on to display information through the Monitor menu. Monitoring functions do not require Operator passwords.*

# Accessing the Monitor Menu Functions

Table 2-1 references the section that describes each of the functions you can access from the Monitor menu.

**Table 2-1. Monitor Menu Options**

| Select Monitor ⇒ Cascade Objects ⇒ | To view | Refer to |
|---|---|---|
| Show All Trunks | Operational status and available bandwidth for any trunk in the network map. | "Viewing the Trunk Status" on page 2-3 |
| Show Circuits | The configuration, status, and routing information for all circuits in the network map. | "Viewing the Circuit Status" on page 2-11 |
| Show All Management VPI/VCIs | Status information about a management connection. | "Viewing All Management VPI/VCIs" on page 2-19 |
| Show All SVC Parameters | A submenu of SVC status information. | "Viewing All SVC Parameters" on page 2-21 |
| Show All Customers/VPNs | A submenu of Customer and VPN information. | "Viewing Customer/VPN Parameters" on page 2-47 |

# Viewing the Trunk Status

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 all trunks configured for this network map:

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

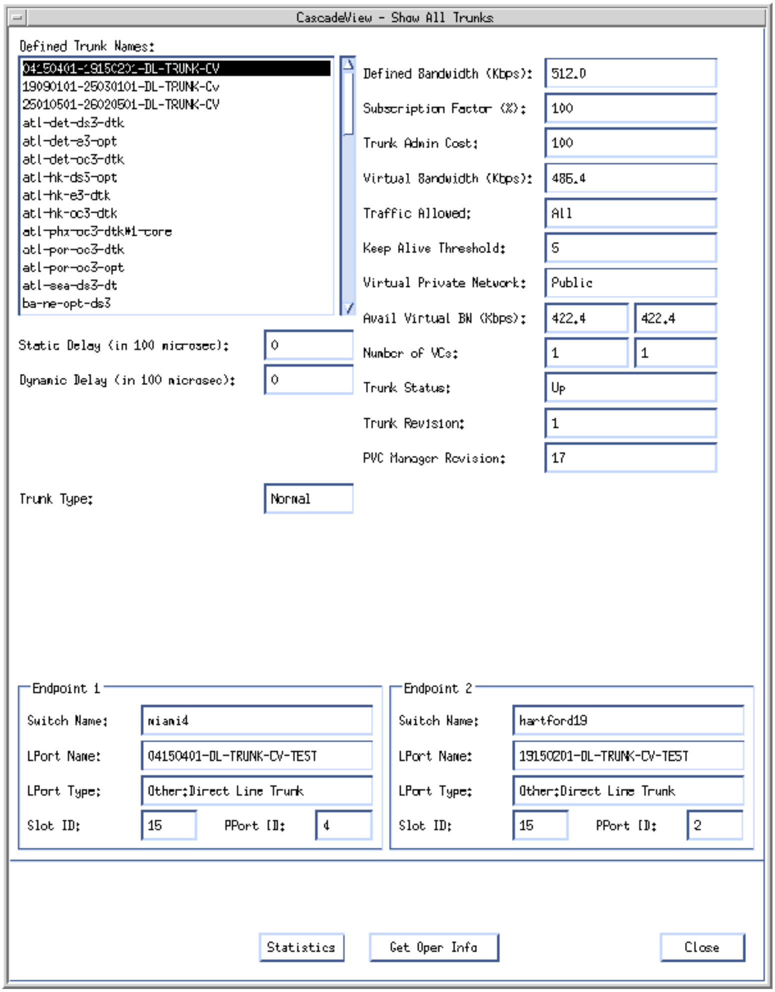



**Figure 2-1. Show All Trunks Dialog Box**

2. In the Defined Trunk Names list box, select the trunk from which you want to retrieve status information.

   Table 2-2 describes the Show All Trunks fields.

**Table 2-2. 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 bandwidth in Kbps for the selected trunk line. |
| Trunk Admin Cost | Displays a value that defines the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch. For more information, refer to the *Network Configuration Guide for CBX 500.* |
| Traffic Allowed | Displays one of the following options, which designates the type of traffic allowed on this trunk:<br>*All* – Trunk can carry SVC, PVC, and network management traffic.<br>*Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS.<br>*Mgmt & Address Restricted* – Trunk can carry PVCs and network management traffic. This trunk does not support SVC addressing information. If this is the only trunk between two nodes and these nodes cannot pass addressing information over other network trunks, then this mode effectively prevents SVCs from traversing this trunk. |
| Keep Alive Threshold | Displays the number of seconds the trunk protocol will continue to exchange Keep Alive (KA) control frames without getting a response from the remote node, before bringing the trunk down. |

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

| Field | Action/Description |
|---|---|
| Number of VCs | Displays the number of virtual circuits configured for this trunk. This value includes VCCs, VPCs, and SVCs. |
| Virtual Private Network | Displays the virtual private network name. |
| Trunk Status | Displays the current status of the selected trunk. Options include:<br>*Unknown* – The NMS cannot communicate with one or both switch endpoints that make up this trunk.<br>*Down* – The switches cannot establish a communication link.<br>*Attempt* – A switch is attempting to contact another switch but has not yet received a response.<br>*Init* – A one-way communication exists between the two switches.<br>*Two-way* – A bi-directional communication exists between the two switches.<br>*Exchange Start* – The two switches are about to exchange the network topology.<br>*Exchange* – The two switches are exchanging network topology.<br>*Loading* – The two switches are requesting the most recent link state information.<br>*Backed-up* – A primary trunk exists and is ready for backup.<br>*Up* – The trunk is up and operational between the two switches.<br>*Defined* – A backup trunk is ready for backup. |

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

| Field | Action/Description |
|---|---|
| Trunk Revision | Displays the revision of link trunk protocol software at each endpoint. |
| PVC Manager Revision | Displays the PVC manager software revision. |
| Static Delay (in 100 microsec) | Represents the measured one-way delay in units of 100 microseconds. This measurement is taken when the trunk initializes and it is only updated when the trunk changes state from down to up. The static delay value is used in conjunction with the end-to-end delay routing metric to enable you to route circuits over trunks with the lowest end-to-end delay. |
| Dynamic Delay (in 100 microsec) | Represents the measured one-way delay in units of 100 microseconds. This measurement is made continually on operational trunks. Under most conditions, the dynamic delay value will match the static delay value. However, if some characteristics of the underlying transmission media for the trunk change such that the dynamic delay changes, this value may differ from the static delay. |
| 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 at each endpoint of the trunk. |
| Lport Type | Displays the configured logical port type. |
| Slot ID | Displays the slot number where the I/O module containing the selected port is installed. |
| PPort ID | Displays the physical port ID number on which the logical port is configured. |

Table 2-3 describes the dialog box command buttons.

**Table 2-3. Show All Trunks Dialog Box Command Buttons**

| Choose | To |
|---|---|
| View QoS Parameters | Display the Show Logical Port QoS Parameters dialog box for the selected trunk. |
| Statistics | Display the summary statistics for the selected trunk. (*Available on Direct trunks only.*) |
| Get Oper Info | Display the status of the selected trunk. A message appears in the Trunk Status field. Refer to the *Network Configuration Guide for CBX 500* for a description of these messages. |
| Close | Exit the Set All Trunks dialog box. |

## Displaying Multiple Trunks between Switches

If you configure more than one trunk between two switches, these trunks appear as a solid line between the switches.

To display all of the trunk connections between two switches:

1. Double-click on the solid line between the switches. A trunk submap window appears, similar to the example shown in Figure 2-2.

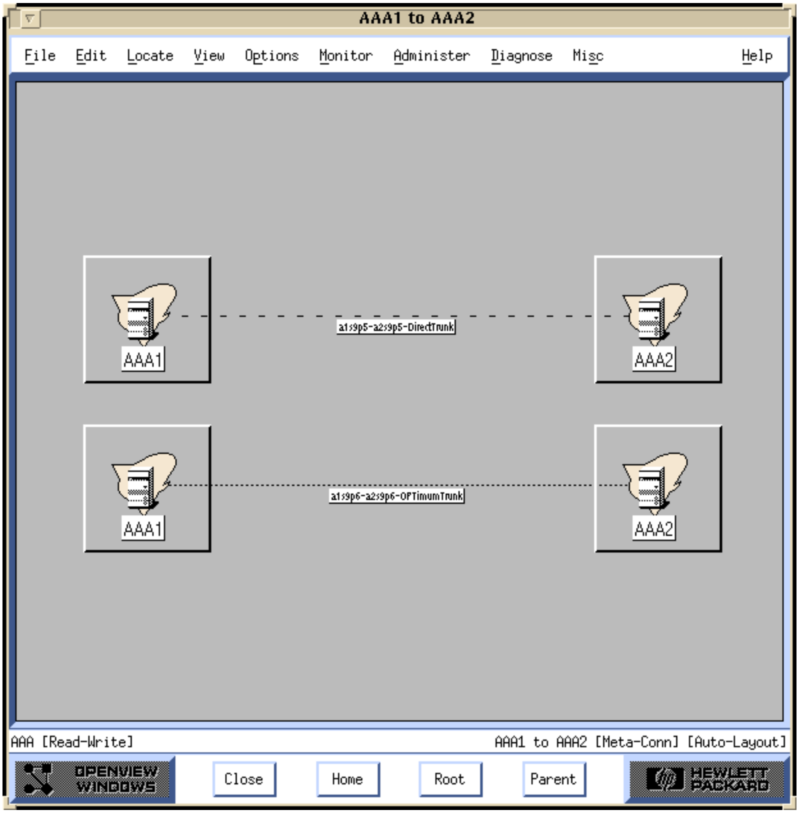



**Figure 2-2. Displaying Multiple Trunks**

2. Choose Close to exit this window and return to the network map.

## Trunk Coloring

The trunk lines on the network map change color based on the polled status and the traps received by the Cascade Event Log. Table 2-4 describes the color scheme used to identify the status of a trunk connection on the network map.

**Table 2-4. Trunk Color Status Indicators**

| Color | Status |
|---|---|
| Black | Either the line connection has not been defined as a trunk or the environment variable $XUSERFILESEARCHPATH does not point to ***/opt/CascadeView/app-defaults***. [1] |
| Red | Trunk is down. |
| Blue | Trunk status is Unknown or Unmanaged. |
| Yellow | Trunk connection is coming up. |
| Green | Trunk connection is Up. |
| Orange | Only one trunk connection out of many connections is Up. |
| Cyan | More than one trunk connection is defined between the two endpoints. At least one trunk is up and one trunk is down. |

[1] If the Trunk graphic is black, set the following environment variable in .profile:

```
$ XUSERFILESEARCHPATH =/opt/CascadeView/app-defaults/%N
$ export XUSERFILESEARCHPATH
```

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

# Viewing the Circuit Status

To display the current configuration, status, and routing information for all circuits in the network:

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

   **All on Map** — Displays a list of all the circuits configured for the current map.

   **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.

   **All by Name** — Use this option to enter a specific circuit name. You can use wild-card characters. To search by name, use an asterisk (*) to replace several characters or use a question mark (?) to replace one character.

   **All on Switch and by Name** — Select a switch on the current map, then use this option to enter a specific circuit to search by name. You can use wild-card characters. Use an asterisk (*) to replace several characters or use a question mark (?) to replace one character.

   After you select an option, the Show [All] PVCs on Map dialog box appears.

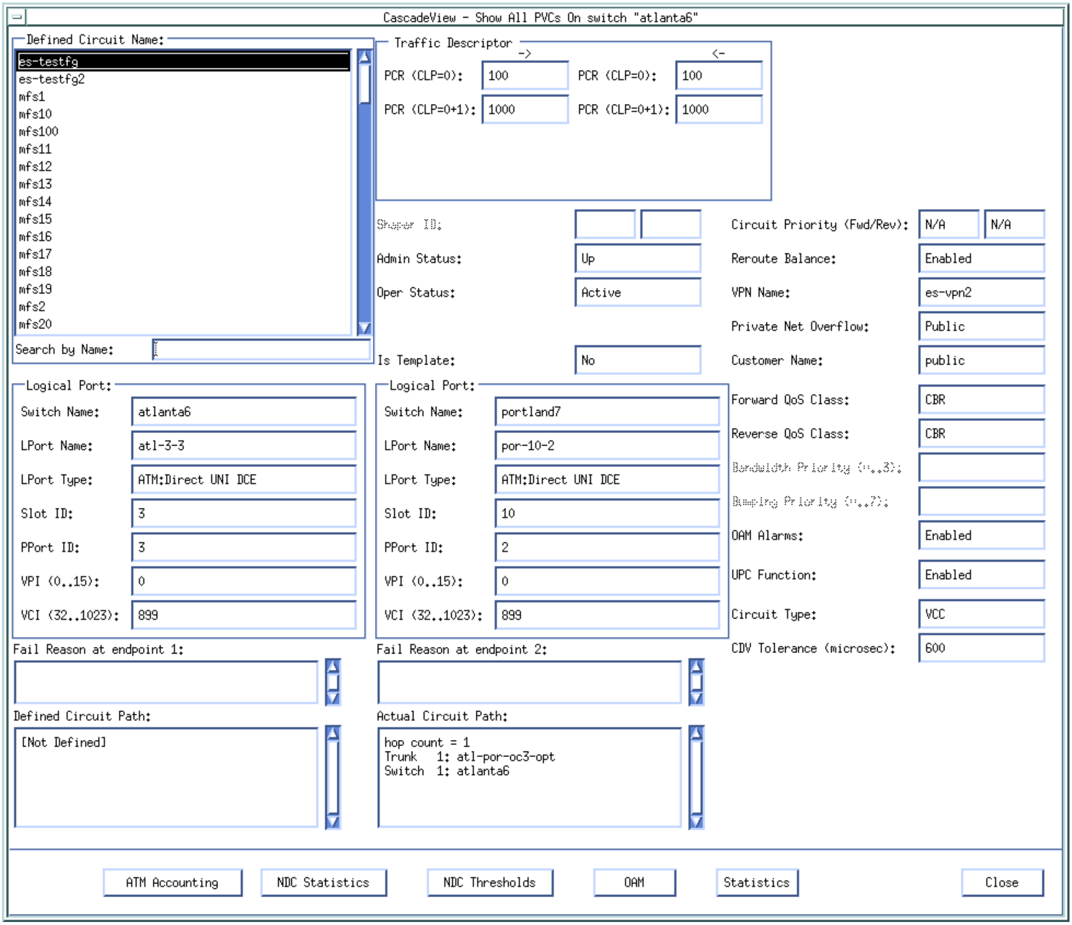



**Figure 2-3. Show All PVCs on Map Dialog Box**

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

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

Table 2-5 briefly describes all the possible fields that may appear on the Show All PVCs dialog box:

**Table 2-5. 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.<br>Use an * to match any number of characters<br>Use a ? to match a single character<br>To match the * character, type **<br>To match the ? character, type \?<br>To match the \ character, type \\ |

**Table 2-5. Show All PVCs Fields (Continued)**

| Field | Action/Description |
|---|---|
| Logical Port | The dialog box displays the following logical port information for each circuit endpoint:<br>*Switch Name* – Displays the name of the switch at each endpoint of the circuit.<br>*LPort Name* – Displays the name of the logical port at each endpoint of the circuit.<br>*LPort Type* – Displays the configured type of the selected logical port.<br>*Slot ID* – Indicates the physical slot number where the I/O module containing the selected port is installed.<br>*PPort ID* – Displays the ID number of the physical port for which the selected logical port is configured.<br>*VPI (0..nnnn)* – Displays the VPI for the selected circuit at this endpoint.<br>*VCI (32..nnnn)* – Displays the VCI for the selected circuit at this endpoint. |

**Table 2-5. Show All PVCs Fields (Continued)**

| Field | Action/Description |
|---|---|
| VPN Name | Displays the VPN name for the selected PVC (if applicable). |
| Private Net Overflow | Displays Public if the customer is allowed to use a public trunk in the event of overflow or trunk failure. Displays Restrict if the customer is restricted to its VPN trunks during overflow or trunk failure. |
| Customer Name | Displays the customer name for the selected PVC (if applicable). |
| Forward QoS Class | Displays the Quality of Service class for forward traffic. |
| Reverse QoS Class | Displays the Quality of Service class for reverse traffic. It does not have to be the same as the Forward QoS Class. |
| OAM Alarms | When enabled, the circuit generates OAM F5 or F4 AIS alarms to indicate that the circuit is down. |
| UPC Function | When enabled, the circuit tags or drops cells that do not conform to the traffic parameters as they come into the port. When disabled, the circuit allows all traffic, including non-conforming traffic, into the port. *Cascade recommends that you enable the UPC function on all circuits.* |
| Circuit Type | Displays the circuit type, either a Virtual Path Connection (VPC) or Virtual Channel Connection (VCC). |
| CDV Tolerance | Displays the Cell Delay Variation Tolerance (CDVT). Valid values are between 1 - 65535 μs. The default is 600 μs. |

**Table 2-5. Show All PVCs Fields (Continued)**

| Field | Action/Description |
|---|---|
| Fail Reason at endpoint 1 (2) | Displays the reason a selected circuit failed (if any) for a given endpoint. |
| Defined Circuit Path | Displays the configured circuit path. |
| Actual Circuit Path | Displays the actual path that OSPF selected for this circuit to use to get to its destination. |
| VPN Name | Displays the VPN name for the selected PVC (if applicable). |

Table 2-6 describes the dialog box command buttons.

**Table 2-6. Show All PVCs on Map Command Buttons**

| Choose | To |
|---|---|
| ATM Accounting | Access the ATM accounting functions for a PVC. For more information, refer to the *Accounting System Administrator's Guide*. |
| NDC Thresholds | Display the configured network data collection (NDC) thresholds for the circuit. |
| NDC Statistics | Display the NDC statistics for the selected circuit. |
| OAM | Run the Operations, Administration, and Management diagnostics for the selected circuit. |
| Statistics | Display the summary statistics for the selected circuit. |
| Close | Exit the Set All PVCs dialog box. |

3. Use Table 2-7 to interpret fail reasons, if necessary.

> *The Show All PVCs on Map dialog box displays the circuit names and circuit attributes as configured in the NMS. The Status, Path, and Fail Reasons are extracted directly from the switch.*

**Table 2-7. 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 circuit. | Reconfigure the circuit to a lower bandwidth or increase the physical or virtual bandwidth of the trunk. You can also add more parallel trunks. |
| 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. | This is a serious problem! Report this error to the Cascade Technical Response Center. |

**Table 2-7. Inactive Operational Status Codes (Continued)**

| Fail Reason | Description | Solution |
|---|---|---|
| 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 in the OPTimum path. |
| Trunk is down at [*node*] | A trunk line in the circuit path is down. | The circuit automatically reroutes if alternate paths are defined. |
| UNI/NNI is down at [*node, lport*] | The UNI or NNI is down at the node/interface number (ifnum). | Make sure the switch is connected to the user device. Display traffic in and out of the port by generating Summary Statistics. |
| PVC segments are not ready to receive beyond [*lport, node*] | (NNI specific problem.) The PVC segment(s) beyond this logical port sent a flow block message stating that it cannot receive data. | A trunk line in the circuit path may be down. Check the status of all PVC segments in the network beyond the logical port noted in the Fail Reason. |
| Warning: Defined Path is not available. The alternate path is in use. PVC segments are inactive beyond [*lport, node*] | The caller node cannot be reached through the defined path. This problem may be caused by a connection failure. | Verify the integrity of the trunk that is being used on the defined circuit path.<br>Once the defined path is re-established, the circuit is routed back to the defined path within 20 seconds of availability. |

# Viewing All Management VPI/VCIs

To display status information about a management VPI/VCI connection:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Management VPI/VCIs. The following dialog box appears.

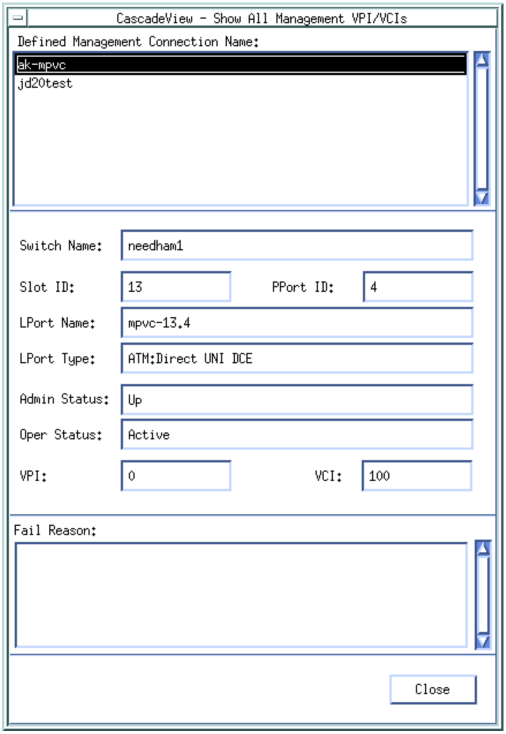



**Figure 2-4. Show All Management VPI/VCIs Dialog Box**

Table 2-8 describes the Show All Management VPI/VCI fields.

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

**Table 2-8. Add Management VPI/VCI Fields**

| Field | Action/Description |
|---|---|
| Switch Name | Displays the name of the switch which connects to the router that serves as the interface for the Network Management VPI/VCI. |
| Slot ID | Displays the I/O slot (number) in which the IOM resides. |
| PPort ID | Displays the port number for the physical port. |
| LPort Name | Displays the name of the logical port. |
| LPort Type | Displays the logical port type. |
| VPI | Displays the VPI that is used for the connection. |
| VCI | Displays the VCI that is used for the connection. |
| Admin Status | Displays either Up or Down to indicate whether the Management VPI/VCI connection is 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 Operational Status is Inactive. |

# Viewing All SVC Parameters

Through the Monitor menu you can also check the status of configured SVC parameters. For SVC configuration information, refer to the *Network Configuration Guide for CBX 500*.

To display configured SVC parameters, refer to the following sections:


- "Viewing All Node Prefixes" on page 2-21
- "Viewing All Port Prefixes" on page 2-24
- "Viewing All Port Addresses" on page 2-26
- "Viewing All Port User Parts" on page 2-29
- "Viewing All Port SVC Configurations" on page 2-31
- "Viewing All Active SVCs" on page 2-34
- "Viewing All ILMI Addresses" on page 2-38
- "Viewing SVC Failed Calls" on page 2-39


## Viewing All Node Prefixes

To display all node prefix formats on a switch:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Node Prefixes. The following dialog box appears.

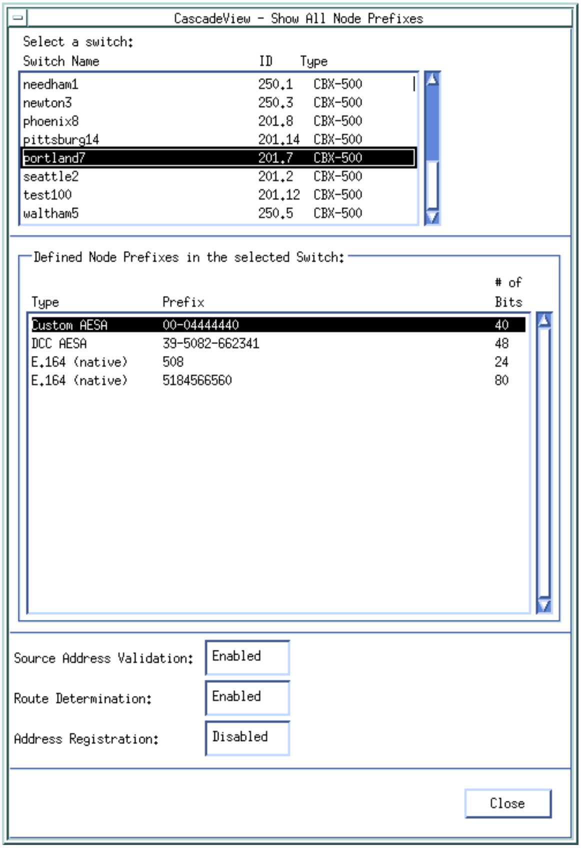



**Figure 2-5. Show All Node Prefixes Dialog Box**

2. Select the switch name for which you want to display node prefixes.

   The Defined Node Prefixes in the selected Switch list box displays the defined node prefixes for this switch.

   Table 2-9 describes the Show All Node Prefixes fields.

3. When you finish viewing the information, choose Close to return to the network map.

**Table 2-9. Show All Node Prefixes Fields**

| Field | Description |
|---|---|
| Source Address Validation | Displays enabled or disabled to indicate the source address validation. Enabled validates the calling party address against the node prefix associated with the UNI logical port which received the call setup message. Disabled indicates this prefix is not used to validate calling party addresses. |
| Route Determination | Displays enabled or disabled to indicate the route determination. Enabled indicates the OSPF protocol uses this node prefix for routing aggregation. Disabled indicates OSPF does not use this node prefix for route determination. |
| Address Registration | Displays enabled or disabled to indicate the address registration. Enabled indicates this node prefix is used for ILMI address registration for all UNI-DCE “network-to-endsystem” logical ports that support ILMI. |

## Viewing All Port Prefixes

To display all port prefixes defined for a selected logical port.

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Port Prefixes. The following dialog box appears.

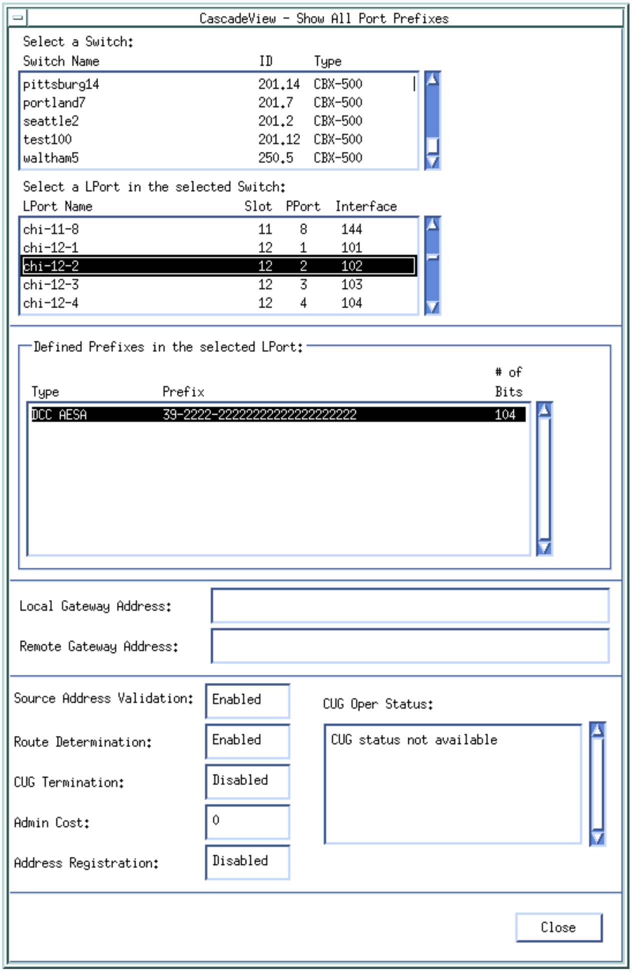



**Figure 2-6. Show All Port Prefixes Dialog Box**

2. Select the switch and logical port names for which you want to display prefixes.

This dialog box displays the defined prefixes for this logical port, as well as the admin cost and local and remote gateway addresses for this logical port.

Table 2-10 describes the Show All Port Prefix fields.

3. When you finish viewing the information, choose Close to return to the map.

**Table 2-10. Show All Port Prefix Fields**

| Field | Description |
|---|---|
| Source Address Validation | Displays Enabled or Disabled to indicated the source address validation. Enabled validates the calling party address against the port prefix associated with the UNI port which received the call setup message. Disabled indicates this port prefix is not used to validate calling party addresses. |
| Route Determination | Displays Enabled or Disabled to indicated the route determination. Enabled indicates OSPF protocol uses this port prefix for route determination. If disabled, OSPF registration is not used. |
| CUG Termination | Displays Enabled or Disabled to indicated the CUG termination. Enabled indicates this prefix is used as part of a Closed User Group (CUG). Incoming and outgoing calls with a calling or called party address that matches this prefix, are subject to CUG security checks. For more information about CUGs, refer to the *Network Configuration Guide for CBX 500*. |
| Admin Cost | Displays the administrative cost associated with the port prefix. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port in the network that has the lowest administrative cost associated with the port prefix. |

**Table 2-10. Show All Port Prefix Fields (Continued)**

| Field | Description |
|---|---|
| Address Registration | Displays Enabled or Disabled to indicated the address registration. Enabled indicates port prefixes are used for ILMI address registration if the ILMI is enabled on this logical port. This option cannot be enabled for AESA port prefixes that are not at least 13 octets long. |
| CUG Oper Status | Displays the current CUG status. |

## Viewing All Port Addresses

If the device attached to a given physical port does not support address registration, you can define SVC addresses for all logical ports on that physical port. To display all SVC addresses:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Port Addresses. The following dialog box appears.

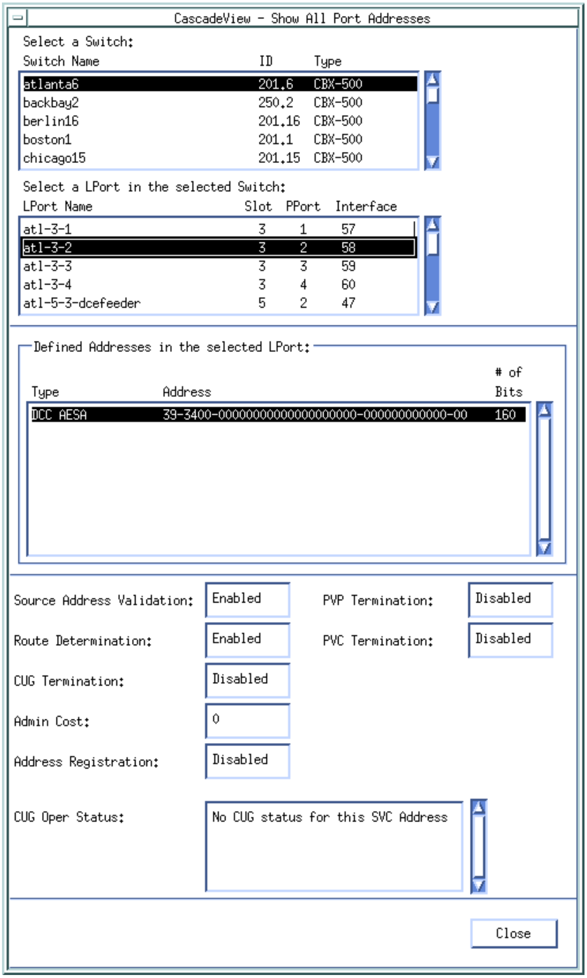



**Figure 2-7. Show All Port Addresses**

2. Select the switch and logical port names for which you want to display SVC addresses. The Defined Address in the selected Switch list box displays the defined addresses for this logical port.

   Table 2-11 describes the Show All Port Addresses fields.

3. When you finish, choose Close to return to the network map.

**Table 2-11. Show All Port Addresses Fields**

| Field | Description |
|---|---|
| Source Address Validation | Displays Enabled or Disabled to indicated the source address validation. Enabled validates the calling party address against the port prefix associated with the UNI port which received the call setup message. Disabled indicates this port prefix is not used to validate calling party addresses. |
| Route Determination | Displays Enabled or Disabled to indicated the route determination. Enabled indicates OSPF protocol uses this port prefix for route determination. If disabled, OSPF registration is not used. |
| CUG Termination | Displays Enabled or Disabled to indicated the CUG termination. Enabled indicates this prefix is used as part of a Closed User Group (CUG). Incoming and outgoing calls, with a calling or called party address that matches this prefix, are subject to CUG security checks. For more information about CUGs, refer to the *Network Configuration Guide for CBX 500*. |
| Admin Cost | Displays the administrative cost associated with the port prefix. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port in the network that has the lowest administrative cost associated with the port prefix. |
| Address Registration | Displays Enabled or Disabled to indicated the address registration. Enabled indicates port prefixes are used for ILMI address registration if the ILMI is enabled on this logical port. This option cannot be enabled for AESA port prefixes that are not at least 13 octets long. |

Table 2-11. Show All Port Addresses Fields (Continued)

| Field | Description |
|---|---|
| CUG Oper Status | Displays the current CUG status. Possible address and prefix status messages include:<br>• A CUG configuration error has occurred at this SVC address (or prefix).<br>• An ambiguous condition exists at this SVC address (or prefix). Decisions will be made at call time.<br>• This SVC address (or prefix) has:<br>Outgoing access<br>Incoming access<br>• This SVC does not belong to any CUGs.<br>• This SVC Address belongs to CUGs:<br>[*CUG name and ID*] |
| PVP Termination | Enabled indicates an SPVC is terminated to this address on this logical port. |
| PVC Termination | Enabled indicates an SVC (spoofing) or SPVCC is terminated to this address on this logical port. |

## Viewing All Port User Parts

The user part of an AESA address is used for DTE (user) ports on a Cascade switch. The user part is used to construct the address table on the DCE device attached to the public side of the UNI. When the receiving node broadcasts its network prefixes, the sending node responds by sending its configured user parts; this enables the receiving node to build the ILMI address table. For more information about user parts, refer to the *Network Configuration Guide for CBX 500*.

To display all user parts defined for a logical port:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Port User Parts. The following dialog box appears.

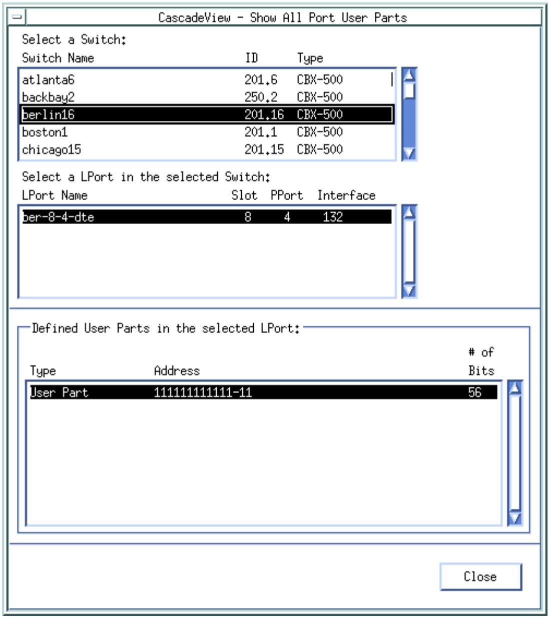



**Figure 2-8. Show All Port User Parts Dialog Box**

2. Select the switch and logical port names for which you want to display user parts. The system displays the user part type, address, and number of bits.

3. Choose Close to return to the network map.

## Viewing All Port SVC Configurations

To display SVC configurations:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Port SVC Configurations. The following dialog box appears.

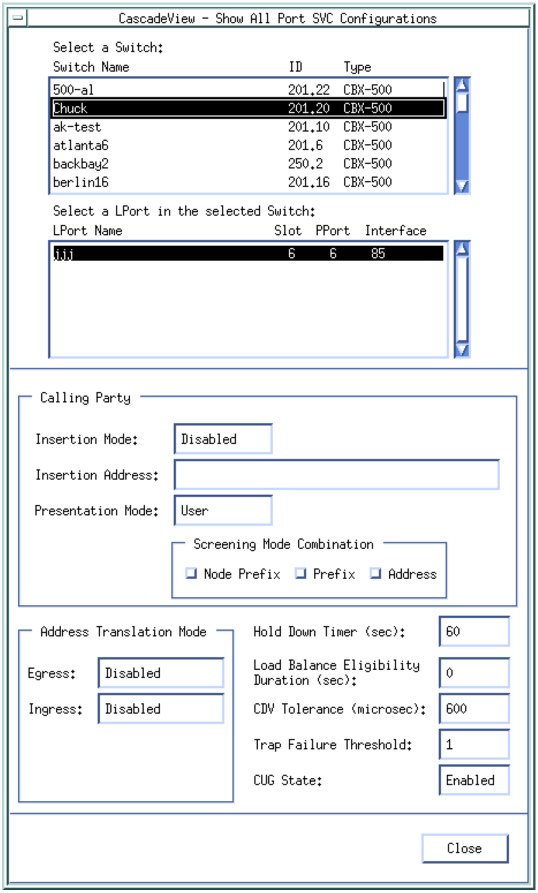



**Figure 2-9. Show All Port SVC Configurations Dialog Box**

2. Select the switch and logical port names for which you want to display SVC configurations.

   Table 2-12 describes the Show All SVC Configurations fields.

3. When you finish viewing the fields, choose Close to return to the network map.

**Table 2-12. Show All SVC Configurations Fields**

| Field | Action/Description |
|---|---|
| **Calling Party Fields** | |
| Insertion Mode | Displays the configured insertion mode. *Insert* indicates the logical port inserts the configured calling party insertion address. *Replace* indicates the logical port inserts the configured calling party insertion address, if there is no calling party address. If there is a calling party address, the logical port overwrites the existing calling party information element with the configured calling party insertion address. *Disabled* indicates the logical port does not insert or replace the calling party address. |
| Insertion Address | Displays the configured insertion address. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| Presentation Mode | Displays the configured presentation mode which specifies whether or not to include the calling party address on outgoing calls. *User* indicates the calling party address is included on outgoing calls, based on the presentation indicator in the SETUP message of the user's call. *Always* indicates the calling party address is included on all outgoing calls, regardless of the presentation indicator. *Never* indicates the calling party address in never included on outgoing calls. |

**Table 2-12. Show All SVC Configurations Fields**

| Field | Action/Description |
|---|---|
| Screening Mode Combination | A read-only field which specifies the port level screening on the calling party address. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| Egress/Ingress Address Translation Mode | Displays the configured address translation mode. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| Hold Down Timer (sec) | Displays the configured number of seconds the network should wait before initiating call clearing. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| Load Balance Eligibility Duration (sec) | Displays the configured number of seconds an SVC must be established before a call is eligible for load balance rerouting. |
| Trap Failure Threshold | Displays the threshold crossing alarm value for SVC failure traps. The switch generates a trap if the internal SVC failure counter crosses this threshold during the current 15-minute time period. |
| CUG State | Displays the configured CUG state. *Enabled* indicates CUG processing is allowed for this logical port. |

# Viewing All Active SVCs

You can use the Show All SVCs dialog box to upload SVC information for a selected logical port. This dialog box provides a hop-by-hop trace of all active SVCs that traverse the network.

You can display a list of SVC records with the following attributes for each record: VPI, VCI, End Reference, Creation Time, Calling Party Address, and Called Party Address. You can also select an SVC record and display its SVC attributes through the Show Attributes command.

To display a list of SVC records:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Active SVCs. The following dialog box appears.

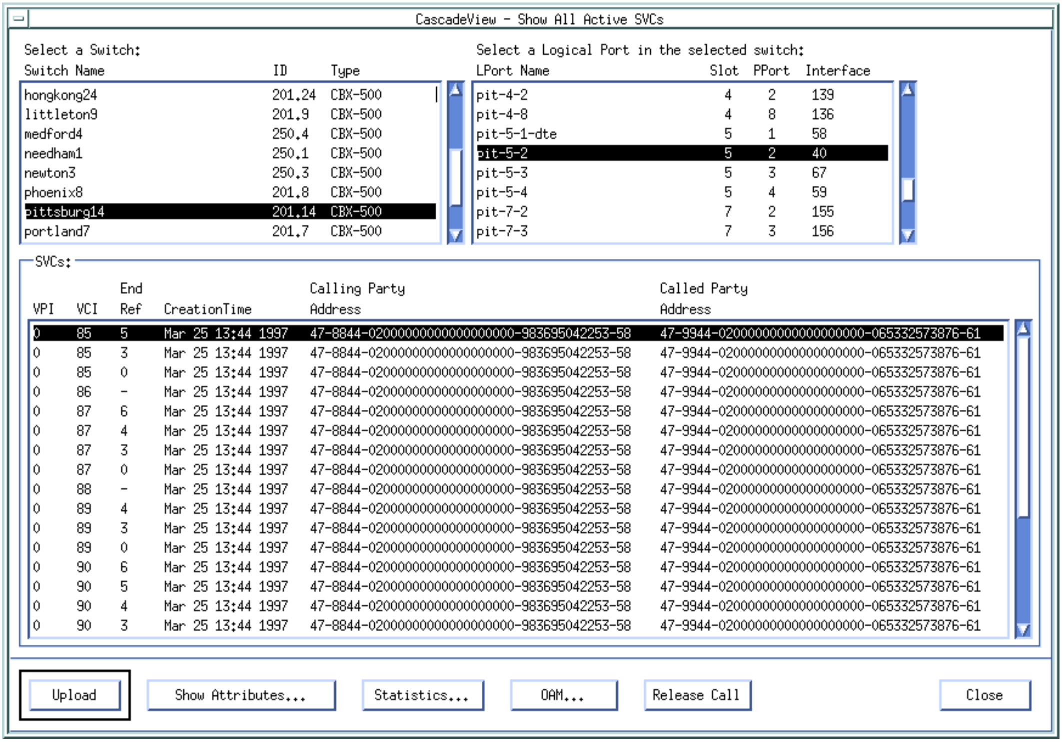



**Figure 2-10. Show All Active SVCs Dialog Box**

2. Select the switch and logical port names and choose Upload to upload all SVC records from the selected logical port.

   Table 2-13 describes the Show All Active SVCs dialog box command buttons.

**Table 2-13. Show All Active SVCs Commands**

| Command | Description |
|---|---|
| Upload | Uploads a list of active SVCs for the logical port you select. |
| Show Attributes | Displays call details, such as creation time and VPI/VCI address, for the SVC you select. |
| Statistics | Displays SVC statistics. For more information, refer to "Displaying SVC Summary Statistics" on page 5-39. |
| OAM | Enables you to initiate an OAM loopback test for the selected SVC. For more information, refer to Chapter 4, "Setting and Monitoring Loopbacks". |
| Release Call | Enables you to release individual SVCs on a UNI port without affecting other SVCs on the same port. |

## Viewing SVC Attributes

Use the Show Attributes command on the Show All Active SVCs dialog box to display information about a specific SVC. This information includes call details, such as creation time and VPI/VCI address, broadband bearer capabilities, and ATM traffic descriptors.

To view SVC attributes:

1. From the Show All Active SVCs dialog box (Figure 2-10 on page 2-34), select an SVC record and choose Show Attributes.

> *SVCs are dynamic and may be set up and taken down by the CPE. A SVC may be released by the CPE between the time upload is selected and show attributes is used. If this situation occurs, you must upload the SVC records to the logical port again.*

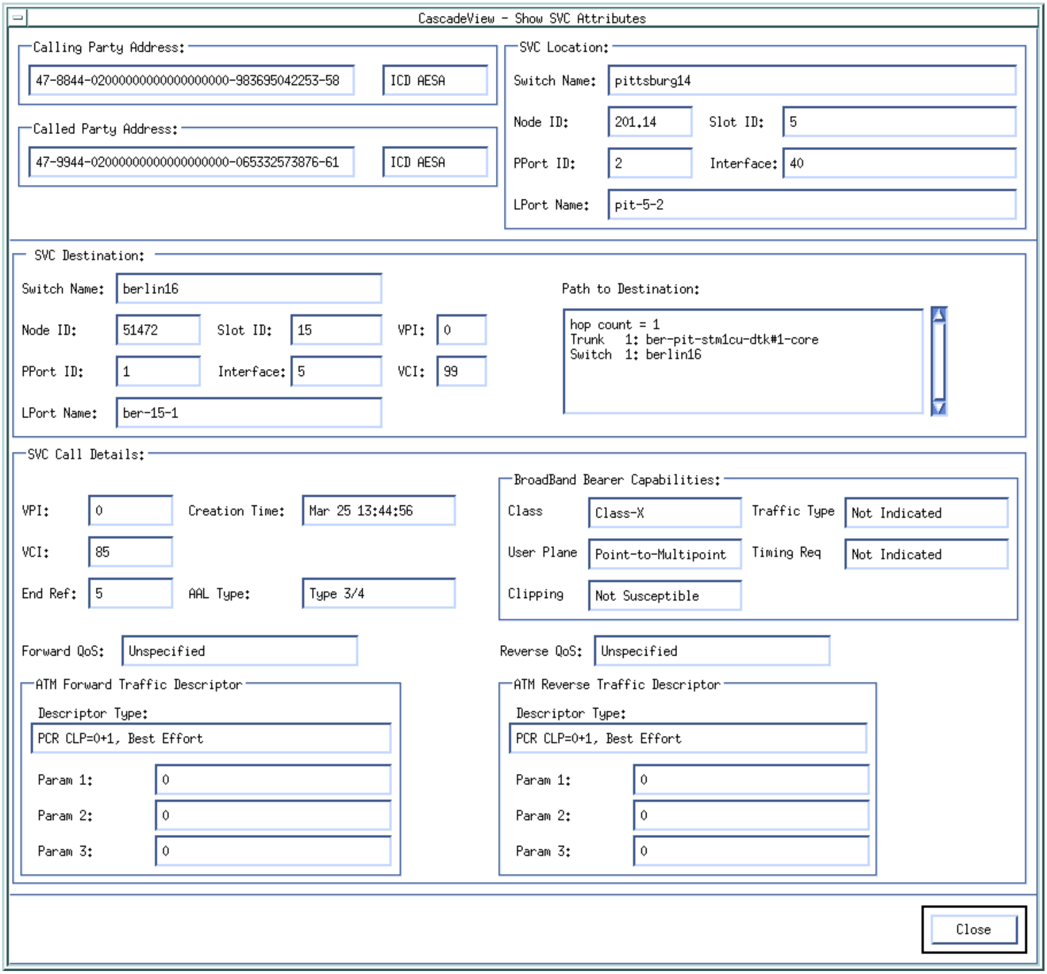



**Figure 2-11. Show SVC Attributes Dialog Box**

Table 2-14 describes the Show SVC Attributes fields.

