Network Configuration Guide for CBX 500

Ascend Communications, Inc.

Product Code: 80049
Revision 00
August 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

7 Configuring ATM Logical Ports

9 Configuring PVCs

10 Configuring SVC Parameters

List of Figures

List of Tables

About This Guide

The *Network Configuration Guide for CBX 500* provides detailed instructions for using CascadeView/UX to set up and manage a network map and configure WAN services on a Cascade-switch network. Specifically, this guide describes how to configure Cascade switches, physical and logical ports, trunks, and circuits.

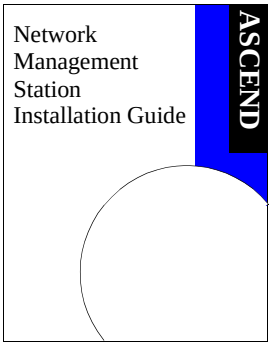
This guide also describes all the features supported in CascadeView/UX Release 2.4 and CBX 500 switch software, Release 2.0.

What You Need to Know

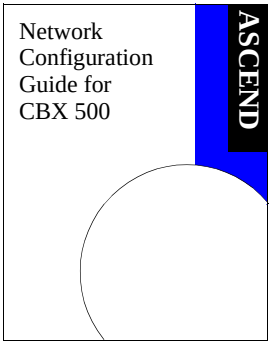
As a reader of this guide, you should know UNIX operating system commands and be familiar with HP OpenView. The system administrator should be familiar with relational database software to properly maintain Sybase, which is the database used by CascadeView. This guide assumes that you have installed the Cascade switch hardware using the *CBX 500 Hardware Installation Guide.*

Documentation Reading Path

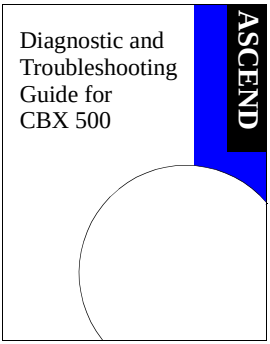
The following manuals provide the complete document set for the NMS Release 2.4:



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 and configure switches, and download your configuration from the NMS to the switch.



After configuring your network, use this guide to fine-tune 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

The following table highlights the chapters in this guide.

Read	To Learn About
Chapter 1	General features of CascadeView/UX and the Network Management Station (NMS).
Chapter 2	The following CascadeView/UX system administration tasks: • NMS startup and shutdown • CascadeView/UX security passwords • Audit Trail utility
Chapter 3	Creating an ATM direct trunk between two switches. This configuration example enables you to verify the software and hardware installation.
Chapter 4	Managing network maps, for example: • Create and add objects to a network map • Designate the Class B IP addressing scheme • Create a Virtual Private Network (VPN)
Chapter 5	Configuring switch attributes, for example: • Configure a gateway switch for routing SNMP information to and from the NMS • Define additional NMS workstations
Chapter 6	Setting the card attributes for each type of I/O module installed in the switch. This chapter also describes how to configure the physical port parameters and performance monitoring statistics.

Read	To Learn About
Chapter 7	Configuring the various ATM logical port types. This chapter also describes how to designate logical ports for fault tolerant PVCs and VPNs.
Chapter 8	Configuring trunk parameters and adding trunk-line connections to your network map. This chapter also describes how to configure a trunk as part of a VPN.
Chapter 9	Defining PVC connections, point-to-multipoint circuits, and management VPI/VCI and PVC connections. This chapter also describes how to: • Configure a circuit as a fault tolerant PVC • Move circuits
Chapter 10	Defining the SVC parameters for the switch, including the node prefixes, port prefixes, addresses, and call screening parameters.
Chapter 11	Creating a soft PVC (SPVC) within the network using signalling.
Chapter 12	Generating a configuration file and downloading it to the switch. This chapter also describes how to: • Synchronize the switch Parameter Random Access Memory (PRAM Synch) • Upload PRAM • Clear or erase PRAM
Chapter 13	Closed User Groups (CUGs) that enable you to divide all network users into logically linked groups of users.
Chapter 14	Using Port Security Screening to ensure that your network cannot be compromised. You do this by creating screens which can allow/disallow incoming and outgoing calls.

The following appendices provide additional information to help you manage your network.