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

**Table 2-14. Show SVC Attributes Fields**

| Field | Action/Description |
|---|---|
| Calling Party Address | Displays the entire SVC calling party address and lists the address type (either AESA or E.164). |
| Called Party Address | Displays the entire SVC called party address and lists the address type (either AESA or E.164). |
| SVC Location | Displays information that identifies the SVC location (for calling party), including switch, logical port, and physical port IDs. |
| SVC Destination | Displays information that identifies SVC location (for called party), including switch, logical port, and physical port IDs, and VPI/VCI addresses. This section also displays a "Path to Destination" listing which provides the hop count and trunk name. |
| SVC Call Details | Displays the calling party VPI/VCI address and call creation time. This section also displays the endpoint reference and AAL Type. |
| Broadband Bearer Capabilities | These fields provide the contents of the broadband bearer capability information element from the SETUP or ADD PARTY message. |
| Forward/Reverse QoS | Displays the configured forward and reverse QoS class: either CBR, VBR-RT, VBR-NRT, or Unspecified. For more information, refer to Appendix E, "Signalled QoS, BBC, and BEI Service Category Mappings".<br><br>***Note**: This field displays the signalled QoS only. Under some conditions, the signalled QoS received by the switch may be different from the actual QoS in the switch.* |
| ATM Forward/Reverse Traffic Descriptor | Displays the forward and reverse ATM traffic descriptors. For more information on ATM traffic descriptors, refer to the *Network Configuration Guide for CBX 500*. |

## Viewing All ILMI Addresses

To view dynamic address (ILMI) information for a selected logical port:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All ILMI Addresses. The following dialog box appears.

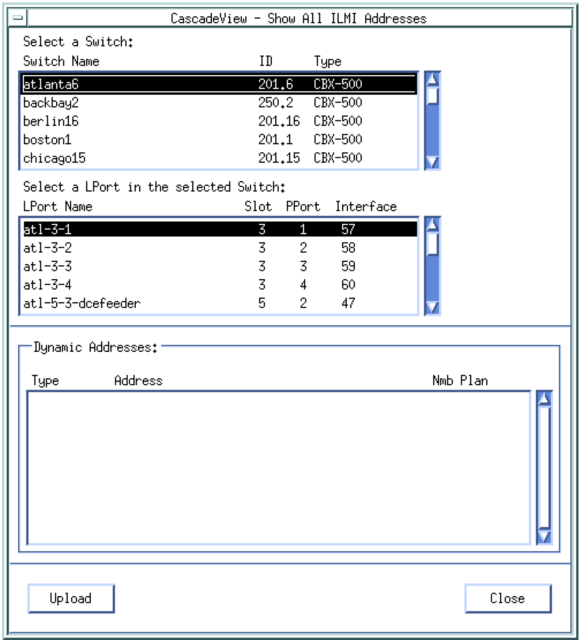



**Figure 2-12. Show All ILMI Addresses Dialog Box**

2. Select the switch and logical port names for which you want to view ILMI address information.

3. Choose Upload to display the ILMI addresses assigned to this port.

4. Choose Close to return to the network map.

## Viewing SVC Failed Calls

To upload and view SVC failed call information:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Failed SVCs. The following dialog box appears.

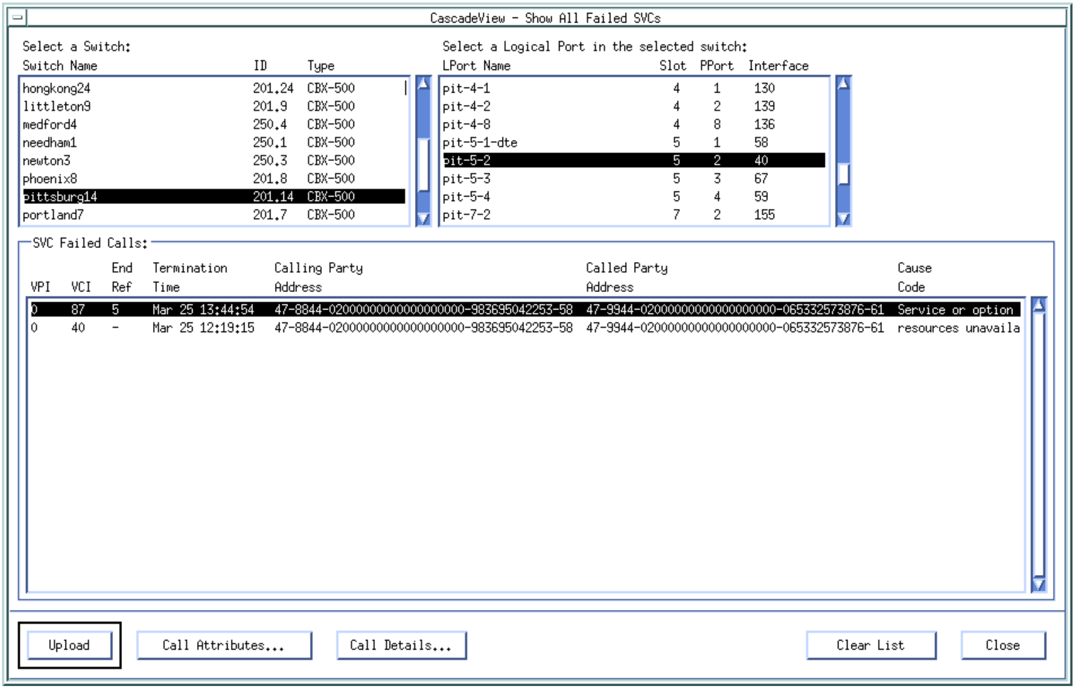



**Figure 2-13. Show All SVC Failed Calls**

2. From the list at the top of the dialog box, select the switch and logical port names and choose Upload to view the failed SVC calls for this logical port.

   Table 2-15 describes the Show All SVC Failed Calls dialog box command buttons.

**Table 2-15. Show All SVCs Failed Calls Commands**

| Command | Description |
|---|---|
| Upload | Uploads a list of active SVCs for the logical port you select. |
| Call Attributes | Displays information about the failed SVC call you select. Refer to page 2-40 for information. |
| Call Details | Displays information about the broadband bearer capabilities and ATM traffic descriptors of the failed call. Refer to page 2-43 for information. |
| Clear List | Deletes the list of failed calls for this logical port from the switch.<br>***Note***: *This action permanently deletes the list from the switch.* |

3. Choose Close to return to the network map.

## Viewing Call Attributes

Use the Call Attributes command on the Show All Failed SVCs dialog box to display information about a specific failed SVC call. This information includes calling party address, failure time, and terminating PDU.

To view failed call information:

1. From the Show All Failed SVCs dialog box (Figure 2-13 on page 2-39), select an SVC record and choose Call Attributes. The following dialog box appears.

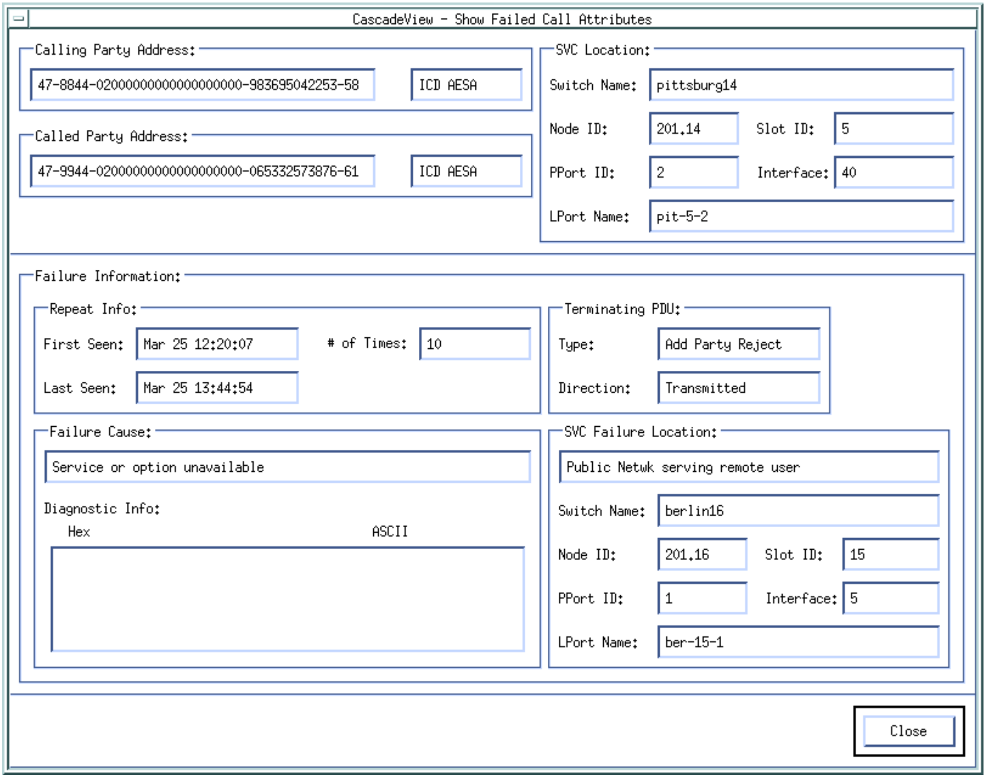



**Figure 2-14. Show Failed Call Attributes Dialog Box**

Table 2-16 describes the Show Failed Call Attributes fields.

2. When you finish, choose Close to return to the Show All Failed Calls dialog box.

**Table 2-16. Show Failed Call Attributes Fields**

| Field | Description |
|---|---|
| Calling Party Address | Displays the entire SVC calling party address and lists the address type (either AESA or E.164). |
| Called Party Address | Displays the entire SVC called party address and lists the address type (either AESA or E.164). |
| SVC Location | Displays information that identifies the SVC location (for calling party), including switch, logical port, and physical port IDs. |
| Repeat Information) | Displays the dates and times of the failure first and most recent occurrence. Displays the number of times this identical failure has consecutively occurred on this port. |
| Terminating PDU | Displays the type of UNI signalling PDU used to terminate the call and indicates whether it was sent from or received by the logical port. |
| Failure Cause | Displays a message describing this failure. The failure cause text is based on the standard ATM forum UNI signalling cause codes. For more information, refer to Appendix F, “Using SVC Failure Information”. |
| Diagnostic Info | Displays the HEX and ASCII values from the release message diagnostic field. This information may assist in troubleshooting certain types of SVC failures. |
| SVC Failure Location | Displays a message describing the location of this failure, as well as the switch name, logical port ID and physical port ID information. |

## Viewing Failed Call Details

The Show Failed Call Details dialog box provides information about the broadband bearer capabilities and ATM traffic descriptors of the failed call.

To view this information:

1. From the Show All Failed SVCs dialog box (Figure 2-13 on page 2-39), select an SVC record and choose Call Attributes. The following dialog box appears.

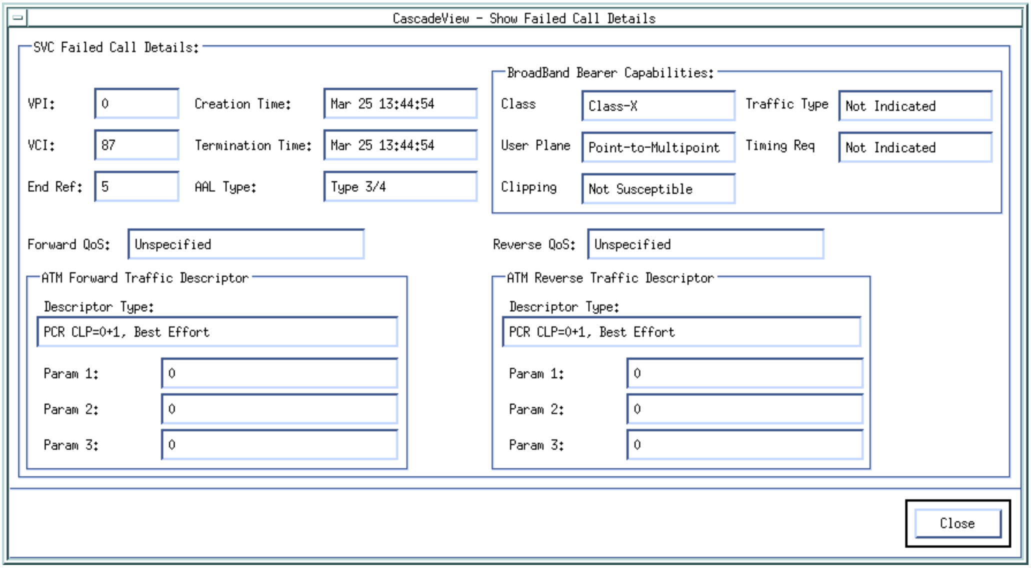



**Figure 2-15. Show Failed Call Details Dialog Box**

Table 2-17 on page 2-44 describes the dialog box fields.

2. When you finish, choose Close to return to the Show All Failed Calls dialog box.

**Table 2-17. Show Failed Call Details Fields**

| Field | Description |
|---|---|
| SVC Call Details | Displays the calling party VPI/VCI address and call creation time. This section also displays the end reference and AAL Type. |
| Broadband Bearer Capabilities | These fields provide the contents of the broadband bearer capability information element from the SETUP or ADD PARTY message. |
| Forward/Reverse QoS | Displays the configured forward and reverse QoS class: either CBR, VBR-RT, VBR-NRT, or Unspecified.<br>***Note**: This field displays the signalled QoS only. Under some conditions, the signalled QoS received by the switch may be different from the actual QoS in the switch.* |
| ATM Forward/Reverse Traffic Descriptor | Displays the forward and reverse ATM traffic descriptors. For more information on ATM traffic descriptors, refer to the *Network Configuration Guide for CBX 500*. |

## Viewing Port Security Screens

The Port Security Screening feature is a mechanism you can use to ensure that your network cannot be compromised. You do this by creating screens which can allow/disallow incoming and outgoing calls. Refer to the *Network Configuration Guide for CBX 500* for information on configuring port security screening.

You can apply the screens to any ATM UNI or NNI logical port in your network. You can use a maximum of 16 different screens per port. Using these screens, the port checks every call it receives for the matching criteria specified in the screen(s). If the call meets the matching criteria specified in at least one of these screens, the port either passes or blocks that call, according to the security screen design.

To view this information:

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters ⇒ Show All Port Security Screens. The following dialog box appears.

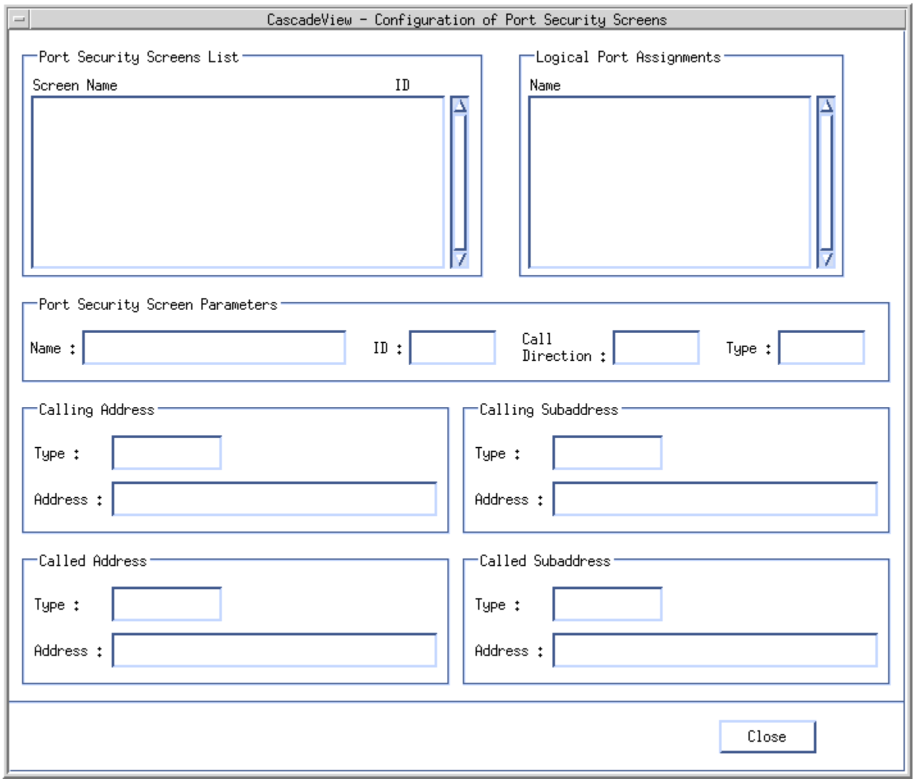



**Figure 2-16. Configuration of Port Security Screens Dialog Box**

Table 2-18 on page 2-46 describes the dialog box fields.

2. When you finish, choose Close to return to the map.

**Table 2-18. Configuration of Port Security Screens Fields**

| Field | Action/Description |
|---|---|
| Name | Displays a name (up to 32 characters) for this security screen. |
| Call Direction | Displays the configured call direction screen.<br>*Ingress* (default) – Screens incoming calls.<br>*Egress* – Screens outgoing calls. |
| Type | Displays the configured screen type which determines the action this screen performs.<br>*Block* (default) – Blocks all calls that match the criteria.<br>*Pass* – Passes all calls that match the criteria. |
| Calling Address | Displays the calling address for incoming calls. |
| Calling Subaddress | Displays the calling subaddress for incoming AESA calls only. This parameter provides an optional level of screening. |
| Called Address | Displays the called address if this screen is for outgoing calls. |
| Called Subaddress | Displays the called subaddress for outgoing AESA calls only. This parameter provides an optional level of screening. |

# Viewing Customer/VPN Parameters

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.*

You can use the following functions to monitor VPN information:

- Show All Customers
- Show All Virtual Private Networks

## Using the VPN/Customer View Function

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

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.

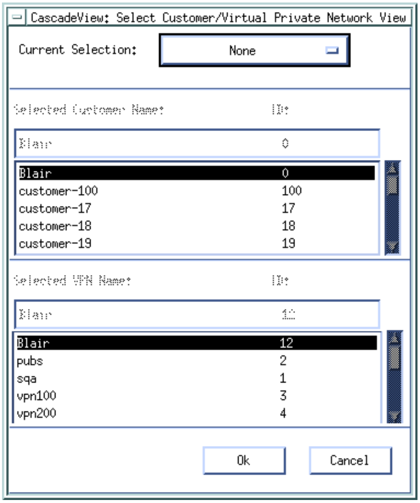



**Figure 2-17. Select Customer/Virtual Private Network Dialog Box**

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. Use None (default) to display all configured logical ports, PVCs, and trunks.

4. Choose OK.
5. Choose Cancel to exit the dialog box.

## Monitoring VPN Customers

Use the following steps to display all customers who have a VPN:

1. From the Monitor menu, select Show All Customer/VPN ⇒ Show All Customers. The following dialog box appears.

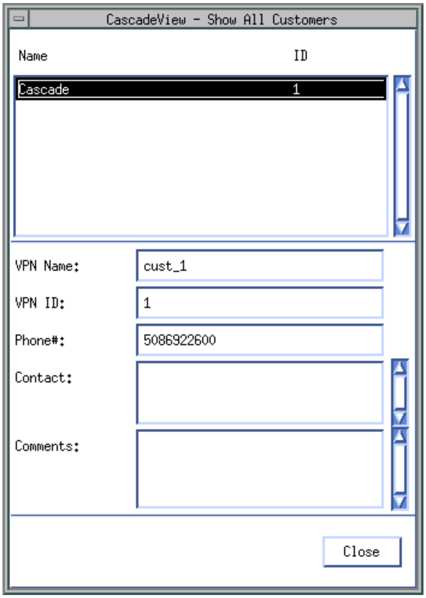



**Figure 2-18. Show All Customers Dialog Box**

Table 2-19 describes the Show All Customers fields.

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

**Table 2-19. Show All Customers Fields**

| Field | 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 VPNs

To display all virtual private networks defined on a map:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Customer/VPN ⇒ Show All Virtual Private Networks. The following dialog box appears.

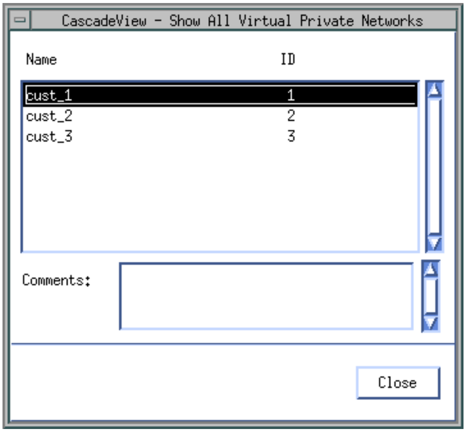



**Figure 2-19. Show All Virtual Private Networks Dialog Box**

2. Select the VPN name.

   The Show All Virtual Private Networks dialog box displays the following fields:

   **Name** — Displays the name of the virtual private network (VPN).

   **ID** — Displays the ID associated with each VPN.

   **Comment** — Displays any applicable comments.

3. When you finish viewing the information, choose Close to return to the network map.

# 3

# Running Diagnostics

This chapter describes how to obtain node-level diagnostic information for a selected switch, as well as physical and logical port-level diagnostic information. CascadeView/UX provides the following diagnostic programs:

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

**Foreground Diagnostics** — Provide current status for all active switches and enable you to test the integrity of the physical and logical ports.

# Background Diagnostics

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

## Problems Background Diagnostics Detect

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

- Corruption of different data structures
- Corruption of code space

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

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

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

**Non-fatal errors** — Includes those conditions whereby system resources are strained by some event, either internally or externally. Non-fatal errors are also reported to the NMS via trap alarms and viewed through the Cascade Events Browser. Refer to Chapter 7 for information about trap alarms.

# Displaying Background Diagnostics

The Background Diagnostics dialog box displays status information for an active switch.

To run background diagnostics:

1. On the network map, select the switch object for which you want to view diagnostic information.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the IOM or switch processor (SP) for which you want to obtain background diagnostic information.
4. Choose Diagnose.

   The Select Card Diagnostics dialog box appears. If you are displaying diagnostics for an SP, you can select either the active or standby card.

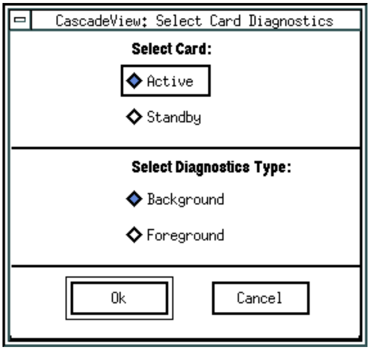



**Figure 3-1. Select Card Diagnostics Dialog Box**

5. Choose Background Diagnostics. The following dialog box appears.

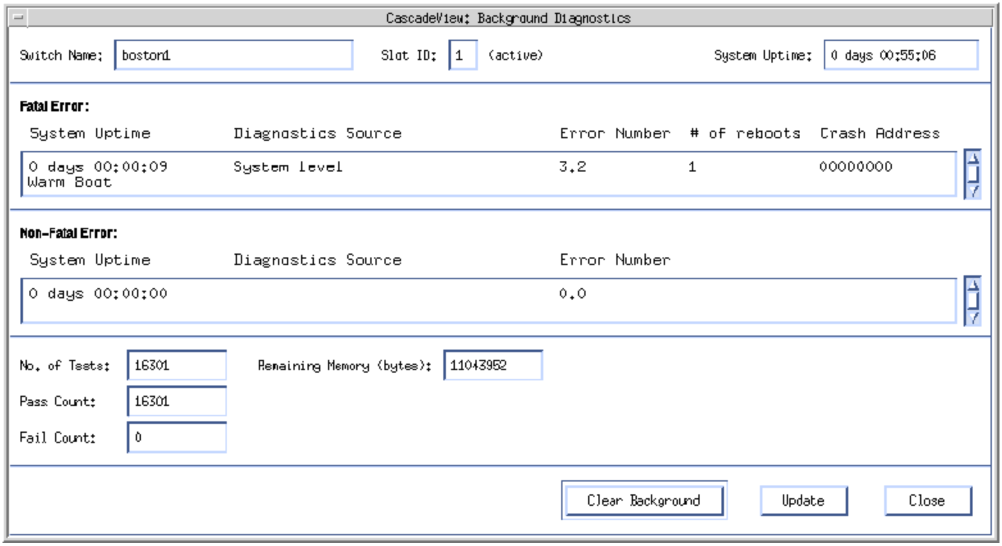



**Figure 3-2. Background Diagnostics Dialog Box**

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 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. |

**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.<br><br>*System Uptime* – Displays the SysUpTime value at the time the error occurred.<br><br>*Diagnostics Source* – Displays the source from which CascadeView/UX collected the error information. Options include:<br>• System level (Packet Processor/Control Processor)<br>• Redundancy Manager<br>• BD Heap (memory)<br>• Power-on diagnostics<br>• Background diagnostics<br>• Fault<br><br>*Error Number* – Displays the error number containing the major and minor error codes in the format of X.Y (X being the major code and Y being the minor code). Refer to Table B-1 on page B-2 for a complete list of error codes.<br><br>*# of Reboots* – Displays the number of times this switch experienced a reboot condition since the last logged fatal error. If this value is greater than three (3), information displayed in the Background Diagnostics dialog box is outdated. |

**Table 3-1. Background Diagnostics Fields (Continued)**

| Field | Action/Description |
|---|---|
| Fatal Error (*continued*) | ***Note**: Although the # of Reboots counter increments with each reboot, there are instances where the hardware reboots or resets but the screen information does not change. These instances include:*<br>• The switch powers off and on.<br>• The hardware resets (for example, when you use the latch to reset a CBX 500 IOM).<br>• The SP card continuously polls IOMs for status. If a card does not respond, the SP resets this card.<br>*Crash Address* – Displays a crash address for certain types of fatal error conditions. The Cascade TRC uses this address for debugging purposes. If the background diagnostics indicate a crash address, make a note of the address and contact the TRC. You cannot resolve a fatal error using the instructions in this manual. |
| Non-Fatal Error | Displays information about those conditions that strain system resources. This information is the same as that described for a fatal error. Refer to the fatal error field. |
| 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. |

**Table 3-1. Background Diagnostics Fields (Continued)**

| Field | Action/Description |
|---|---|
| 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. |
| Total Invalid ATM cells Received | Displays the total number of invalid VPI/VCI cells received on this IOM. |
| Invalid Cell Reporting | Displays the last invalid VPI/VCI cell received on a per-IOM basis. In this case, invalid cell traffic is defined as cells that are received on a physical port that does not have a corresponding PVC or SVC mapped to the received cell's VPI or VCI. |

6. (*Optional*) Choose Clear Background to clear the information in the Background Diagnostics log.

   Note that the system does not clear the screen after you choose Clear Background. However, the next time you display the Background Diagnostics dialog box, a new set of background diagnostics is displayed. The Clear Background option is useful to monitor certain non-fatal errors to verify whether or not an error persists.

7. Choose Close to return to the network map.

# Foreground Diagnostics

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

## Problems Foreground Diagnostics Detect

Foreground diagnostics enable you to:

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

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

**Internal** — Tests the IOM hardware only. You can use this test on all cards. This checks the internal hardware of a specific physical port. The port's Admin Status must be set to *Down* before you can run an internal test.

**External** — Performs an external test that directs 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 being tested.

## Before You Begin

You can run diagnostics on an IOM, a physical port, or a logical port. Before you use these tests, make sure you:

- Set the applicable IOM, physical port, or logical port's Admin Status to *Down*.
- Review the Clock Source Selection field on the Set Physical Port Attributes dialog box and make sure it *is not* set to Loop-timed. The foreground diagnostic tests also require the physical port to provide clocking (set to Internal).

Review the following steps to modify the admin status and clock source selection for an IOM, a physical port, or a logical port.

## Changing an IOM's Admin Status

1. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Change the admin status for all physical ports to *Down* (refer to the following instructions).
3. Change the admin status for all logical ports to *Down* (refer to the following instructions).

## Changing a Physical Port'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 port you need to modify. The Set Physical Port Attributes dialog box appears.
3. Change the admin status to *Down*.
4. If the clock source selection on the Set Physical Port Attributes dialog box is set to Loop-timed, change this field temporarily to *Internal*.
5. Choose Apply and then choose OK to save your changes.

## Changing a Logical Port'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 port you need to modify. The Set Physical Port Attributes dialog box appears.
3. Choose Logical Port. The Set Logical Ports dialog box appears. Select a port and choose Modify to change the logical port settings.
4. Change the admin status to *Down*.
5. Choose Apply and then choose OK to save your changes.

## Displaying 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.

3. Select the IOM, physical port, or logical port you want to test.

   *To test an I/O module:*

   a. Select the I/O module and choose Diagnose. The Select Card Diagnostic dialog box appears, enabling you to select either the active or standby card (see Figure 3-1 on page 3-3).

   b. Choose Foreground Diagnostics. The Perform Foreground Diagnostic Test dialog box appears.

   *To test a physical port* :

   a. Select the physical port and choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears.

   *To test a logical port*:

   a. Select the physical port where the logical port resides and choose Set Attr. The Set Physical Port Attributes dialog box appears.

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

   c. Choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears.

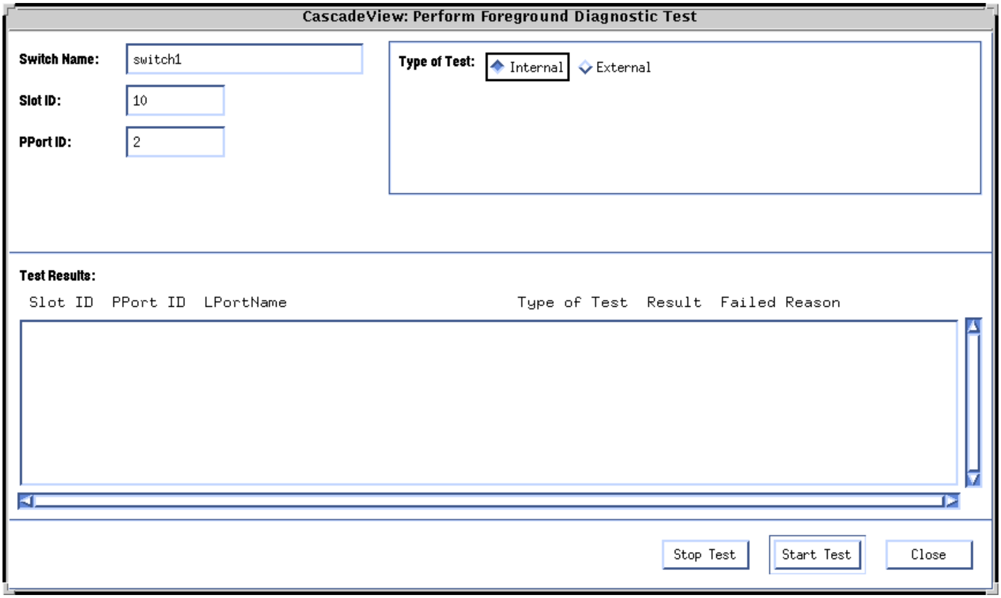



**Figure 3-3. Perform Foreground Diagnostic Test Dialog Box**

4. Select the type of test.

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

   *External* – Performs an external loopback test on channelized modules. 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 you are testing.

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

5. Choose Apply and then choose OK. The results display in the Test Results window.

6. Choose Close to return to the network map.

# 4

# Setting and Monitoring Loopbacks

This chapter describes how to initiate and monitor loopback diagnostic functions for the CBX 500. Loopback testing can be used on physical ports, logical ports, and individual circuits as a means of verifying data integrity and for general troubleshooting purposes. The loopback may be performed either on-line or off-line, depending on the loopback type.

The CBX 500 supports the following loopback tests:

**OAM Loopbacks** — As part of the CBX 500's support of ATM layer OAM functions, the switch provides the capability to generate OAM loopback cells on any UNI or NNI logical port. Refer to page 4-2 for more information. The OAM loopback tests can be run on an *on-line* basis.

**Physical Port Loopbacks** — For each IOM type, the CBX 500 supports a variety of physical line loopbacks. At a minimum, each physical port type supports basic internal and external loopback tests. Additional types of loopbacks specific to the individual media type are also available for each of the physical ports. Refer to page 4-12 for more information. The physical port loopback tests must be run on an *off-line* basis (you must set the physical port's admin status to *down*).

# About OAM

The CBX 500 supports the OAM functions described in the ATM Layer Specification (section 3.5) of the *ATM Forum's UNI 3.0/3.1 Specifications*. For more information on OAM, refer to the *ATM Forum UNI 3.0 or 3.1 Specifications*. OAM supports all circuit types on the CBX 500 (PVCs and SVCs).

This section describes how OAM cells are used with ATM Layer Fault Management to provide the following functions:

- OAM Connectivity Verification
- OAM Alarm Surveillance

The CBX 500 does not support OAM performance monitoring (pm) functions.

## OAM Connectivity Verification

The CBX 500 supports two types of OAM connectivity verification:

- OAM cells sent to a CBX 500 UNI/NNI port from an attached device
- OAM Loopback Cell Generation

### OAM Cells Sent to a CBX 500 UNI Port from an Attached Device

The CBX 500 responds in accordance with the ATM Forum's UNI specifications when OAM Virtual Path (VP) (F4) or Virtual Channel (VC) (F5) segment loopback cells are sent to a CBX 500 UNI port. In most cases, this means that the cell's Loopback Indication field decrements and the switch sends the cell back to the originating device. If no VP or VC associated with the VPI or VCI of the OAM cell exists on the UNI port that received the cell, the OAM cell is discarded. The OAM cell is also discarded if it is improperly formatted.

In most cases, the CBX 500 assumes the role of an intermediate switch from an OAM perspective. If OAM F4 or F5 end-to-end (not segment) loopback cells are sent to a CBX 500 UNI port, the cells are passed through the switch unmodified over the VP or VC (since the CBX 500 is only the intermediate switch for the VP or VC, no action is taken). The device at the circuit's terminating point performs the loopback action for an end-to-end loopback cell.

### OAM Loopback Cell Generation

You can generate loopbacks on PVCs, SVCs, and SPVCs. Using the OAM loopback function, you can generate OAM loopback cells from a CBX 500 UNI/NNI interface toward the attached device, or into the CBX 500 network as shown in Figure 4-1.

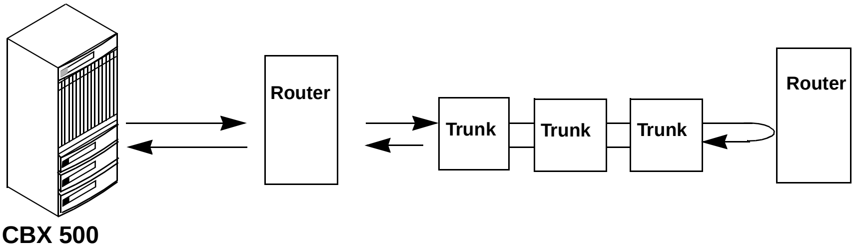



**Figure 4-1. OAM Loopback Process**

## Running OAM Loopback Tests

You can perform the following types of OAM loopback tests on the CBX 500:

- OAM PVC loopback
- OAM SPVC loopback
- OAM SVC loopback

The procedure for running each OAM loopback test type is similar. To run the OAM loopback test, use the following sequence:

**Step 1.** (*Optional*) Set the OAM loopback time interval as described in the next section. If you want to accept the default polling interval (five (5) seconds), skip this procedure.

**Step 2.** Access the OAM loopback functions (page 4-5).

**Step 3.** Run the loopback test (page 4-6).

## Setting the OAM Loopback Time Interval

CascadeView/UX monitors the progress of the loopback once per polling interval. Slow response time indicates network congestion. To set a time interval other than the default interval (5 seconds):

1. From the Misc menu, select Cascade Time Intervals ⇒ Set OAM Time Interval. The Change OAM Polling Interval dialog box appears.

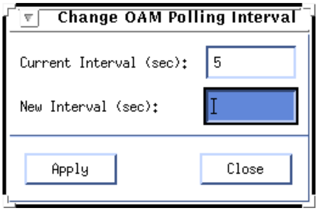



**Figure 4-2. Change OAM Polling Interval Dialog Box**

2. Enter the new time interval (in seconds) to collect loopback diagnostics.

3. Choose Apply.

# Accessing OAM Loopback Test Functions

To access the OAM loopback test functions:

1. On the network map, select the appropriate switch icon.
2. From the Monitor menu, select Cascade Objects ⇒ Show Circuits.
3. Use one of the following options to select a PVC, SVC, or SPVC with a UNI logical port at both endpoints:

   *All on Map* — Displays a list of all the circuits configured for the current map. Choose the circuit on which to perform the loopback.

   *All on Switch* — Displays a list of all the circuits configured for a selected switch. Choose the circuit on which to perform the loopback.

   *All by Name* — Enables you to specify the name of the circuit on which to perform the loopback. You can also use wild card characters to search for a circuit name, an asterisk (*) to replace several characters, or a question mark (?) to replace one character.

   *All on Switch and by Name* — Enables you to specify the circuit name (within the selected switch) on which you want to perform the loopback. You can also use wild card characters, an asterisk (*) to replace several characters, or a question mark (?) to replace one character.

   The Show All Circuits dialog box appears for the selected circuit.

> *Before you start OAM Loopback testing, make sure the equipment to be tested supports OAM.*

4. Choose OAM. The OAM Loopback dialog box appears.

   You can set the following parameters on the OAM loopback dialog box.

   – Loopback type (segment or end-to-end)

   – Number of OAM cells

   – Loopback direction

   The OAM Loopback dialog box also displays a negative or positive loopback cell test result.

## Starting PVC, SVC, and SPVC OAM Loopback Tests

To start a PVC, SVC, and SPVC OAM loopback test:

1. Access the loopback test functions as described on page 4-5.

   The PVC, SVC, or SPVC OAM Loopback dialog box appears as shown in Figure 4-3 and Figure 4-4.

   CascadeView updates the following information at each polling interval until you choose Stop to end the test:

   - Response time
   - Responses received
   - Responses timed-out

2. Complete the fields described in Table 4-1 on page 4-9.

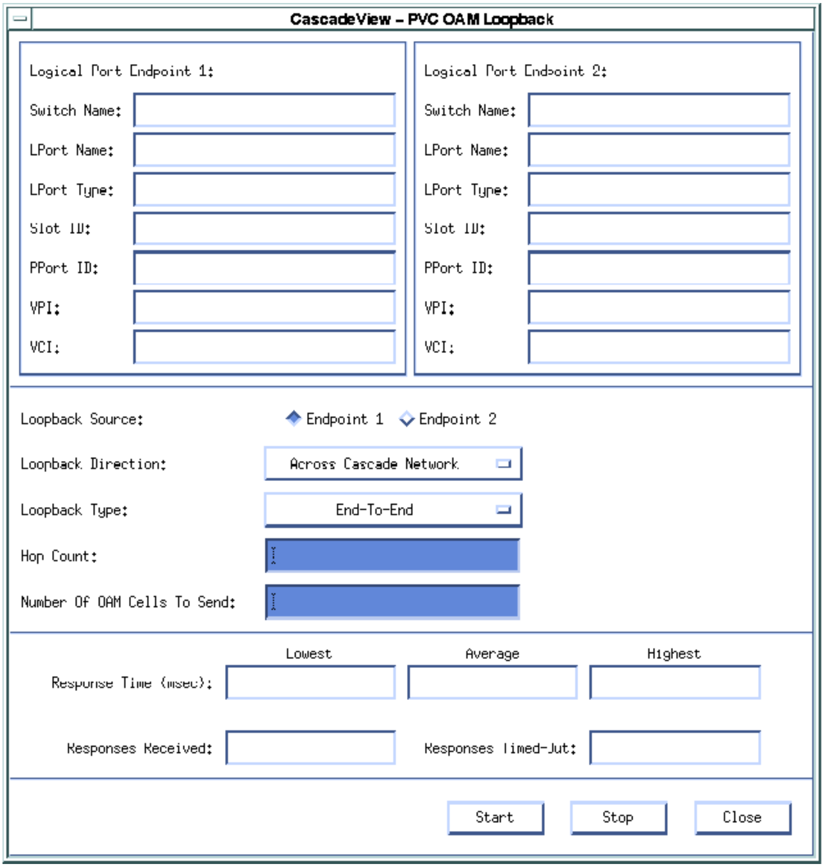



**Figure 4-3. PVC OAM Loopback Dialog Box**

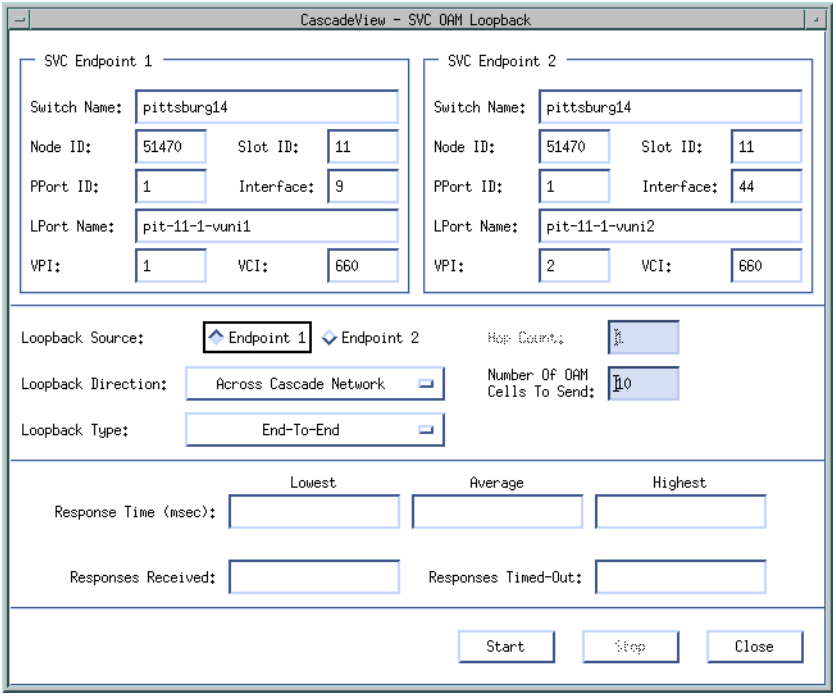



**Figure 4-4. SVC OAM Loopback Dialog Box**

**Table 4-1. PVC, SVC, and SPVC OAM Loopback Fields**

| Field | Action/Description |
|---|---|
| Loopback Source | Select either Endpoint 1 or Endpoint 2 as the source of the loopback signal. |
| Loopback Direction | Select either Out Interface or Across Cascade Network.<br>*Out Interface* – Enables you to send the OAM cells out the UNI/NNI port to the attached ATM device.<br>*Across Cascade Network* – Enables you to send the OAM cells over the trunk to the connected Cascade switch. |
| Loopback Type | Select either Segment or End-To-End.<br>*Segment* – Sends OAM loopback segment cells to the next attached device. If you are sending the loopback across the Cascade network, this option sends the loopback cells to the other endpoint switch (unless the specified Hop Count is less than the number of hops required to reach the other endpoint).<br>*End-To-End* – Sends a signal across the network to the circuit endpoint. |
| Hop Count | Specify the number of hops for this circuit. This option is available only if you select *Across the Cascade Network* in the Loopback Direction field and *Segment* in the Loopback Type field. Initially you specify a minimum number of hops and gradually increase this number until you isolate the problem. |
| Number of OAM Cells to Send | Specify the number of OAM cells to send. Initially, send a minimum number of cells, for example, 10 cells. |

**Table 4-1. PVC, SVC, and SPVC OAM Loopback Fields (Continued)**

| Field | Action/Description |
|---|---|
| Response Time (msec) | Displays the lowest, average, and highest response time. |
| Responses Received | Displays the number of responses received. |
| Responses Timed-Out | Displays the number of responses that have timed out. |

3. Choose Start to begin loopback testing. The system displays the test results at the bottom of the OAM Loopback dialog box.

4. Choose Stop to stop the test and return to a normal operating state.

# Loopback Tests for Physical Ports

Before running a physical port loopback test, you must set the physical port's admin status to *down*. This effectively disables the physical port. All logical ports and circuits that traverse this physical port will become inactive.

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

## Disabling a Physical Port

To disable a physical port:

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 physical port you want to test and choose Set Attr. The Set Physical Port Attributes dialog box appears.
3. Disable the physical port during the loopback test as follows:
   a. Change the port admin status value from Up to Down.
   b. Choose Apply. The system prompts you to confirm the change.
   c. Choose OK.
   d. Choose Close to return to the Set Switch Back Panel dialog box.

## Loopback Tests for All Physical Ports

You can perform the following loopback tests on all CBX 500 physical ports:

**Internal** — Loops the physical port framer device back towards the SP. Test traffic is then sent from the SP to ensure that the looped back framer device passes traffic. It is not necessary to place the physical port in external loopback at the IOA or to have an external signal present at the IOA (the IOA should be installed however) for this test to pass. The test will pass if the traffic sent from the SP is received back by the SP, after passing through the looped back port.

**External** — To perform an external test, you must place an external loopback on the IOA physical port. Test traffic is then sent from the SP to ensure that the entire physical port passes traffic. This test will fail if the physical port is not placed in loopback at the IOA or elsewhere downstream in the transmission path. The test will pass if the traffic sent from the SP is received back by the SP, after passing through the looped back port.

**Near-end Line Loopback** — Places the physical port in a line loopback such that the incoming signal from the device attached to the physical port is looped back before the physical port framer device. This loopback effectively loops a signal from the outside back to the source device before traversing the CBX 500 IOM physical port. The physical port remains in this state until you stop the test.

## Loopback Tests for DS3 and E3 Ports

You can perform the following loopback tests on DS3 and E3 ports:

**Payload Loopback** — This type of loopback is similar to a near-end line loopback in that the incoming signal from the device attached to the physical port is looped back. However, with the payload loopback, the loopback is made after the physical port framer device, such that the signal from the outside traverses the framer device and is then looped back. This (in some regards) is a more comprehensive test than the near-end line loopback because when you verify the integrity of the signal passing through the loopback, the integrity of the CBX 500 IOM framer is also verified. The physical port remains in this state until you stop the test.

**Far-end Loopback (DS3 only)** — This type of loopback involves sending an in-band FEAC loop-up signal to the device attached to the physical port. When you start this test, the attached device responds by placing itself in the FEAC loop-up state (assuming the attached device supports FEAC loop-up and down signalling). The attached device will remain in that state until you stop the test (which causes a FEAC loop-down signal to be sent). Running this test has no effect on the DS3 physical port (other than the attached device entering a FEAC loop-up state).

This loopback test can be used in conjunction with the external loopback test, as the attached device can first be placed in a FEAC loop-up state using the far-end loopback test and then the external loopback test can be run. The fact that the attached device will be in a FEAC loop-up state means that if the transmission path is good, the test should pass.

Figure 4-5 shows the Perform Foreground Diagnostic Test (DS3/E3) dialog box. To start the test refer to page 4-20.

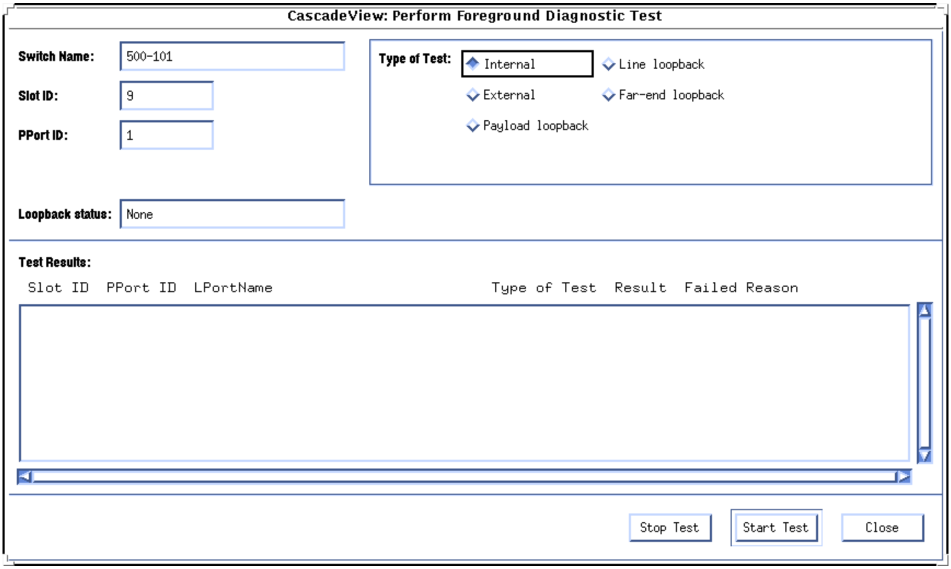



**Figure 4-5. Perform Foreground Diagnostic Test Dialog Box (DS3/E3 port)**

## Loopback Tests for OC3/OC12 and STM-1/STM-4 Ports

You can perform the following loopback tests on the OC3/OC12 and STM-1/STM-4 ports:

**Line Loopback** — Enables the IOA to transmit received cells back to the sender, without passing the cells to the IOM. When you initiate a line loopback, the entire physical port is put into the loopback from the near-end. This enables you to generate and receive line loopback code from the physical port of these modules.

**Internal Loopback** — Sets up a cell loopback signal between the IOM and IOA. This signal does not go “off card”. Use this test to check IOM and IOA internal hardware.

**External Loopback** — Performs a cell loopback test that directs a signal back towards the source. This tests the ability of the port to send and receive data. You must install a fiber optic loopback connector on the physical port you are testing.

Figure 4-6 shows the OC12/STM-4 physical port loopback test dialog box. To start the test refer to page 4-20.

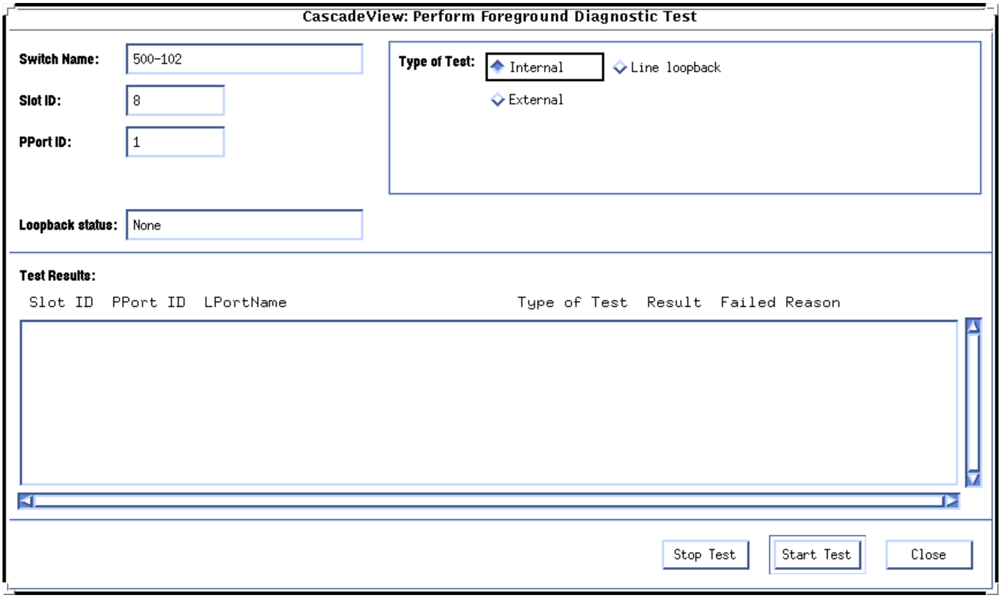



**Figure 4-6. Perform Foreground Diagnostic Test Dialog Box (OC12/STM-4 )**

## Loopback Tests for T1 and E1 Ports

The type of loopback tests that are available for the T1 and E1 modules depends on the physical port's configured circuit type (Superframe or Extended Superframe). Refer to the *Network Configuration Guide for CBX 500* for information about configuring a circuit type.

Table 4-2 describes the types of T1/E1 loopback tests.

**Table 4-2. T1/E1 Loopback Tests**

| Test | Circuit Type | Module | Description |
|---|---|---|---|
| Metallic | Both | T1, E1 | Performs a cell loopback test that checks the IOM and IOA hardware. |
| Payload loopback | Both | T1, E1 | This type of loopback is similar to a near-end line loopback in that the incoming signal from the device attached to the physical port is looped back. However, with the payload loopback, the loopback is made after the physical port framer device such that the signal from the outside traverses the framer device and is then looped back. This (in some regards) is a more comprehensive test than the near-end line loopback because when you verify the integrity of the signal passing through the loopback, the integrity of the CBX 500 IOM framer is also verified. The physical port remains in this state until you stop the test. |
| Line | Both | T1, E1 | A near-end loopback where the external data stream is looped back prior to clock recovery and framing. The external device therefore receives its own clocked signal back. |

Table 4-2. T1/E1 Loopback Tests (Continued)

| Test | Circuit Type | Module | Description |
|---|---|---|---|
| Framed inband line | Both | T1 | A static loopback command mode where the far-end equipment is commanded into line loopback via the previously selected in-band line loopback code CSU or NI (refer to the *Network Configuration Guide for CBX 500*). Using this command, framed loopback control commands are sent to the far end.<br>• Choose Start Test to send loop-up code for 5 seconds; the far-end equipment responds by initiating a line loopback.<br>• Choose Stop Test to send loop down code for 5 seconds; the far end equipment responds by terminating the line loopback mode. |
| Unframed inband line | Both | T1 | A static loopback command mode where the far-end equipment is commanded into line loopback via the previously selected in-band line loopback code CSU or NI (refer to the *Network Configuration Guide for CBX 500*). Using this command, unframed loopback control commands are sent to the far end.<br>• Choose Start Test to send loop up code for 5 seconds; the far-end equipment responds by initiating a line loopback.<br>• Choose Stop Test to send loop-down code for 5 seconds; the far-end equipment responds by terminating the line loopback mode. |

**Table 4-2. T1/E1 Loopback Tests (Continued)**

| Test | Circuit Type | Module | Description |
|---|---|---|---|
| ESF FDL line (ANSI) | Extended Superframe | T1 | A static loopback command mode where the far-end equipment is commanded into line loopback via the T1 ESF out-of-band FDL loopback control commands. This option is only available if you configure the physical port with Extended Superframe ESF and FDL *enabled* (refer to the *Network Configuration Guide for CBX 500*).<br>• Choose Start Test to send loop-up code; the far-end equipment responds by initiating a line loopback.<br>• Choose Stop Test to send loop-down code; the far-end equipment terminates the line loopback mode. |
| ESF FDL payload (ANSI) | Extended Superframe | T1 | A static loopback command mode where the far end equipment is commanded into payload loopback via the T1 ESF out-of-band FDL loopback control commands. This option is only available if you configure the physical port with Extended Superframe ESF and FDL *enabled* (refer to the *Network Configuration Guide for CBX 500*).<br>• Choose Start Test to send loop-up code; the far end equipment responds by initiating a payload loopback.<br>• Choose Stop Test to send loop-down code; the far-end equipment terminates the payload loopback mode. |

Figure 4-7 shows the T1/E1 physical port loopback test dialog box. To start the test, refer to page 4-20.

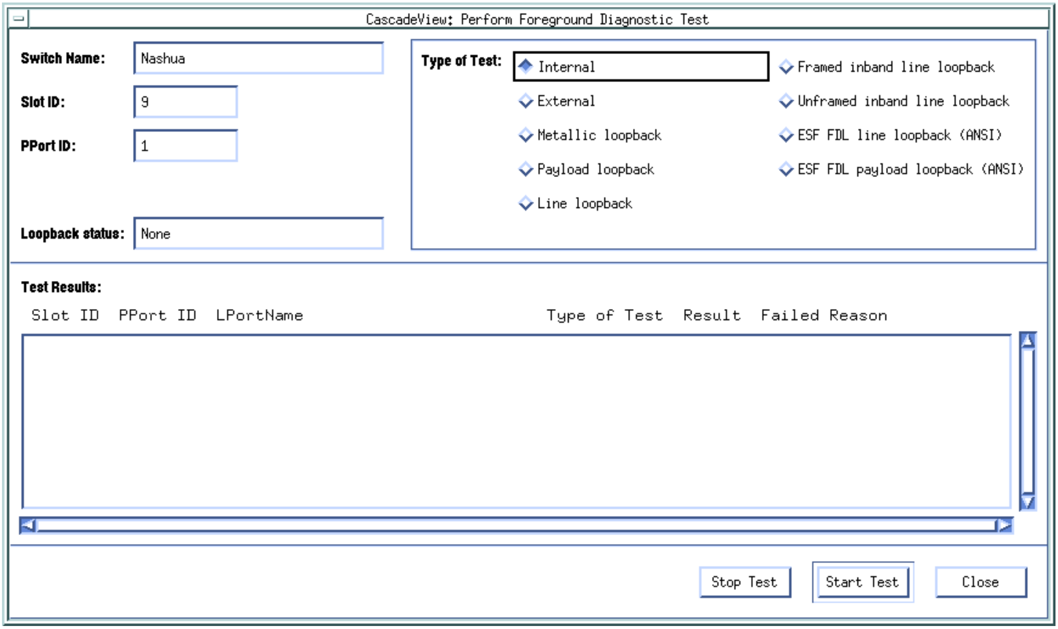



**Figure 4-7. Perform Foreground Diagnostic Test Dialog Box (T1)**

## Starting and Ending a Loopback Test

To perform a loopback test:

1. Disable the physical port as described in “Disabling a Physical Port” on page 4-11.
2. From the Set Switch Back Panel dialog box, select the physical to test and choose Diagnose. The Perform Foreground Diagnostic Test dialog box appears.
3. Select the test type. Refer to the following sections for test information:
   - “Loopback Tests for All Physical Ports” on page 4-12
   - “Loopback Tests for DS3 and E3 Ports” on page 4-13
   - “Loopback Tests for OC3/OC12 and STM-1/STM-4 Ports” on page 4-14
   - “Loopback Tests for T1 and E1 Ports” on page 4-16
4. Choose Start Test to start the test pattern generation from the switch associated with this physical port. The system displays the test results at the bottom of the Perform Foreground Diagnostic Test dialog box.
5. Choose Stop Test to return the port to a normal state.

# 5

# Generating Statistics

This chapter describes how to generate and display real-time statistics to monitor and troubleshoot a Cascade network. You set the polling interval to retrieve summary statistics and use CascadeView/UX to display statistics for a selected physical port, logical port, circuit, and trunk. If necessary, you can use either scripts or CascadeView/UX to generate the reports you need for a node, network, circuit, or trunk.

# Setting the Polling Interval

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

To modify the current default time interval:

1. From the Misc menu, select Cascade Time Intervals ⇒ Set Statistics Time Interval. The following dialog box appears, displaying the current time interval.

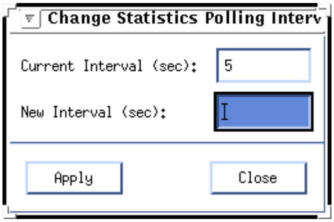



**Figure 5-1. Change Statistics Polling Interval Dialog Box**

2. Enter a new value in seconds. The default is five (5) seconds.
3. Choose Apply to save the changes.
4. Choose Close to exit the dialog box.

# Displaying Physical Port Summary Statistics

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

To generate physical port summary statistics:

1. Select the appropriate switch icon on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box appears as shown in Figure 5-2.

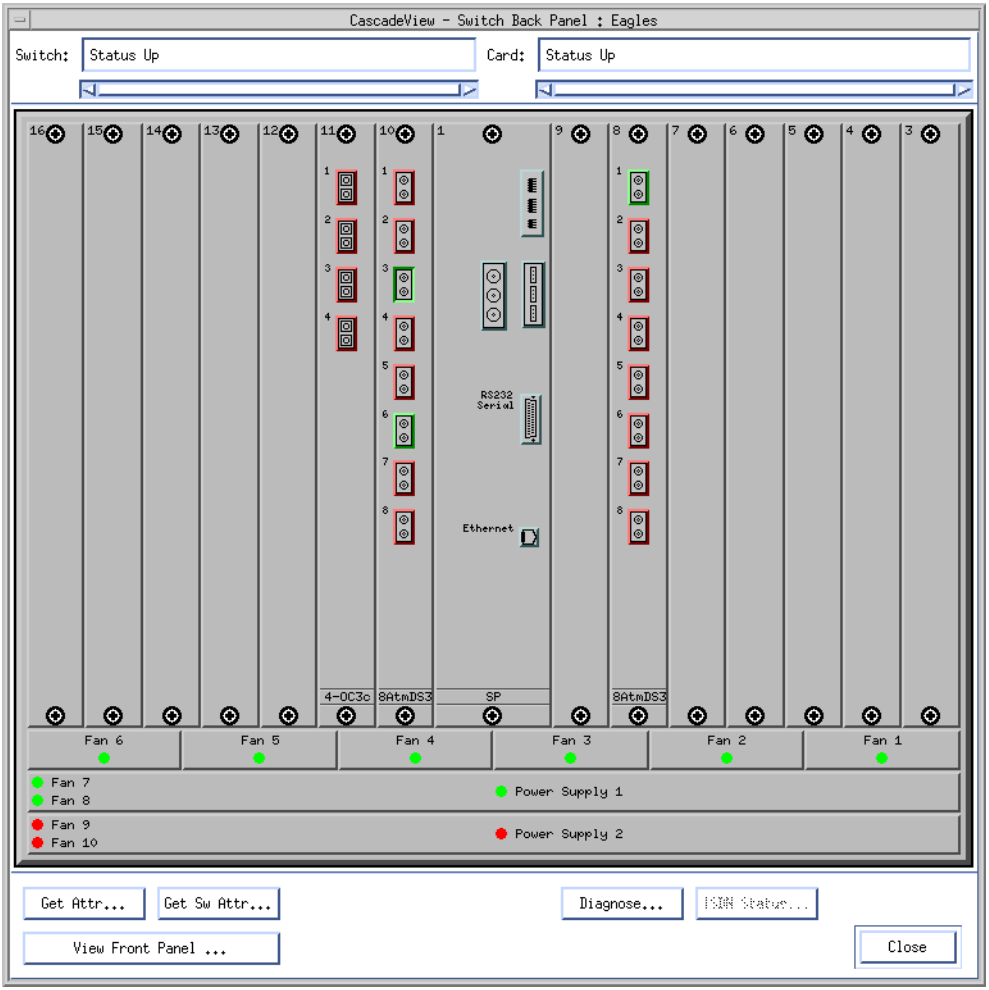



**Figure 5-2. Switch Back Panel Dialog Box**

3. Select the physical port. The View Physical Port Attributes dialog box appears for the selected physical port as shown in Figure 5-3.

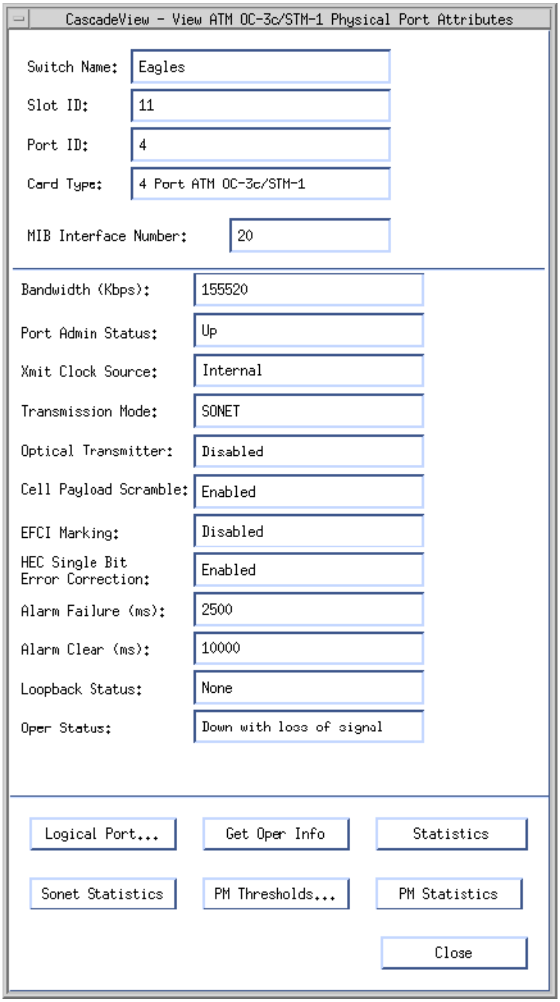



**Figure 5-3. View Physical Port Attributes Dialog Box**

4. Choose Statistics. The following dialog box appears.

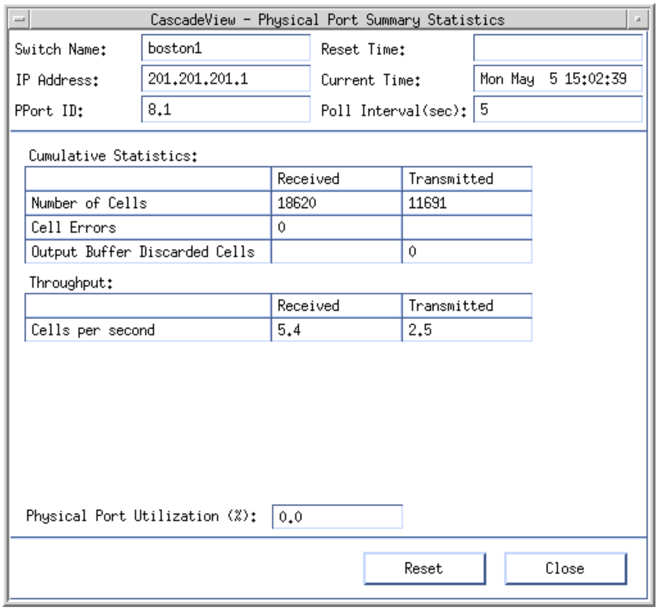



**Figure 5-4. Physical Port Summary Statistics Dialog Box**

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

Table 5-1 describes each of the fields on the Physical Port Summary Statistics dialog box.

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

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

**Table 5-1. Physical Port Summary Statistics Fields**

| Statistic | Description |
|---|---|
| Cumulative Statistics | Lists the number of each type of cell (received, transmitted, or tagged due to an error).<br><br>*Number of Cells* – The total number of cells received and transmitted by the port since the last reset.<br><br>*Cell Errors* – The total number of cells that were received with a Header Error Control (HEC) error. An HEC error indicates a discrepancy between what the port expected in the header and what it actually received. The number of cell errors appears in the Received column.<br><br>*Output Buffer Discarded Cells* – The total number of cells discarded by the port since the last reset. |
| Throughput Statistics | Displays the cells per second for the physical port.<br><br>*Cells per second* – The total number of cells received and transmitted by the port each second.<br><br>*Physical Port Utilization (%)* – The amount of traffic queued for transmission on a physical port measured as a percentage of link speed. This value does not measure the amount of bandwidth of the physical port being used. For this reason, the displayed value can exceed 100%. |

# Displaying DS3 Statistics

You select each of the DS3 summary statistics options from the View Physical Port Attributes dialog box. The DS3 Statistics function enables you to display alarm, statistic, and configuration information from the DS3 MIB.

You can access the following DS3 statistics from the View Physical Port Attributes dialog box:

**Configuration** — Displays the configured statistics from the DS3 MIB.

**Current** — Displays up-to-date statistics. The counter tracks errors encountered by the DS3 interface during the previous 15-minute interval.

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

**Total** — Displays statistics for the sum of all intervals and the current interval. The counter tracks errors encountered by the DS3 interface during the previous 24-hour interval.

## Accessing DS3 Statistics Options

To access DS3 statistics:

1. Select the appropriate switch icon on the network map.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box appears as shown in Figure 5-2 on page 5-3.
3. Select the ATM DS3 physical port. The ATM DS3 View Physical Port Attributes dialog box appears as shown in Figure 5-5.


**Figure 5-5. View ATM DS3 Physical Port Attributes Dialog Box**

4. Choose DS3 Statistics. The DS3 Statistics dialog box appears as shown in Figure 5-6.

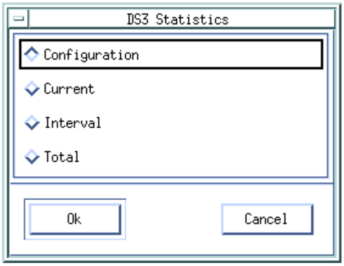



**Figure 5-6. DS3 Statistics Dialog Box**

5. Select from the following types of statistics and choose OK. One of the following DS3 Statistics dialog boxes appear, depending on your selection.

   All DS3 Statistic 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 page 5-14 for more information.

   **DS3 Interval** — Displays statistics 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 page 5-14 for more information.

   **DS3 Total** — Displays statistics for the sum of all intervals and the current interval. Refer to page 5-14 for more information.

## DS3 Configuration Statistics

To display configuration statistics from the DS3 MIB:

1. From the DS3 Statistics dialog box (Figure 5-6), select Configuration and choose OK. The DS3 Statistics dialog box appears as shown in Figure 5-7.

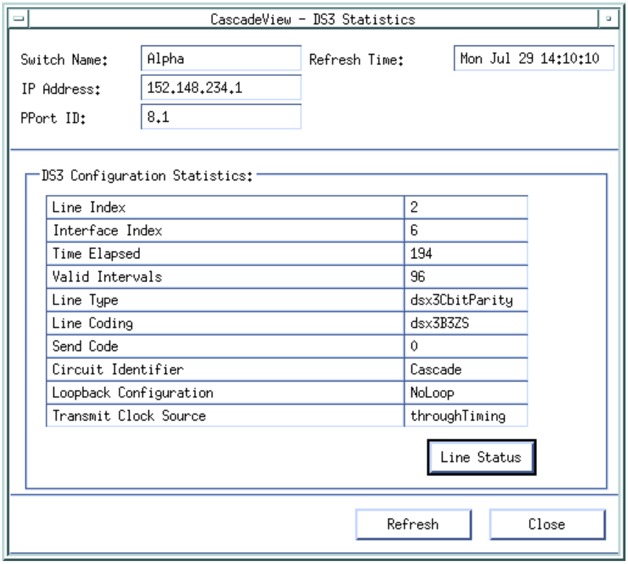



**Figure 5-7. DS3 Statistics Dialog Box**

2. Use the Refresh command to update the DS3 configuration statistics.

3. Use Table 5-2 to interpret the DS3 configuration statistics.

**Table 5-2. DS3 Configuration Statistics Fields**

| Statistic | Description |
|---|---|
| Line Index | The DS3 interface on a managed device. |
| Interface Index | The value of ifIndex from the Interface table of MIB II. |
| Time Elapsed | The number of seconds that have elapsed since the beginning of the current error measurement period. |
| Valid Intervals | The number of previous near-end intervals for which valid data was collected. |
| Line Type | The DS3 C-bit applications implementing this interface. Possible values: dsx3other, dsxM23, dsx3SYNTRAN, dsx3CbitParity, dsx3ClearChannel. |
| Line Coding | The type of Zero Code Suppression used on this interface. Possible values: dsx3Other, dsx3B3ZS. |
| Send Code | The type of code the device sends across the DS3 interface. Possible values: SendNoCode, SendLineCode, SendPayloadCode, SendResetCode, SendDS1LoopCode, SendTestPattern. |
| Circuit Identifier | The transmission vendor's circuit identifier which you can use for troubleshooting. |
| Loopback Configuration | The loopback configuration of the DS3 interface. Possible values: NoLoop, PayloadLoop, LineLoop, OtherLoop. |
| Transmit Clock Source | The Transmit Clock. Possible values: loopTiming, localTiming, throughTiming. |

4. Choose Line Status to display the line status of the associated interface. The DS3 Configuration Line Status dialog box appears as shown in Figure 5-8.

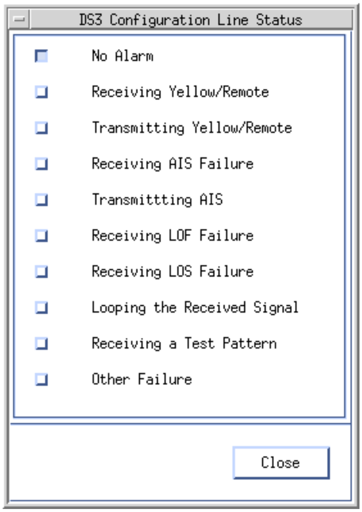



**Figure 5-8. DS3 Configuration Line Status Dialog Box**

5. Use Table 5-3 to review the possible error conditions.

**Table 5-3. DS3 Line Status Conditions**

| Status | Description |
|---|---|
| No Alarm | No alarm present. |
| Receiving Yellow/Remote | Far-end SEF/AIS detected. |
| Transmitting Yellow/Remote | Transmitting a yellow/remote alarm. |
| Receiving AIS Failure | Near-end SEF/AIS detected. |
| Transmitting AIS | Transmitting an alarm indication signal. |
| Receiving LOF Failure | Receiving loss of frame condition. |
| Receiving LOS Failure | Receiving loss of signal. No signal detected. |
| Looping the Received Signal | Loopback enabled/disabled. |
| Receiving a Test Pattern | FEAC (Far end alarm code) signal received. |

**Table 5-3. DS3 Line Status Conditions (Continued)**

| Status | Description |
|---|---|
| Other Failure | Any failures not covered by the above conditions. |

6. Choose Close to exit.

## DS3 Current, Interval, and Total Statistics

To display additional statistics from the DS3 MIB:

1. From the DS3 Statistics dialog box (Figure 5-6 on page 5-10), select Current, Interval, or Total and choose OK. The DS3 Current, Interval, or Total Statistics dialog box appears. Figure 5-9 displays the DS3 Current Statistics dialog box. The Interval and Total Statistics dialog boxes display similar statistics.

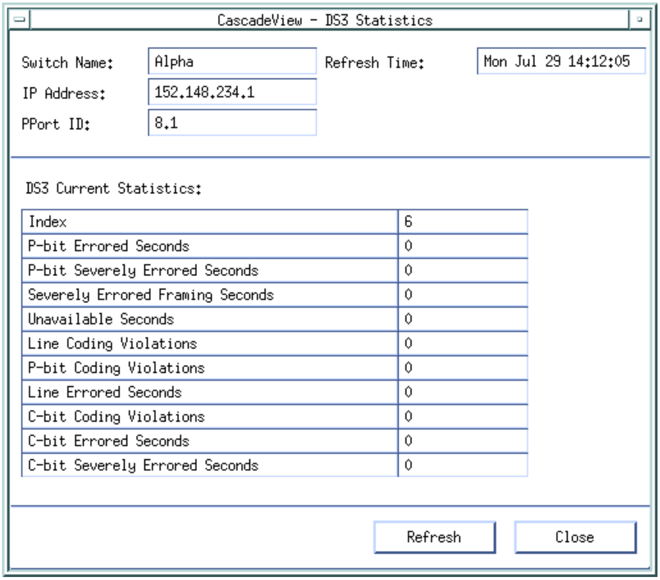



**Figure 5-9. DS3 Current Statistics Dialog Box**

2. Use Table 5-4 to review these statistics.

3. When you finish viewing the statistics choose Close to exit the dialog box.

**Table 5-4. DS3 Current Statistics Fields**

| Statistic | Displays | Definition |
|---|---|---|
| P-bit Errored Seconds | The number of P-bit Errored Seconds (PES). | A second with one or more P-coding Violations (PCVs), one or more out-of-frame defects, or a detected incoming AIS. |
| P-bit Severely Errored Seconds | The number of P-bit Severely Errored Seconds (PSES). | A second with 44 or more PCVs or one or more out-of-frame defects, or a detected incoming AIS. |
| Severely Errored Framing Seconds | The number of Severely Errored Framing Seconds (SEFS). | A second with one or more out-of-frame defects, or a detected incoming AIS. |
| Unavailable Seconds | The number of Unavailable Seconds (UAS). | The number of seconds the interface is unavailable. |
| Line Coding Violations | The number of Line Coding Violations (LCV). | A count of BPVs and EXZs occurring over the accumulation period. |
| P-bit Coding Violations | The number of P-bit Coding Violations (PCV). | Occurs when the received P-bit code on the DS3 M-frame does not match the local code. |
| Line Errored Seconds | The number of Line Errored Seconds (LES). | A second in which one or more CVs or one or more LOS occurred. |
| C-bit Coding Violations | The number of C-bit Coding Violations (CCV). | The number of coding violations reported via the C-bits. |
| C-bit Errored Seconds | The number of C-bit Errored Seconds(CES). | A second with one or more CCVs or one or more out-of-frame defects, or a detected incoming AIS. |

**Table 5-4. DS3 Current Statistics Fields (Continued)**

| Statistic | Displays | Definition |
|---|---|---|
| C-bit Severely Errored Seconds | The number of C-bit Severely Errored Seconds (CSES). | A second with 44 or more CCVs or one or more out-of-frame defects, or detected incoming AIS. |

## Displaying SONET/SDH Statistics

The Set (and View) Physical Port Attributes dialog box for an OC3/OC12 physical port provides the SONET Statistics function, which enables you to display alarm, statistic, and configuration information from the SONET MIB.

You can view the following OC12/STM-4 statistics:

**Medium** — Displays statistical information for the physical medium.

**Current** — Displays up-to-date statistical information. The counter tracks errors that the interface encounters during the previous 15-minute interval.

**Interval** — Displays statistics for the previous 24 hours using the number of 15 minute intervals you specify.

To display these statistics:

1. Open either the Set Physical Port Attributes dialog box or View Physical Port Attributes dialog box (Figure 5-3 on page 5-4).
2. Choose SONET Statistics. The following dialog box appears.

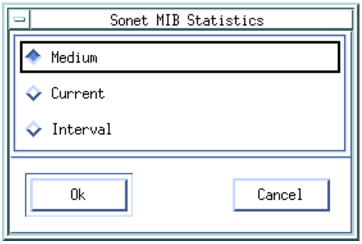



**Figure 5-10. Sonet SDH Statistics Dialog Box**

3. Select one of the following statistics:

- Select Medium and choose OK to display medium Sonet statistics. The system displays the Sonet/SDH Medium Statistics dialog box shown in Figure 5-11. Table 5-5 on page 5-17 describes the statistics.
- Select Current or Internal and choose OK to display current or internal sonet statistics. The system displays the Sonet/SDH Current Statistics dialog box (Figure 5-12) or the Sonet/SDH Internal Statistics dialog box, which displays similar fields. Table 5-6 on page 5-20 describes the statistics.

4. Choose Refresh to update the Sonet/SDH statistics.

5. Choose Close to exit.

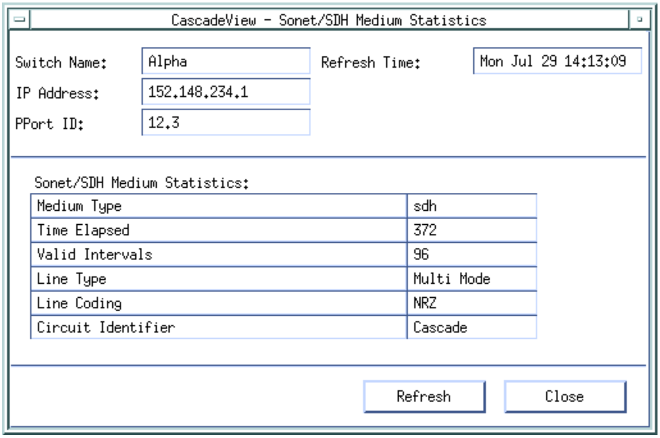



**Figure 5-11. Sonet/SDH Medium Statistics Dialog Box**

**Table 5-5. Sonet/SDH Medium Statistics Fields**

| Field | Description |
|---|---|
| Medium Type | Identifies whether a SONET or an SDH signal is used across this interface. Values may be “Sonet” or “SDH”. |
| Time Elapsed | The number of seconds, including partial seconds, that have elapsed since the beginning of the current error-measurement period. |

**Table 5-5. Sonet/SDH Medium Statistics Fields (Continued)**

| Field | Description |
|---|---|
| Valid Intervals | The number of previous intervals for which valid data has been stored. |
| Line Type | Displays the line type for the interface. Values are:<br>Short Single Mode, Long Single Mode, MultiMode, Coax, UTP, Other. |
| Line Coding | Displays the line coding for this interface. Values are:<br>Other, B3ZA, CMI, NRZ, RZ. |
| Circuit Identifier | The transmission vendor’s circuit identifier which you can use for troubleshooting. |

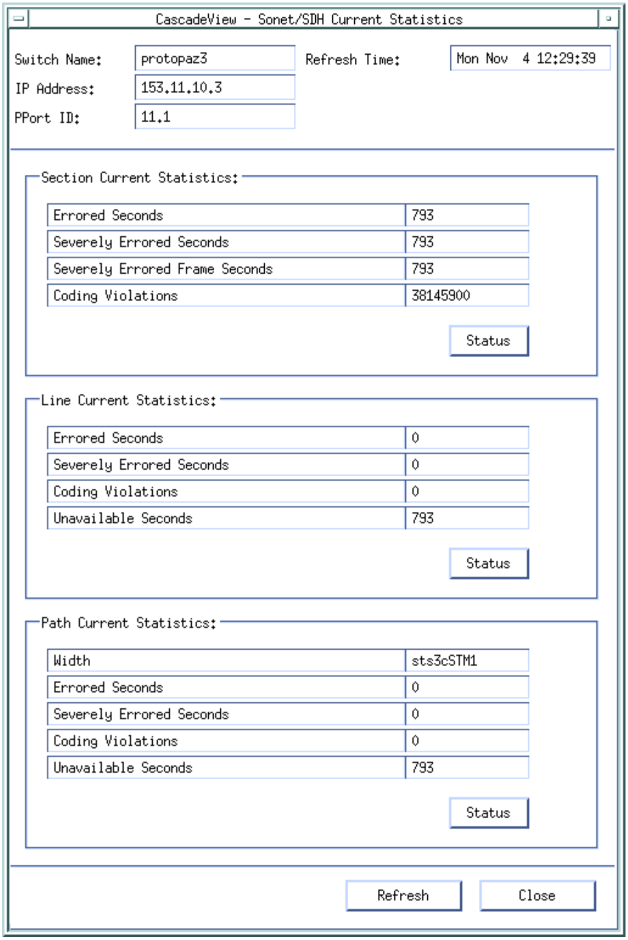



**Figure 5-12. Sonet/SDH Current Statistics Dialog Box**

This dialog box displays the following types of statistics:

**Section Current Statistics** — Displays information encountered by the Sonet/SDH *section* in the current 15-minute interval.

**Line Current Statistics** — Displays information encountered by the Sonet/SDH *line* in the current 15-minute interval.

**Path Current Statistics** — Displays information encountered by the Sonet/SDH *path* in the current 15-minute interval.

Table 5-6 lists and describes the current statistics. Interval statistics display similar fields.

**Table 5-6. Sonet/SDH Current Statistics Fields**

| Field | Description |
|---|---|
| **Section Current Statistics** | |
| Errored Seconds | Count of 1 second intervals containing one or more BIP-8 section errors, one or more LOS (loss of signal), or one or more SEF (severely errored frame) defects. |
| Severely Errored Seconds | Count of 1-second intervals containing x or more BIP-8 section errors, one or more LOS (loss of signal), or one or more SEF (severely errored frame) defects.<br>***Note:*** *The SES Threshold standard (refer to the* Network Configuration Guide for CBX 500*) sets the value of x for SES-S. For ANSI standards, this value is 8800; for Bellcore standards, this value is 63; for Sonet this value is 32.* |
| Severely Errored Frame Seconds | Count of 1-second intervals containing one or more SEF (severely errored frame) defects. |
| Coding Violations | Count of BIP-8 errors detected in the section layer. |
| Use the Status button to display the line status of the associated interface. One or more of the following error conditions may appear:<br>No Defect, LOS, LOF. | |

**Table 5-6. Sonet/SDH Current Statistics Fields (Continued)**

| Field | Description |
|---|---|
| **Line Current Statistics** | |
| Errored Seconds | Count of 1-second intervals containing one or more BIP-8 line errors, or one or more AIS (alarm indication signal) defects. |
| Severely Errored Seconds | Count of 1-second intervals containing x or more BIP-8 line errors, or one or more AIS-L (alarm indication signal line) defects. For Line, x=32 as defined by SONET MIB.<br>***Note:*** *The SES Threshold standard (refer to the* Network Configuration Guide for CBX 500*) sets the value of x for SES-L. For ANSI standards, this value is 10000; for Bellcore standards, this value is 124.* |
| Coding Violations | Count of BIP-8 errors detected in the line layer. |
| Unavailable Seconds | Count of 1-second intervals for which the SONET/SDH line is unavailable. The Line is considered unavailable at the onset of 10 consecutive Severely Errored Seconds. |
| Use the Status button to display the line status of the associated interface. One or more of the following error conditions may appear:<br>No Defect, AIS, RDI. | |

**Table 5-6. Sonet/SDH Current Statistics Fields (Continued)**

| Field | Description |
|---|---|
| **Path Current Statistics** | |
| Width | SONET/SDH level (STS-n, STM-n). |
| Errored Seconds | Count of 1-second intervals containing one or more BIP-8 path errors, one or more AIS-P (alarm indication signal path) defects, or one or more LOP (loss of pointer) defects. |
| Severely Errored Seconds | Count of 1 second intervals containing x or more BIP-8 path errors, one or more AIS-P (alarm indication signal path) defects. For Path x=32, as defined by the SONET MIB.<br>***Note:*** *The SES Threshold standard (refer to the Network Configuration Guide for CBX 500) sets the value of x for SES-P. For ANSI standards, this value is 8800; for Bellcore standards, this value is 63.* |
| Coding Violations | Count of BIP-8 errors detected in the path layer. |
| Unavailable Seconds | Count of 1-second intervals for which the SONET/SDH path is unavailable. The Path is considered unavailable at the onset of 10 consecutive Severely Errored Seconds. |
| Use the Status button to display the line status of the associated interface. One or more of the following error conditions may appear:<br>No Defect, STS LOP, STS AIS, STS RDI, Unequipped, Signal Label Mismatch. | |

# Displaying Logical Port Summary Statistics

You can use logical port summary statistics to display the error codes a logical port receives.

To display logical port summary statistics:

1. On the network map, select the appropriate switch icon.
2. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box appears as shown in Figure 5-2 on page 5-3.
3. Select the physical port. The View Physical Port Attributes dialog box appears (Figure 5-3).
4. Choose Logical Port. The Show All Logical Ports in PPort dialog box appears as shown in Figure 5-13.

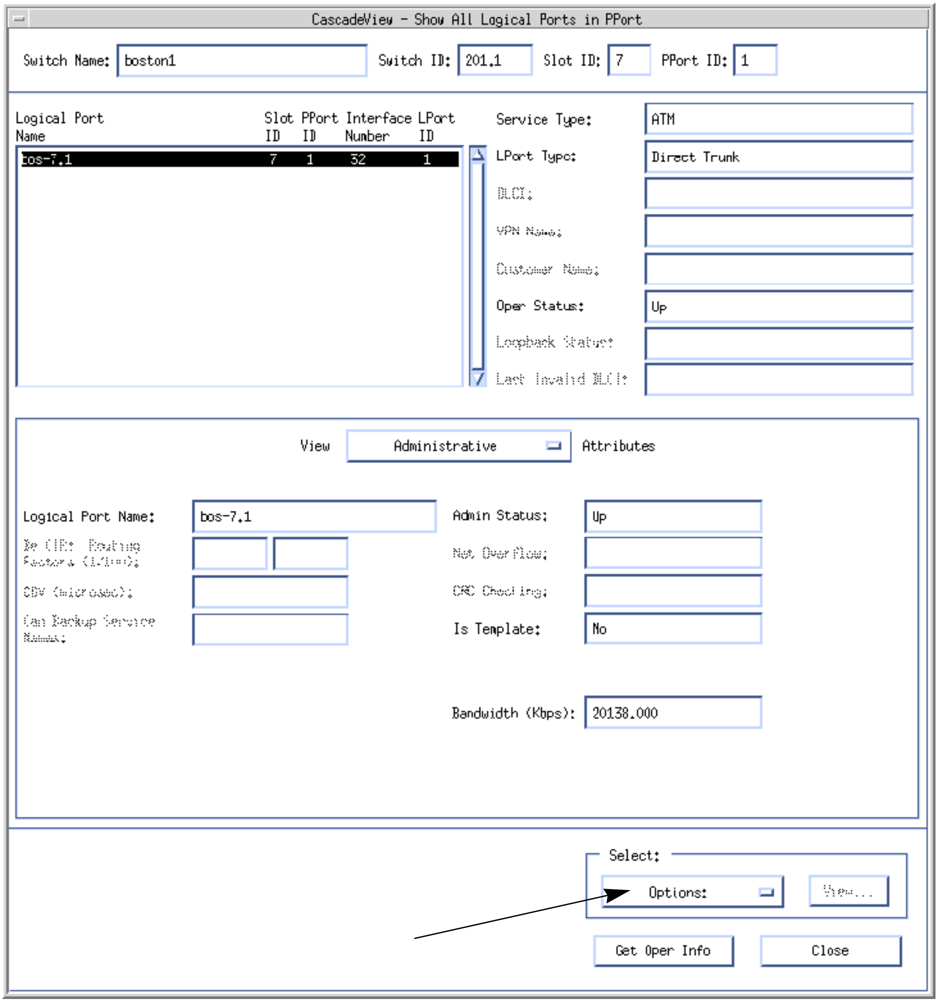



**Figure 5-13. Show All Logical Ports in PPort Dialog Box**

5. Select Options ⇒ Statistics.

6. Choose View. The following dialog box appears.

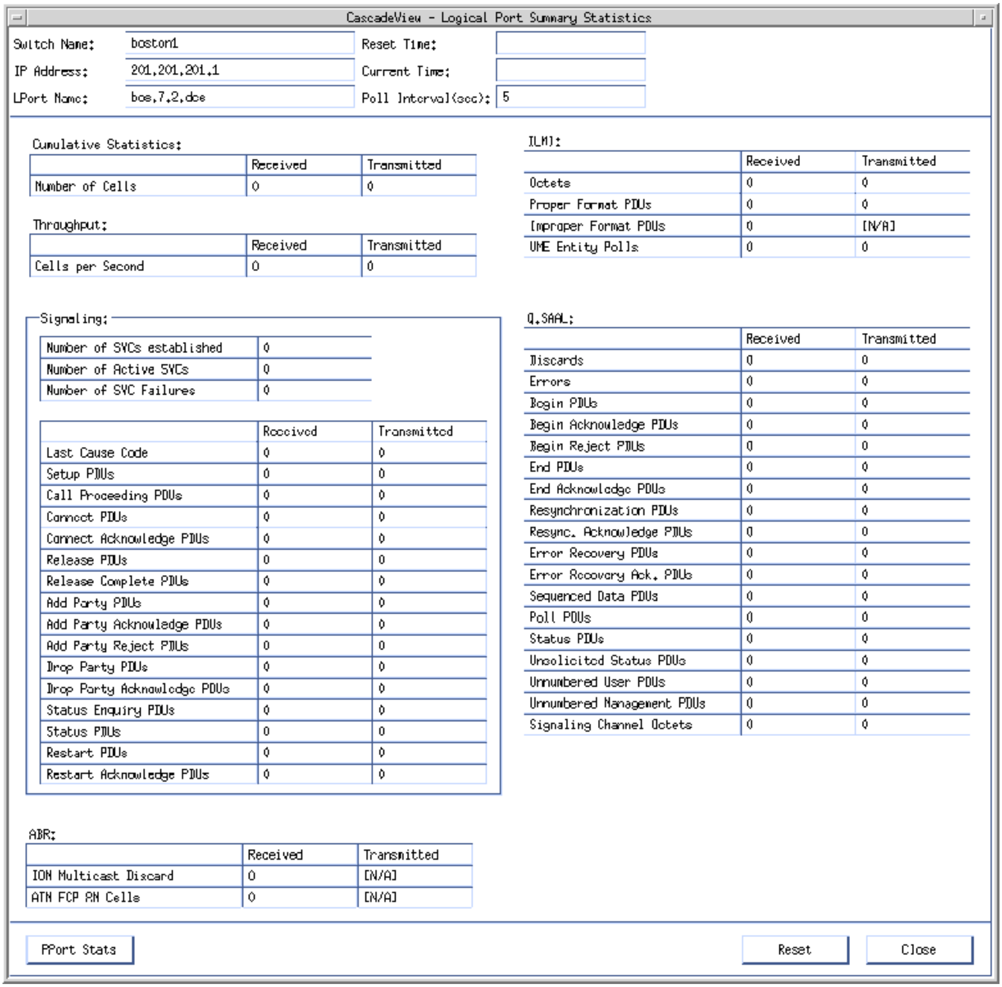



**Figure 5-14. Logical Port Summary Statistics Dialog Box**

This dialog box provides the following command buttons:

**PPort Stats** — Displays the Physical Port Summary Statistics dialog box. For details, refer to "Displaying Physical Port Summary Statistics" on page 5-2.