Read	To Learn About
Appendix A	Tuning Cascade's Call Master Connection Admission Control (CAC) function to optimize your network resources.
Appendix B	Configuration options provided by the *cascadeview.cfg* file.
Appendix C	The Poll Server function, which can reduce CascadeView's status polling overhead when there are multiple CascadeView users monitoring the network simultaneously.
Appendix D	How each ATM traffic descriptor combination affects the cell streams under different traffic conditions.
Glossary	Technical terms used in this guide.

What's New in this Guide?

Table 1 lists the new product features in this release, as well as the enhancements and changes made to this guide.

Table 1. NMS Release 2.4 Features

NMS Release 2.4 New Features	Enables You to...	Described in
STM-1 Copper	Support the STM-1 copper input/output adapter (IOA) daughter card. This IOA complies with the G.703 specification.	Chapter 6
Configurable Alarm Soak/Alarm Clear Timers	Modify the following ANSI standard values: • A 2.5 second alarm failure timer that determines how long the switch waits ("soaks") before declaring a physical layer problem (i.e., loss of signal) a failure. • A 10 second alarm clear timer that determines how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved.	Chapter 6
T1 Far-End Loopback	Enable or disable an individual T1 ports ability to automatically respond to inband loop-up requests.	Chapter 6
Header Error Correction (HEC)	Enable or disable header error correction (HEC) on all CBX 500 physical ports.	Chapter 6
OC12/STM-4 APS	Use Automatic Protection Switching (APS) on the OC12/STM4 module. This feature allows you to use the second port on this module as a backup.	Chapter 6

Table 1. NMS Release 2.4 Features (Continued)

NMS Release 2.4 New Features	Enables You to...	Described in
ANSI.231 Performance Monitoring for DS3/E3 and OC3/STM1 modules	Configure performance monitoring functions, as derived from ANSI.231. Performance monitoring enables you to detect performance degradation in network elements at the device driver level.	Chapter 6
Virtual UNI	Configure multiple UNI logical ports on one physical port. This feature is useful when you need to support multiple UNI signalling channels on a single physical port. This feature also allows you to use signalling and ILMI channels on VPIs other than zero.	Chapter 7
NNI Logical Port Type/B-ICI 1.1	Use the B-ISDN Inter-Carrier Interface (B-ICI) protocol to interconnect ATM-based public networks belonging to two different carriers.	Chapter 7
SVC VPI/VCI Range	Use one VPI/VCI range for PVCs on a logical port and a different (smaller) VPI/VCI range for SVCs on the same logical port. This feature enables a CBX 500 to interoperate with an SVC-capable CPE that only supports the use of VPI 0 for SVCs. Use the SVC range to limit SVCs to VPI 0; PVCs still use the full VPI range.	Chapter 7

Table 1. NMS Release 2.4 Features (Continued)

NMS Release 2.4 New Features	Enables You to...	Described in
Management PVCs	Use the CBX 500 management port as a circuit endpoint, and connect this endpoint to any UNI or NNI logical port type to create the management PVC (MPVC). The MPVC is a data path that provides an access point to the CBX 500 network management plane. Use an MPVC as the NMS path when you need to retrieve billing and accounting information from a switch.	Chapter 5 and Chapter 9
SVC ILMI Address Registration	Enable or Disable ILMI address registration on a per-address or prefix basis. You can now enable ILMI on a UNI port for management purposes, and at the same time block ILMI address registration for SVCs.	Chapter 10
SVC Load Balancing	Mark UNI ports supporting SVCs as "load balancing eligible." This enables you to specify (on a per-port basis) how long an SVC should be up before being eligible for load balancing reroutes. This feature is useful for those SVCs that are long-term, and may encounter a forced reroute due to trunk failure.	Chapter 10

Table 1. NMS Release 2.4 Features (Continued)