**Reset** — Clears the current statistics and updates the time in the Reset Time field.

The Logical Port Summary Statistics dialog box displays data in separate columns to reflect the transmission and receipt of data on the logical port. The following fields display cumulative, throughput, and ILMI statistics.

**Number of Cells** — The total number of cells received and transmitted by the port since the last reset.

**Cells per second** — The total number of cells received and transmitted by the port each second.

**Num. of Octets** — The total number of octets received and transmitted by the port since the last reset.

**Num. of Proper Format PDUs** — The total number of Protocol Data Units (PDUs) that were received with a proper format and transmitted.

**Num. of Improper Format PDUs** — The total number of PDUs that were received with an improper format.

**Num. of UME Entity Polls** — The total number of ILMI received status polls issued by the User Management Entity (UME) at this port.

Table 5-7 lists and describes the Q.93B statistics shown on the Logical Port Summary Statistics dialog box.

**Table 5-7. Q.93B Statistics Fields**

| Statistic | Description |
|---|---|
| Number or SVCs Established | The total number of SVCs established since the card became active. |
| Number of Active SVCs | A counter that indicates the number of SVCs that are currently active. The reset statistics function (that you select by using the Reset option button) does not update this statistic. |

**Table 5-7. Q.93B Statistics Fields (Continued)**

| Statistic | Description |
|---|---|
| Last Cause Code | Cause codes are listed in the ATM/UNI Forum specifications. This statistic displays the last received and transmitted cause code. The reset statistics function (that you select by using the Reset option button) does not update this statistic. |
| Num. of Setup PDUs | A counter that indicates the number of Protocol Data Units (PDUs). A Setup PDU is used to place a call. |
| Num. of Call Proceeding PDUs | A counter that indicates the number of local acknowledgments of a Setup PDU. The local acknowledgment specifies that the call is being processed. |
| Num. of Connect PDUs | A counter that indicates the number of Connect PDUs. A Connect PDU is used to accept a call. |
| Num. of Connect Ack. PDUs | A counter that indicates the number of local acknowledgments that the Connect PDU was received. |
| Num. of release PDUs | A counter that indicates the number of Release PDUs. A Release PDU is used to terminate calls. A value in this field that exceeds the value for the number of Connect PDUs indicates that the system is dropping calls. |
| Num. of Release Complete PDUs | A counter that indicates the number of Release Complete PDUs. A Release Complete PDU is a local acknowledgment that the Release PDU was received. |

**Table 5-7. Q.93B Statistics Fields (Continued)**

| Statistic | Description |
|---|---|
| Num. of Add Party PDUs | A counter that indicates the number of Add Party PDUs. An Add Party PDU is used to add a leaf to a point-to-multipoint connection. |
| Num. of Add Party Ack. PDUs | A counter that indicates the number of Add Party Acknowledgement PDUs. An Add Party Acknowledgement PDU is a local acknowledgment that the Add party PDU was received. |
| Num. of Add Party Reject PDUs | A counter that indicates the number of Add Party Reject PDUs. An Add Party Reject PDU is used to reject an add party request. |
| Num. of Drop Party PDUs | A counter that indicates the number of Drop Party PDUs. A Drop Party PDU is a PDU used to terminate a leaf from a point-to-multipoint connection. |
| Num. of Drop Party Ack. PDUs | A counter that indicates the number of Drop Party Acknowledgement PDUs. A Drop Party Acknowledgement PDU is a local acknowledgment that the Drop Party PDU was received. |
| Num. of Status Enquiry PDUs | A counter that indicates the number of Status Enquiry PDUs. A Status Enquiry PDU is an unsolicited status request for a call. One endpoint signals that the connection seems valid and expects verification from the other endpoint. |
| Num. of Status PDUs | A counter that indicates the number of Status PDUs. A Status PDU is a response to a Status Enquiry PDU. The PDU indicates the state of the call. |

**Table 5-7. Q.93B Statistics Fields (Continued)**

| Statistic | Description |
|---|---|
| Num. of Restart PDUs | A counter that indicates the number of Restart PDUs. A Restart PDU is used to restart a single call or the entire signalling VC. |
| Num. of Restart Ack. PDUs | A counter that indicates the number of Restart Acknowledgement PDUs. A Restart Acknowledgement PDU is a local acknowledgment of a Restart PDU. |

Table 5-8 lists and describes the Q.SAAL statistics shown on the Logical Port Summary Statistics dialog box.

**Table 5-8. Q.SAAL Statistics**

| Statistic | Description |
|---|---|
| Discards | A counter that indicates the total number of discards. |
| Errors | A counter that indicates the total number of errors. |
| Num. of Begin PDUs | A counter that indicates the number of Begin PDUs. A Begin PDU is used to establish the Q.SAAL connection. |
| Num. of Begin Ack. PDUs | A counter that indicates the number of Begin Acknowledgement PDUs. A Begin Acknowledgement PDU is used to accept establishment of the Q.SAAL connection. |
| Num. of Begin Reject PDUs | A counter that indicates the number of Begin Reject PDUs. A Begin Reject PDU is used to reject the Q.SAAL connection establish request. |

**Table 5-8. Q.SAAL Statistics (Continued)**

| Statistic | Description |
|---|---|
| Num. of End PDUs | A counter that indicates the number of End PDUs. An End PDU is used to terminate a Q.SAAL connection. |
| Num. of End Ack. PDUs | A counter that indicates the number of End Acknowledgement PDUs. An End Acknowledgement PDU is a local acknowledgment of an End PDU. |
| Num. of Resync. PDUs | A counter that indicates the number of Resynchronized PDUs. A Resync. PDU is used in error recovery. If two endpoints are out-of-sync, the protocol resynchronizes both ends. |
| Num. of Resync. Ack. PDUs | A counter that indicates the number of Resynchronized Acknowledgement PDUs. A Resync. Ack. PDU is a local acknowledgement of a Resync. PDU. |
| Num. of error recov. PDUs | A counter that indicates the number of Error Recovery PDUs. An Error Recovery PDU is used to correct an error condition. |
| Num. of error recov. ack. PDUs | A counter that indicates the number of Error Recovery Acknowledgement PDUs. An Error Recovery Acknowledgement PDU is a local acknowledgment of an Error Recov. PDU. |
| Num. of sequenced data PDUs | A counter that indicates the number of Sequenced Data PDUs. |
| Num. of poll PDUs | A counter that indicates the number of Poll PDUs. A Poll PDU is used as a keep-alive signal for the Q.SAAL connection. |

**Table 5-8. Q.SAAL Statistics (Continued)**

| Statistic | Description |
|---|---|
| Num. of status PDUs | A counter that indicates the number of Status PDUs. A Status PDU is a response to a Poll PDU. |
| Num. of unsolicit status PDUs | A counter that indicates the number of Unsolicited Status PDUs. An Unsolicited Status PDU is used to inform the sender of one or more sequence errors. |
| Num. of unnumbered user PDUs | Not used. |
| Num. of unnumbered mgmt PDUs | Not used. |
| Num. of signalling chnl octets | A counter that indicates the number of octets transmitted or received on the Q.SAAL connection. |

# Displaying Trunk Summary Statistics

Use trunk summary statistics to display data that reflects the transmission and receipt of data from endpoint A to B and B to A. Trunk statistics are only available for ATM Direct Trunks.

> *Trunk summary statistics are not available for CBX 500 ATM OPTimum trunks.*

To display trunk statistics:

1. From the Monitor menu, select Cascade Objects ⇒ Show All Trunks. The Show All Trunks dialog box appears.
2. To display summary statistics for the selected trunk, choose Statistics. The following dialog box appears.

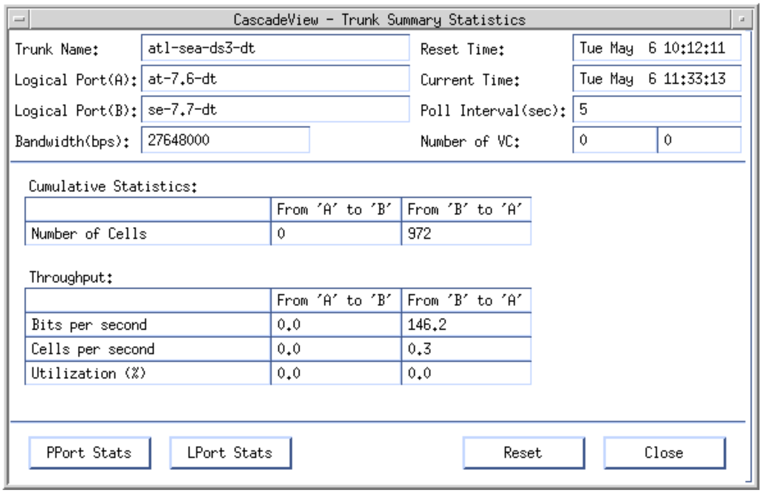



**Figure 5-15. Trunk Summary Statistics Dialog Box**

Table 5-9 describes the trunk summary statistics command buttons and fields.

**Table 5-9. Trunk Summary Statistics Buttons and Fields**

| Buttons/Fields | Description |
|---|---|
| Number of cells | The total number of cells transmitted from one endpoint to the other. |
| Bits per second | The total number of bits per second transmitted from one endpoint to the other. |
| Packets per second | The total number of packets per second transmitted from one endpoint to the other. |
| Utilization (%) | The percentage of trunk speed. |
| PPort Stats | Display physical port summary statistics for each physical port endpoint of this trunk. Refer to page 5-2 for more information. |
| LPort Stats | Display logical port summary statistics for each logical port endpoint of this trunk. Refer to page 5-23 for more information. |
| Reset | Update the trunk summary statistics |

# Displaying Circuit Summary Statistics

Circuit summary statistics display the cells a circuit has sent and received, the round-trip delay, and other Quality of Service statistics for the circuit.

> *Resource Management (RM) cells are counted as passed CLP 0 or passed CLP 1 cells. The Logical Port Statistics dialog box provides separate RM cell statistics on a per logical port basis (see "Displaying Logical Port Summary Statistics" on page 5-23).*

To display circuit statistics:

1. From the Monitor menu, select Cascade Objects ⇒ Show Circuits.

2. 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 wild card characters; an asterisk (*) to replace several characters or a question mark (?) to replace one character.

   *All on Switch and by Name* – Select a switch on the current map, then use this option to enter a specific circuit name located in the switch. You can also search for a circuit by name using wild card characters; an asterisk (*) to replace several characters or a question mark (?) to replace one character.

   The Show [All] Circuits on Map dialog box appears.

3. Choose Statistics to display Circuit Summary Statistics. The following dialog box appears.

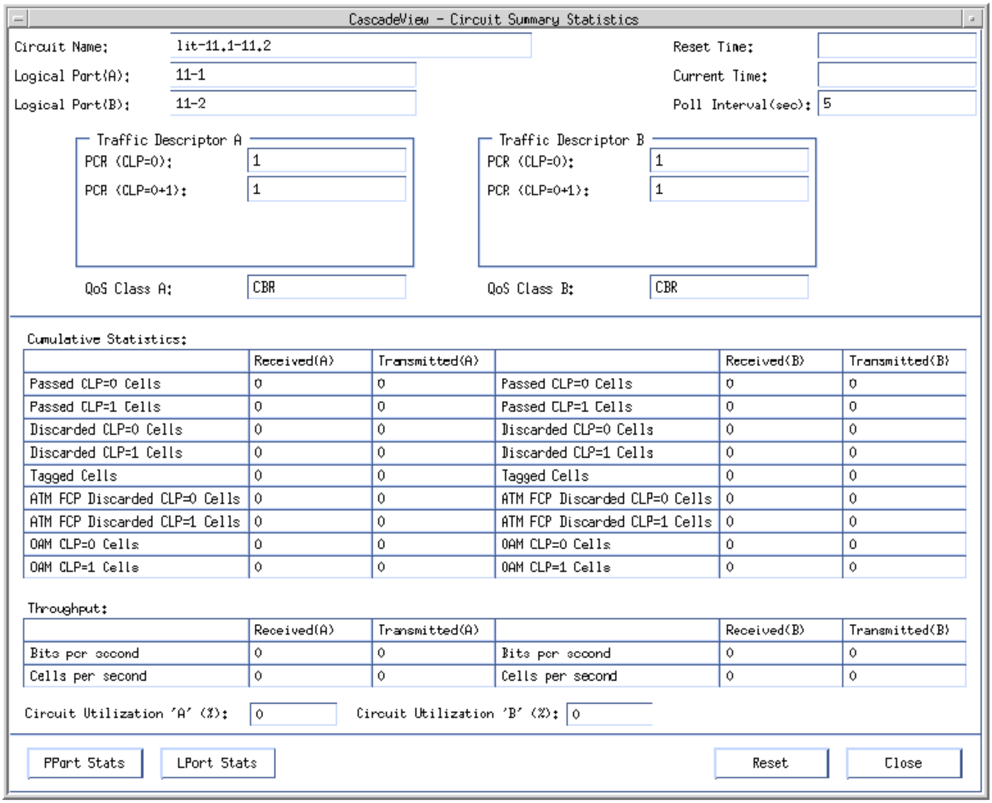



**Figure 5-16. Circuit Summary Statistics Dialog Box**

This dialog box displays statistics for transmitted and received data for each circuit endpoint. These statistics reflect how a circuit's data is used over the network.

The Circuit Summary Statistics dialog box displays cumulative and throughput statistics in the following fields:

**Cumulative Statistics** — This field lists the number of each type of cell (passed, dropped, or tagged) and whether those cells are being transmitted or dropped due to conditions in the network.

*Passed CLP=0 Cells* – The total number of cells that were received and transmitted.

*Passed CLP=1 Cells* – The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged as CLP=1 cells because of a traffic descriptor violation (they are counted as tagged cells).

*Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission or that you should reconfigure the traffic descriptors to reflect the source speed.*

*Discarded CLP=0 Cells* – The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor.

*Discarded CLP=1 Cells* – The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor.

*Tagged Cells* – The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit.

*OAM CLP=0 Cells* – The total number of F4 and F5 OAM CLP=0 cells that were transmitted by the circuit.

*OAM CLP=1 Cells* – The total number of F4 and F5 OAM CLP=1 cells that were transmitted by the circuit.

**Throughput Statistics** — Lists the cells per second and bits per second for each side of the circuit.

*Bits per second* – The total number of bits received and transmitted by the circuit each second.

*Cells per second* – The total number of cells received and transmitted by the circuit each second.

*Circuit Utilization A (%)* – The amount of traffic queued for transmission on a circuit measured as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.

*Circuit Utilization B (%)* – The amount of traffic queued for transmission on a circuit measured as a percentage of link speed. Therefore, the circuit utilization value can exceed 100%.

# Displaying Point-to-Multipoint Circuit Statistics

To display Point-to-Multipoint circuit statistics:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Multipoint. The Set All Point-to-Multipoint Circuit Roots dialog box appears.

2. Choose Statistics. The Point-to-Multipoint Circuit Statistics dialog box appears.

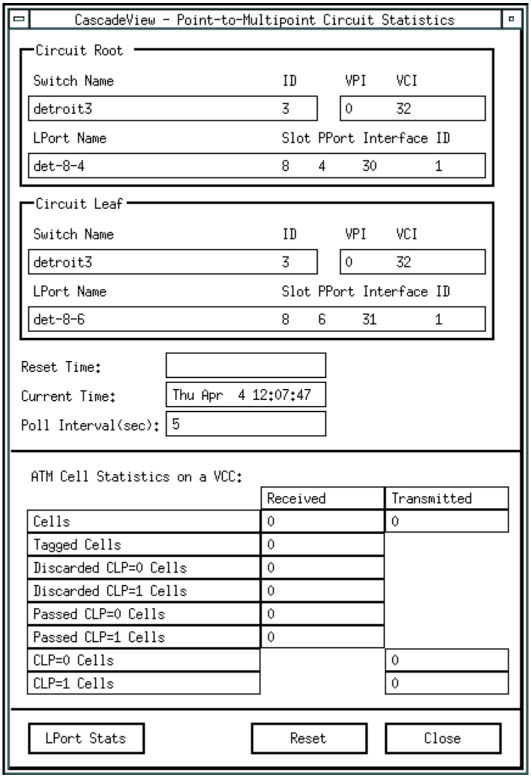



**Figure 5-17. Point-to-Multipoint Circuit Statistics Dialog Box**

The Point-to-Multipoint Statistics dialog box displays ATM cell statistics for a Point-to-Multipoint Circuit ( transmitted and received data for each circuit endpoint) in the following fields:

**Cells** — The total number of cells that were received and transmitted.

**Tagged Cells** — The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit.

**Discarded CLP=0 Cells** — The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor.

**Discarded CLP=1 Cells** — The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor.

**Passed CLP=0 Cells** — Indicates the number of received CLP=0 cells that were passed for transmission.

**Passed CLP=1 Cells** — The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged as CLP=1 cells because of a traffic descriptor violation (they are counted as Tagged Cells).

**CLP=0 Cells** — Indicates the number of CLP=0 cells that were transmitted.

**CLP=1 Cells** — Indicates the number of CLP=1 cells that were tagged as CLP=1 and were transmitted.

*Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells Fields indicate that either the source may need to slow transmission or that you need to reconfigure the traffic descriptors to reflect the source speed.*

*If one leaf of a point-to-multipoint connection indicates problems, check the other leaves of the connection. If the problems only exist on one leaf, check the configuration for that leaf.*

# Displaying SVC Summary Statistics

To display SVC summary statistics:

> *Resource Management (RM) cells are counted as passed CLP 0 or passed CLP 1 cells. The Logical Port Statistics dialog box provides separate RM cell statistics on a per logical port basis (see “Displaying Logical Port Summary Statistics” on page 5-23).*

1. From the Monitor menu, select Cascade Objects ⇒ Show All SVC Parameters⇒ Show All Active SVCs.

   The Show All Active SVCs dialog box appears as shown in Figure 5-18.

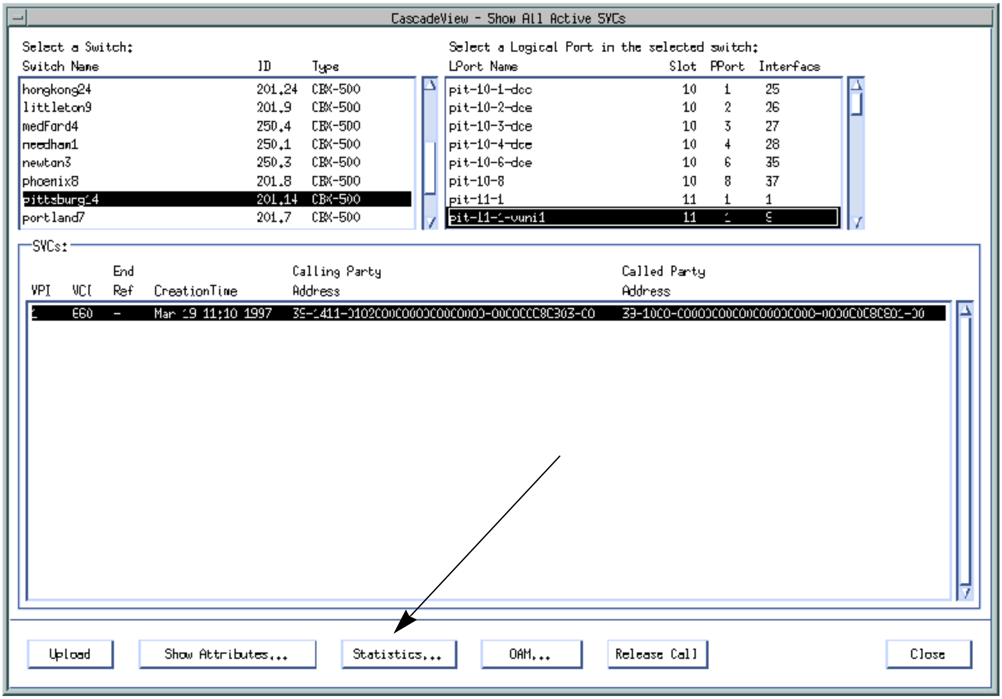



**Figure 5-18. Show All Active SVCs Dialog Box**

2. Select a switch from the list box on the left.

3. Select a corresponding logical port from the list box on the right.

4. Choose Statistics to display SVC summary statistics. The system displays the SVC Summary Statistics dialog box shown in Figure 5-19.

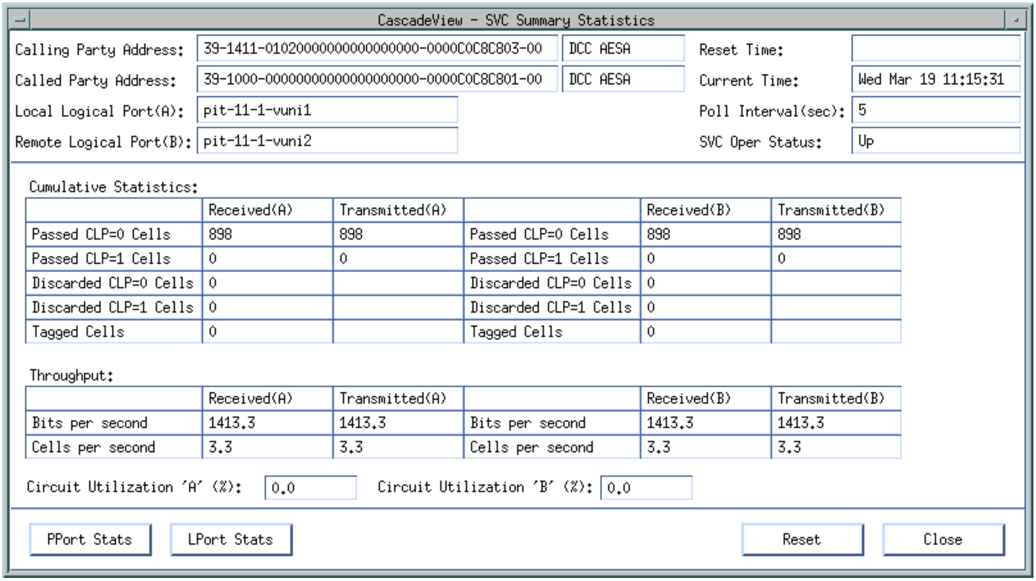



**Figure 5-19. SVC Summary Statistics Dialog Box**

The SVC Summary Statistics dialog box (Figure 5-19) displays data in separate columns to reflect the transmission and receipt of data on each side of the circuit.

The SVC Summary Statistics dialog box displays the following types of statistics:

**Cumulative Statistics** — The number of each type of cell (passed, dropped, or tagged) and whether those cells are being transmitted or dropped due to conditions in the network.

**Throughput Statistics** — The cells per second and bits per second for each side of the circuit.

Table 5-10 lists and describes the SVC summary statistics and fields.

**Table 5-10. SVC Summary Statistics**

| Statistic | Description |
|---|---|
| **Cumulative Statistics** | |
| Passed CLP=0 Cells | The total number of cells that were received and transmitted. |
| Passed CLP=1 Cells | The total number of CLP=1 cells received at the port. This does not include CLP=0 cells that were received and then tagged as CLP=1 cells because of a traffic descriptor violation (they are counted as tagged cells).<br>***Note***: *Consistently high values in the Discarded CLP=0, Discarded CLP=1 Cells, and Tagged Cells fields indicate that either the source may need to slow transmission or that you should reconfigure the traffic descriptors to reflect the source speed.* |
| Discarded CLP=0 Cells | The total number of received CLP=0 cells that are dropped because the cell violates the defined traffic descriptor. |
| Discarded CLP=1 Cells | The total number of CLP=1 cells that are discarded because the cells violate the defined traffic descriptor. |
| Tagged Cells | The total number of CLP=0 cells that were tagged as CLP=1 cells. Cells are tagged if they do not conform to the defined traffic descriptor for the circuit. |
| OAM CLP=0 Cells | The total number of F4 and F5 OAM CLP=0 cells that were transmitted by the circuit. |
| OAM CLP=1 Cells | The total number of F4 and F5 OAM CLP=1 cells that were transmitted by the circuit. |

**Table 5-10. SVC Summary Statistics (Continued)**

| Statistic | Description |
|---|---|
| **Throughput Statistics** | |
| Bits per second | The number of bits transmitted and/or received each second. |
| Cells per second | The number of cells transmitted and/or received each second. |

# Generating Reports

This section describes how to generate reports using scripts and the CascadeView/UX Report menu.

## Using Scripts

Table 5-11 lists the scripts you can run to generate reports at the network, node, circuit, and trunk level.

**Table 5-11. Report Scripts**

| Report Script Command | Report Name | Report Type |
|---|---|---|
| /opt/CascadeView/bin/cv-network-rpt.sh | allnetwork.lis | Network |
| /opt/CascadeView/bin/cv-circuit-rpt.sh | allckt.lis | Circuit |
| /opt/CascadeView/bin/cv-node-rpt.sh | allnode.lis | Node |
| /opt/CascadeView/bin/cv-trunk-rpt.sh | alltrk.lis | Trunk |

> *You must have the Sybase SQR package installed to run these scripts.*
>
> *These scripts create the .lis report in the directory where you run them. Run the script from your home directory. The scripts will attempt to write to the current directory. Errors occur if you do not have write permission for the directory.*

## Using the CascadeView/UX Report Menu

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

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

Table 5-12 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 report that does not exist.

**Table 5-12. Generate and View Report Options**

| Report Option | Action/Description |
|---|---|
| Generate or View Single Node Report | To select this option, click the mouse on a node to select the node for use in a report, and then choose 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. |

Table 5-12. Generate and View Report Options (Continued)

| Report Option | Action/Description |
|---|---|
| Generate or View All Nodes Report | No further input is required after you select this option from the Report menu. All nodes in the NMS database (specified in *cascadeview.cfg*) are applied in the report. |
| Generate or View Network Report | The system prompts you for the network number. If you enter the network number, the system generates a report for the specified network.<br><br>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 you select the Generate option to generate another report. |
| Generate or View Trunk Report | The system prompts you for the network number. If you enter the network number, the system generates a trunk report for the specified network.<br><br>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 you select the Generate option to generate another report. |
| Generate or View Circuit Report | The system prompts you for the network number. If you enter the network number, the system generates a circuit report for the specified network.<br><br>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 you select the Generate option to generate another report. |
| Transparency | All reports are sent to the user's HOME directory in */opt/CascadeView.var/cvReport*. |

# 6

# Performance Monitoring

This chapter describes how to retrieve and display performance monitoring data for physical ports. CascadeView provides scheduled periodic performance-monitoring reports for current data based on a configured interval from 1-900 seconds. You specify this interval when you set the polling interval for performance statistics (refer to page 6-2).

The performance monitoring function enables you to create a report for the current day or previous days. You can display the total performance data for a day or for a specified interval.

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

# Setting the Polling Interval for Performance Statistics

The *Polling* function sets the time interval for collecting and retrieving performance-monitoring statistical data during the current session of CascadeView/UX.

To set the time interval for the current session of CascadeView/UX:

1. From the Misc menu, select Cascade Time Intervals ⇒ Set Performance Statistics Time Interval. The Change Performance Statistics Polling Interval dialog box appears, displaying the current time interval.

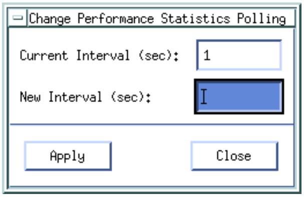



**Figure 6-1. Change Performance Statistics Polling Dialog Box**

2. Enter a value, in seconds, from 1-900. This polling interval is used for all physical port Performance Statistics (Current) reports.

3. Choose Apply to save the changes.

4. Choose Close to return to the network map.

# Displaying Performance-Monitoring Data

To access performance-monitoring statistics for a physical port:

1. Select the switch that contains the module from which you want to obtain performance statistics.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the desired physical port and choose Set Attr. The Set ATM Physical Port Attributes dialog box appears.
4. Choose PM Statistics to display the associated Performance Monitoring Statistics dialog box.
5. Table 6-1 describes the Performance Monitoring Statistics dialog box fields.

**Table 6-1. Performance Monitoring Statistics Fields**

| Field | Description |
|---|---|
| Status | Displays "Data Valid" if these statistics are valid; displays "Data Invalid" if there is no valid data for the specified time period. Note that this dialog box displays all zeroes when there is no valid data. |
| SES Threshold Settings | A read-only field that indicates the standard (ANSI or Bellcore) used to calculate the SES values. This is the option you selected when you configured the performance thresholds (refer to the *Network Configuration Guide for CBX 500* for more information). |
| Valid Intervals (*Interval reports only*) | Displays the number of intervals for which data is available. |
| Time Elapsed | Displays the time elapsed in the current time period. |

**Table 6-1. Performance Monitoring Statistics Fields (Continued)**

| Field | Description |
|---|---|
| Far End Status | Indicates any problems with remote/far-end equipment that could affect the accuracy of this data. |

Performance-monitoring parameters are measured in 15-minute and one-day thresholds.

Refer to the following sections for detailed information on performance monitoring statistics and parameters by port type:

- "Displaying OC3/OC12 and STM-1/STM-4 Port Data" on page 6-5.
- "Displaying T1/E1 Port Data" on page 6-10.
- "Displaying DS3/E3 Port Data" on page 6-16.

# Displaying OC3/OC12 and STM-1/STM-4 Port Data

The Performance Monitoring Statistics dialog box displays the Current statistics by default as shown in Figure 6-2.

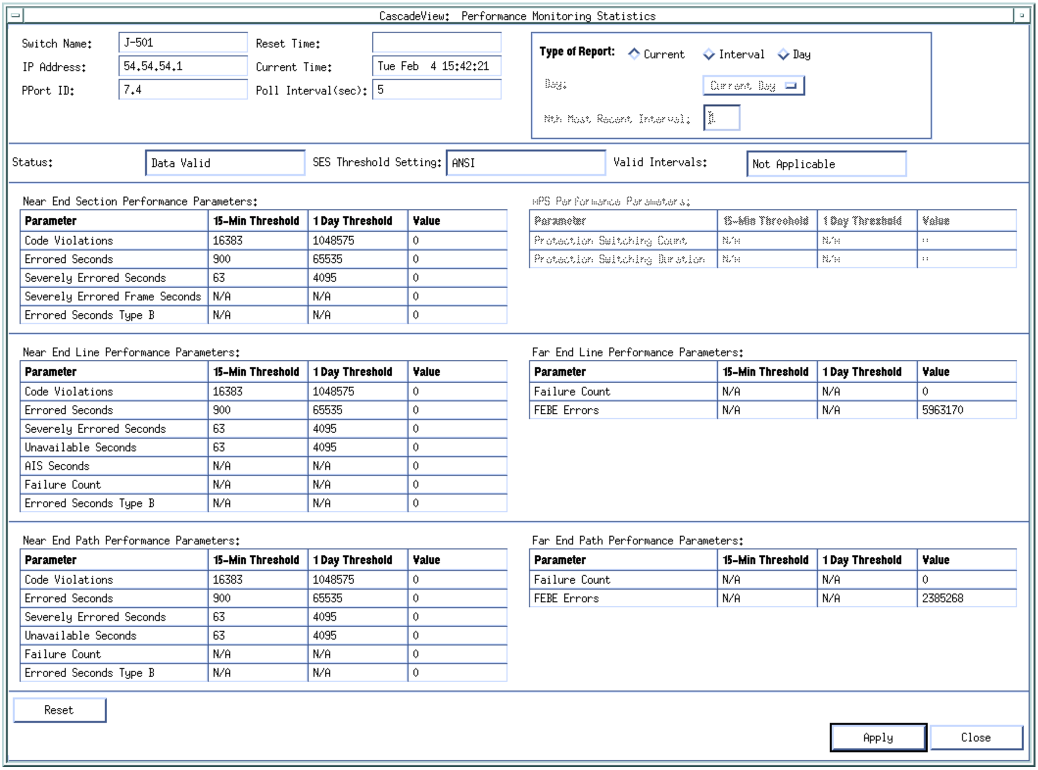



**Figure 6-2. Performance Monitoring Statistics (OC12/STM-4) Dialog Box**

1. To View additional statistics, select one of the following options in the Type of Report field:

   **Current** (*default*) — Displays real-time current interval data updated at the specified polling frequency.

   **Interval** — Displays an interval report based on an interval value you specify, from 1-96.

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

2. Choose Apply to display the data. The dialog boxes that appear if you choose the Total and Interval options provide information similar to that shown in Figure 6-2.

3. Choose Reset to update these statistics.

4. Use Table 6-2 to interpret performance monitoring parameters.

5. Choose Close to exit.

**Table 6-2. OC3/OC12 and STM-1/STM-4 Performance Monitoring Statistics**

| Parameter | Threshold | Description |
|---|---|---|
| **Near End Section Performance Parameters** | | |
| Code Violations | CV-S | A count of BIP-8 (bit interleaved parity) errors that are detected at the section layer of the incoming signal. Section CV counters increment for each BIP-8 error detected. That is, each BIP-8 can detect up to eight errors per STS-N (synchronous transport signal level N) frame with each error incrementing the CV counter. CVs for the section layer are collected using the BIP-8 in the B1 byte located in the section overhead of STS-1 number 1. |
| Errored Seconds | ES-S | A count of one-second intervals containing one or more BIP-8 errors (B1 byte), one or more severely errored frame (SEF) defects, or one or more loss of signal (LOS) defects. |
| Severely Errored Seconds | SES-S | A count of one-second intervals containing x or more BIP-8 errors (B1 byte), one or more SEF defects, or one or more LOS defects.<br><br>***Note:*** *The SES Threshold standard (described in the* Network Configuration Guide for CBX 500*) sets the value of x for SES-S. For ANSI standards, this value is 8800; for Bellcore standards, 63.* |
| Severely Errored Frame Seconds | SESF-S | A count of one-second intervals containing one or more SEF defects. |

**Table 6-2. OC3/OC12 and STM-1/STM-4 Performance Monitoring Statistics (Continued)**

| Parameter | Threshold | Description |
|---|---|---|
| **Near End Line Performance Parameters** | | |
| Code Violations | CV-L | A count of the BIP-8 errors detected at the line layer of the incoming signal. The line CV counter increments for each BIP-8 error detected. That is, each line BIP-8 can detect up to 8 errors per STS-1 frame with each error incrementing the CV counter. CVs for the line layer are collected using the BIP-8s in the B2 byte located in the line overhead of each STS-1. |
| Errored Seconds | ES-L | A count of one-second intervals containing one or more BIP-8 errors (B2 byte), or one or more alarm indication signal (AIS) defects. |
| Severely Errored Seconds | SES-L | A count of one-second intervals containing x or more BIP-8 errors (B2 byte) or one or more AIS defects.<br>***Note:*** *The SES Threshold standard (described in the* Network Configuration Guide for CBX 500*) sets the value of* x *for SES-L. For ANSI standards, this value is 10000; for Bellcore standards, this value is 124.* |
| Unavailable Seconds | UAS-L | A count of one-second intervals for which the SONET line is unavailable, which begins at the onset of 10 contiguous SES-Ls. The unavailable time period includes the 10 SES-Ls.<br>Once the SONET line is unavailable, it becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from the unavailable time period. |
| AIS Seconds | AISS-L | A count of one-second intervals containing one or more AIS defects. |
| Failure Count | FC-L | A count of near-end line failure (AIS-L) events. |

**Table 6-2. OC3/OC12 and STM-1/STM-4 Performance Monitoring Statistics (Continued)**

| Parameter | Threshold | Description |
|---|---|---|
| **Near End Path Performance Parameters** | | |
| Code Violations | CV-P | A count of BIP-8 errors that are detected at the STS path layer of the incoming signal. The CV counters increment for each BIP-8 error detected. CVs for the STS path layer are collected using the BIP-8 in the B3 byte located in the STS path overhead. |
| Errored Seconds | ES-P | A count of one-second intervals containing one or more BIP-8 errors (B3 byte), one or more AIS defects, or one or more LOP-P defects. |
| Severely Errored Seconds | SES-P | A count of one-second intervals containing x or more BIP-8 errors (B3 byte), one or more LOP-P defects, or one or more AIS defects. The default value of x for the STS-1 and STS-3c synchronous payload envelope (SPE) is 2400.<br>***Note:*** *The SES Threshold standard (described in the* Network Configuration Guide for CBX 500*) sets the value of* x *for SES-P. For ANSI standards, this value is 8800; for Bellcore standards, 63.* |
| Unavailable Seconds | UAS-P | A count of one-second intervals for which the SONET STS path is unavailable, which begins at the onset of 10 contiguous SESs. The unavailable time period includes the 10 SESs.<br>Once the SONET STS-path is unavailable, it becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are excluded from the unavailable time period. |
| Failure Count | FC-P | A count of near-end STS path failure (LOP-P or AIS-P) events. |

**Table 6-2. OC3/OC12 and STM-1/STM-4 Performance Monitoring Statistics (Continued)**

| Parameter | Threshold | Description |
|---|---|---|
| Errored Seconds Type B | ESB-L | A count of one-second intervals containing one or more BIP-8 errors (B2 byte), and no alarm indication signal (AIS) defects. |
| **APS Performance Parameters** | | |
| Protection Switching Count | PSC | The number of switching events on the working line and the protection line. |
| Protection Switching Duration | PSD | The length of time in seconds when a working line is out of service due to protection switching event, or the length of time a protection line is in service due to a protection switching event. |
| **Far End Line Performance Parameters** | | |
| Failure Count | FC-LFE | A number of far-end line failure (RFI-L) events. |
| FEBE errors | CV-LFE | Far-end block line errors. |
| **Far End Path Performance Parameters** | | |
| Failure Count | FC-PFE | A count of far-end STS path failure (RFI-P) events. |
| FEBE errors | CV-PFE | Far-end block path errors. |

## Displaying T1/E1 Port Data

1. To view statistics, select one of the following reports:

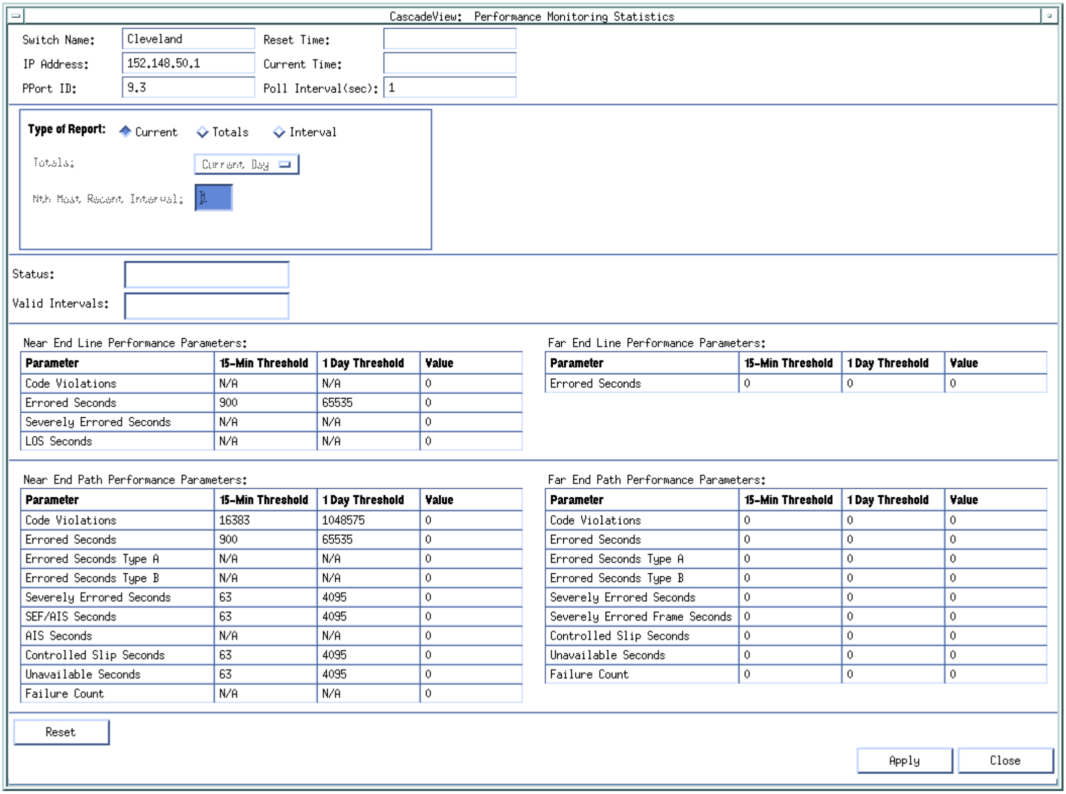
   **Current** (*default*) — Displays real-time current interval data updated at the specified polling frequency.

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

   **Interval** — Displays an interval report based on the interval value you specify, from 1-96.

   The following dialog box appears if you choose the “Current” report option. The Total and Interval options provide similar information.

2. Choose Apply to display the data. Figure 6-3 displays the Current report type fields.



CascadeView: Performance Monitoring Statistics

Switch Name: Cleveland
IP Address: 152.148.50.1
PPort ID: 9.3
Reset Time:
Current Time:
Poll Interval(sec): 1

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

Status:
Valid Intervals:

Near End Line Performance Parameters:

| Parameter | 15-Min Threshold | 1 Day Threshold | Value |
|---|---|---|---|
| Code Violations | N/A | N/A | 0 |
| Errored Seconds | 900 | 65535 | 0 |
| Severely Errored Seconds | N/A | N/A | 0 |
| LOS Seconds | N/A | N/A | 0 |

Far End Line Performance Parameters:

| Parameter | 15-Min Threshold | 1 Day Threshold | Value |
|---|---|---|---|
| Errored Seconds | 0 | 0 | 0 |

Near End Path Performance Parameters:

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

Far End Path Performance Parameters:

| Parameter | 15-Min Threshold | 1 Day Threshold | Value |
|---|---|---|---|
| Code Violations | 0 | 0 | 0 |
| Errored Seconds | 0 | 0 | 0 |
| Errored Seconds Type A | 0 | 0 | 0 |
| Errored Seconds Type B | 0 | 0 | 0 |
| Severely Errored Seconds | 0 | 0 | 0 |
| Severely Errored Frame Seconds | 0 | 0 | 0 |
| Controlled Slip Seconds | 0 | 0 | 0 |
| Unavailable Seconds | 0 | 0 | 0 |
| Failure Count | 0 | 0 | 0 |

Reset Apply Close

**Figure 6-3. Performance Monitoring Statistics (T1/E1) Dialog Box**

3. Choose Reset to update these statistics.

4. Use Table 6-3 to interpret the performance-monitoring statistics.

5. Chose Close to exit this dialog box.

**Table 6-3. T1/E1 Performance Monitoring Statistics Fields**

| Parameter | Threshold | Description |
|---|---|---|
| **Near End Line Performance Parameters** | | |
| Code Violations | CV-L | A count of both BPVs (bipolar violations) and EXZs (excessive zeros) occurring over the accumulation period. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded from the count. |
| Errored Seconds | ES-L | A count of one-second intervals with one or more BPVs, one or more EXZs, or one or more LOS (loss of signal) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded. |
| Severely Errored Seconds | SES-L | A count of one-second intervals with 1544 or more BPVs plus EXZs, or one or more LOS defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded. |
| LOS Seconds | LOSS-L | A count of one-second intervals containing one or more LOS defects. |
| **Near End Path Performance Parameters** | | |
| Code Violations | CV-P | A count of frame synchronization bit errors (FE) in the SF (Superframe) format, or a count of cyclic redundancy check (CRC)-6 errors in the ESF (Extended Superframe) format occurring during the accumulation period. |

**Table 6-3. T1/E1 Performance Monitoring Statistics Fields (Continued)**

| Parameter | Threshold | Description |
|---|---|---|
| Errored Seconds | ES-P | In the case of DS1 ESF, a count of one-second intervals containing one or more CRC-6 errors, one or more CS events, or one or more SEF or AIS defects. In the case of DS1 SF, this parameter is a count of one-second intervals containing one or more FE events, one or more SEF or AIS defects, or one or more CS events. |
| Errored Seconds Type A | ESA-P | This parameter applies to DS1 ESF paths only. A count of one-second intervals with exactly one CRC-6 error and no SEF or AIS defects. |
| Errored Seconds Type B | ESB-P | This parameters applies to DS1 ESF paths only. A count of one-second intervals with no less than 2, and not more than 319 CRC-6 errors, no SEF defects, and no AIS defects. |
| Severely Errored Seconds | SES-P | This parameter applies to both SF and ESF frame formats of DS1. In the case of ESF, it is a count of one-second intervals with 320 or more CRC-6 errors, or one or more SEF or AIS defects. In the case of SF, it is a count of one-second intervals with eight or more FE events (if $F_t$ and $F_8$ bits are measured) or four or more FE events (if $F_t$ bits only are measured), or an SEF or AIS defect. |
| SEF/AIS Seconds | SAS-P | A count of one-second intervals containing one or more SEF defects or one or more AIS defects. |
| **Near End Path Performance Parameters** | | |
| AIS Seconds | AISS-P | A count of one-second intervals containing one or more AIS defects. |

Table 6-3. T1/E1 Performance Monitoring Statistics Fields (Continued)

| Parameter | Threshold | Description |
|---|---|---|
| Controlled Slip Seconds | CSS-P | A count of one-second intervals containing one or more controlled slips. Counts of controlled slips can be made accurately only in the path-terminating network element of the DS1 signal, where the controlled slip takes place. |
| Unavailable Seconds | UAS-P | A count of one-second intervals for which the DS1 path is unavailable. The DS1 path becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time period.<br><br>Once it is unavailable, the DS1 path becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are excluded from the unavailable time period. |
| Failure Count | FC-P | Count of Loss of Frame or AIS events within the accumulation period. |
| **Far End Line Performance Parameters** | | |
| Errored Seconds | ES-LFE | A count of one second PRM intervals containing an LV=1. |
| **Far End Path Performance Parameters** | | |
| Code Violations | CV-PFE | A count of the number of far end CVs occurring during the accumulation period. |
| Errored Seconds | ES-PFE | A count of one second PRM intervals containing a G1, G2, G3, G4, G5, or G6 or SE or SL=1, or an RAI signal. |
| Errored Seconds Type A | ESA-PFE | A count of one second PRM intervals containing a G1=1 and SE=0. |

**Table 6-3. T1/E1 Performance Monitoring Statistics Fields (Continued)**

| Parameter | Threshold | Description |
|---|---|---|
| Errored Seconds Type B | ESB-PFE | A count of one second PRM intervals containing a G2, G3, G4, or G5=1, and SE=0. |
| Severely Errored Seconds | SES-PFE | A count of one second PRM intervals containing a G6 or SE=1, or an RAI signal. |
| Severely Errored Frame Seconds | SEFS-PFE | A count of one second PRM intervals containing an SE=1. |
| Controlled Slip Seconds | CSS-PFE | A count of one second PRM intervals containing an SL=1. |
| Unavailable Seconds | UAS-PFE | A count of one-second intervals for which the DS1 path is unavailable. |
| Failure Count | FC-PFE | Count of RAI (yellow alarm) events within the accumulation period. |

## Displaying DS3/E3 Port Data

1. To view statistics, select one of the following reports:

   **Config** — Displays the current configuration information.

   **Current** (*default*) — Displays real-time current 15-minute interval counters, updated at the specified polling frequency.

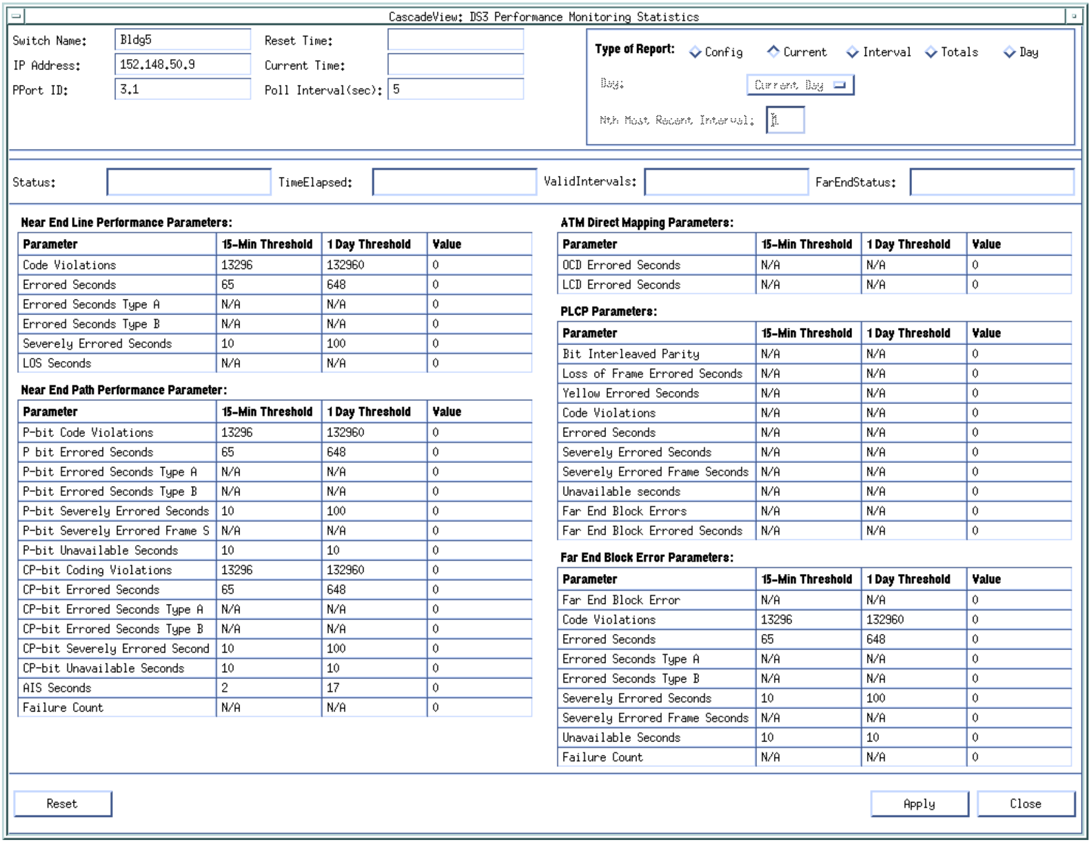
   **Interval** — Displays counters for a previous 15-minute interval, based on the interval value (1-96) you specify, with 1 being chronologically the most recent.

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

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

2. Choose Apply to display the data.

   The following dialog box appears if you choose the “Current” report type. The Total and Interval reports provide similar information.



CascadeView: DS3 Performance Monitoring Statistics

Switch Name: Bldg5
IP Address: 152.148.50.9
PPort ID: 3.1
Reset Time:
Current Time:
Poll Interval(sec): 5

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

Status: TimeElapsed: ValidIntervals: FarEndStatus:

**Near End Line Performance Parameters:**

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

**Near End Path Performance Parameter:**

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

**ATM Direct Mapping Parameters:**

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

**PLCP Parameters:**

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

**Far End Block Error Parameters:**

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

Reset Apply Close

**Figure 6-4. Performance Monitoring Statistics (DS3/E3) Dialog Box**

3. Choose Reset to update these statistics.
4. Use Table 6-4 to interpret the performance monitoring statistics.
5. Choose Close to exit this dialog box.

**Table 6-4. DS3/E3 Performance Monitoring Statistics Fields**

| Parameter | Threshold | Description |
|---|---|---|
| **Near End Line Performance Parameters** | | |
| Code Violations | CV-L | A count of both BPVs and EXZs occurring over the accumulation period. |
| Errored Seconds | ES-L | A count of one-second intervals containing one or more BPVs, one or more EXZs, or one or more LOS defects. |
| Errored Seconds Type A | ESA-L | A count of one-second intervals containing one BPV or EXZ and no LOS defects. |
| Error Seconds Type B | ESB-L | A count of one-second intervals containing more than one but less than x BPVs plus EXZs and no LOS defects. |
| Severely Errored Seconds | SES-L | A count of one-second intervals with more than x BPVs plus EXZs, or one or more LOS defects. |
| LOS Seconds | LOS-L | A count of one-second intervals containing one or more LOS defects. |
| **Near End Path Performance Parameters** | | |
| P-bit Code Violations | CVP-P | A count of error events occurring in the accumulation period. |
| P-bit Errored Seconds | ESP-P | A count of one-second intervals containing the occurrence of one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects. |
| P-bit Errored Seconds Type A | ESAP-P | The count of one-second intervals containing exactly one P-bit parity error and no SEF or AIS defects. |
| P-bit Errored Seconds Type B | ESBP-P | The count of one-second intervals containing more than one but less than x P-bit parity errors and no SEF or AIS defects. |

Table 6-4. DS3/E3 Performance Monitoring Statistics Fields (Continued)

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

Table 6-4. DS3/E3 Performance Monitoring Statistics Fields (Continued)

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

Table 6-4. DS3/E3 Performance Monitoring Statistics Fields (Continued)

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

7

# Trap Alarms

Trap alarms notify the operator of events taking place on switches configured to report to the NMS. You can display a list of logged trap alarms at any time through the Cascade Events option from the Event Categories window in CascadeView/UX.

This chapter describes how to:

- Display and delete events
- Add event categories
- Move events from one category to another
- Mask traps so that selected traps are not reported in the Events Browser
- Modify alarm relay status and trap transmission rate

Appendix A lists and describes each of the trap alarm messages that the system reports and displays in the Events Browser.

# The Event Categories Window

The Event Categories window appears each time you run CascadeView/UX and notifies you of any significant trap alarm conditions. This window has a button for each event category, including Cascade Events. The following screen illustrates the Event Categories window.

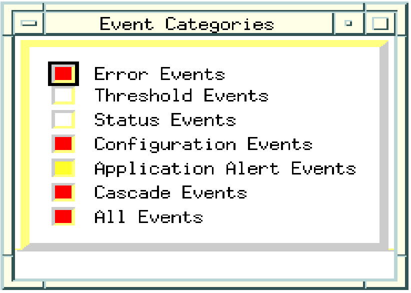



**Figure 7-1. Event Categories Window**

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

You can customize the Event Categories window by adding categories. For example, you may want to add a category that holds all acknowledged events or one that holds all canceled events. Refer to "Adding Event Categories" on page 7-5 for instructions about adding event categories.

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

# Displaying the All Events Browser Dialog Box

To display the All Events Browser dialog box, choose Cascade Events from the Event Categories window. The following dialog box appears.

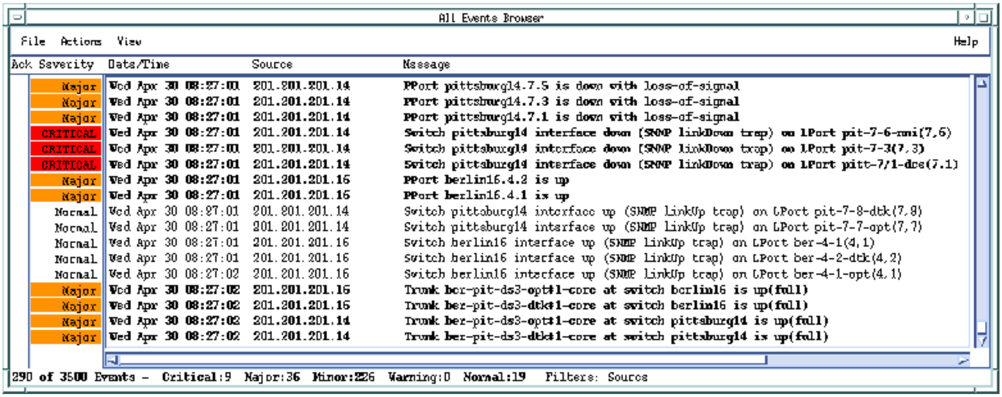



**Figure 7-2. All Events Browser Dialog Box**

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

**Severity** — Displays the severity level. Possible values include: Critical, Major, Minor, Warning, or Normal.

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

**Source** — Displays the name of the system on which the trap alarm occurred.

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

See Appendix A for a list and description of the trap alarm messages reported and displayed in the All Events Browser dialog box.

## Viewing a Switch from the Events Browser

To view the switch that generated an event:

1. Select the event from the list.
2. From the Action menu, select 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 Events Browser, refer to the *HP OpenView Network Node Manager User's Guide* or choose Help.

## Deleting an Event from the Events Browser

To delete an event:

1. Select the event from the list.
2. From the Action menu, select Delete ⇒ Selected Event.
3. To delete all the listed events, from the Action menu, select 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 different categories as necessary.

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

## Moving Events from One Category to Another

To move an event from one category to another:

1. From the Monitor menu, select the Events: SNMP option. The All Events Browser dialog box appears.
2. Select the event(s) you want to move.
3. From the Action menu, select Assign Category. The Assign Category: All Events dialog box appears.
4. Select the Category to which you want to move the event.
5. Choose OK.

# About Trap Filtering

The trap filtering feature enables you to filter traps that you do not want the switch to send to the Events Browser. The switch forwards *only* unfiltered traps to the NMS. You can filter specific traps or traps based on severity level. For example, filtering all non-alarm traps results in no non-alarm traps being sent to the Events Browser.

## Setting Trap-Filtering Parameters

To filter traps that you do not want the switch to report to the Events Browser:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trap Parameters ⇒ Set All Trap Filtering Parameters. The Modify Trap Masks dialog box appears as shown in Figure 7-3.

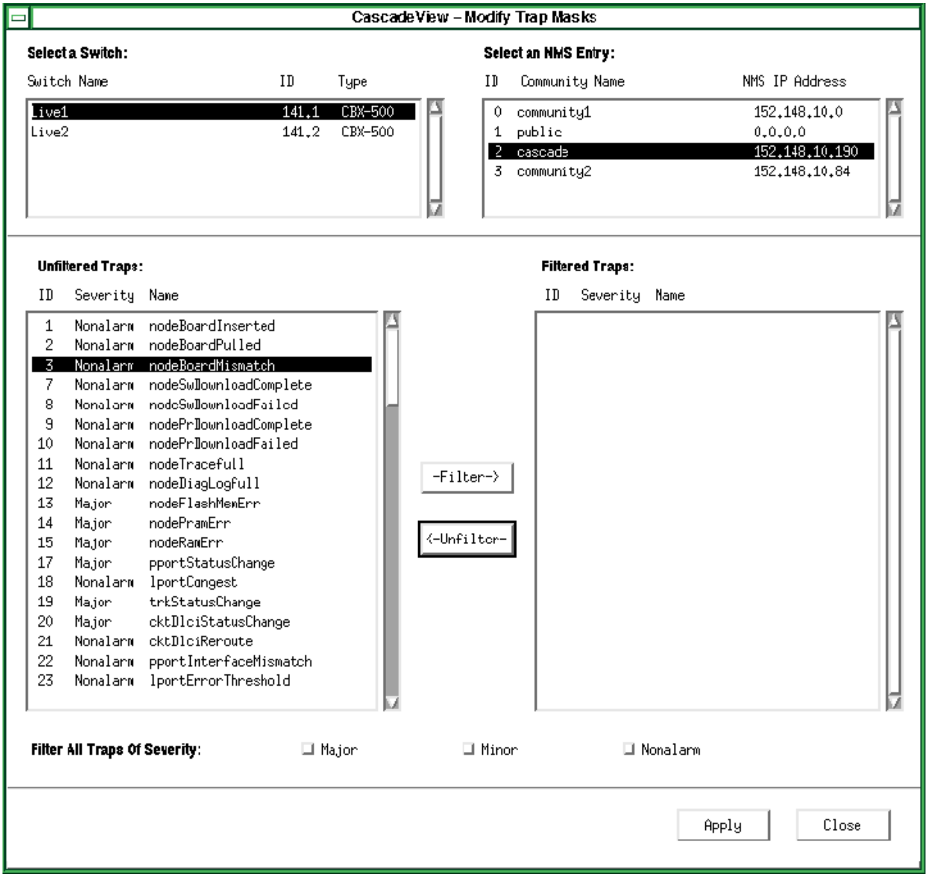



**Figure 7-3. Modify Trap Masks Dialog Box**

The Modify Trap Masks dialog box displays the switch name, community name, and NMS IP address. Traps are displayed by their corresponding MIB ID.

2. Select the switch from the list box on the left. The corresponding community name and IP address for the selected switch appear in the list box on the right.

3. Select an NMS entry. The default is the community name of your NMS.

4. From the Unfiltered Traps list box on the left, select the trap(s) that you want to filter. You can select multiple traps at the same time. To select non-sequential traps, hold down the control key and select each trap ID.

5. Choose Filter. The system moves the trap(s) to the Filtered Traps list box on the right as shown in Figure 7-4.

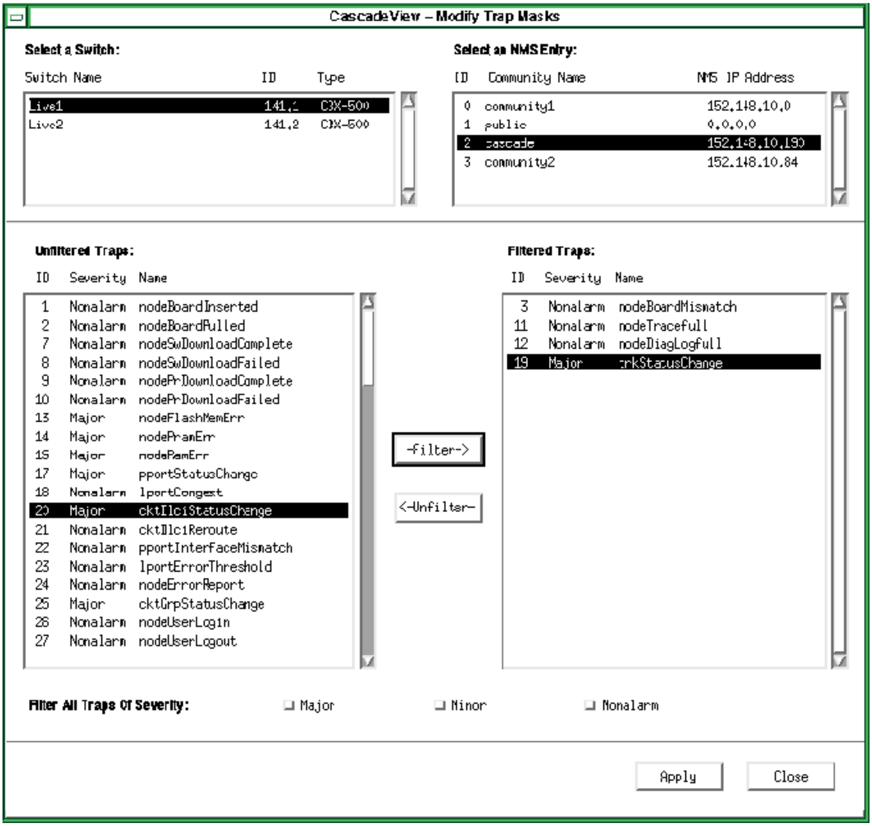



**Figure 7-4. Modify Trap Mask (Filtered Traps) Dialog Box**

6. (*Optional*) Select a severity level (*major, minor, or non-alarm*) to filter traps based on trap severity.

> *You cannot filter critical traps. All critical traps are sent to the NMS.*

7. Choose Apply to confirm the changes.

8. Choose Close to exit the dialog box and return to the network map.

## Removing Trap-Filtering Parameters

To remove the filtering parameters and add traps to the unfiltered list:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trap Parameters ⇒ Set All Trap Filtering Parameters. The Modify Trap Masks dialog box appears as shown in Figure 7-3 on page 7-7.
2. Select the switch from the list box on the left. The corresponding community name and IP address for the selected switch appear in the list box on the right.
3. Select an NMS entry. The default is the community name of your NMS.

   The filtered traps appear in the Filtered Traps list box on the right (see Figure 7-4 on page 7-8).
4. Select the trap(s) from the Filtered list box and choose Unfilter. The system moves the trap(s) to the Unfiltered Traps list box on the left.
5. To remove the filtering parameters on severity traps, deselect major, minor, or non-alarm. This unfilters all of the *deselected* severity level traps.
6. Choose Apply to confirm the changes.
7. Choose Close to exit the dialog box and return to the network map.

# Using Contact Alarm Relays

The CBX 500 SPA module contains an eight-position terminal strip that enables you to connect remote audio and visual alarms. These relay contacts alert you to critical, major, and minor alarm conditions in the switch and power supply. Refer to the *CBX 500 Hardware Installation Guide* for information on connecting these alarms. If necessary, you can use the NMS to disable the contact alarm relay feature.

To clear these alarms for a specific switch, use the Modify Trap Configuration dialog box (Figure 7-7 on page 7-13). This dialog box enables you to adjust the trap transmit rate, which determines the maximum number of traps per second the switch sends to the NMS. For example, if you enter 5 (*default*), the switch sends a maximum of 5 traps to the NMS every second and queues any remaining traps.

To access the Modify Trap Configuration dialog box:

1. Select the switch object and from the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.


**Figure 7-5. Switch Back Panel Dialog Box**

2. Choose Set Sw Attr. The Set Switch Attributes dialog box appears.

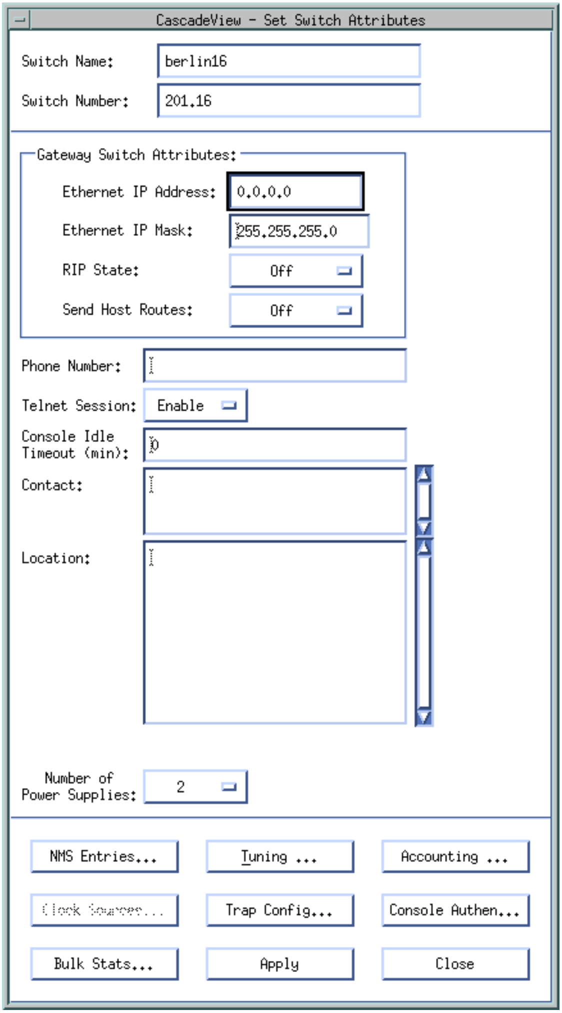



**Figure 7-6. Set Switch Attributes Dialog Box**

3. Choose Trap Config. The Modify Trap Configuration dialog box appears.

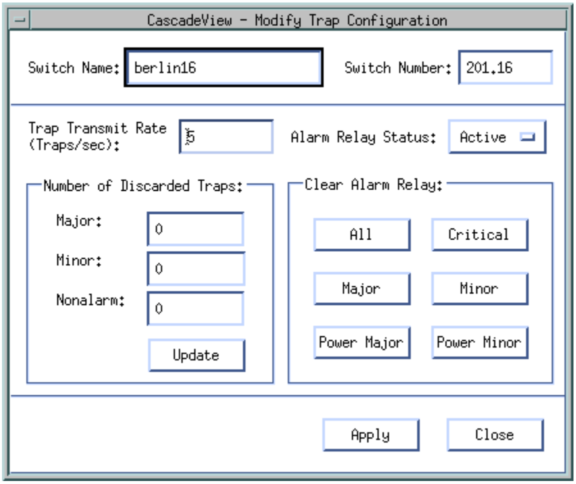



**Figure 7-7. Modify Trap Configuration Dialog Box**

4. Complete the fields described in Table 7-1.

**Table 7-1. Modify Trap Configuration Fields**

| Field | Action/Description |
|---|---|
| Trap Transmit Rate (Traps/sec) | Use the Update command to display the number of discarded traps according to their severity (*major, minor, non-alarm*).<br><br>***Note:*** *The switch discards traps under peak problem conditions when the trap transmit queues overflow.*<br><br>If the switch discards traps, increase the trap transmit rate. Valid values range from 1 to 10. |

**Table 7-1. Modify Trap Configuration Fields (Continued)**

| Field | Action/Description |
|---|---|
| Clear Alarm Relays | Enables you to clear an alarm relay (i.e., turn off an audible/visual contact alarm) immediately. Choose one of the following Clear Alarm Relay commands:<br><br>*All* – Clears all alarm relays.<br><br>**Note:** *This function does not clear the alarm condition, only the audible/visual alarm contact relay.*<br><br>*Critical* – Clears a Critical alarm relay. These alarms indicate severe, service-affecting conditions that require immediate corrective action, for example, a power supply fails.<br><br>*Major* – Clears a Major alarm relay. These alarms indicate a hardware or software condition that can cause a serious disruption of service or circuit failure. An example would be an IOM or physical port down.<br><br>*Minor* – Clears a Minor alarm relay. These alarms indicate non-service effecting conditions, for example, a performance monitoring threshold is exceeded.<br><br>*Power Major* – Clears a major power alarm relay, for example, the second power supply is out of service. In the case of an N+1 chassis, this alarm is generated if two out of three power supplies fail.<br><br>*Power Minor* – Clears a minor power alarm relay. With an N+1 chassis, this alarm is generated if one of the three power supplies fails. |
| Alarm Relay Status | Set the Alarm Relay Status to Inactive to disable the alarm relay function. |

5. Choose Apply to send the change to the switch.

# 8

# NTM and NDC

This chapter describes how to configure and use Network Traffic Management (NTM) and Network Data Collection (NDC) on the CBX 500 switch. Cascade has based the functional requirements for NTM and NDC on the Bellcore GR-1248 specification [GR1248].

NTM and NDC are disabled by default. To enable network traffic management and data collection, you first configure the NTM congestion thresholds for the “feeder” logical port. The feeder port can be any UNI, Direct Trunk, or NNI logical port. Then, you set the NDC thresholds on a per-PVC basis. You can then monitor the NTM and NDC data that the logical port and PVC collect.

You can enable the NTM and NDC functions when you first configure your switch, or you can take the logical port/PVCs off-line to enable these functions once you establish a basic switch-to-NMS configuration.

# About Network Traffic Management

The purpose of NTM is to improve PVC traffic performance during overloads and failures in the network. NTM provides the following functions:

**Measures of Congestion** (MOCs) — Defined at the ATM level based on percentage of cell loss.

**NTM surveillance functions** — Used to detect overloads based on MOCs.

**NTM control functions** — Used to regulate/reroute the traffic flow during overloads.

## Measures of Congestion

NTM applies a MOC to all congestable ATM modules. A congestable ATM module is any entity within an ATM Network Element (ATM NE) that can experience traffic congestion. The CBX 500 MOC is based on the count of CLP=0+1 cells discarded due to congestion in the output process. This count is sampled at each feeder logical port every 20 ms.

To prevent traffic bursts from corrupting the measurement, a MOC is subject to a smoothing algorithm that averages the congestion measurement over a period of time. The smoothed MOC is subject to four congestion thresholds ($CT_0$-$CT_3$), which you define for the logical port. The thresholds default to zero, which prevents the accumulation of congestion statistics. $CT_3$ is designated as the severe congestion threshold, and $CT_0$ is designated as the severe congestion abatement threshold. The $CT_1$ – $CT_3$ thresholds define four corresponding Machine Congestion levels, $MC_0$ – $MC_3$.

## NTM Surveillance Measurements

The NTM surveillance measurements are based on 5-minute intervals. The timestamp of the counts corresponds to the end of the 5-minute interval.

For each logical port, the following counts are maintained for the 5-minute period:

- Total number of discarded CLP=0+1 cells.
- For each $MC_0$-$MC_3$ level, the number of 20 ms periods spent in that level (from 0 to 15,000).
- For each $MC_0$-$MC_3$ level, the number of times (based on 20 ms sampling) this level was entered (from 0 to 7,500). This includes transitions from both the higher and lower levels.

For each logical port, CascadeView/UX provides a variety of NTM statistics, including the current plus three 5-minute history counts, as well as the timestamps for the history counts and the time elapsed (measured in seconds) in the current 5-minute period. The timestamps use the Universal Coordinated Time (UCT) available on the switch and have a 1-second resolution.

## NTM State Change Notifications

When the smoothed MOC exceeds $CT_3$ and stays above $CT_0$ for the specified time interval (T), an SNMP trap is issued to the NMS. Once this first trap is sent, when the smoothed MOC falls below $CT_0$, another SNMP trap is sent. The interval T defaults to 30 seconds. Traps are issued within 5 seconds of the respective event detection.

## NTM Controls

Only automatic NTM controls are used to alleviate congestion. The NMS is not used to specify alternate routes. Currently, the hardware output process implements selective cell discards without software intervention.

# About Network Data Collection

You configure the NDC measurements to detect any violation of PVC service subscription parameters, and establish trends in network traffic patterns and loads. Scheduled measurements are taken on a regular basis as soon as the ATM NE is put into service. The measurements monitor the usage and health of the network.

The CBX 500 switch supports NDC scheduled measurements for up to 360 simultaneously monitored circuits per IOM.

For each feeder port and PVC, CascadeView/UX provides a variety of NDC statistics including:

- The current plus two 15-minute history counts.
- The timestamps for the history counts (taken at the end of respective 15-minute periods). The timestamps use the Universal Coordinated Time (UCT) available on the switch and have a 1-second resolution.
- The time elapsed in the current 15-minute period.

There are three types of NDC scheduled measurements:

**Traffic load measurements** — Count the number of incoming/outgoing cells on a per-interface and per-VC basis. Refer to page 8-5.

**UPC/NPC disagreement measurements** — Collect the number of cells discarded due to UPC/NPC violations on a per-VC basis. Refer to page 8-5.

**Traffic load and congestion measurements** — Count the cells processed and discarded by a congestable ATM NE module, respectively. These counts do not include cells discarded due to UPC/NPC disagreements. Refer to page 8-6.

## Traffic Load Measurements

The traffic load measurements count all NDC-valid cells. These are all user+OAM cells submitted to UPC/NPC before policing actions occur. Traffic load measurements maintain a count of the number of incoming/outgoing CLP=0+1 user+OAM cells in a 15-minute period for all UNI and NNI logical ports.

For the PVC endpoint you select, these measurements also maintain a count of the following user/OAM cells at the ingress/egress node in a 15-minute period:

- Number of incoming CLP=0+1 cells
- Number of outgoing CLP=0+1 cells

## UPC/NPC Disagreement Measurements

The UPC/NPC disagreement measurements count the number of cells the network discards due to peak cell rate violation at the UNI (UPC) and at ingress VC at B-ICI (NPC). Two counts of incoming cells discarded due to traffic descriptor violations are collected on a per-VC basis:

- Number of incoming discarded CLP=0+1 cells.
- Number of incoming discarded high-priority (CLP=0) cells. Includes cells tagged as CLP=1 and then dropped. Performed only if the ATM NE supports loss priority.

  In these two cases, NDC measurements count both the user and OAM cells. These measurements are applied to selected PVC endpoints.

  If the ATM NE implements cell tagging, NDC measurements count the number of CLP=0 cells that are tagged as CLP=1 cells.

## Traffic Load and Congestion Measurements

The NDC MOC is based on the number of CLP=0+1 cells discarded per-port. The sampling period is 20 ms, same as for NTM. The NDC uses the same congestion thresholds $CT_1$-$CT_3$, and consequently the same Machine Congestion levels $MC_0$-$MC_3$ as defined for NTM. This enables a simple accumulation of the 5-minute NTM values to provide the 15-minute value.

The following counts of user+OAM cells per port are maintained in the 15-minute period:

- Number of discarded CLP=0+1 cells.
- For each $MC_0$-$MC_3$ level, number of 20 ms periods spent in that level (from 0 to 45,000).
- For each $MC_0$-$MC_3$ level, number of times (based on 20 ms sampling) this level is entered (from 0 to 22,500). This includes transitions from both the higher and lower levels.

# Configuring NTM Attributes for a Logical Port

To define the NTM attributes for a feeder logical port:

1. From the network map, select the appropriate switch icon.
2. From the Misc menu, select Cascadeview ⇒ Logon.
3. Enter the Operator password.
4. From the Administer menu, select Cascade Parameters ⇒ Set Parameters to access the Switch Back Panel dialog box.
5. Select the desired physical port, then choose *Set Attr* to display the Set ATM Physical Port Attributes dialog box.
6. Choose Logical Port to access the Set All Logical Ports in PPort dialog box.
7. Select the feeder logical port and choose Modify. The Modify Logical Port dialog box appears.
8. Choose OK. The Modify Logical Port dialog box reappears.
9. Choose Options ⇒ NTM Parameters.
10. Choose Set. The NMT Congestion Threshold dialog box appears.

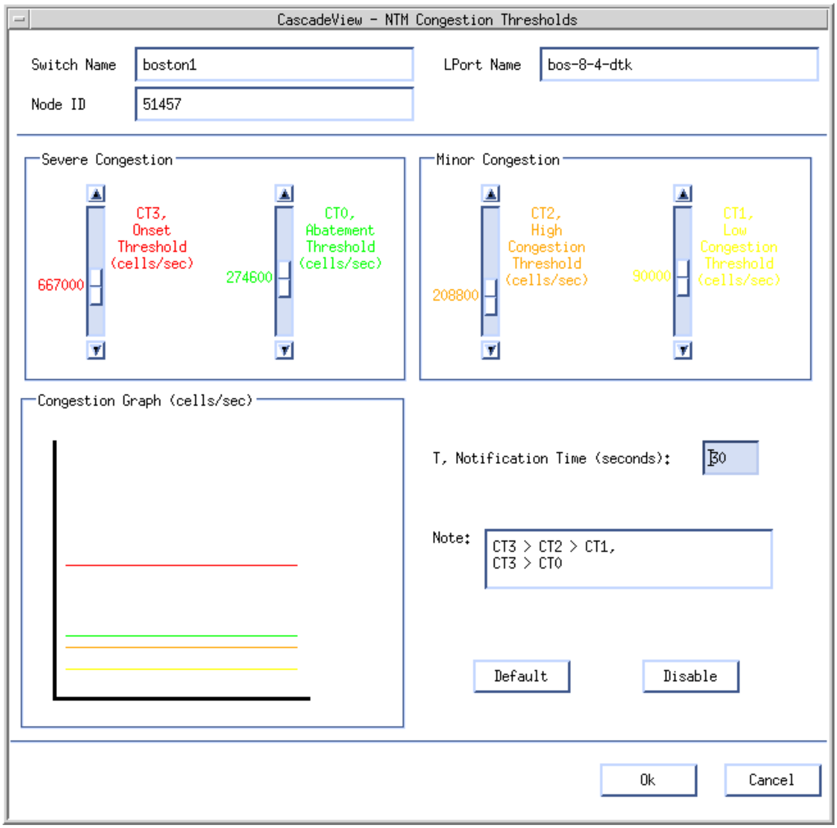



**Figure 8-1. NTM Congestion Threshold Dialog Box**

11. To use the default NTM settings, choose Default. The defaults vary with respect to the IOM. Use the scroll bars or arrows to decrease the default setting to make this logical port more sensitive to congestion or increase these values to make it less sensitive.

    If the congestion level on this logical port exceeds the CT3 setting, and stays above the CT0 setting for at least 30 seconds, the port generates a trap. When the congestion level returns to the CT0 level for the specified time period, a second trap is generated.

12. When you finish, choose OK.

# Viewing NTM Parameters

To view NTM parameters:

1. From the Show All Logical Ports dialog box (Figure 5-13 on page 5-24), select Options ⇒ NTM Parameters.

2. Choose View. The following dialog box appears.

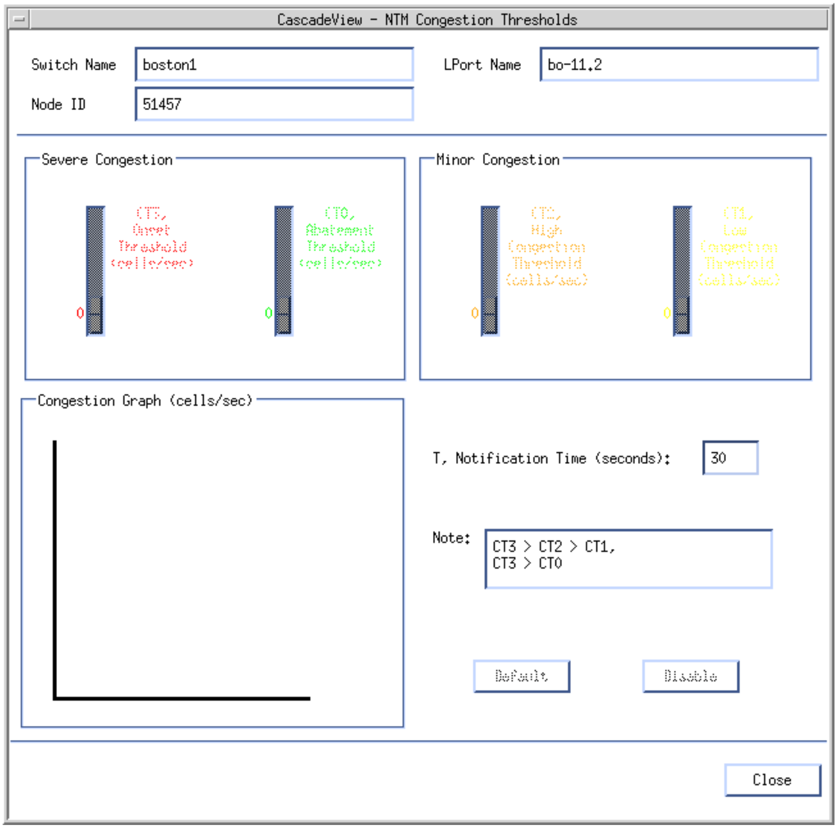



**Figure 8-2. NTM Congestion Threshold Dialog Box**

If the congestion level on this logical port exceeds the CT3 setting, and stays above the CT0 setting for at least 30 seconds, the port generates a trap. When the congestion level returns to the CT0 level for the specified time period, a second trap is generated.

3. When you finish, choose Close.

## Viewing NTM Logical Port Statistics

To View NTM logical port statistics:

1. From the Show All Logical Ports dialog box (Figure 5-13 on page 5-24), select Options ⇒ NTM Statistics.
2. Choose View. The following dialog box appears.

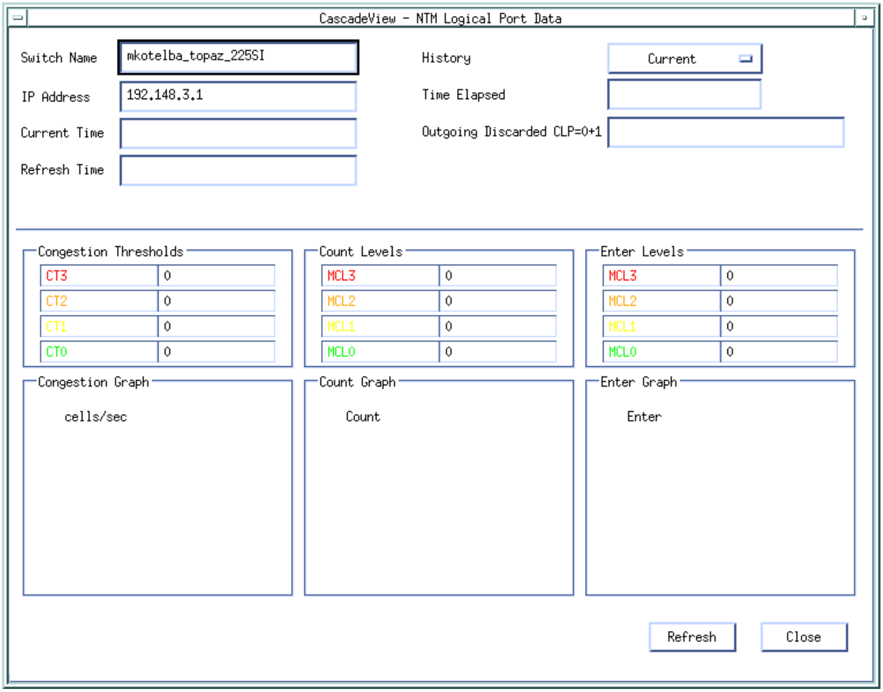



**Figure 8-3. NTM Logical Port Data Dialog Box**

The NTM Logical Port Data dialog box tracks the NTM statistics, including the number of outgoing discarded CLP=0+1 cells, and displays the following:

**History** — Displays current NTM data, or data from three previous 5-minute intervals.

**Time Elapsed/Timestamp** — Displays the seconds elapsed in the current time period. For a previous 5-minute interval, this field displays the UTC date and time.

This dialog box displays congestion thresholds and statistics using both text and graphs. Graphs are color coded as follows:

**Table 8-1. NTM Data Graph Color Key**

| Statistic | Color |
|---|---|
| CT3/MC3 | Red |
| CT2/MC2 | Orange |
| CT1/MC1 | Yellow |
| CT0/MC0 | Green |

3. Use the Refresh button to update these statistics.

4. Choose Close to return to the Show All Logical Ports dialog box.

## Viewing NDC Logical Port Statistics

To View NDC logical port statistics:

1. From the Show All Logical Ports dialog box (Figure 5-13 on page 5-24), select Options ⇒ NDC Statistics.

2. Choose View. The following dialog box appears.

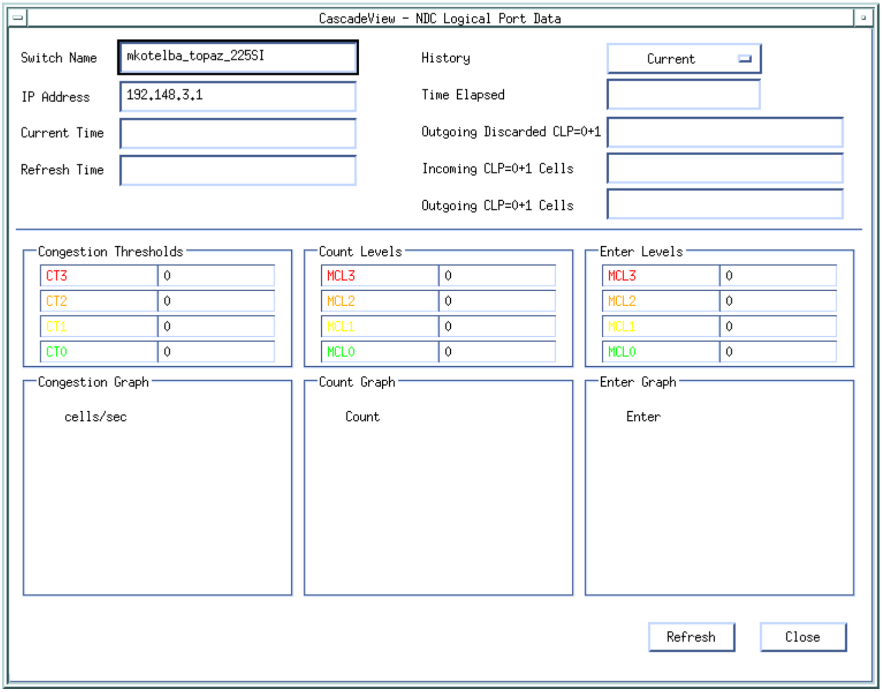



**Figure 8-4. NDC Logical Port Data Dialog Box**

The NDC Logical Port Data dialog box tracks the NDC statistics, including the number of:

- Outgoing discarded CLP=0+1 cells
- Incoming CLP=0+1 cells
- Outgoing CLP=0+1 cells

You can use the History button to display current NDC data or data from previous 15-minute intervals. The Time Elapsed field displays the minutes elapsed in the current time period.