NMS Release 2.4 New Features	Enables You to...	Described in
Configurable SVC Trap Thresholds	Configure a value for the number of SVC failures that can occur on a UNI port before a trap is issued.	Chapter 10
Soft PVCs (SPVCs)	Connect a non-SVC terminal to the CBX 500 using a PVC that is established using a VPI or VPI/VCI address. This configuration allows SVC-capable network devices to signal an SVC request to this address, and in turn, the port associated with this address establishes a connection to the non-SVC terminal.	Chapter 11
SVC Closed User Group (CUG)	Divide all network users into logically linked groups of users. Members of the same CUG have particular calling privileges that members of different CUGs may not have. The CUG feature allocates and enforces the CUG concepts as defined in ITU-T Recommendation Q.2955.1.	Chapter 13
Port Security Screening	Create screens that can allow/disallow incoming and outgoing calls, thus ensuring that your network cannot be compromised. This feature adds intelligent network call screening functionality to the existing basic call support.	Chapter 14

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* (Product code: 80011)
- *Diagnostic and Troubleshooting Guide for CBX 500* (Product code: 80050)
- *ATM Flow-Control Processor User's Guide* (Product code: 80048)
- *Accounting System Administrator's Guide* (Product code: 80046)
- *Bulk Statistics Collector for CBX 500 User's Guide* (Product code: 80047)
- *Networking Services Technology Overview* (Product code: 80001)
- *Network Management Station Installation Guide* (Product code: 80014)
- *Network Configuration Guide for B-STDX/STDX* (Product code: 80017)
- *Cascade Enterprise MIB Definitions* (Product code: 80015)
- *SYBASE 11 SQL Server Upgrade Guide* (Product code: 80040)
- *Upgrading to Solaris 2.5.1 and HP OpenView 4.11* (Product code: 80045)

Third Party

- *Solaris 2.4 System Configuration and Installation Guide*
- *HP OpenView Windows User's Guide* (for HP 9000 Series and Sun SPARCstation)
- *SYBASE Command 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 to avoid equipment damage or personal harm.

1

Overview

CascadeView/UX is an integrated network management software package that runs over HP OpenView on a Network Management Station (NMS). CascadeView/UX enables you to:

- Create and edit network maps
- Configure Cascade switches
- Configure multiple networks from a single NMS
- Create trunks and circuits
- Monitor and troubleshoot the network

Combined, these software programs present an easy-to-use graphical user interface that allows you to configure and maintain a Cascade network. HP OpenView provides the interface to add, modify, and delete nodes, trunks, and switch configurations from the network map and database.

About the Network Management Platform

CascadeView/UX resides on the HP OpenView platform, which provides integrated network and systems management solutions on an industry-standard platform. HP OpenView software enables you to create a graphical network map and use pull-down menus to configure, monitor, and diagnose equipment in the network.

CascadeView/UX provides a logical network configuration interface for setting network-wide parameters, provisioning individual circuits, and configuring other switch functions. CascadeView/UX provides defaults for all required parameters and prompts you for missing parameters, if necessary.

You download the initial network configuration and any updates from the NMS to the switch. The switch stores this configuration in Parameter Random Access Memory (PRAM).

About the Network Management Station

The Cascade family of multiservice WAN switches contains a Simple Network Management Protocol (SNMP) agent, which means you can manage a Cascade switch from any SNMP management system that supports the Cascade Enterprise MIB extensions. When you configure an NMS with CascadeView/UX, the NMS communicates with the switches through either the Internet Protocol (IP) for in-band management connections, or the Serial Line Internet Protocol (SLIP) for out-of-band management.

The NMS running CascadeView/UX supports in-band management using an Ethernet connection to a local Cascade switch; alternately, you can configure the NMS and the switch on the same IP network. The NMS can also access any out-of-band switch via a dial-up modem.

Monitoring

After you create your Cascade network, you can closely monitor network activity using the CascadeView/UX monitoring features. CascadeView/UX provides several options for obtaining status information from the network. The Monitor menu Cascade Objects selection enables you to obtain status information for a switch, port, trunk, circuit, and SVC. You can also monitor the network by running diagnostics, collecting statistical data, generating reports, and reviewing the traps log. For more information, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.

Troubleshooting

CascadeView/UX uses a color scheme to identify network problems. When you open a network map, all nodes that are operational and communicating with the NMS appear green. Nodes that are either not operational or unable to communicate with the NMS appear red or wheat, respectively. CascadeView/UX also uses a color scheme to indicate the status of a configured trunk link between two Cascade switches. For more information, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.

2

Managing the NMS

This chapter describes the following administrative tasks:

- Starting the NMS and running CascadeView/UX. This procedure includes starting the Sybase Server and initiating an HP OpenView session.
- Defining passwords and assigning access levels.
- Using the Audit Trail feature to keep track of changes.
- Shutting down the NMS.

Starting the NMS

Before you can access CascadeView/UX, you must start the Sybase server and initiate an HP OpenView session as described in the following procedure. If you need to start a remote session to the NMS, consult your UNIX system administrator to set up an Xterm session.

To start the NMS:

1. Power on the SparcStation.
2. At the console prompt, log in as the nms user and type the appropriate password. (This is the login you entered when you installed Solaris.)

   The system starts Solaris OpenWindows and displays the $ prompt in the Cmdtool (CONSOLE) window.
3. *If you are using Sybase 11*, skip to Step 11 on page 2-3. Otherwise, follow Step 4 through Step 10 to start the Sybase Server and access HP OpenView.
4. Log in as the sybase user by entering:

   ```
   su - sybase
   ```
5. At the prompt, enter [*your Sybase password*].
6. Enter the following commands to start the Sybase Server:

   ```
   cd install <Return>
   startserver -f RUN_CASCADE <Return>
   ```
7. When the system displays the last line of text, ‘iso_1’ (ID = 1)., press Return.
8. At the $ prompt, enter **exit** to log out as the sybase user.
9. Log in as the root user and at the prompt, enter the root password.
10. To start HP OpenView processes enter:

    ```
    /usr/OV/bin/ovstart
    ```

11. To start HP OpenView, enter **/usr/OV/bin/ovw &** in a console window. The default HP OpenView window appears.

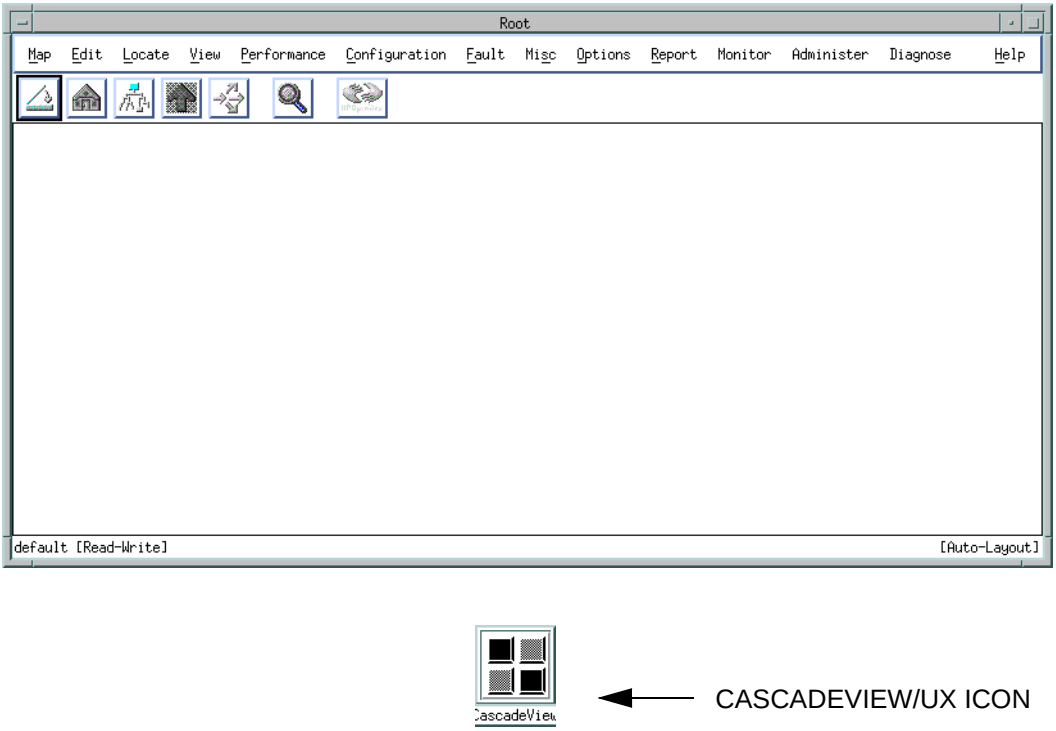


Figure 2-1. CascadeView/UX Window

The Cascadeview icon should appear on the window manager desktop. This indicates that CascadeView/UX is running. Do not invoke any CascadeView/UX commands until this icon appears. Do not close this icon unless one of the supporting programs (such as HP OpenView) stops processing.