This dialog box displays congestion thresholds and statistics using both text and graphs. The graphs use the same color coding scheme as the NTM statistics (refer to Table 8-1 on page 8-11).

3. Use the Refresh button to update these statistics.

4. Choose Close to return to the Show All Logical Ports dialog box.

# Configuring the NDC Attributes for a PVC

To configure the NDC thresholds and attributes on a Point-to-Point circuit:

> *To configure the NDC thresholds and attributes on a Point-to-Multipoint circuit, refer to the* Network Configuration Guide for CBX 500.

1. From the Administer menu, choose Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs On Map dialog box appears.
2. Choose Modify. The Modify End Logical Ports dialog box appears.
3. Choose OK. The Modify PVC dialog box appears.
4. Choose Set NDC Attributes. The dialog box displays the following fields:

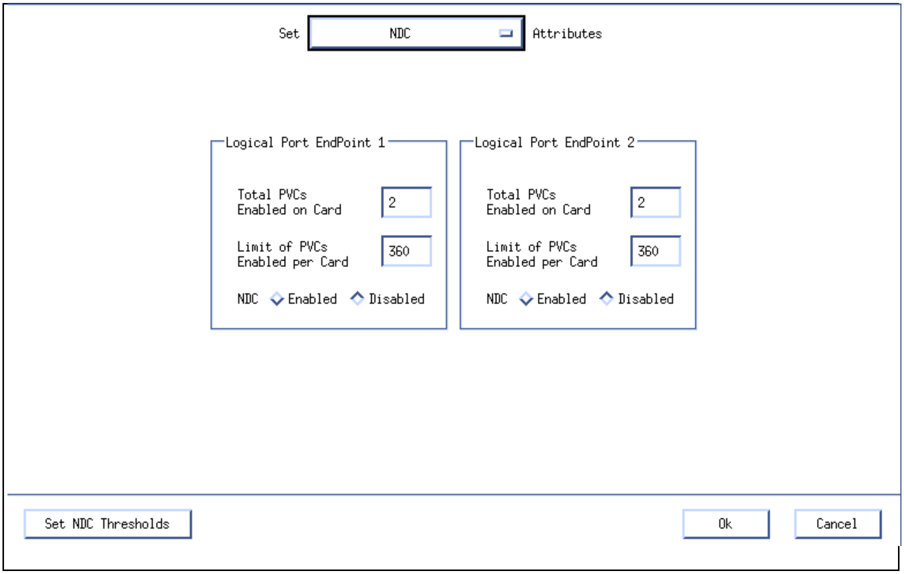



**Figure 8-5. Modify PVC-Set NDC Attributes Dialog Box**

For each logical port endpoint the following NDC parameters appear:

**Total PVCs Enabled on Card** — Displays the current number of NDC-enabled endpoints for this card.

**Limit of PVCs Enabled on Card** — Displays the limit (360) of NDC-enabled endpoints you can configure on a card.

**NDC** — Choose Enable to collect NDC statistics for this circuit endpoint. The default is disabled.

5. Choose Set NDC Thresholds. The NDC Thresholds dialog box appears.

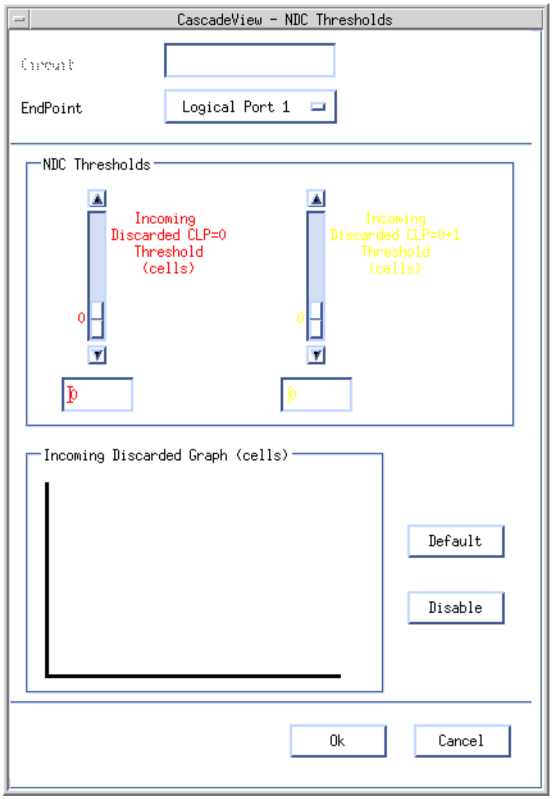



**Figure 8-6. NDC Thresholds Dialog Box**

You can configure the NDC Threshold for a single logical port endpoint or both endpoints. To configure the NDC threshold for a Point-to-Multipoint circuit, refer to the *Network Configuration Guide for CBX 500*.

6. Choose Default to use the default threshold.

7. To configure the threshold, use the scroll bar and arrows or enter a cell value below each scroll bar.

   These thresholds apply to the number of incoming CLP=0 and CLP=0+1 cells which have been discarded. If the number of discarded cells for this endpoint exceeds the value you configure, a trap is generated.

8. Choose OK to set these thresholds.

9. Choose OK to return to the Set All PVCs dialog box.

## Viewing NDC Thresholds

The NDC Thresholds function enables you to view NDC thresholds for either endpoint of the PVC you select.

To view NDC thresholds:

1. From the Show All PVCs dialog box, choose NDC Thresholds. The following dialog box appears.

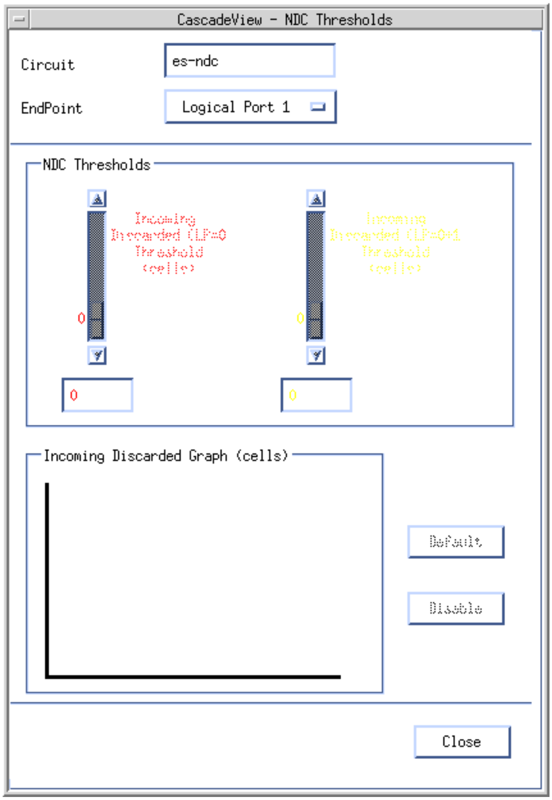



**Figure 8-7. View NDC Thresholds Dialog Box**

This dialog box displays the configured settings as well as a graph of discarded cells.

2. Choose Close to exit this dialog box.

## Viewing NDC PVC Data

The NDC Statistics function enables you to view NDC PVC statistics for either endpoint of the PVC you select.

To view NDC PVC data:

1. From the Show All PVCs dialog box, choose NDC Statistics. The following dialog box appears.

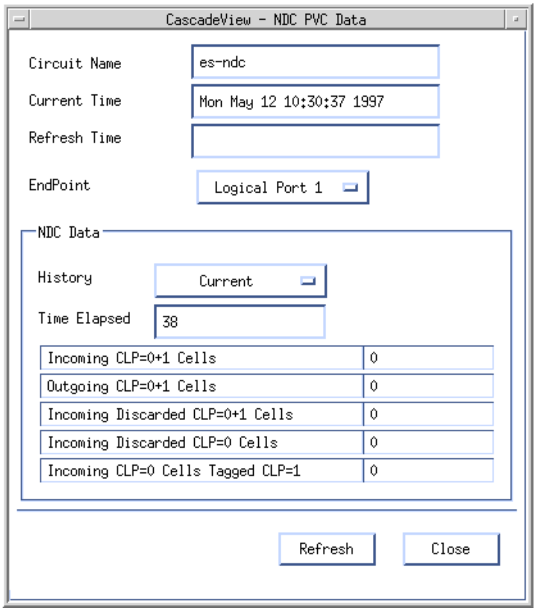



**Figure 8-8. NDC PVC Data Dialog Box**

For each logical port endpoint, this dialog box tracks the NDC PVC statistics, including the number of:

- Incoming CLP=0+1 cells
- Outgoing CLP=0+1 cells
- Incoming discarded CLP=0+1 cells

- Incoming discarded CLP=0 cells
- Incoming CLP=0 cells tagged CLP=1

You can use the History button to display current NDC data or data from the two previous 15-minute intervals. The Time Elapsed field displays either the seconds elapsed in the current time period, or the UTC Timestamp for the specified 15-minute interval.

2. Use the Refresh button to update these statistics.
3. Choose Close to return to the Show All PVCs dialog box.
4. Choose Close to return to the network map.

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.

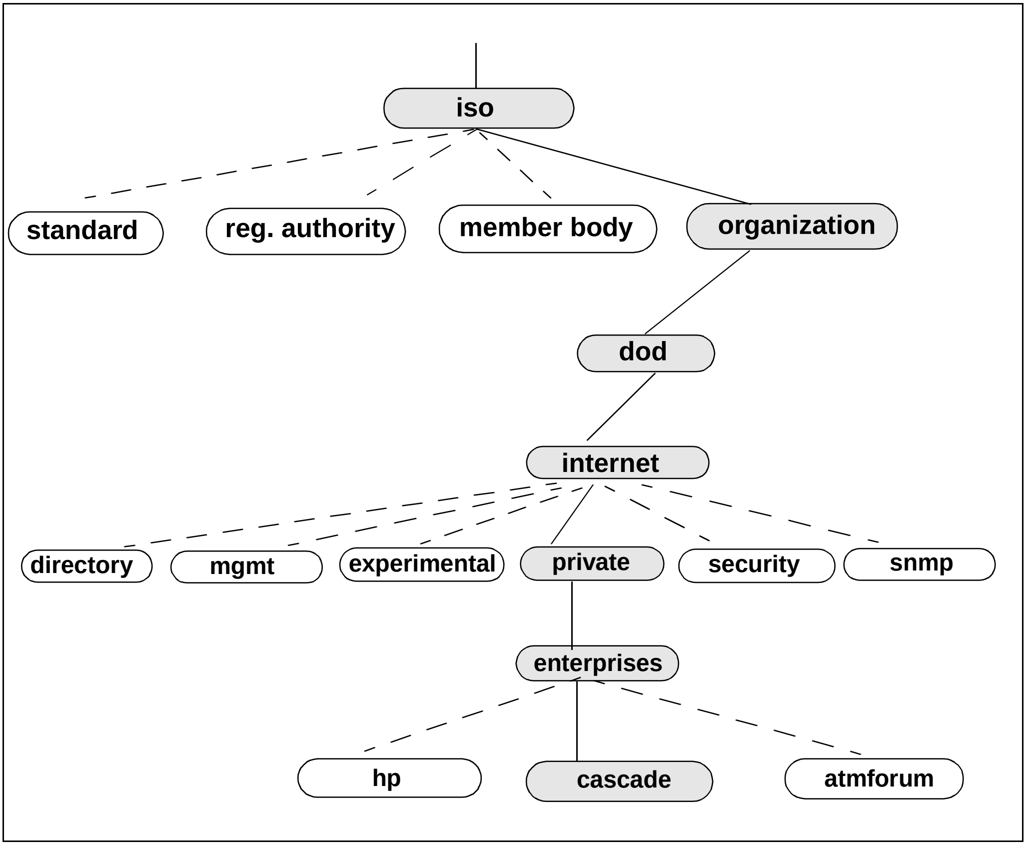



**Figure 9-1. Cascade MIB Tree Hierarchy**

## 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

## 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 want to use the MIB to check a card's Admin status, you would 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 displays the Browse MIB dialog box (Figure 9-2).

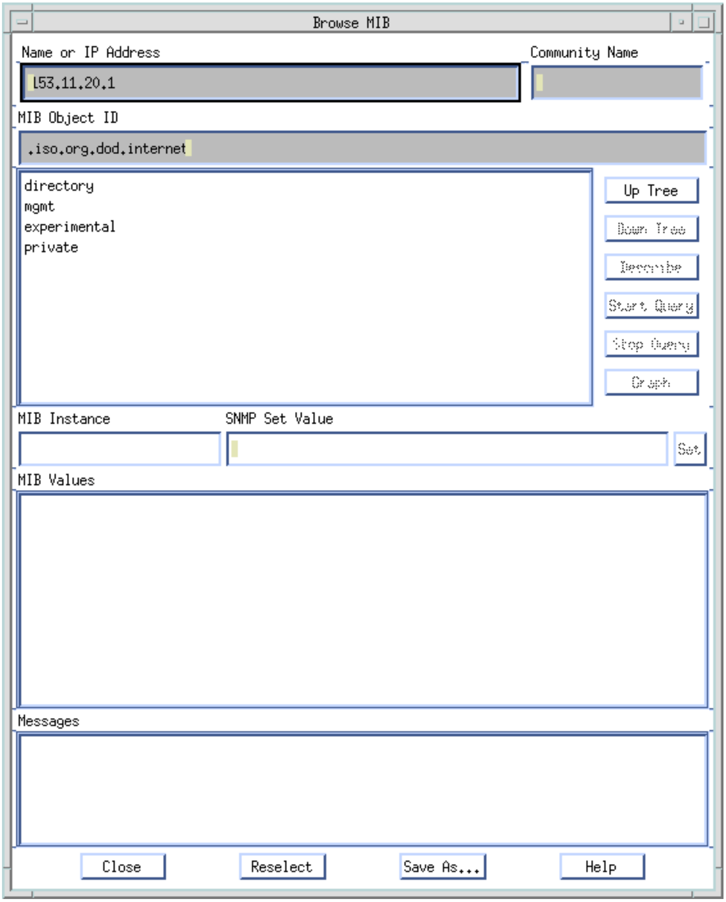



**Figure 9-2. Browse MIB Dialog Box**

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 Enterprise 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 could 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.

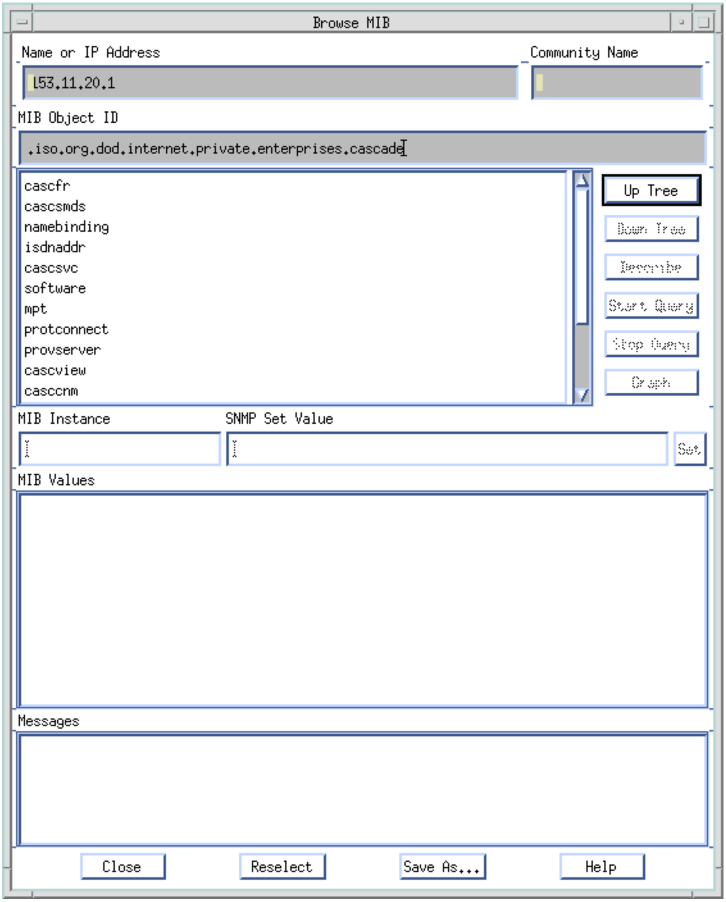



**Figure 9-3. Displaying Groups in the Browse MIB Dialog Box**

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 as shown in Figure 9-4.

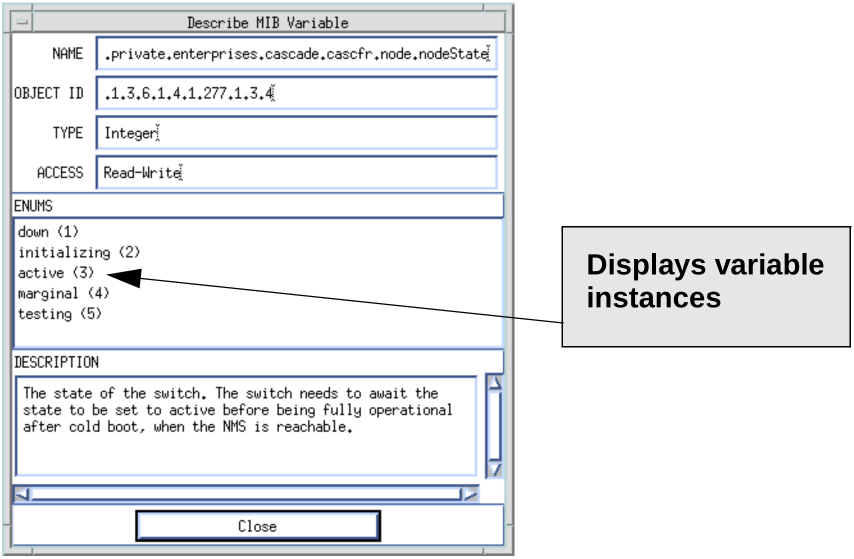



**Figure 9-4. Describe MIB Variable Dialog Box**

7. Choose Close to exit the dialog box.

# 10

# Resolving Problems

This chapter provides general troubleshooting solutions for resolving problems with the NMS software applications. Unless otherwise noted, this guide only addresses software problems and their solutions. If you suspect hardware problems, refer to the *CBX 500 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 10-1.

**Table 10-1. 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 with 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.

## 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. Enter the following command:

   **`/usr/bin/dmesg`**

   – This command provides system boot-up information and displays the installed physical memory in (MB).

   – If the system has been running, the information that you need is not displayed properly. Shut down and restart the system. Repeat Steps 1 and 2 to display the amount of available memory.

## I’m having trouble installing Solaris 2.5.

Verify that you have identified your hardware correctly and partitioned your disks properly.

1. To 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. Enter **boot cdrom**.
4. Refer to the *Network Management Station Installation Guide* for installation instructions.

## 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, enter:

   **`/usr/openwin/bin/filemgr &`**

3. From the File menu, select Check for Floppy. A file manager window appears and displays the contents of the floppy. The switch software files are listed in the window.
4. Make sure the system File Manager is set to the following directory:

   `/opt/CascadeView.var/switchSoftware`

5. Select the switch software window. Select a file and drag it to the system file manager window.
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 CBX 500*.

## How do I start CascadeView/UX?

1. Verify that you are logged in as the nms user by entering the following command:

   **`whoami`**

2. Verify that you are in the **/opt/nms** directory by entering the following command:

   **`pwd`**

3. Execute 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 CBX 500* for more information.

## Where do I get an HP OpenView key?

A key is associated with each copy of HP OpenView. The key matches the IP address of the UNIX workstation for which it was purchased. Register the key with Hewlett Packard by sending the completed software certificate included with your HP OpenView package to Hewlett Packard.

## I get the error “Cannot connect to database”.

If you receive the error “cannot connect to database” when you try to start CascadeView, do the following:

1. Log in as the root user and enter the appropriate password.

2. To verify that all OV daemons are RUNNING and their behavior is OVs_WELL_BEHAVED, enter the following command:

   **/usr/OV/bin/ovstatus**

3. If all OV daemons are not running, restart the OV daemons by entering:

   **/usr/OV/bin/ovstart ovwdb**

4. To start all daemons, enter the following command:

   **/usr/OV/bin/ovstart**

5. To confirm that all daemons are running, enter:

   **/usr/OV/bin/ovstatus**

## What kind of hardware do I need?

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.

## I can't start Sybase!

To start Sybase, you must be in the $SYBASE directory and logged in as the sybase user.

1. Enter **cd $SYBASE**
2. Enter **whoami** to verify that you are logged in as the sybase user.
3. Enter **ls -l** to list the files in long format.
4. Verify that the correct read and execute permissions are set.
5. Enter **cd install**.
6. Enter **ls -al RUN_CASCADE**.
7. Verify that the file has the correct group and ownership and sybase and dba appear in the third and fourth columns.
8. Verify that the line begins with -r-xr--r--.

## I get a "cannot allocate shared memory" error when I start Sybase.

1. Make sure that the shared-memory allocation was added to the */etc/system* file and the system was rebooted after the file was edited.
2. Move the files *CASCADE.krg* and *CASCADE.srg0* in the */opt/sybase* directory to *CASCADE.krg.old* and *CASCADE.srg0.old* by entering the following commands:

```
mv CASCADE.krg CASCADE.krg.old

mv CASCADE.srg0 CASCADE.srg0.old
```

3. Restart the Sybase server again.

> *Corrupt files are caused by improperly shutting down the Sybase server. These files are shared-memory files that Sybase uses. If these files become corrupt, you cannot start the server.*

## How do I know if 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.

## I keep getting the message "access denied."

You are not logged on.

1. From the Misc menu, select CascadeView ⇒ Logon.
2. Enter your operator password.

## I get error "1997" in the same window I started Open Windows.

1. The Sybase server cannot be accessed by 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. Enter **showserver**.

## How do I know the Sybase server is running?

1. Log in as the sybase user.
2. Change to the following directory:

   **`/opt/sybase/install`**

3. Enter **showserver**.

## How do I start the Sybase server?

1. Log in as the sybase user.
2. Change to the following directory:

   **/sybase/install**

3. Enter **startserver -f RUN_CASCADE**.

## How do I shut down the Sybase server?

1. Log in as the sybase user as follows:

```
su - sybase
```

2. Shut down the Sybase server as follows:

```
isql -U sa -P superbase
```

3. Enter the following commands:

```
1> shutdown
2> go
```

## My mouse does not seem to be working.

The SPARCstation uses an optical mouse. Make sure you have the shiny mousepad.

## After upgrading Solaris, I cannot pram sync. The 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.

Use the following steps to add the line to inittab:

1. Enter the following command:

   ```
   vi /etc/inittab
   ```

2. While holding down the Shift key, enter **$G** to go to the end of the file.
3. While holding down the Shift key, enter **A** and press the Return key to append a line onto the file.
4. Add the following line to the end of the file:

   ```
   tf:3:respawn:/opt/CascadeView/bin/tftpserv > /dev/null
   ```

   These commands invoke the 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. Enter **:wq!**
7. At the # prompt, enter the following command:

   ```
   init Q
   ```

This command forces the system to read the inittab file. The system then starts the 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.*

## 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.

# Common Operating Problems

## My switch will not turn green.

1. Make sure you can ping the switch.
2. Make sure the initial configuration (performed through script download, PRAM Kermit, or console install) was successful.
3. Check the cable connections.
4. Review the configuration.

## I can’t ping my switch

1. Check the route to the switch. To do this, log on as the root user and enter **netstat -r**. This command causes the system to list the destination networks and gateways. Make sure the appropriate route is listed. You can also look at the Use column which lists the route to the switch.

   An H in the flag field of this route indicates you added a host route instead of a net route. (A UG in the flag field indicates a net route.) Make sure you use the keyword net in the route add statement. Note that Solaris follows traditional subnetting. For this reason the lowest route in a subnet always reverts to its IP class (for example, 152.148.50.0 becomes 152.148.0.0).

2. If you cannot find the ping utility, it is in the ***/usr/sbin*** directory.

## I am locked out of a node that no one else is using.

This problem occurs if you improperly exit from HP OpenView or if HP OpenView windows is hung and 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, enter **sh cv-release-locks.sh [*first line of display*]**

   Using the example shown in Step 1, you would release the lock by typing the following:

   ```
   sh cv-release-locks.sh Net0x00000005.Sw0x00000011.
   Card0x00000019.Ppt0x00000025.Lpt0x0000003c
   ```

## Performance is being degraded.

1. Find out how many X-terms you have logged 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 (Refer to "Displaying the All Events Browser Dialog Box" on page 7-3.)
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 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 CBX 500* to recheck those configurations.

## I am experiencing OPTimum Trunk Problems

If you modify the VPI of an OPTimum trunk, the trunk will fail to come up with a new VPI. You must delete the previous OPTimum trunk and its associated logical ports, and re-add the logical ports with the desired VPI 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 the *Network Configuration Guide for CBX 500* for instructions.

## What is the Event Monitor and what does it do for me?

In the CascadeView/UX Network Management Station (NMS), the trap daemon is a separate process. The Event Monitor is the display for this process. Therefore, if you do not use Event Monitor you can close this process without affecting the rest of the NMS. See “Displaying the All Events Browser Dialog Box” on page 7-3 of this guide for more information.

## I keep getting the error / or /var is full.

1. The wtmp and wtmpx files may be too large. Enter the following to check the size of the */var/adm/wtmp* and */var/adm/wtmpx* files.

   **`ls -al`**

2. The file may have tftpserv errors. Use the following command to check for tftpserv errors.

   **`tail wtmp`**

> *If the wtmp and wtmpx files are not very large or if the wtmp file is filled with errors other than tftpserv errors you should consult with your System Administrator.*

3. Check to see if tftpserv is actually running. To do this, enter the following:

   **`ps -ef|grep tftp`**

   Null results indicate that tftpserv is not running. Contact the 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. Enter the following commands:

```
rm wtmp

touch wtmp

chown adm wtmp

chgrp adm wtmp

chmod 664 wtmp

rm wtmpx

touch wtmpx

chown adm wtmpx

chgrp adm wtmpx

chmod 664 wtmpx
```

c. Enter the following commands to move to the *tmp* directory and check to see if there are more than two tftpserv error logs.

```
cd /tmp

ls tftp.error.log.*
```

d. If there are a large number of error logs, enter the following to remove all of the error logs:

```
rm tftp.error.log.*
```

e. Periodically check the */opt/CascadeView.var/initFiles* and */opt/CascadeView.var/cfgSyncFiles* directories. The system creates these files each time you create a text file or PRAM sync a card or switch. Delete these files if you no longer have a need for them.

## How do I change a logical port name?

You cannot use the CascadeView/UX NMS to make this change. Use the following steps to make this change:

1. Change directories to */opt/CascadeView/bin.*
2. Run the **renamelp.sh** shell script.

   In addition, if your installation has access to the CascadeView/UX Toolbox product, you can use a utility called *cvtool_rename_lport* to rename logical ports.

## What is a core file?

A core file is a UNIX process that dumps the entire system contents when it crashes. UNIX programmers can interpret this core file to determine what caused the system crash. If the 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?

Enter **./filename** instead of **filename**.

## How do I change the IP address of my machine?

The following steps cannot be used in an NIS domain.

1. Change the IP address in the */etc/hosts* table for the entry corresponding to the machine. If it is part of an NIS domain, consult with your network administrator.
2. Change the Sybase map.
3. Enter the following command to delete the current configuration and add a new configuration.

```
/opt/sybase/sybtli
```

# What do I do if I get an error that the log device is full?

The following two procedures describe 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. Enter the following commands.

```
1> dump transaction cascview with truncate_only

2> go
```

**Procedure 2**

> *The following steps leave the database in an inconsistent state. For this reason you must back up the database immediately after completing this procedure.*

1. Log into ISQL and enter the following commands.

```
1> dump transaction cascview with no_log

2> go
```

2. Enter the following command to leave isql.

```
1> quit
```

# NMS to Network Connectivity Problems

The following table provides basic troubleshooting solutions for resolving problems when you test the connectivity of the CascadeView/UX NMS software applications and the ATM network.

**Table 10-2. Connectivity Troubleshooting Solutions**

| Problem | Possible Causes | Solutions |
|---|---|---|
| Changes that you entered to the **netstat -nr** configuration have not taken affect. | Wrong order of addition to table not in script. | Use the **netstat -nr** 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.<br><br>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 10-2. Connectivity Troubleshooting Solutions (Continued)**

| 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.<br>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 10-2. Connectivity Troubleshooting Solutions (Continued)

| 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:<br>• The NMS may be sending the wrong ARP and ICMP requests.<br>• You may have a faulty network interface card installed on the SPARC.<br>• There may be an error in the network media.<br>• The SPARC IP Address may be wrong.<br>• The NMS Path is incorrect.<br>• 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.<br>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.<br>If the IP Address is different from the IP address assigned to your SPARC when you configured the switch, do one of the following:<br>• 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.<br>• Change the SPARC's entry in the **/etc/hosts** file to the new IP address and reboot the SPARC. |

# Technical Support Checklist

Before calling the Cascade Technical Response Center for assistance, make sure you have the following information:

☑ If you are experiencing NMS SPARCstation problems, check the SPARC and make note of the following:

- Model type
- Amount of available memory
- Operating system and version number
- Network interface card type
- NMS IP address
- Subnet mask

Also, display, print, and note any changes to the configuration files: *netstat -r, ifconfig -a, ovstatus,* and *showserver*. Pipe the results to a separate file to review later.

☑ If you cannot make a connection from the NMS to the switch, check and note the following:

- Connection method used, (Ethernet, Indirect Ethernet, SLIP, Management VPI/VCI, etc.)
- Type of modem used (if any)
- Cable and connection types (if applicable)
- All IP addresses for the NMS path, Primary NMS, second and third NMS (if any), and Ethernet IP address (if any) configured on the switch.
- If using the Indirect Ethernet or Management VPI/VCI connection method, note the IP addresses of the associated routers.
- Static route has been added.

Please have access to your NMS SPARCstation when calling the Cascade Technical Response Center.

- [x] If you are having trouble configuring a PVC, check and note the following:
    - Physical and logical port configurations
    - PCR
    - SCR
    - MBS
- [x] If you are trying to diagnose physical port problems, check and note the following:
    - Physical attributes configured on the ports
    - Cables, pinouts, and DSU/CSU equipment and related configurations
    - Admin status
- [x] If you are trying to diagnose logical port problems, check and note the following:
    - ILMF configuration set for the port
    - Poll timers and verification timers configured for the port
    - DSU/CSU equipment and related configurations
    - Admin status

# Contacting the Cascade Technical Response Center

Cascade provides a full range of support services to ensure that maximum network uptime is achieved with low equipment cost. The staff at the Cascade Technical Response Center is also available to assist with any problems you encounter while using the NMS software. You can contact the Cascade Technical Response Center by phone, email, or fax.

## Calling by Phone

Cascade provides customer support 24 hours a day, 7 days a week. To contact the Cascade Technical Response Center by phone, call the following number:

**1-800-DIAL-WAN (1-800-342-5926) or direct, 1-508-692-2600 (U.S and Canada)**

**1-508-952-1299 (outside the U.S., Canada, and United Kingdom)**

**0-800-96-2229 (in the United Kingdom)**

### Sending Electronic Messages or Faxes

To contact the Cascade Technical Response Center by email, address your requests to

**cs@casc.com**

To fax the Cascade Technical Response Center, call

**1-508-692-1218**

Include the following information when requesting support through electronic mail or a fax message:

- Your name and telephone number
- Name of contact person and telephone number (if different from above)
- Brief description of the problem
- List of symptoms
- Information identified in the Technical Support Checklist.

A

# Trap Alarm Condition Messages

The following list describes in alphabetical order, each of the trap alarm condition messages that the system reports in the Events Browser. Some events are informational, while others indicate a problem or potential problem within the network configuration.

The list indicates each trap alarm condition message along with a description of the trap and, where possible, a resolution for the condition. Italicized words indicate variable values. For example, *name* specifies the name of the switch, physical port, or logical port. The trap ID has also been provided for use in masking individual traps.

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

This trap (ID =3) indicates that the IOM installed in the slot does not match the NMS configuration for this slot. Use the switch console command "show system" to verify what is actually installed in the switch slot.

**An authentication has failed on *login user* console authentication *login user* due to console authentication.**

This trap (ID = 102) login fail reason indicates a user console authentication login failure.

**A PM threshold crossing has occurred at *slot number, port number* in *switch name* (PM threshold object).**

This trap (ID=109) indicates that a threshold crossing was detected on the specified physical port on the specified slot on the specified switch for the performance parameter identified by the PM threshold object. This may indicate a physical layer problem with the port or the transmission media carrying the signal.

**At *slot number, port number* in *switch name* the protection line is now *state.***

This trap (ID = 118) indicates that a protection switching (APS) event has just taken place on the specified port on the specified slot on the specified switch.

**At *slot number, port number* in *switch name* the specified working line has resumed carrying user traffic.**

This trap (ID = 119) indicates that the specified working line physical port (APS related) on the specified slot on the specified switch has resumed carrying user traffic. This may be due to an auto switch condition that has cleared or due to a problem detected on the protection line.

**At *slot number, port number* in *switch name* a mode mismatch has been detected.**

This trap (ID = 120) indicates that a mode mismatch has been detected based on this pport's APS configuration and the received K2 byte. This happens when one LTE is configured for 1+1 APS and the other for 1:n APS. The LTE configured for 1:n will fall back to 1+1 mode.

**At *slot number, port number* in *switch name* the protection line is now in a failed state.**

This trap (ID = 121) indicates that the protection line is now in a failed state. APS switch-over to protection is now inhibited. If the protection line was carrying user traffic, it is switched back to the working line.

**At *slot number, port number* in *switch name* the protection line is now in an operational state.**

This trap (ID = 122) indicates that the protection line is now in an operational state. APS switchover to protection is now possible.

**At *slot number, port number* in *switch name* the protection line has declared a protection.**

This trap (ID = 123) indicates that the protection line has declared a protection byte failure. This happens when a protection byte defect or inconsistent K1 byte is received and the condition persists for 2.5 seconds. APS switchover to protection is inhibited. If the protection line was carrying user traffic, it is switched back to the working line.

**At *slot number, port number* in *switch name* a far end protection line failure has been declared.**

This trap (ID = 124) indicates that a far end protection line failure has been declared. This happens when the received K1 byte indicates SF on the protection line and the condition persists for 2.5 seconds.

**At *slot number, port number* in *switch name* the far end protection line failure has cleared.**

This trap (ID = 125) indicates that the far-end protection line failure has cleared. This happens after 10 seconds without an indication of SF on the protection line in the received K1 byte.

**At *slot number, port number* in *switch name* a channel mismatch has been detected.**

This trap (ID = 126) indicates that a channel mismatch has been detected. When the pportAPSconfigStatus is indicated as invalid, the user should check pportAPSadminDir, pportAPSlineType, pportAPSrevertiveMode, and pportAPSwtrPeriod for a mismatched configuration between the two physical ports.

**At *slot number, port number* in *switch name* the APS configuration status has changed to *new status*, the paired-with APS pport at *slot number, port number*.**

This trap (ID = 127) indicates that the APS configuration status has changed. When the pportAPSconfigStatus is indicated as invalid, the user should check pportAPSadminDir, pportAPSlineType, pportAPSrevertiveMode, and pportAPSwtrPeriod for a mismatched configuration between the two pports.

**At *slot number, port number* in *switch name* a direction mode mismatch has been detected.**

This trap (ID = 131) indicates that a direction mode mismatch has been detected on the indicated pport (the indicated pport is an APS protection line pport). This happens when one LTE is configured for Unidirectional and the other for Bidirectional mode.

***Circuit name* at *switch name* is *state* with *fail reason* (FailNode: *node ID*, FailPort: *lport IF index*).**

This trap indicates the specified point-to-point ATM PVC on the specified switch has changed state. The possible states for the circuit include active, inactive, and invalid. When the circuit is inactive, the reason it went inactive is provided in the fail reason portion of the message. The node where the failure occurred is also indicated (the last 2 octets of the internal node ID is provided) along with the interface (IF) index of the logical port where the failure occurred. Use the Show All Logical Ports dialog box to determine the mapping between logical port names and IF indexes.

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 name* at *switch name* has been re-routed.

This trap (ID=21) indicates that an ATM PVC has been re-routed.

#### CUG: Configuration error for *prefix name* on *switch name.*

This trap (ID=95) indicates a run-time configuration error on the number of CUGs allowed per address.

#### CUG: Configuration error for *address name* on *switch name.*

This trap (ID=94) indicates a run-time configuration error on the number of CUGs allowed per address.

#### CUG: Configuration error for *node prefix name* on *switch name*

This trap (ID=96) indicates a run-time configuration error on the number of CUGs allowed per node prefix.

**DS1 at *channel number, port number, slot number*, *switch name* has changed loopback state to *state.***

This trap (ID=97) indicates when the DS1 has changed its current loopback state.

The loopback state can change to one of the following:

- ds1ClearLoop (1)
- ds1PayloadLoop (2)
- ds1LineLoop (3)
- ds1DiagLoop (4)

***Fan number* at *switch name* is *state.***

This trap indicates that the specified fan in the specified switch has changed state to either up, down, or marginal.

**In *switch name* the time server fails to respond and no other time server is available.**

This trap (ID = 128) indicates that a time server fails to respond and no other time server is available. If the error occurs on power up it shall be reported as critical; otherwise it shall be reported as a warning.

***Lport name* in s*witch name* is down, following PVCs are also down: *circuit name list*.**

The specified logical port is down; as a result, the specified circuits are also down.

***Lport name* in s*witch name* is up, following PVCs are also up: *circuit name list*.**

The specified logical port is now active; as a result, the specified circuits are now active.

***Lport name* in s*witch name* has *congestion rate* % (exceeded threshold threshold %).**

The specified logical port is congested (threshold %).

**Point-to-multipoint ATM PVC Status changed (*switch name*, Src interface:*number*, VPI:*number* VCI:*number*, End Index:*number* ) Ckt Leaf Oper Status:*status* Ckt leaf Fail reason:*reason* Ckt Leaf Fail Node:*node* Ckt Fail Port:*port number.***

This trap (ID=116) indicates that the point-to-multipoint ATM PVC state has been changed

**Power supply *number* at *switch name* is *state.***

This trap (ID=113) indicates the specified chassis power supply in the specified switch has changed state.

**PPort *switch name, slot number, port number* is *state* with *alarm type.***

The specified physical port on the specified IOM slot on the specified switch has changed state. Possible state values for the physical port are Up, Down, or Testing. Possible values for the alarm type are as follows:

- None (0) - No alarm condition.
- Red (1) - A loss of signal or out of frame error.

An out of frame error occurs when the receiver detects one of the following conditions:

- Two or more framing-bit errors within a 3 millisecond period.
- Two or more errors within five or fewer consecutive framing bits.

A loss of signal error occurs if the device detects 175+/-75 contiguous pulse positions of either positive or negative polarity.

After declaring a Red Alarm, the device sends a Yellow Alarm Signal to the far-end. The far-end then declares a Yellow Alarm.

- Yellow (2) – A remote CSU is transmitting a Red Alarm. The remote CSU is not receiving any transmission signals from your circuit and the circuit is acting as a one-way link.
- Blue (4) – A keep-alive condition exists. This condition occurs when the T1 multiplexer fails or is disconnected and the CSU sends continuous unframed 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, "Setting and Monitoring Loopbacks" for more information about loopbacks.

#### ***PPort*** **at** ***switch name, slot number, port number*** **has mismatched interface type (actual: interface, configured: interface).**

This trap (ID=22) indicates the actual physical interface is different than the configured physical interface.

#### ***Pport number*** **on** ***slot number***, ***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.

#### **Power supply #3 at** ***switch name*** **has changed state to** ***power supply status.***

This trap indicates power supply #3 has changed state (toggled between up and down states). Power supply status values include the following:

- up (1)
- down (2)
- marginal (4)

### ***PRAM filename* download to *switch name* is complete.**

The download of the specified file from the NMS to the specified switch is complete. This trap should follow any PRAM synchronization attempt that the user performs from the NMS.  Note that the affected SP or IOM still must complete the automatic post-download warmboot before returning to full operation.

### ***PRAM filename* download to *switch name* has failed.**

The download of the specified file from the NMS to the specified switch has failed. This trap may follow a PRAM synchronization attempt that the user performs from the NMS if the file download is unsuccessful for any reason.  If this occurs, the PRAM synchronization should be reattempted.

### ***Slot number* in *switch name* did not respond to the poll from the CP/SP.**

This trap indicates that the IOM or SP in the specified slot in the specified switch has stopped responding to polls from the CP or SP.  This may be an indication of a problem with the IOM as under normal conditions, the IOM or SP should always respond to a poll from the CP or SP.  This trap will occur anytime a card is either warm or cold booted and may occur during heavy congestion of the IOM CPU.

### ***Slot number* in *switch name* has just come up.**

This trap indicates that the IOM or SP in the specified slot in the specified switch has started to respond to polls from the CP or SP.  This trap normally occurs after an IOM or SP has completed its reboot cycle.

### ***Slot number* in *switch name*, *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 inService (1), outOfService (2).

### ***Slot number* at *switch name* transmit clock synchronization has changed state to *synchronization status*.**

The IOM transmit clock PLL synchronization status has changed.

***Slot number* at *switch name* primary clock reference has changed state to *primary clock status*.**

The IOM system primary clock reference status has changed. Status values are normal (1) and failure (2).

***Slot number* at *switch name* secondary clock reference has changed state to *secondary clock status.***

The IOM system secondary clock reference status has changed. Status values are normal (1) and failure (2).

***Slot number* at *switch name* transmit clock synchronization has changed state to *PLL synch status.***

This trap indicates the IOM transmit clock synchronization status has changed. The PLL synch status variable indicates the transmit clock PLL synchronization status of the card.

***Slot number* at *switch name* clock reference has changed state to *sys primary clk status.***

Indicates that the IOM system primary clock reference has changed to the specified system primary clock status as detected on the card. The sys primary clk stat variable can be either normal (1) or failure (2).

***Slot number* at *switch name* secondary clock reference has changed state to *system secondary clk status*.**

Indicates that the IOM system secondary clock reference status has changed to the specified system secondary clock status as detected on the card. The system secondary clk stat value can be either normal (1) or failure (2).

**SVC failure threshold has been exceeded on *Lport name* at *switch name.***

This trap indicates that the number of SVC failures that have occurred on the specified lport on the specified switch has exceeded the provisioned threshold. The default value of this threshold hold is 1 failure every 15 minutes (meaning that if 1 failure occurs in a 15 minute period, this trap will be displayed). If more than one failure occurs, another trap will not be displayed for another 15 minutes. Use the Show All Failed SVCs dialog box for specific information about the failures.

***SW filename* download to *switch name* is complete.**

This trap indicates that an NMS initiated download of the specified software file to the specified switch has succeeded and is now complete.

***SW filename* download to *switch name* has failed.**

This trap indicates that an NMS initiated download of the specified software file to the specified switch has failed. If this occurs, the user should reattempt the download.

***Switch 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 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 name* interface state (SNMP linkDown trap) on *lport name.***

The sending protocol entity recognizes a failure in one of the communication links in your network configuration. The following conditions cause this trap to occur:

- The Admin Status of a physical port was set to down.
- The Admin Status of a logical port was set to down.
- A physical port has lost its input modem signals.
- An IOM was removed.

- An active optimum trunk had a status change and is now inactive.
- An active ATM virtual circuit had a status change and is now inactive.
- An active T3 channel had a status change and is now inactive.
- An active SLIP connection had a status change and is now inactive.
- A timeout was detected on an ethernet line.
- A persistent transmit stall was detected on a physical port.
- An active trunk received no response to five consecutive Keep Alive messages.
- An active trunk received an incorrect response to a Keep Alive message.
- An active trunk received a logical down response to a Keep Alive message.

#### ***Switch name*** **interface up (SNMP linkUp trap) on** ***lport name.***

The sending protocol entity recognizes that one of the communication links represented in your network configuration has become active. The following conditions cause this trap to occur:

- The Admin Status of a physical port was set to up.
- The Admin Status of a logical port was set to up.
- A physical port has recovered its input modem signals.
- An IOM which was removed is now active.
- An inactive optimum trunk had a status change and is now active.
- An inactive ATM virtual circuit had a status change and is now active.
- An inactive T3 channel had a status change and is now active.
- An inactive SLIP connection had a status change and is now active.
- An inactive ethernet line is now active.

#### *Switch name*: Incorrect community *name* (SNMP authentication failure trap).

The sending protocol entity has received a protocol message that is not properly authenticated.

#### *Switch name*: EGP neighbor down (SNMP egpNeighborLoss Trap) for neighbor ifIndex egpNeighAddr.

An EGP neighbor is down.

#### *Switch name* is reachable.

This trap indicates that the specified switch is now reachable by the NMS.

#### *Switch name* is unreachable.

This trap indicates that the specified switch is no longer reachable by the NMS.  If this occurs, you should verify that the connectivity between the NMS workstation and the switch (Ethernet or ATM) is intact and functioning (i.e. try using an NMS workstation to **ping** the switch).

#### *Switch name* trace table full.

This trap (ID=11) indicates the node trace table was full and, for this reason, was copied to a TFTP buffer that will be transferred to the NMS.