About Passwords

When you access HP OpenView, you can display network maps and use any of the monitoring functions without having to log on. However, you cannot perform any network management functions without logging on with the appropriate password.

When you install Sybase, the maximum number of users is set to 50. In a typical network operations center, you assign only one administrator password. You then need at least one operator logon to use all network features.

You can define three levels of access for CascadeView. These include:

Administrator — Create passwords. The default is *admin*. For security reasons, you should first create a new administrator password, then create operator and provisioning passwords.

Operator — Provision (configure) and manage all network features. The default is *cascade*. You must log on with this password to configure physical ports and download a switch configuration.

Provisioning — Configure and monitor logical ports, trunks, and circuits on the network. The default is *provision*. The provisioning password only allows you to perform these basic configuration tasks. You log on as *operator* to download software and configure switch and physical port parameters.

Defining Passwords

To define access levels and modify the default passwords:

1. From the Administer menu, select CascadeView ⇒ Set Password and select one of three access levels: Provisioning, Operator, or Administrator. The CV – Change [*level*] Password dialog box appears.

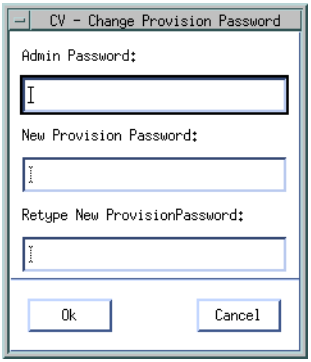


Figure 2-2. Change [level] Password Dialog Box

2. Enter the Admin Password.
3. Enter a new [*level*] password.
4. Retype the password in the field provided.
5. Choose OK.
6. Repeat Step 1 through Step 5 to define additional passwords for each access level.

Logging On

To access the CascadeView logon dialog box, from the HP OpenView Misc menu, select CascadeView ⇒ Logon and enter the appropriate password.

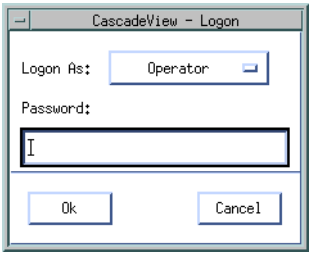


Figure 2-3. CascadeView Logon Dialog Box

Using the Audit Trail

The Audit Trail function keeps a record of the changes you make to a network map. You can retrieve this information from the database whenever you need to review these changes.

The Audit Trail function logs the following network activity:

- Switch becomes reachable or unreachable
- Invalid login
- Log in or log off
- Add, modify, or delete a switch, module, logical port, trunk, or circuit
- Reboot a switch or module
- Download switch software, initialization script file, or PRAM synch file
- Standby module takes over in a redundant pair
- Add, delete, or modify an NMS path or NMS entry
- User session timeout

Enabling Audit Trail

To enable the Audit Trail:

1. Log in as the root user by entering **su - root**. At the prompt, enter the root password.
2. In a command window, edit the *cascadeview.cfg* file by entering:

   ```
   vi /opt/CascadeView/etc/cascadeview.cfg
   ```

3. Set the **CV_AUDIT_TRAIL_ENABLE** environment variable in *cascadeview.cfg* by entering:

   ```
   CV_AUDIT_TRAIL_ENABLE=TRUE <Return>
   export CV_AUDIT_TRAIL_ENABLE <Return>
   ```

*To disable Audit Trail, enter: **CV_AUDIT_TRAIL_ENABLE=FALSE***

4. Enter **:wq!** to exit the vi editor and save your changes.
5. You must now shut down and then restart CascadeView/UX, as follows:
   a. From the File menu, select File ⇒ Exit to exit CascadeView/UX.
   b. Enter **su - root**.
   c. At the prompt, enter the root password.
   d. Enter the following lines to shut down HP OpenView services:

      ```
      cd /usr/OV/bin <Return>
      ./ovstop <Return>
      ```

   e. Enter **/usr/OV/bin/ovstart** to restart HP OpenView.
   f. Enter **/usr/OV/bin/ovw &** to restart CascadeView.
6. The Audit Trail creates an ASCII log file in the directory */opt/CascadeView.var /auditlog*. The directory and file permissions are set for the world, read/write (“rw”).