#### *Switch name* diagnostic log table full.

This trap (ID=12) indicates the diagnostic log table was full and, for this reason, was copied to a TFTP buffer that will be transferred to the NMS.

#### *Switch name* checksum error or battery problem occurred in PRAM.

This trap (ID=13) indicates a checksum error or battery problem occurred in the PRAM.

### ***Switch name*** **fatal internal error encountered and system needs to be rebooted.**

This trap (ID=16) indicates the system encountered a fatal internal hardware or software error. Reboot the system in order to correct this problem.

### ***Switch name*** **IO error occurred in DRAM or SRAM.**

This trap (ID=15) indicates an I/O error occurred in DRAM or in SRAM.

### ***Switch name*** **non fatal error report: Slot=*slot number*, Src=*source*, Time=*time*, Major=*major errcode*, Minor=*minor errcode*, String=*ASCII string*.**

This trap (ID=24) indicates a component in the switch discovered a non-fatal error condition in the specified slot. Possible values for the source variable are:

- power-on diagnostics (1)
- background-diagnostics (2)
- fault (3)
- frame-heap (4)

The time variable indicates the time that the last non-fatal error was reported. The major error code variable indicates the major error code of the last non-fatal error. The minor error code variable indicates the minor error code of the last non-fatal error. The ASCII string variable indicates the ASCII string that describes the last non-fatal error.

***Switch name* primary synchronization reference operational state has changed to *primary clock synchronization reference*.**

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values include the following:

- externala (1) – T1 Rate External Clock 1
- externalb (2) – T1 Rate External Clock 2
- portrefa (3) – IOM Port Reference Clock 1
- portrefb (4) – IOM Port Reference Clock 2
- internal (5) – Internal Free Running Clock

***Switch name* secondary synchronization reference operational state has just changed to *primary clock synchronization reference.***

Specifies that the Primary Synchronization Reference operational state has changed to the specified primary clock synchronization reference. Possible values for the Primary Synchronization Reference include the following:

- externala (1) – T1 Rate External Clock 1
- externalb (2) – T1 Rate External Clock 2
- portrefa (3) – IOM Port Reference Clock 1
- portrefb (4) – IOM Port Reference Clock 2
- internal (5) – Internal Free Running Clock

### ***Switch name*** **external reference clock *number* operational state has just changed to *state.***

This trap indicates that the specified external reference clock (the T1 or E1 clock wired to the back of the switch SPA) has changed state on the specified switch has changed state.  The following states are possible:

- Active –The clock has been restored and is operational
- Detected Loss of Signal – The clock signal is no longer present
- Detected AIS Alarm – An AIS alarm has been received on the external clock port
- Detected Loss of Frame – The framing has been lost on the received signal

### ***Switch name*** **port reference clock 1 operational state has just changed to *current state port reference clock A.***

The port reference clock 1 operational state has changed to the current state of port reference clock A. Possible states include the following:

- active (1) – Valid
- down (2) – Invalid

### **Switch to Accounting Server communication for *service number* has failed and a usage file transfer has failed to complete.**

This trap (ID=98) indicates that switch to Accounting Server communication has failed and that a usage file transfer has failed to complete.

### **Switch to ATM Bulk Statistics Server communication has failed for *switch name* (Server Address = number).  A usage file transfer has failed to complete. Switch-to-Server communication failures have occurred during the day.**

This trap (ID=111) indicates that switch to ATM Bulk Statistics Adjunct Processor communication has failed and that a data file transfer has failed to complete.

**The NDC Threshold has been crossed (*switch name*, *interface number*, *source DLCI number*) with Incoming Discarded CLP0 Cells = *number* for the associated threshold value of *value*.**

This trap is a Network Data Collection Threshold Crossing Alarm for the number of CLP0 cells discarded in a PVC on an IOM. It is generated not more than once within the 15-minute NDC measurement interval.

**The NDC Threshold has been crossed (*switch name*, interface number, source DLCI number) with Incoming Discarded CLP0+1 Cells = *number* for the associated threshold value of *value.***

This trap (ID=100) indicates a Network Data Collection Threshold Crossing Alarm for the number of CLP0+1 cells discarded in a PVC on an IOM. It is generated not more than once within the 15-minute NDC measurement interval.

**The time on the *switch name* has changed spanning a second boundary.**

This trap (ID = 129) indicates that the time on the switch has changed spanning a second boundary.

**The LPort NTM Congestion status of *interface index* at *switch name* has changed to severe congestion status.**

This trap (ID=99) indicates that there is a change of congestion status on a logical port on an IOM. Possible values for the severe congestion status include the following:

- Not congested (1)
- Congested (2)

**The specified PVC has been rerouted.**

The specified PVC was rerouted.

**The stand-by card in *slot number* at *switch name* has become the active card.**

This trap (ID=33) indicates 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 name* at *switch name.***

Notification that the status of the ATM signaling function has changed on the logical port. Status indicates the operational status of this function on the specified port.

**The status of the ATM ILMI function has changed to *state* on *Lport name* at *switch name.***

This trap (ID = 138) indicates that the ATM ILMI function has changed state for the specified logical port on the specified switch. This trap will only occur if the ILMI option on the logical port has been set to enabled. The following states are possible:

- Up – Indicates that the logical port is successfully exchanging ILMI poll traffic between the switch and the attached device.
- Down – Indicates that the logical port is no longer successfully exchanging ILMI poll traffic between the switch and the attached device. The logical port statistics screen can be used to help determine the specific cause of this problem.

**The status of the ATM signalling function has change to *state* on *LPort name* at *switch name.***

The ATM UNI or NNI signalling function has changed state for the specified logical port on the specified switch.  This trap will only occur if the signalling option on the logical port has been set to enabled.  The following states are possible:

- Up – Indicates that the logical port is successfully exchanging Q.SAAL traffic (for UNI signalling) between the switch and the attached device.
- Down – Indicates that the logical port is no longer successfully exchanging Q.SAAL traffic between the switch and the attached device.  The logical port statistics screen can be used to help determine the specific cause of this problem.
- Connecting – Indicates that the logical port is transmitting Q.SAAL traffic to the attached device but is not receiving any response from the attached device.  The logical port statistics screen can be used to provide additional information.

**The time-of-day clock on *switch name* is invalid or has not been configured.**

This trap (ID = 117) indicates that notification that the time-of-day clock on the specified switch is invalid or has not been configured.  This trap is generated only at SP boot-time.

**Trunk *trunkname* in *switch name* is down. Following PVCs are also down: *circuit name list*.**

The specified trunk is down; as a result, the specified circuits are also down.

### ***Trunk name* at *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)
- nfull (7)

### ***User name* has logged on to *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 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).

# B

# Summary of Error Codes

Table B-1 on page B-2 summarizes the major and minor error codes. Refer to "Background Diagnostics" on page 3-2 for instructions on displaying these error codes.

*An asterisk (*) appears after the Major Error Number to indicate that additional information about the error is included in the 960 trace area. If any of these errors occur on your system, contact the TRC at* **1-800-DIAL-WAN (1-800-342-5926)**. *Your TRC Representative can create a dump of the 960 trace area to determine the cause of the error.*

*This table also specifies those error numbers that indicate fatal error conditions. For fatal error conditions,* ***call the TRC.This manual does not describe how to resolve fatal errors.***

**Table B-1. Summary of Error Codes**

| Major Error | Minor Error | Fatal? | 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 switch processor (SP) or there is an internal software problem.<br><br>To resolve, configure the I/O slot and reinitialize the switch. Refer to the *Network Configuration Guide for CBX 500* for more information about initializing the switch. Call the Technical Response Center for assistance. |
| 2 - 16 | See Explanation | Non-Fatal | Link-stall detection. Transmit completions stalled. This error occurs when the switch cannot transmit because there is no clock present on the outbound interface. The major error number indicates the slot number, and the minor error number indicates the port number.<br><br>To resolve, check the physical port configuration, particularly the IOM attributes. Refer to the *Network Configuration Guide for CBX 500.* Specify the clock configuration if there is no clock present. |
| 3.2 | See Explanation | Fatal | When this error appears on an SP card, it indicates a warm boot has occurred. This is an informational error message and it requires no intervention. |
| 4 | See Explanation | Fatal | Indicates chain corruption in a memory block. Call the TRC for assistance. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 5 | See Explanation | Fatal | Indicates a fatal error that you cannot resolve without assistance. Call the TRC. |
| 20* | 0 | Fatal | Interrupt vectors corrupted. Call the TRC. |
| 21* | See Explanation | Fatal | 960 SRAM corrupted. The minor error number is the pointer to the bad SRAM location. Call the TRC. |
| 22* | 0 | Fatal | Fault table corrupted. Call the TRC. |
| 23 | 0 | Fatal | Interrupts disabled. Call the TRC. |
| 24 | 1 | Fatal | Processor kernel force bad parity bit is on. Call the TRC. |
| 24 | 2 | Fatal | IOM force bad parity bit is on. Call the TRC. |
| 25 | 0 | Fatal | OS counter/timer is disabled. Call the TRC. |
| 26* | See Explanation | Fatal | Stack overflowed. The minor error number specifies the ID of the corrupted stack. Call the TRC. |
| 30* | 2 | Fatal | Heap error — invalid heap header on free. Call the TRC. |
| 30* | 3 | Fatal | Heap error — out of memory on allocate. Call the TRC. |
| 30 | 4 | Fatal | Heap error — heap corrupted. Call the TRC. |
| 31 | 1 | Non-Fatal | PRAM initialized. This error is caused by resetting the PRAM.<br><br>To resolve, resynchronize the PRAM in the card. Refer to the *Network Configuration Guide for CBX 500*. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 31 | 2 | Non-Fatal | PRAM corrupted.<br><br>To resolve, resynchronize the PRAM in the card. Refer to the *Network Configuration Guide for CBX 500*. |
| 32 | 0 | Fatal | SRAM code space corrupted. Call the TRC. |
| 33 | 0 | Fatal | IRAM code space corrupted. Call the TRC. |
| 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.<br><br>To resolve, resynchronize the PRAM in the card. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| 35* | 0 | Fatal | 960 fault 1. Call the TRC. |
| 36* | 0 | Fatal | 960 fault 2. Call the TRC. |
| 37* | 0 | Fatal | 960 fault 3. Call the TRC. |
| 38* | 0 | Fatal | 960 fault 4. Call the TRC. |
| 39* | 0 | Fatal | 960 fault 5. Call the TRC. |
| 40* | 0 | Fatal | 960 fault 6. Call the TRC. |
| 41* | 0 | Fatal | 960 fault 7. Call the TRC. |
| 42* | 0 | Fatal | 960 fault 8. Call the TRC. |
| 43* | 0 | Fatal | 960 fault 9. Call the TRC. |
| 44* | 0 | Fatal | 960 fault 10. Call the TRC. |
| 46 | 0 | Fatal | Parity error — IRAM (3000/6000). Call the TRC. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 47 | 0 | Fatal | Parity error — FMEM (3000/6000). Call the TRC. |
| 48 | 0 | Fatal | FMEM self test failure. Call the TRC. |
| 49 | 0 | Fatal | Initialization error — device tables (3000/6000). Call the TRC. |
| 50 | 0 | Fatal | Initialization error — bd out heap (3000/6000). Call the TRC. |
| 51 | 0 | Fatal | Initialization error — bd in heap (3000/6000). Call the TRC. |
| 52 | 0 | Fatal | Initialization error — bd initialization (3000/6000). Call the TRC. |
| 55 | 0 | Fatal | Ethernet driver error. Call the TRC. |
| 56 | 0 | Fatal | Fatal internal error. Call the TRC. |
| 57 | 0 | Fatal | Obsolete |
| 58 | 0 | Fatal | Circular virtual circuit list on the rate enforcement queue. Call the TRC. |
| 59 | 0 | Fatal | Obsolete |
| 128 | 0 | Fatal | Cannot download bus. Call the TRC. |
| 129 | 0 | Fatal | Warm boot. Call the TRC. |
| 130 | 0 | Fatal | Cold boot. Call the TRC. |
| 132 | 0 | Fatal | The standby side of a redundant pair is shooting the active side. Call the TRC. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 133 | 0 | Non-Fatal | The PRAM is in conflict; PRAM is configured for another node. Each node has a unique ID. A card configured for one switch is now in use in a different switch.<br><br>To resolve, resynchronize the PRAM in the card. Refer to the *Network Configuration Guide for CBX 500*. |
| 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.<br><br>To resolve, reactivate the card by setting the Admin Status field to Up on the Modify Logical Port dialog box. Refer to the *Network Configuration Guide for CBX 500* for more information. |
| 135 | 0 | Non-Fatal | Unused. |
| 136 | 0 | Fatal | The NMS caused a redundant switchover. This is a normal NMS procedure. |
| 137 | See Explanation | Fatal | Illegal interrupt vector. This condition could be caused by either a software or hardware problem. The minor error number specifies the vector code. Call the TRC. |
| 138 | 0 | Fatal | Proxy message from the wrong card. Call the TRC. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 144 | 0 | Non-Fatal | A standby card is using a different version of the software. This error code indicates that the software revisions on the standby and active cards do not match. This is a warning condition and will not cause an interrupt in service. However, if you have to switch to the standby card, the older software revision may not support some features you are using on the active card.<br><br>To resolve, update the standby card with the new software. |
| 145 | 0 | Fatal | IOM configured for MULTI. Call the TRC. |
| 146 | 0 | Fatal | Card service change. Call the TRC. |
| 147 | 0 | Fatal | Some I/O to PRAM failed. Call the TRC. |
| 148 | 0 | Fatal | One of the SPs in a redundant pair of SPs is incapable of the requested admin capability. Call the TRC. |
| 149 | 0 | Non-Fatal | A standby SP card type is incapable of a requested administrative task. This error code indicates that the standby model type does not match the active model type. This is a warning condition and will not interrupt service. However, if you have to switch to the standby model type, the older version may not support some features you are using on the active type.<br><br>To resolve, replace the standby SP card type so that it matches the active SP type. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 149 | 1 | Non-Fatal | A standby SP card type is incapable of a requested admin capability, however, the system allowed the admin change to be made. This warning condition will not interrupt service. However, if you have to switch to the standby SP card type, the older version may not support some features that you are using on the active card.<br><br>To resolve, replace the standby SP card type so that it matches the active SP card. |
| 149 | 2 | Non-Fatal | A standby SP card type is incapable of a requested admin capability or SNMP set specified an invalid type. This condition is a warning condition and will not cause an interrupt in service. However, if you have to switch to the standby SP card type, the older version may not support some features that you are using on the active card type.<br><br>To resolve, replace the standby SP card type so that it matches the active SP card. |
| 149 | 3 | Non-Fatal | The active IOM cannot perform a requested operation capability. For example, an SMDS request could have been made for a card that is for Frame Relay only.<br><br>To resolve, replace the IOM with the correct card type. |
| 149 | 4 | Non-Fatal | The standby IOM cannot perform a requested operation capability.<br><br>To resolve, replace the standby card with the correct card type at your earliest convenience. |

**Table B-1. Summary of Error Codes (Continued)**

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 150 | 1 | Fatal | OSPF error — RTR Link State Address (LSA) is too big. Call the TRC. |
| 150 | 2 | Fatal | OSPF error — No LSA in the age bin. Call the TRC. |
| 150 | 3 | Fatal | OSPF error — Link State (LS) database is corrupted. Call the TRC. |
| 150 | 4 | Fatal | OSPF error — Bad LSA in NBR queue. Call the TRC. |
| 150 | 5 | Fatal | OSPF error — Bad LSA in NBR2 queue. Call the TRC. |
| 150 | 6 | Fatal | OSPF error — LSA not found. Call the TRC. |
| 150 | 7 | Fatal | OSPF error — NBR not found. Call the TRC. |
| 150 | 8 | Fatal | OSPF error — Error in timer queue. Call the TRC. |
| 150 | 9 | Fatal | OSPF error — Bad LSA in send Link State Uppath (LSU). Call the TRC. |
| 150 | 10 | Fatal | OSPF error — Duplicate Autonomous System Entry (ASE). Call the TRC. |
| 150 | 11 | Fatal | OSPF error — No areas. Call the TRC. |
| 150 | 12 | Fatal | OSPF error — Bad VL. Call the TRC. |
| 150 | 13 | Fatal | OSPF error — No BB Ifs. Call the TRC. |
| 150 | 14 | Fatal | OSPF error — No BB. Call the TRC. |
| 150 | 15 | Fatal | OSPF error — No memory. Call the TRC. |
| 150 | 16 | Fatal | OSPF error — Bad receive packet. Call the TRC. |

Table B-1. Summary of Error Codes (Continued)

| Major Error | Minor Error | Fatal? | Explanation |
|---|---|---|---|
| 151 | 1 | Fatal | OSPF error — Console logging errors. Call the TRC. |
| 152 | 0 | Fatal | Permanent Virtual Circuit (PVC) manager errors. Call the TRC. |
| 153 | 0 | Non-Fatal | Virtual circuit table errors; buffer limit reached. There are too many PVCs defined between two logical ports.<br><br>To resolve, check the network configuration and reroute some PVCs. Refer to the *Network Configuration Guide for CBX 500* for more information about how to configure PVCs. |
| 154 | 1 | Fatal | Fatal internal error. Call the TRC. |
| 154 | 2 | Fatal | The card cannot read the configuration. Call the TRC. |
| 155 | See Explanation | Fatal | Memory protection NMI. Call the TRC. |
| 156 | 0 | Non-Fatal | System timing reference problem.<br><br>To resolve, check the source(s) for the system timing reference (refer to the *Network Configuration Guide for CBX 500*). Make sure the timing source is properly configured and functional.<br><br>If you cannot resolve the problem, contact the TRC for assistance. |

C

# 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 console remembers the last ten commands that you enter. ^B can be used to recall previous commands as needed.*

# Console Commands

Table C-1 provides a summary of all Console Commands.

**Table C-1. Console Commands**

| Command | Description |
|---|---|
| Press BREAK to log in to console | The first command you see |
| CBX-500 (nodename)<br>login:<br>password: | The login procedure |
| CBX-500 Configuration Console | The Console Header |
| Name: | Switch name as shown in NMS |
| Location: | Location as entered on Set Switch Attributes dialog box. |
| Model: CBX-500 | Switch chassis serial number. |
| Serial#<br>SW Rev:<br>> | Version of SP application code running in the active SP. |
| get <oid string> | SNMP get |
| enable | Go into master mode |
| exit, end, bye, logout, quit | Exit from console |
| help | Displays help message |
| > Idle log out | Appears when you have not used the console for a few minutes (timeout value depends on the setting from the Set Switch Attributes dialog box). |
| next <oid string> | SNMP next |
| ping <ip address> | ICMP ping (page C-7) |

**Table C-1. Console Commands (Continued)**

| | |
|---|---|
| reset pvc | Sets the Admin status down and then up to quickly reset the PVC. Can only be used in debug mode. (page C-7) |
| reset svc statistics | Resets the SVC statistics counters (page C-7) |
| >>set debug password | Old password:<br>New password:<br>Verify new password:<br>Debug password has been changed (page C-8) |
| show ? | Displays parameters. |
| show atmizer | Displays summary statistics for SP ATMizer. |
| show atmizer all | Displays detailed statistics for SP ATMizer. |
| show billing | Displays the ATM billing administrative and operational state (page C-8) |
| show card <slot_number> | Displays a card configuration (page C-9) |
| show community | Displays community name parameters (page C-9) |
| show dump file | Display the dump file contents (page C-10) |
| show external | Displays OSPF Autonomous System Externals (ASE) such as the static routes in OSPF (page C-11) |

**Table C-1. Console Commands (Continued)**

| | |
|---|---|
| show hardware | Displays manufacturing part numbers, revision information, and serial numbers for IOMs in a switch. (page C-11) |
| show icmp | ICMP statistics (page C-12) |
| show ip | IP statistics (page C-13) |
| show lport<br>attributes <interface><br>statistics <interface> | Displays logical port statistics and attributes (page C-14, page C-15) |
| show ntp | Network timing protocol configuration and status (page C-15) |
| show ospf adv [link type] [internal ip] | Displays a specified link-state advertisement (page C-16) |
| show ospf database | Displays a link-state database, one per line per each LSA (page C-17) |
| show ospf interface | Shows the state of all OSPF trunks (page C-18) |
| show ospf mcpath | Displays the path that a point-to-multipoint virtual circuit will take, with circuit parameters specified by the user. (page C-18) |
| show ospf namedpath | Shows the routing table for resilient names (page C-19) |
| show ospf names | Displays a line for every name known to the switch. Names can be Resilient UNI/NNI names, E.164 addresses, and NSAP addresses. (page C-20) |

**Table C-1. Console Commands (Continued)**

| | |
|---|---|
| show ospf pathdb | Displays all paths, or those paths going through a given trunk, present on a particular card. (page C-21) |
| show ospf qospath | Shows the QoS path (page C-21) |
| show ospf route | Shows the OSPF routing table (page C-22) |
| show ospf statistics | Displays OSPF statistics (page C-22) |
| show ospf trunk | Displays OSPF trunk statistics (page C-23) |
| show ospf vcpath [destination internal ip address] | Displays the virtual circuit path (page C-23) |
| show ospf vcroute | Displays the route a virtual circuit will take (page C-24) |
| show pport<br>statistics <slot.port><br>attributes <slot.port> | Displays physical port statistics and attributes (page C-25) |
| show pram | Displays information about the contents of the parameter RAM (PRAM) files for SPs and IOMs on the PCMCIA disk (page C-26) |
| show pvc<br>attributes <interface.dlci><br>statistics <interface.dlci> | Displays PVC statistics and attributes (page C-30) |
| show rip statistics | Displays information about the routing information protocol statistics (page C-30). |
| show software | Displays all cards and the software information for them (page C-31) |

**Table C-1. Console Commands (Continued)**

| | |
|---|---|
| show software flash | Displays software versions in the SP(s) Flash memory (page C-32) |
| show system | Shows general system information and status (page C-32) |
| show svc statistics <interface> | Displays information about SVC statistics (page C-33) |
| show tcp | TCP statistics (page C-34) |
| show tproto | Trunk protocol information (page C-35) |
| show trap | Trap queue counts and dropped traps (page C-36) |
| show udp | UDP statistics (page C-36) |
| show users | Displays current users logged into the switch through console or telnet (page C-37) |
| synchronize svc statistics <interface> | Sets the minimum and maximum objects to the actual (current) value (page C-37) |

# Console Command Examples

The following pages list each of the console commands along with an example.

## ping

Seeks a response from another network device.

```
> ping 192.9.200.22
```

Reply in < 100 ms

## reset pvc [interface.vpi_vci]

If you enable debug mode, you can use this command to set the PVC's Admin Status value to down and then up. This quickly resets the PVC. Use the interface index (ifnum) of the logical port endpoint and a concatenated vpi/vci value to specify the circuit. To calculate the vpi_vci value:

1. Multiply the vpi by 65536.
2. Add the vci to this value.

```
# reset pvc [interface.vpi_vci]
```

## reset svc statistics [interface]

This command resets all counters to zero. If bulk statistics is enabled, there will be an automatic "synchronize" every 15 minutes. You should disable bulk statistics *before* running this command.

```
# reset svc [interface
```

## set debug password

Changes the debug password. You must first enter debug mode.

```
> set debug password

Old password:
New password:
Verify new password
Debug password has been changed
```

## show billing

This command displays the ATM billing administrative and operational state.

```
> show billing

Billing System Manager State: Running

ATM Billing -- Administrative state  : enabled
                 Operational state   : enabled

        Primary Accounting Server    : 152.148.81.129
        Secondary Accounting Server  : 0.0.0.0
        Accounting Server Control    : Primary
        Accounting Server Comm State : Green

       Snapshot Period ends        : 4 min 24 sec (21:19:56 - 21:24:55)

        File transfer successes      :        12
        File transfer failures       :         0
        File transfer retries        :         0
        Average billing data rate    :         1 bps
              Burst data rate --min :     93151 bps
                                avg :     234650 bps
                                max :     540526 bps

        Bulk stats TFTP successes    :         0
        Bulk stats TFTP failures     :         0
        Average bulk stats data rate :         0 bps
              Burst data rate --min :        -1 bps
                                avg :         0 bps
                                max :         0 bps
```

```
Disk-recovery write successes:          0
Disk-recovery write failures :          0
Disk-recovery read successes :          0
Disk-recovery read failures  :          0
```

## show card [*slot number*]

This command displays information about the serial number, hardware, EPROM, software revisions, and status.

```
>show card (slot number)

Serial#:                 012345    Configured Card Type:        DS1-8
Hardware Revision:                  Actual Card Type:            DS1-8
EPROM Revision:        01.00.00.00    Physical Slot:                 3
Software Revision:      02.00.00.00    Logical Slot:                 3
Actual IOA Type:    8 prt T1 120 ohm

Redund State:                  Active
Card State:                  Active    Memory Available:       5178544
Administrative Status:           Up    CPU Utilization:             2%
Operational Status:                Up
Diagnostics Status:                Up
```

## show community

This command displays community names and associated IP addresses.

```
## show community

0       constitution    152.148.81.20
        MIB: 0x00 Severity: 0x00 Enterprise:
        00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00
        00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
1       public
2       roamer          201.201.201.111
        MIB: 0x00 Severity: 0x00 Enterprise:
        01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
3       cascade
4       bud             152.148.81.125
        MIB: 0x00 Severity: 0x00 Enterprise:
```

```
        01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
5       undefined
6       undefined
7       undefined
8       undefined
9       undefined
10      undefined
11      undefined
12      undefined
13      undefined
14      undefined
15      undefined
```

## show dump file

This command displays the dump file contents.

```
> show dump file
```

```
                  Failed                                        Keep
SP      File     Card    Store Time                          Dump    Activity

1        1        13       Tue Jan 02 01:31:30 1996             Y
1        2        15       Sun Jan 21 07:48:30 1996             Y
1        3        15       Mon Jan 01 00:17:40 1996             Y

2        1        13       Mon Jan 01 01:12:59 1996             Y
2        2        6        Mon Jan 01 00:18:30 1996             Y
2        3        6        Mon Jan 01 00:17:50 1996             Y
```

## show external

This command displays OSPF Autonomous System Externals (ASE), 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

This command displays the manufacturing part numbers, revision information, and serial numbers for all populated IOMs and IOAs in the switch.

```
> show hardware
```

```
## show hardware
Slot        Product Code        MFG. #      H/W Rev.        S/N
1                  11020 810-00038-01             02   A0000323
1   IOA               23     00111-02             1A       5004
8                  11030 810-00051-02             00   A0000022
8   IOA            11031 810-00139-01             00   A2105824
12                 11058 810-00058-01             01   A0000309
12  IOA               41     00041-01             0A      04655
##
```

## show icmp

This command displays ICMP statistics.

```
> show icmp
```

```
                       Receive      Transmit
Messages:              142          201
Errors:                1            0
Dest Unreachables:     142          201
Time Exceeds:          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 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 lport attribute [*interface number*]

This command displays information about the logical port you specify. Use the interface number (*ifnum*) to specify the logical port.

This command can be used for UNI/NNI as well as trunk logical ports to provide various details about the port. The bandwidth values are provided in cells per second. This command requires that the interface index of the logical port in question be entered. The mapping between physical port ID, logical port name, and interface index can be easily obtained from the Show All Logical Ports dialog box.

**> show lport attribute (interface index) (sample output for trunk logical port)**

```
Slot:          15
Port:          3
Interface:     41
Data Rate:     100000000

Trunk Status:               Full   Trunk Overhead:              5%
Remote Node:        201.201.201.16   Remote Interface:         61
      Trunk                In BW        In BW         Out BW      Out BW
      Oversub.:            Avail.       Alloc.        Avail.      Alloc.
Qos1    100%             95000000     5000000       95000000     5000000
Qos2   1000%            950000000           0      950000000           0
Qos3    500%            475000000           0      475000000           0
Qos4    200%            190000000           0      190000000           0
Administrative Status:             Up   Operational Status:           Up
```

**> show lport attribute (interface index) (sample output for UNI/NNI logical port)**

```
Slot:          10
Port:          4
Interface:     28
Data Rate:     40704000
      Port                 In BW        In BW         Out BW      Out BW
      Oversub.:            Avail.       Alloc.        Avail.      Alloc.
Qos1    100%              40704000          0        40704000          0
Qos2    100%              40704000          0        40704000          0
Qos3    100%              40704000          0        40704000          0
Qos4    100%              40704000          0        40704000          0
Administrative Status:             Up   Operational Status:         Down
```

## show lport statistics [*ifnum*]

This command can be used to view the cell counts as well as the other relevant counts for all types of logical ports. Control frames and octet counters will only indicate values on trunk logical ports or UNI/NNI logical ports where UNI signalling and/or ILMI is in use.

```
> show lport statistics (interface index)

                    Receive         Transmit
Control Frames:      175592          175602
Control Octets:     3511840         4390050
Control Discards:         0               0
Control Errors:           0               0
Cells:               215049          214454
```

## show ntp

This command can be used to show the network timing protocol configuration and status.

```
> show ntp

SYSTEM CLOCK SETTINGS
Ntp Clock 862352807
Precision Ntp Time 862352807 sec 32 msec
System Clock Chip Time 862352807Network Timing Protocol Status
Current Time of Day       :22:26:47  Current NTP TIME         :22:26:47
Last Transmit Time             :22:26:14
Next Transmit Time             :22:26:56
Number of Configured Reference Servers : 0
Number of Time Requests          : 0
Last IP Destination Address      : 0.0.0.0
Number of UDP Messages Received : 0
IP address of last UDP Message  : 0.0.0.0
Last System Offset    0 sec, 0 msec
Max System Offset     0 sec, 0 msec

MaxDeviation        0, AT 0
Previous MaxDeviation 0, AT 0

Last        Deviation 0, AT 0
```

# Show ospf commands

The following OSPF console commands can be executed from a direct attached console or a telnet session. The parameters specified within [...] are optional. Most of these commands use the <card#> as an optional argument. If you specify the slot number, the requested information will be retrieved from the card in that slot and displayed.

## show ospf adv

Displays details of a specified OSPF database entry. <lstype>, <ls-id> and < adv-switch> can be taken from the show ospf database output. The optional parameter <adv-switch> is needed for all ls-types except 1 (LS_RTR) and 2 (LS_NET). Cascade's OSPF does not support LS_NET.

```
> show ospf adv <lstype> <ls-id> [<adv-switch>]
```

```
show ospf adv 201.201.201.14 201.201.201.14

        LS age:         910
        LS options:     0x0
        LS type:        Router-LSA
        LS ID:          201.201.201.14
        Adv rtr:        201.201.201.14
        LS Seq #:       0x8000007a
        LS Xsum:        0x97ba (good)
        LS Length:      176
        # interfaces:   7

                Link Type:      1
                Link ID:        201.201.201.16
                Link Data:      0.0.0.32
                TOS 0 Cost:     100
                TOS 253 Cost:   8

                Link Type:      1
                Link ID:        201.201.201.16
                Link Data:      0.0.0.41
                TOS 0 Cost:     101
              TOS 253 Cost:   8
```

```
Link Type:       1
Link ID:         201.201.201.16
Link Data:       0.0.0.39
TOS 0 Cost:      101
TOS 16 Cost:     2
TOS 17 Cost:     45
TOS 250 Cost:    28
TOS 253 Cost:    3843
```

## show ospf database

Displays the contents of the link state database, one line per each LSA.

```
> show ospf database
```

```
Type   ID                Adv-Switch        Seq#       Age
 1(8) 201.201.201.14    201.201.201.14    0x8000007a 580
 1(8) 201.201.201.16    201.201.201.16    0x8000006a 1696
 1(8) 201.201.201.24    201.201.201.24    0x800000dd 1655
 1(8) 201.201.201.3     201.201.201.3     0x800000ae 1662
 1(8) 201.201.201.6     201.201.201.6     0x800000df 1661
 1(8) 201.201.201.7     201.201.201.7     0x800000b2 1658
 1(8) 201.201.201.8     201.201.201.8     0x800000b5 538
 5    152.148.81.129    201.201.201.8     0x80000075 1271
 5    152.148.81.67     201.201.201.24    0x80000074 1670
 5    152.148.81.5      201.201.201.3     0x80000072 260
 5    152.148.81.17     201.201.201.3     0x80000072 260
 5    152.148.81.20     201.201.201.24    0x80000074 1670
 5    152.148.81.53     201.201.201.3     0x80000072 260
 5    152.148.81.125    201.201.201.24    0x80000074 1670
 5    152.148.81.125    201.201.201.14    0x8000003c 244
 5    152.148.81.125    201.201.201.3     0x80000072 260
14    0.0.0.31          201.201.201.16    0x80000011 242
14    0.0.0.32          201.201.201.14    0x80000030 244
14    0.0.0.4           201.201.201.7     0x80000003 1138
```

## show ospf interface

This command shows the state of all OSPF trunks.

**> show ospf interface**

```
LPort Neighbor       Nbr_State             Vers    #Rxmt   #LSReq #DBsum
Int 0.0.0.3          Full                   8        0       0      0
Int 0.0.0.14         Full                   8        0       0      0
Int 0.0.0.15         Full                   8        0       0      0
Int 0.0.0.16         Full                   8        0       0      0
1 201.201.201.16     Full                   8        0       0      0
7 201.201.201.8      Full                   8        0       0      0
32 201.201.201.16    Full                   8        0       0      0
34 201.201.201.8     Down                   0        0       0      0
36 0.0.0.0           Down                   8        0       0      0
38 0.0.0.0           Down                   8        0       0      0
39 201.201.201.16    Full                   8        0       0      0
41 201.201.201.16    Full                   8        0       0      0
```

## show ospf mcpath

This command displays the path that a point-to-multipoint virtual circuit will take, with circuit parameters specified by the user.

**> show ospf mcpath <dest-ip-addr> [<card#>]**

```
## show ospf mcpath 201.201.201.14
        Forward BW (Kbytes): 100
        Reverse BW (Kbytes): 100
        Forward QoS (1-4): 1
        Reverse QoS (1-4): 1
        Routing priority (0-15):
        Metric (0-3 adm/dly/cdv/hop):
        Leaf 0 Path ID:
        S/W version (2-8):
        Characteristics vp=1,cell=2,prv=4,mgt=8:
        E-E Delay (milliseconds):
        Private Net ID:
        Void trunk (switch/IFIndex):

        Dest:         201.201.201.14
        Result:       Success
        #Hops:        1
```

```
  Cost:        101
  Path:        201.16/28
 Forward BW: 555750 Kbytes
  Reverse BW: 555750 Kbytes
  Delay:      0.2 milliseconds
```

## 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 0x47884402 32 1
```

```
Prefix:      0x47884402/32
Node/Port:   201.14/40

Dest:        201.201.201.14
Result:      Success
#Hops:       0
```

### show ospf namedpath 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 0x47884402. If you do not know the name, refer to “show ospf names” on page C-20 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 32. If you do not know the length, refer to “show ospf names” on page C-20 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 Flags      Cost  State   Name/Len Primary(Secondaries)
1    0x00000000 127   Primary 0x01000000/32 201.7/64
1    0x00000000 127   Primary 0x02000000/32 201.7/32
2    0x00000000 0     N/A     4490000/56 201.7/40
2    0x00000000 0     N/A     4492000/56 201.7/40
2    0x00000000 0     N/A     508/24 201.7/0
2    0x00000000 0     N/A     5184566560/80 201.7/0
2    0x00000000 0     N/A     5550000/56 201.7/18
2    0x00000000 0     N/A     5551212/56 201.7/18
2    0x00000000 0     N/A     5553333/56 201.7/18
2    0x00000000 0     N/A     5559000/56 201.24/10
2    0x00000000 0     N/A     5559999/56 201.7/18
2    0x00000000 0     N/A     707/24 201.16/81
2    0x00000000 0     N/A     911/24 201.6/35
```

### show ospf names 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 0x01000000 and the length is 32 bits.

**Secondary** — Any secondary locations for the name.

## show ospf pathbd

Displays all paths, or those paths going through a given trunk, present on a particular card.

```
> show ospf pathdb 4
```

```
ID        # VCs    Path
4.1       0        201.16/31
```

## show ospf qospath [*IP address of destination node*] [*card*]

This command displays various qospath statistics.

```
> show ospf qospath 201.201.201.16
```

```
Forward BW (Kbytes): 1000
Reverse BW (Kbytes): 1000
Forward QoS (1-4): 1
Reverse QoS (1-4): 1
Routing priority (0-15):
Metric (0-3 adm/dly/cdv/hop):
Current Path ID:
S/W version (2-8):
Characteristics vp=1,cell=2,prv=4,mgt=8:
E-E Delay (milliseconds):
Private Net ID:
Void trunk (switch/IFIndex):

Dest:        201.201.201.16
Result:      Success
#Hops:       1
Cost:        101
Path:        201.14/39
Forward BW: 555750 Kbytes
Reverse BW: 555750 Kbytes
Delay:       0.2 milliseconds
pittsburg14>
```

## 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 detailed OSPF statistics. The default displays statistics of the OSPF process that is run on the CP/SP. If the <card#> is specified, the system displays the OSPF statistics run on the specified IOP.

**> show ospf statistics [<card#>]**

```
## show ospf statistics

      # switches:              7           # reachable switches: 7
      # Dijkstra runs:         247         # Trunks:           44 (53)
        Max LSA size:          296         # Stub links:        7 (7)
      # LSAs:                  94          Database checksum: 0x2cf338
      # router-LSAs:           7           # AS-external-LSAs:   12
      # name-LSAs:             31

      # 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

  Max task latency (ms):72               Max lookup time (ms): 0

# OSPF trunk inst ch:     0          # VCMGR trunk inst ch:0
# Bad paths reg:          0          # VCs using old rev:  0
# VCMGR call backs:       0          # VCMGR rpt old inst: 0
# Trunk cost chg neg:     0

# trunk congestion:       0          # path congestion:    0
# VC congestion:          0

  Routing S/W revision: 8            Network S/W revision: 8
```

## show ospf trunk

This command displays OSPF trunk statistics.

**> show ospf trunk**

```
sw/prt       sw/prt  fbw2/0   rbw2/0     delay    cost    comments
201.14/1     201.16/?2783203  ?            ?      100     Mgmt
201.14/39    201.16/28 5557500557500       2      101
201.14/41    201.16/?463867   ?            ?      101     Mgmt
201.14/77    201.16/?37761    ?            ?      100     MMg
```

## show ospf vcpath

This command displays the default VC paths to each switch, along with their cost, current bandwidth and the maximum bandwidth available (if different) to the node.

**> show ospf vcpath 201.201.201.16**

```
Dest:       201.201.201.16
Result:     Success
#Hops:      1
Cost:       101
Path:       201.14/39
Forward BW: 5557500 Kbytes
Reverse BW: 5557500 Kbytes
```

```
Delay:      0.2 milliseconds
```

## show ospf vcroute

This command displays the default VC route.

```
> show ospf vcroute
```

```
> show ospf route
Dest                Mask                Next_hop            State     Cost Age
152.148.81.0        255.255.255.0       0.0.0.0             Direct    1    0
152.148.81.5        255.255.255.255     201.201.201.14      OSPFE1    401  0
152.148.81.17       255.255.255.255     201.201.201.14      OSPFE1    401  0
152.148.81.20       255.255.255.255     0.0.0.0             Static    1    0
152.148.81.53       255.255.255.255     201.201.201.14      OSPFE1    401  0
152.148.81.67       255.255.255.255     201.201.201.14      OSPFE1    302  0
152.148.81.125      255.255.255.255     201.201.201.14      OSPFE1    101  0
152.148.81.129      255.255.255.255     201.201.201.14      OSPFE1    201  0
201.201.201.3       255.255.255.255     201.201.201.14      OSPF      400  0
201.201.201.6       255.255.255.255     201.201.201.14      OSPF      300  0
201.201.201.7       255.255.255.255     201.201.201.14      OSPF      400  0
201.201.201.8       255.255.255.255     201.201.201.14      OSPF      200  0
201.201.201.14      255.255.255.255     201.201.201.14      OSPF      100  0
201.201.201.16      255.255.255.255     0.0.0.0             Direct    1    0
201.201.201.24      255.255.255.255     201.201.201.14      OSPF      301  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 attri 7.1
```

```
Port Type:                DS3-T3-8    Operational Status:             Down
Interface Type:                N/A    Administrative Status:            Up
Data Rate:                44736000    Clock Source:               Internal
Link Down Reason:        Loss of signal
```

## 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 7

pport   type        # of lports    datarate      status
1       DS3-T3-8             1     44736000        Down
2       DS3-T3-8             1     44736000        Down
3       DS3-T3-8             1     44736000        Down
4       DS3-T3-8             1     44736000          Up
5       DS3-T3-8             1     44736000        Down
6       DS3-T3-8             1     44736000        Down
7       DS3-T3-8             2     44736000          Up
8       DS3-T3-8             1     44736000          Up
```

## 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
Control Octets:            0               0
Control Frames:            0               0
Control Discards:          0               0
Control Errors:            0               0
Cells:            1375881519      1375042369
Out Discard Cells:                     33364
Frames:                    0               0
```

## show pram

The show pram command provides information about the contents of the parameter RAM (PRAM) files for SPs and IOMs on the PCMCIA disk. For the active SP, the file output is much longer (the example below shows the typical output for the standby SP or an IOM).

**> show pram 2**

```
                         Configuration Database

version=5.6, tables=16, checksum=00004C04 signature=335F8D4E
size=262144

 Table   Start     End       Length  RSize   Max  Count
   net   902F74D0  902F759A     202    82      1      1
  node   902F759A  902F7807     621   481      1      1
  card   902F7807  902F7875     110    86      1      1
   ase   902F7875  902F7B11     668    20     32      1
   cac   902F7B11  902F7B95     132    12     10      0
  comm   902F7B95  902F802D    1176    72     16      5
 addrs   902F802D  902FDB75   23368    91    256      1
 trmgr   902FDB75  902FDBB9      68     4     14      0
   cug   902FDBB9  902FEBBD    4100     4   1024      0
cugmbr   902FEBBD  9030ABC9   49164    48   1024      0
 assoc   9030ABC9  90322BD5   98316     6  16384       0
abglob   90322BD5  90322BF6      33    13      1      1
  name   90322BF6  9032388A    3220    25    128      0
   ckt   9032388A  90324106    2172    64     32      0
  auth   90324106  90324DB6    3248    57     56      0
 tdmgr   90324DB6  90327DD6   12320    24    512      0
```

## show pvc attribute [*interface.vpi/vci*]

This command displays information about the specified circuit. Use the interface index (ifnum) of the logical port endpoint and a concatenated vpi/vci value to specify the circuit. In the following example, the vpi would be 1 and the vci would be 300. To calculate the vpi_vci value:

1. Multiply the vpi by 65536.
2. Add the vci to this value.

```
> show pvc attri 40.65836
```

```
Src Interface:                    40 Src vpi_vci:                  65836
Src VPI:                           1 Src VCI:                        300
Dst Interface:                    89 Dst vpi_vci:                 327780
Dst VPI:                           5 Dst VCI:                        100
In Priority:                       1 Out Priority                      1
In Effective BW(bps):            424 Out Effective BW(bps)           424
In QoS:                         VBR2 Out QoS                        VBR2
In Traffic Desc.:                  3 (pcr-01-scr-0-mbs-0)
Out Traffic Desc.:                 3 (pcr-01-scr-0-mbs-0)
In TD Param1:                      1 Out TD Param1                     1
In TD Param2:                      1 Out TD Param2                     1
In TD Param3:                      1 Out TD Param3                     1
Type of Service:                  0 Discard enable:                1(On)
Creation time:               5634280 Last change:                5634280
DCE state:                         2 DTE state:                        2
DTE status:                        2 Receive ready:                  Yes
Interface state:                   0 Data flow:                        1
Admin Status:          2(Active)
PVC state:             6(Active)
Operation status:      2(Active)
```

## show pvc attribute output description

The following list describes each of the attributes for the show pvc attribute output. See the *Network Configuration Guide for CBX 500* for detailed descriptions of these parameters.

**Src Interface** — The source interface index (same as II or ifnum).

**Src DLCI** — The source DLCI index (same as DD).

**Src VPI** — The source VPI (an 8-bit field in the header of an ATM cell that is used to route cell traffic).

**Src VCI** — The source VCI (a 16-bit field in the header of an ATM cell that is used to route cell traffic).

**Dst Interface** — The destination interface index.

**Dst DLCI** — The PVC's destination DLCI.

**Dst VPI** — The destination VPI.

**Dst VCI** — The destination VCI.

**In Priority** — The PVC's configured in priority.

**Out Priority** — The PVC's configured out priority.

**In Effective BW** — The amount of bandwidth (for traffic coming into the switch) in bits/second that is reserved for this circuit at the specified interface. This value is derived using the CAC function.

**Out Effective BW** — The amount of bandwidth (for traffic coming out of the switch) in bits/second that is reserved for this circuit at the specified interface. This value is derived using the CAC function.

**In Qos** — The in value for the Quality of Service parameters. Possible values are CBR, VBR, or UBR.

**Out Qos** — The out value for the Quality of Service parameters. Possible values are CBR, VBR, or UBR.

**In TDesc Type** — The in traffic descriptor for the PVC.

**In Param1** — An ATM traffic descriptor.

**In Param2** — An ATM traffic descriptor.

**In Param3** — An ATM traffic descriptor.

**Out TDesc Type** — The out traffic descriptor type for the PVC.

**Out Param1** — An ATM traffic descriptor.

**Out Param2** — An ATM traffic descriptor.

**Out Param3** — An ATM traffic descriptor.

**Type of Service** — The PVC service type.

**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 unchanged 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.

**Operation Status** — The external PVC state.

## show pvc statistics [*interface.vpi_vci*]

This command displays statistics for the specified circuit. Use the interface index (ifnum) of the logical port endpoint and a concatenated vpi/vci value to specify the circuit. To calculate the vpi_vci value:

1. Multiply the vpi by 65536.
2. Add the vci to this value.

In the example below, the vpi would be 0 and the vci would be 100.

```
> show pvc statistics 13.65636
```

```
                   Receive     Transmit
Discarded CLP0:    0           -
Discarded CLP1:    0           -
Tagged:            0           -
CLP0:              0           676
CLPI:              0           0
```

## 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          4413   # Pkts Transmitted:  850
Received:
```

```
# 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 software

This command lists all cards and the software information running on each card.

**> show software**

| Slot | Type | Redund | SW Revision | Software ID | Date |
|---|---|---|---|---|---|
| 1 | SP10 | Active | 01.00.00.08 | 00-B00000563 | 14-Mar-1996.08:30:54 |
| 7 | DS3-T3-8 | Active | 01.01.00.08 | 00-B000006E0 | 14-Mar-1996.08:01:49 |
| 8 | OC3-4 | Active | 01.00.00.08 | 00-B000006E0 | 14-Mar-1996.08:01:49 |
| 11 | DS3-T3-8 | Active | 01.00.00.08 | 00-B000006E0 | 14-Mar-1996.08:01:49 |

## show software flash

This command shows all software in the SP's flash memory.

```
> show software flash

Active SP has the following software:

Part#          Revision     Size  Description
7000913800   2.00.00.00   352054  SP Boot Flash [75-B00000015]
7000903800   2.00.00.00   559384  SP Application [75-B00000039]
7000914100   2.00.00.00   419368  IOM1 Boot Flash [75-B00000014]
7000904100   2.00.00.00   711004  IOM1 Application [75-B0000008C]

Standby SP has the following software:

Part#          Revision     Size  Description
7000913800   2.00.00.00   352054  SP Boot Flash [75-B00000015]
7000903800   2.00.00.00   559384  SP Application [75-B00000039]
7000914100   2.00.00.00   419368  IOM1 Boot Flash [75-B00000014]
7000904100   2.00.00.00   711004  IOM1 Application [75-B0000008C]
```

## show system

This command shows all switch details.

```
> show system

Switch Name:    pittsburg14
System Desc:    Cascade Communications Corporation CBX-500
Model:          CBX-500
Location:       08:005A3BF1B0
Contact:

System State:   Active
Uptime:         1 days 26 minutes 36 seconds

Current time:   Thu Apr 24 13:27:11 1997 UTC

Serial Number:                    Internal IP Addr:   201.201.201.14
Hardware Rev:                      Ethernet IP Addr:   152.148.81.62
EPROM Rev:      01.00.00.00         Network Wide Addr:  201.201.0.0
Software Rev:   02.00.00.00         Network Mask:       255.255.0.0
Ethernet Addr:  00:04:AC:90:BF:1D
```

```
Slot Type            Redund  State    SW Rev      HW Rev      EPROM    Serial#
                        State
1    SP20             Active  Active   02.00.00.00 00         01.00.00.00
22A084
94
```

## show svc statistics [interface]

This command displays information about svc statistics.

**> show svc statistics 29**

```
                                   Originating  Terminating
Minimum PPP Connections            0            0
Current PPP Connections            0            0
Maximum PP Connections             0            0
Minimum PMP Connections            0            0
Current PMP Connections            0            0
Maximum PMP Connections            0            0
Minimum PMP Parties                0            0
Current PMP Parties                0            0
Maximum PMP Parties                0            0
                                   0            0
PP Connection Attempts             0            0
PP Connection Network Rejects      0            N/A
PP Connection User Rejects         0            0
PP Connection Network Failures     0            0
PMP Connection Attempts            0            0
```

```
PMP Connection Network Rejects    0             N/A
PMP Connection User Rejects       0             0
PMP Connection Network Failures   0             0
PMP Party Attempts                0             0
PMP Party Network Rejects         0             N/A
PMP Party User Rejects            0             0
PMP Party Network Failures        0             0
```

## 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

                         TCP Connections Counts
Connections Requested:   0
Connections Accepted:    0
Connections Failed:      0
Connections Reset:       0
Current Connections:     0
```

## show tproto

This command can be used to view the trunk protocol activity on direct and OPTimum trunks.

```
> show tproto 1

TRUNK PROTOCOL INFO FOR INTERFACE 1:

State:                    UP
Phy Link State:           UP
Reason:                   NONE
KA gap:                1000ms       Static delay:           2(in 100us)
KA threshold:           5           Dynamic delay:          2(in 100us)
Last 16 delays measured (in 100us):
                         2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2

Trk proto up cnt:         1              PLinkUp evt cnt:         3
Trk proto dn cnt:         0              PLinkDn evt cnt:         2
KA req tx cnt:           89033          KA req rx cnt:           89035
KA rep rx cnt:           89033          KA rep tx cnt:           89035
KA unknown rx cnt:        0              KA timeout cnt:          0
KA corrupt rx cnt:        0
Spur Trk proto up cnt:    0              Spur PLnkUp cnt:         0
Spur Trk proto dn cnt:    31498          Spur PLnkDown cnt:       0
Lnk up time:             15:51 hrs     Last lnk dn time:       0:00 hrs

PLnkUp evt cnt in last cycle (1 hour):                           0
PLnkUp evt cnt in curr cycle in progress (elapsed time: 32 min): 0
```

## show trap

This command displays trap activity and configuration information for the switch

```
> show trap
```

```
Trap Tx/sec rate: 5
TRAP QUEUE COUNTS:
Startup: 0  Major: 0, Minor: 0, Clear: 0, Nonalarm: 0
TRAPS DROPPED:
Heap low: 0  Internal error: 0
Queue full: Major: 0, Minor: 0, Clear: 0, Nonalarm: 0
TRAP RESEND QUEUE COUNTS:
constitution: size: 128, entries: 128, insertions: 135, resends: 0
roamer: size: 128, entries: 128, insertions: 135, resends: 0
cascade not registered for traps
bud: size: 128, entries: 128, insertions: 135, resends: 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 occurred.

```
> 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

yourname    console     14 minutes 21 seconds
```

## synchronize svc statistics [interface]

This command sets the minimum and maximum objects to the actual (current value) for all the gauges. This enables you to view the highest and lowest values for a counter since the last “synchronize” command. If bulk statistics is enabled, there will be an automatic “synchronize” every 15 minutes. You should disable bulk statistics *before* running this command.

```
> synchronize svc statistics 29


                                  Originating  Terminating
 Minimum PPP Connections          0            0
 Current PPP Connections          0            0
 Maximum PP Connections           0            0
 Minimum PMP Connections          0            0
 Current PMP Connections          0            0
 Maximum PMP Connections          0            0
 Minimum PMP Parties              0            0
 Current PMP Parties              0            0
 Maximum PMP Parties              0            0
                                  0            0
```

```
PP Connection Attempts            0             0
PP Connection Network Rejects     0             N/A
PP Connection User Rejects        0             0
PP Connection Network Failures    0             0
PMP Connection Attempts           0             0
PMP Connection Network Rejects    0             N/A
PMP Connection User Rejects       0             0
PMP Connection Network Failures   0             0
PMP Party Attempts                0             0
PMP Party Network Rejects         0             N/A
PMP Party User Rejects            0             0
PMP Party Network Failures        0             0
```

# DEBUG LEVEL

```
> enable debug

Password:
DEBUG ACCESS LEVEL GRANTED.
## << DEBUG PROMPT
```

Table C-2 shows the debug commands.

**Table C-2. Debug Commands**

| Command | Description |
|---|---|
| disable [master] | Return to normal read-only mode |
| dump | Dump memory contents |
| heapwalk | Check heap |
| install | Invoke installation procedure<br>(You should only use this command to bring the switch to a readable state from the NMS.) |
| mb | Modify a byte in memory |
| modify | Modify a word (4 bytes) in memory |
| reset ?<br>reset lport <interface><br>reset pram <slot><br>reset pport <slot.port><br>reset pvc <interface.dlci><br>reset system | Reset PRAM, system, pport, lport, or pvc |
| set ? | Set parameters |
| telnet <host> [term] | Telnet to another switch |

D

# 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

For example, if you were copying a database named Boston, the tar file name would be:

CVCOPY_boston_data.tar

# Processing

Figure D-1 illustrates the process flow for the Copy Database utility when you use the utility to copy in data.

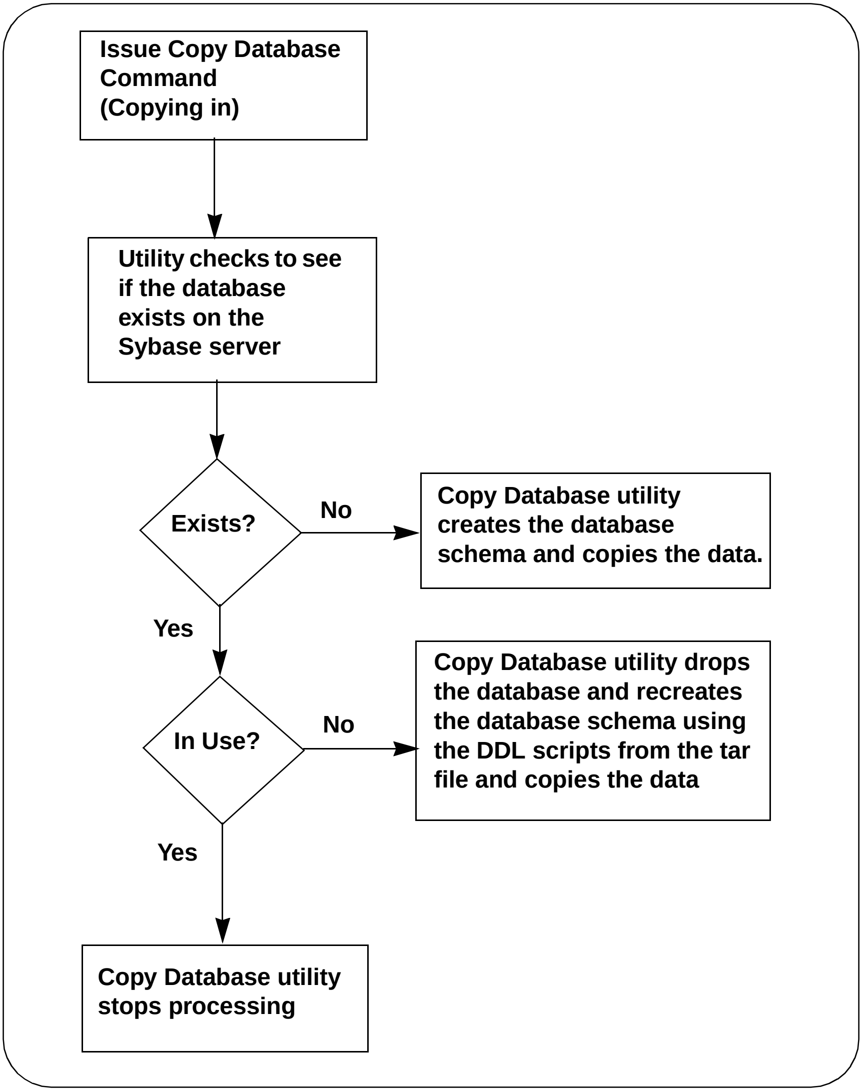



**Figure D-1. Process Flow for Using Copy Database to Copy In**

Figure D-2 illustrates the process flow for the Copy Database utility when you use the utility to copy in data.

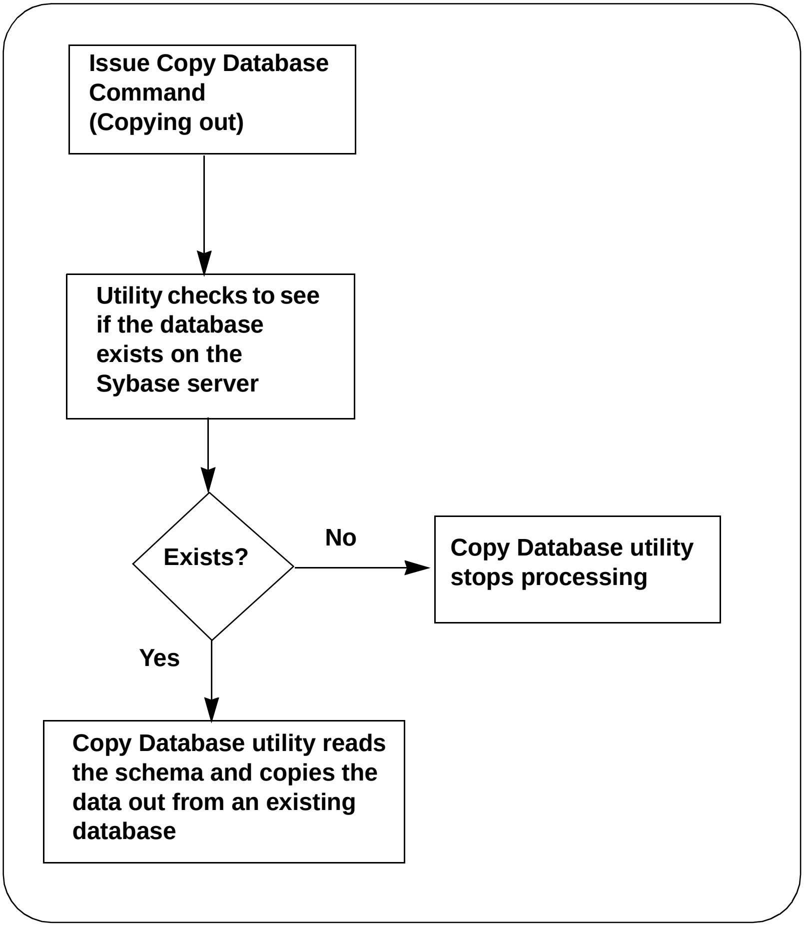



**Figure D-2. Process Flow for Using Copy Database to Copy Out**

# Command Format

Issue the following command to run the Copy Database utility.

```
cv-copydb.sh (out/in) db_name [/server_name] password
directory new_db_name [/server_name]
```

Table D-1 describes the Copy Database Utility commands.

**Table D-1. Copy Database Utility Commands**

| Parameter | Specifies |
|---|---|
| in | That the utility should copy in data from a saved tar file to a new database. |
| out | That the utility should copy out data from an existing database. |
| db_name [/server_name] | One of the following depending on whether you are copying data in or out:<br>db_name<br>• **If you are copying data in,** this is the database name that the utility uses to find the correct tar file for the database.<br>• **If you are copying data out,** this is the database that the utility copies.<br>server_name<br>• *(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.<br>• (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. |

**Table D-1. Copy Database Utility Commands (Continued)**

| Parameter | Specifies |
|---|---|
| directory | One of the following depending on whether you are copying data in or out:<br>• **If you are copying data in,** this is the directory where the saved tar file is located.<br>• **If you are copying data out,** this is the directory that the utility copies the data files to. |
| new_db_name [/server_name] | (Optional, for copying data **in** only) The name of the new database. This name must be at least 6 characters in length. |

## Examples

```
cv-copydb.sh out cascview superbase /cn/home/xxx
```

This command causes the Copy Database utility to copy out data from an existing database named cascview. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh in cascview superbase /cn/home/xxx
```

This command causes the Copy Database utility to copy in data from a data file named CVCOPY_cascview_data.tar, and specifies the file's location as /cn/home/xxx. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh in cascview superbase /cn/home/xxx testdb
```

This command causes the Copy Database utility to copy in data from a data file named CVCOPY_cascview_data.tar to another database named testdb. The DSQUERY and Sybase environment variables are specified in the cvdb.cfg file.

```
cv-copydb.sh out cascview/WEST11 superbase/tmp
```

This command causes the Copy Database utility to copy out data from an existing database named *cascview* from server *WEST11*. Sybase is set according to the environment variable specified in cvdb.cfg. The DSQUERY environment variable is overridden by the *WEST11* parameter value.

# Errors

The following errors can result when you are using the Copy Database utility.

## General Errors

**The Sybase server defined in cvdb.cfg is not accessible.**

This problem can be caused by a number of factors. The most common cause is a lack of space. Contact the Technical Response Center for further information about how to resolve this error.

**Cannot log into the database server $DSQUERY. Please check your input parameters, exiting now.**

The specified database does not exist in the Sybase server. Check the database name and server name and reenter using a valid name.

**Cannot locate the database $DB_NAME from server $DSQUERY, exiting now.**

You have not specified a valid input database name for the db_name parameter. Check the value and reenter the command.

**Make sure that no one else is running cv-copydb.sh with the directory $DATA_DIR. If no one is running the utility, remove the files CVOPY_${DB_NAME}_dbschema, CVCOPY_${DB_NAME}_crdb and all files that have the file name prefix of CVCOPY_BCP_${DB_NAME}, then run the utility again.**

This error is due to one of the following problems:

- The specified database exists in the Sybase server and is in use. You cannot copy a database while it is in use. Use the Copy Database utility at another time.

- Another user is running the copy database utility using the same directory. You cannot copy a database while it is in use. Use the Copy Database utility at another time.
- The files specified in the error message need to be removed.

After you check and resolve the cause of the error, reissue the copy database command.

## Copy-Out Errors

**Error discovered when running dbschema to generate schema output file. Please check to make sure you have installed perl5 files and the dbschema file provided by Cascade under ${CV_ROOT} directory. Exiting now.**

The copy database utility discovered an error when generating the schema output file. Check to make sure that the files specified in the message are installed.

**Error discovered while using bulkcopy to copy out data for table *$table.***

Contact the Technical Response Center.

## Copy-In Errors

**Cannot drop the database $TEMP_DB_NAME, because it is in use.**

The specified database is in use. Rerun the copy database utility at another time.

**Error discovered when trying to create the database $TEMP_DB_NAME. Make sure that you have enough device space before running the utility. The output is saved in $TMPFILE1.**

The utility discovered an error due to lack of available device space when creating the temporary database. Free the available device space and rerun the utility.

**Error: unable to allocate enough data space for the database. Check CVCOPY_${TEMP_DB_NAME}_crdb file to make sure that the data size in the create database command is correct. Get instructions about how to change the data size in the CVCOPY_${TEMP_DB_NAME}_crdb file.**

Change the data size for the database and run the utility again.

**Unable to allocate enough log space for the database. Check CVCOPY_${TEMP_DB_NAME}_crdb file to make sure that the log size in the create database command is correct. Get instructions about how to change the log size in the CVCOPY_${TEMP_DB_NAME}_crdb file.**

Change the log space value and run the utility again.

**Fatal error discovered when trying to create the schema for $TEMP. For more information about the error, please read $TMPFILE.**

Review the $TMPFILE for more information about this error.

# E

# Signalled QoS, BBC, and BEI Service Category Mappings

This appendix describes how the CBX 500 maps ATM Forum QoS classes (QoS), Broadband Bearer Classes (BBC), and the Best Effort Indicator (BEI) to the CBX 500 service categories. When PVCs are provisioned, the CBX 500 service category is selected by the operator as part of the provisioning process. For SVCs, the CBX 500 selects the service category, based on the QoS, BBC, and BEI contained in the received UNI Signalling SETUP message.

This appendix references specific sections from the *ATM Forum's UNI Appendix A specifications (3.0 and 3.1)*. Comments specific to the CBX 500 are noted in italics. For detailed information on the QoS, BBC, and BEI role, refer to the *ATM Forum's UNI Appendix A specifications (3.0 and 3.1)* .

# Definition of Specified QoS Classes

*From ATMF UNI 3.1 Appendix A, Section A.4.1:*

This section describes the ATM Forum's definition of the specified QoS classes. It is helpful to review these definitions in order to understand how the CBX 500 maps ATMF QoS elements. The following text is an excerpt from ATMF UNI 3.1 Appendix A, Section A.4.1.

A Specified QoS class provides a quality of service to an ATM virtual connection (VCC or VPC) in terms of a subset of the ATM performance parameters defined in Section 3 of this appendix. For each Specified QoS class, there is one specified objective value for each performance parameter identified as defined in section 3 of this appendix.

Initially, each network provider should define objective values for a subset of the ATM performance parameters of section 3 for at least one of the following Service Classes from ITU-T recommendation I.362 in a reference configuration that may depend on mileage and other factors:

- **Service Class A**: Circuit Emulation, Constant Bit Rate Video (*CBX 500 CBR service category*)
- **Service Class B**: Variable bit Rate Audio and Video (*CBX 500 VBR-RT service category*)
- **Service Class C**: Connection-Oriented Data Transfer (*CBX 500 VBR-NRT service category*)
- **Service Class D**: Connectionless Data Transfer (*CBX 500 UBR service category*)

In the future, more 'QoS Classes' may be defined for a given 'Service Class' described above. The following Specified QoS Classes are currently defined:

- **Specified QoS Class 1**: support a QoS that will meet Service Class A performance requirements
- **Specified QoS Class 2**: support a QoS that will meet Service Class B performance requirements
- **Specified QoS Class 3**: support a QoS that will meet Service Class C performance requirements

- **Specified QoS Class 4**: support a QoS that will meet Service Class D performance requirements

The Specified QoS Class 1 should yield performance comparable to current digital private line performance. Specified QoS Class 2 is intended for packetized video and audio in teleconferencing and multi-media applications. Specified QoS Class 3 is intended for interoperation of connection oriented protocols, such as Frame Relay. Specified QoS Class 4 is intended for interoperation of connectionless protocols, such as IP, or SMDS.

You may configure the same performance for all, or a subset of Specified QoS Classes, provided the requirements of the most stringent Service Class are met. (*The CBX 500 provides a separate service category for each of the specified QoS classes*.)

For example, assuming the SVC SETUP message contains the proper combination and structure, the following guidelines apply:

- *A signalled QoS class of 1 will result in a CBX 500 service category of CBR.*
- *A signalled QoS class of 2 will result in a CBX 500 service category of VBR-RT.*
- *A signalled QoS class of 3 will result in a CBX 500 service category of VBR-NRT.*
- *A signalled QoS class of 4 will result in a CBX 500 service category of UBR.*

# Definition of Unspecified QoS Class

*From ATMF UNI 3.1 Appendix A, Section A.4.2:*

The Unspecified QoS class requires special handling by the CBX 500 because the ATMF Unspecified QoS does not directly map to any specific service category. This is reinforced in the following excerpts from ATMF UNI 3.1 Appendix A, Section A.4.2. Comments specific to the CBX 500 are noted in italics.

In the Unspecified QoS class, no objective is specified for the performance parameters. However, the network provider may determine a set of internal objectives for the performance parameters. In fact, these internal performance parameter objectives need not be constant during the duration of a call. Thus, for the Unspecified QoS class there is no explicitly specified QoS commitment on either the CLP=0 or the CLP=1 cell flow. Services using the Unspecified QoS class may have explicitly specified traffic parameters. This means the "network provider" (*or the CBX 500*) has several options for handling unspecified QoS. This involves the role of the BBC and BEI.

An example application of the Unspecified QoS class is the support of "best effort" service. For this type of service, the user selects the Best-Effort Capability, the Unspecified QoS class and only the traffic parameter for the Peak Cell Rate on CLP=0+1. As indicated in Section 3.6.2.4, this capability can be used to support users that are capable of regulating the traffic flow into the network and to adapt to time-variable available resources. (*The Unspecified QoS class with a signalled Best Effort traffic descriptor is the type of service requested by the majority of ATM SVC capable CPE. This maps directly to the CBX 500 UBR service category.*)

The Unspecified QoS class is identified by the integer zero (0) in the ILMI MIB or a code point in a signaling message for the requested QoS class. (*This is why unspecified QoS class is also called QoS class 0.*)

*Using unspecified QoS, the CBX 500 uses the BBC information element and the presence (or non presence) of the BEI to determine what service category should be used for the SVC. For a detailed description of each BBC, refer to the ATMF UNI specifications.*

# Support of Class X, Class A, and Class C ATM Transport Services

*From ATMF UNI 3.1 Chapter 5, Section 5.1.2.6:*

When dealing with unspecified QoS, the CBX 500 uses the BBC information and the presence (or lack of) of the BEI as a means of determining what service category should be used for the SVC. The ATMF UNI specifications also provide information on each BBC meaning. The following ATMF excerpts describe the BBC in greater detail.

Class X service is a connection oriented ATM transport service where the AAL, traffic type (VBR or CBR) and timing requirements are user defined (i.e., transparent to the network). The user chooses only the desired bandwidth and QoS with appropriate information elements in a SETUP message to establish a class X connection.

Class A service is a connection oriented, constant bit rate ATM transport service. Class A service has end-to-end timing requirements. Class A service may require stringent cell loss, cell delay and cell delay variation performance. The user chooses the desired bandwidth and the appropriate QoS in the SETUP message to establish a class A connection.

Class C service is a connection oriented, variable bit rate ATM transport service. Class C service has no end-to-end timing requirements. The user chooses the desired bandwidth and QoS with appropriate information elements in a SETUP message to establish a class C connection.

The Phase 1 Signalling specified in this document supports Class X, Class A and Class C service. Class D service is not directly supported by signalling. It can be supported via a Class X or Class C connection to a connectionless server.

The ATMF specifications do not directly indicate how a network provider (i.e. Cascade) should map BBC to service category. In switch software Release 1.1.x (and previous releases), the CBX 500 always mapped unspecified QoS to the UBR service category, regardless of the BBC. In switch software Release 1.2.1 (and future releases), changes were made to utilize the BBC when deciding which service category to map to unspecified QoS.

The specific mappings of unspecified QoS+BBC+BEI were made as a result of the ATMF guidelines and customer requirements. Because the BBC information element also contains traffic type and timing requirement fields, it is difficult to make general statements about which BBC maps to which CBX 500 service category. Instead, it is important to reference ATMF UNI 3.1 Appendix F. This appendix lists several guidelines and describes the valid combinations of BBC and QoS. An excerpt of this appendix is provided in the following section.

## Guidelines on the Use of Bearer Class, Traffic Parameters and QoS

*From ATMF UNI 3.1 Appendix F.1:*

The following provides a brief description of the various BCOB classes in the Bearer capability information element (see ITU-T Recommendation F.811 for additional information).

### BCOB-A (*Section F.1.1*)

When the user specifies BCOB-A, the user is requesting more than an ATM only service. The network may look at the AAL IE to provide interworking based upon its contents. One example of such interworking would be between an ATM user calling a non-ATM user who has switched DS1 capability. In this case, the network interworking function would need to know the AAL to be able to perform this interworking function.

### BCOB-C (*Section F.1.2*)

When the user specifies BCOB-C, the user is requesting more than an ATM only service. The network interworking function may look at the AAL and provide service based on it.

### BCOB-X (*Section F.1.3*)

When the user specifies BCOB-X, the user is requesting an ATM only service from the network. In this case, the network shall not process any higher layer protocols (e.g. AAL protocols).

The difference between BCOB-X and the other classes is what service is being requested from the network. For the VBR user that wants only a ATM cell relay service, the user should specify BCOB-X and Traffic Type VBR.

A user, that is placing a DS1 circuit emulation call but does not want to allow interworking, should specify BCOB-X and Traffic Type CBR. If the user wishes to allow interworking then the user should specify BCOB-A.

## Allowed Combination of Bearer Capabilities, Traffic Parameters, and QoS

*From Section F.2:*

The parameters specified in the Broadband Bearer Capability IE, the Traffic Descriptor IE, and the Quality of Service Parameters IE of the SETUP message should be consistent. Table E-1 shows the allowable combinations of the Broadband Bearer Capability classes, the Traffic Descriptor parameters and the Quality of Service classes based on tables 5-7 and 5-8. If an illegal combination of parameters is specified, the call should be cleared with cause #63 “service or option not available, unspecified”.

Table E-1 (*from Table F-1 in ATMF UNI 3.1*) uses the following entries:

- PCR = Peak Cell Rate, SCR = Sustainable Cell Rate, MBS = Maximum Burst Size
- Y = Yes, N = No, S= Specified
- Y/N = either "Yes" or "No" is allowed.
- * = allowed QOS class values are a network option. Class 0 is always supported for alignment with ITU-T.
- & = parameter is coded to either "no indication" or "VBR" or octet 5a (Traffic Type/Timing Required) is absent; these three codings are treated as equivalent.
- && = parameter is coded to either "No indication" or "No" or octet 5a (Traffic Type / Timing Required) is absent; these three codings are treated as equivalent.
- A blank entry in the table indicates that the parameter is not present.

**Table E-1. Allowable Combinations of Traffic Related Parameters in the SETUP message**

| Broadband Bearer Capability | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Broadband Bearer | A,C | X | X | C | X | C | X | A,C | X | X | C | X |
| Traffic Type | | CBR | & | | & | | & | | CBR | & | | & |
| Timing Required | | Y | && | | && | | && | | Y | && | | && |
| Traffic Descriptor | | | | | | | | | | | | |
| PCR (CLP=0) | S | S | S | | | | | | | | | |
| PCR (CLP=0+1) | S | S | S | S | S | S | S | S | S | S | S | S |
| SCR (CLP=0) | | | | S | S | | | | | | | |
| SCR (CLP=0+1) | | | | | | S | S | | | | | |
| MBS (CLP=0) | | | | S | S | | | | | | | |
| MBS (CLP=0+1) | | | | | | S | S | | | | | |
| Best Effort | | | | | | | | | | | S | S |
| Tagging | Y/N | Y/N | Y/N | Y/N | Y/N | N | N | N | N | N | N | N |
| QoS Classes | * | * | * | * | * | * | * | * | * | * | 0 | 0 |

# Specific CBX 500 Service Category Mappings

In an effort to simplify the interpretation of the ATMF UNI 3.1 Appendix F specification and other specification excerpts in this appendix, this section provides a table that simplifies the process of determining the specific CBX 500 service category mappings.

Table E-2 lists the CBX 500 service category for a number of QoS and BBC combinations. The table uses the following entries:

- BEI = NO indicates the BEI is not present.
- BEI = YES indicates the BEI is present.
- N/A indicates the parameter is either not applicable or not allowed.
- CC 63 indicates the CBX 500 will reject the SVC with the cause code of 63 or "service or option not available, unspecified."

The QoS information presented in this table (and in the Show All Failed SVCs dialog box) is the signalled QoS, not the actual service category. For signalled QoS classes 1 through 4, the mapping is clear. For unspecified QoS, you must look at the BBC contents and use the following table to determine the actual service category. Although you can use the View QoS Parameters screen to determine the service category, if many VCs exist on a logical port it may be difficult to interpret.

**Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI)**

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 0 | A | NO | N/A | N/A | CBR | x |
| 1 | 0 | C | NO | N/A | N/A | VBR-NRT | x |
| 1 | 1 | A | NO | N/A | N/A | CBR | x |
| 1 | 1 | C | NO | N/A | N/A | CBR | x |
| 1 | 2 | A | NO | N/A | N/A | VBR-RT | x |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 2 | C | NO | N/A | N/A | VBR-RT | x |
| 1 | 3 | A | NO | N/A | N/A | VBR-NRT | x |
| 1 | 3 | C | NO | N/A | N/A | VBR-NRT | x |
| 1 | 4 | A | NO | N/A | N/A | UBR | x |
| 1 | 4 | C | NO | N/A | N/A | UBR | x |
| 2 | 0 | X | NO | CBR | e/e tmg req'd | CBR | x |
| 2 | 1 | X | NO | CBR | e/e tmg req'd | CBR | x |
| 2 | 2 | X | NO | CBR | e/e tmg req'd | N/A | CC 63 |
| 2 | 3 | X | NO | CBR | e/e tmg req'd | N/A | CC 63 |
| 2 | 4 | X | NO | CBR | e/e tmg req'd | N/A | CC 63 |
| 3 | 0 | X | NO | no indication | no indication | VBR-NRT | x |
| 3 | 1 | X | NO | no indication | no indication | N/A | CC 63 |
| 3 | 2 | X | NO | no indication | no indication | VBR-RT | x |
| 3 | 3 | X | NO | no indication | no indication | VBR-NRT | x |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 3 | 4 | X | NO | no indication | no indication | UBR | x |
| 3 | 0 | X | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 3 | 1 | X | NO | VBR | e/e tmg not req'd | N/A | CC 63 |
| 3 | 2 | X | NO | VBR | e/e tmg not req'd | VBR-RT | x |
| 3 | 3 | X | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 3 | 4 | X | NO | VBR | e/e tmg not req'd | UBR | x |
| 4 | 0 | C | NO | N/A | N/A | VBR-NRT | x |
| 4 | 1 | C | NO | N/A | N/A | CBR | x |
| 4 | 2 | C | NO | N/A | N/A | VBR-RT | x |
| 4 | 3 | C | NO | N/A | N/A | VBR-NRT | x |
| 4 | 4 | C | NO | N/A | N/A | UBR | x |
| 5 | 0 | X | NO | no indication | no indication | VBR-NRT | x |
| 5 | 1 | X | NO | no indication | no indication | N/A | CC 63 |
| 5 | 2 | X | NO | no indication | no indication | VBR-RT | x |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 5 | 3 | X | NO | no indication | no indication | VBR-NRT | x |
| 5 | 4 | X | NO | no indication | no indication | UBR | x |
| 5 | 0 | X | NO | VBR | e/e tmg not req’d | VBR-NRT | x |
| 5 | 1 | X | NO | VBR | e/e tmg not req’d | N/A | CC 63 |
| 5 | 2 | X | NO | VBR | e/e tmg not req’d | VBR-RT | xx |
| 5 | 3 | X | NO | VBR | e/e tmg not req’d | VBR-NRT | x |
| 5 | 4 | X | NO | VBR | e/e tmg not req’d | UBR | x |
| 6 | 0 | C | NO | N/A | N/A | VBR-NRT | x |
| 6 | 1 | C | NO | N/A | N/A | CBR | x |
| 6 | 2 | C | NO | N/A | N/A | VBR-RT | x |
| 6 | 3 | C | NO | N/A | N/A | VBR-NRT | x |
| 6 | 4 | C | NO | N/A | N/A | UBR | x |
| 7 | 0 | X | NO | no indication | no indication | VBR-NRT | x |
| 7 | 1 | X | NO | no indication | no indication | N/A | CC 63 |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 7 | 2 | X | NO | no indication | no indication | VBR-RT | x |
| 7 | 3 | X | NO | no indication | no indication | VBR-NRT | x |
| 7 | 4 | X | NO | no indication | no indication | UBR | x |
| 7 | 0 | X | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 7 | 1 | X | NO | VBR | e/e tmg not req'd | N/A | CC 63 |
| 7 | 2 | X | NO | VBR | e/e tmg not req'd | VBR-RT | x |
| 7 | 3 | X | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 7 | 4 | X | NO | VBR | e/e tmg not req'd | UBR | x |
| 8 | 0 | A | NO | no indication | no indication | CBR | x |
| 8 | 1 | A | NO | no indication | no indication | CBR | x |
| 8 | 2 | A | NO | no indication | no indication | VBR-RT | x |
| 8 | 3 | A | NO | no indication | no indication | VBR-NRT | x |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 8 | 4 | A | NO | no indication | no indication | UBR | x |
| 8 | 0 | C | NO | no indication | no indication | CBR | x |
| 8 | 1 | C | NO | no indication | no indication | CBR | x |
| 8 | 2 | C | NO | no indication | no indication | VBR-RT | x |
| 8 | 3 | C | NO | no indication | no indication | VBR-NRT | x |
| 8 | 4 | C | NO | no indication | no indication | UBR | x |
| 9 | 0 | X | NO | CBR | e/e tmg req’d | CBR | xx |
| 9 | 1 | X | NO | CBR | e/e tmg req’d | CBR | x |
| 9 | 2 | X | NO | CBR | e/e tmg req’d | N/A | CC 63 |
| 9 | 3 | X | NO | CBR | e/e tmg req’d | N/A | CC 63 |
| 9 | 4 | X | NO | CBR | e/e tmg req’d | N/A | CC 63 |
| 10 | 0 | C | NO | no indication | no indication | VBR-NRT | x |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 10 | 1 | C | NO | no indication | no indication | N/A | CC 63 |
| 10 | 2 | C | NO | no indication | no indication | VBR-RT | x |
| 10 | 3 | C | NO | no indication | no indication | VBR-NRT | x |
| 10 | 4 | C | NO | no indication | no indication | UBR | x |
| 10 | 0 | C | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 10 | 1 | C | NO | VBR | e/e tmg not req'd | N/A | CC 63 |
| 10 | 2 | C | NO | VBR | e/e tmg not req'd | VBR-RT | x |
| 10 | 3 | C | NO | VBR | e/e tmg not req'd | VBR-NRT | x |
| 10 | 4 | C | NO | VBR | e/e tmg not req'd | UBR | x |
| 11 | 0 | C | YES | N/A | N/A | UBR | x |
| 11 | 1 | C | YES | N/A | N/A | N/A | CC 63 |
| 11 | 2 | C | YES | N/A | N/A | N/A | CC 63 |
| 11 | 3 | C | YES | N/A | N/A | N/A | CC 63 |
| 11 | 4 | C | YES | N/A | N/A | N/A | CC 63 |

Table E-2. CBX 500 Service Category Mappings (Based on Signalled QoS, BBC, BEI) (Continued)

| Table E-1 (App F.) Column | QoS | BBC | BEI | Traffic Type | Timing Req. | CBX 500 Service Category | Notes |
|---|---|---|---|---|---|---|---|
| 12 | 0 | X | YES | no indication | no indication | UBR | x |
| 12 | 1 | X | YES | no indication | no indication | N/A | CC 63 |
| 12 | 2 | X | YES | no indication | no indication | N/A | CC 63 |
| 12 | 3 | X | YES | no indication | no indication | N/A | CC 63 |
| 12 | 4 | X | YES | no indication | no indication | N/A | CC 63 |
| 12 | 0 | X | YES | VBR | e/e tmg not req'd | UBR | x |
| 12 | 1 | X | YES | VBR | e/e tmg not req'd | N/A | CC 63 |
| 12 | 2 | X | YES | VBR | e/e tmg not req'd | N/A | CC 63 |
| 12 | 3 | X | YES | VBR | e/e tmg not req'd | N/A | CC 63 |
| 12 | 4 | X | YES | VBR | e/e tmg not req'd | N/A | CC 63 |

# F

# Using SVC Failure Information

This appendix describes how to use SVC failure location information displayed in the failure location and failure cause fields on the Show Failed Call Attributes dialog box (see Figure 2-14 on page 2-41). The Show Failed Call Attributes dialog box displays the reason for the SVC failure (using the ATM Forum UNI 3.0/3.1 standard cause codes), and the location where the failure occurred.

Using the sample network shown in Figure F-1, the CBX 500 switches are deployed in a UNI signalling environment where Links A-D are running UNI signalling (for example 3.0, 3.1, or IISP). The majority of UNI signalling activity involves users (workstation and routers) at Campus ATM Network #1 using SVCs to establish ATM connectivity with users at Campus ATM Network #2. If one of these SVC attempts fail, the CBX 500 records the event.

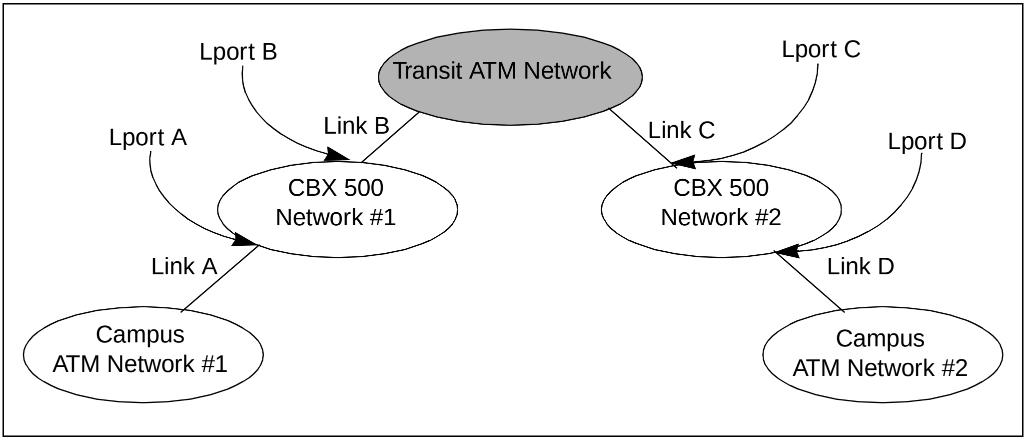



**Figure F-1. Transit ATM Network**

Table F-1 describes an example of the failure conditions that may occur and displays the Show All Failed SVC log information (see Figure 2-13 on page 2-39). The information in Table F-1 uses the sample network shown in Figure F-1 as an example. All SVC attempts described in this table are from Campus Network 1 to Campus Network 2.

The following abbreviations are used in the table:

- loc = the switch/lport reported in the SVC Failure Location fields.
- no entry = no SVC failure reported at this lport.
- rel = whether the RELEASE was received (rx) on the logical port or transmitted (tx) by the logical port.

Table F-1. SVC Failure Location information for Sample Transit Network

| Failure Type | Failure location Entry at | | | | Notes |
|---|---|---|---|---|---|
| | LPort A | LPort B | LPort C | LPort D | |
| link A down | no entry | no entry | no entry | no entry | link A is down - call never reaches CBX 500 #1. |
| link B down | loc=A rel=tx | no entry | no entry | no entry | link B is down - routing never sends attempt to B. Failure is only reported at A. |
| link C is down | loc=B rel=tx | loc=B rel=rx | no entry | no entry | link C is down - SVC attempts sent to transit network but release is returned from transit network. |
| link D is down | loc=B rel=tx | loc=B rel=rx | loc=C rel=tx | no entry | link D is down - SVC attempt is sent to transit network but release is returned from CBX 500 #2 and passed back to CBX 500 #1 via transit network. |
| called party user down at Campus 2 | loc=B rel=tx | loc=B rel=rx | loc=D rel=tx | loc=D rel=rx | release is received from Campus 2 and forwarded back to CBX 500 #2, transit, CBX 500 #1. |

The public/private network indication is extracted from the release message that is either transmitted by the CBX 500 or received by the CBX 500. You should take the following into consideration when you use the SVC failure location information:

- If the release message is transmitted by the CBX 500, the CBX 500 inserts "public" or "private" based on the lport setting (for DCE lports).
- If the release message is received by the CBX 500, the information inserted by the other switch is used in the SVC failure location field.

In general, different switches exhibit different behavior in this area. For this reason it is difficult to use public/private as a true indication of where the failure occurs

The configuration shown in Figure F-1 on page F-2 uses a transit network between two CBX 500 networks. In this configuration, troubleshooting is more difficult. The SVC failure location information shown in Figure F-2 is more useful because SVC information can be shared between the two networks (over the direct or OPTimum trunks). This is not the case when a UNI interface exists between the two networks.

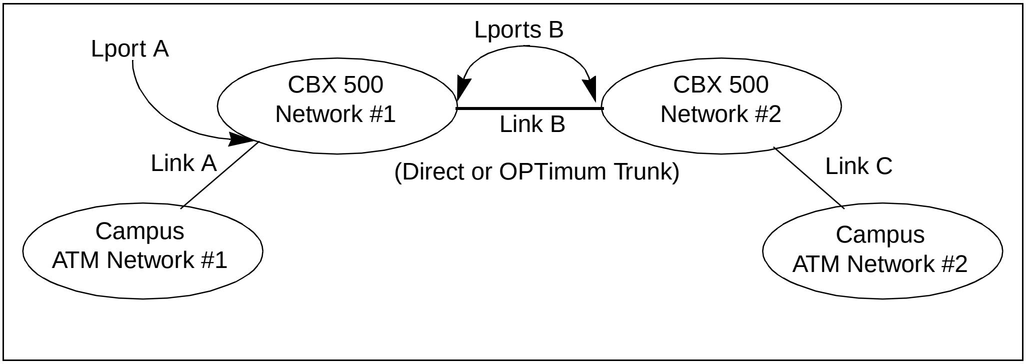



**Figure F-2. Two CBX 500 Networks (Direct or OPTimum Trunk)**

Table F-2 describes the failure conditions that may occur (using the example in Figure F-2) and displays the Show All Failed SVC log information. All SVC attempts described in this table are from Campus Network 1 to Campus Network 2.

**Table F-2. SVC Failure Location Information for all CBX 500 Scenarios**

| Failure Type | Failure location Entry at | | | Notes |
|---|---|---|---|---|
| | LPort A | LPorts B | LPort C | |
| link A down | no entry | failure info only provided on UNI ports (not trunk ports) | no entry | link A is down - call never reaches CBX 500 #1. |
| link B down | loc=A rel=tx | failure info only provided on UNI ports (not trunk ports) | no entry | link B is down - routing never sends attempt to B. Failure is only reported at A. |
| link C down | loc=B rel=tx | failure info only provided on UNI ports (not trunk ports) | no entry | link C is down - routing never sends attempt to B, so failure is only reported at A. |
| called party user down at Campus 2 | loc=B rel=tx | failure info only provided on UNI ports (not trunk ports) | loc=D rel=tx | release is received from Campus 2 and forwarded back to CBX #2 and CBX #1. |

# Index

**T**