The filename format is *cv-audit-log.[day of the week].[date]*. For example, the file *cv-audit-log.thu.1-4-97* contains information for January 4, 1997.

The Audit Trail function creates a different file for each day of operation (a file for Monday, a file for Tuesday, and so on).

7. To view the ASCII log file, enter:

```
cd /opt/CascadeView.var <Return>
more cv-audit-log.[day of the week].[date] <Return>
```

The Audit Trail Window (Figure 2-4) shows an example log file using the "more" command.

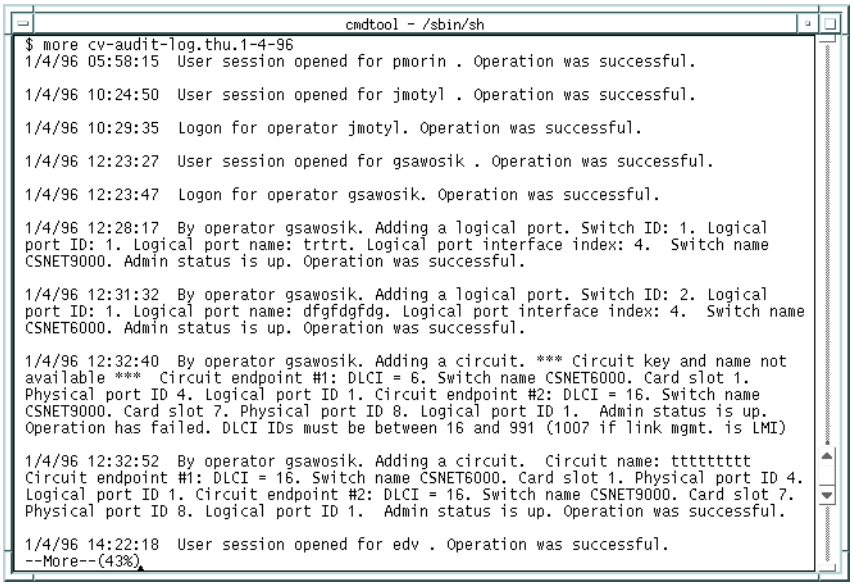


Figure 2-4. Audit Trail Window

Shutting Down CascadeView/UX

Use the following steps to close all NMS processes and power off the UNIX station:

1. From the HP OpenView File menu, select File ⇒ Exit to exit CascadeView/UX.
2. Log in as the root user by entering **su - root**.
3. At the prompt, enter the root password.
4. Enter the following command to shut down HP OpenView services:

   ```
   /usr/OV/bin/ovstop
   ```

5. Log in as the Sybase user by entering **su - sybase**.
6. At the prompt, enter the Sybase password.
7. *If you are using Sybase 11*, enter the following commands to shut down the backup server. Otherwise, proceed with Step 8.

   ```
   isql -U sa -P superbase <Return>
   1>shutdown SYB_BACKUP <Return>
   2>go <Return>
   ```

8. To shut down the Sybase server, enter:

   ```
   isql -U sa -P superbase <Return>
   1>shutdown <Return>
   2>go <Return>
   ```

9. Log in as the root user by entering **su - root**.
10. At the prompt, enter the root password.
11. At the # prompt, enter **init 0** to halt the system. This may take a few seconds.
12. At the ok prompt, power off the system.

Backup Procedures

As the CascadeView/UX administrator, you should back up the NMS database on a regular basis. For more information on Sybase and HP OpenView backup procedures, refer to the *Network Management Station Installation Guide*.

The Cascade Technical Response Center recommends that you perform daily backups of the Sybase server and the HP OpenView database.

If you need to recover switch data in the cascview database, contact the Technical Response Center for specific instructions. ***Do not*** *attempt to restore this database without Cascade's help. You can contact the Technical Response Center at one of the following numbers:*

1-800-DIAL-WAN (1-800-342-5926) or 1-508-692-2600 (in the United States and Canada)

1-508-952-1299 (outside the U.S., Canada, and United Kingdom)

0-800-96-2229 (in the United Kingdom)

3

Getting Started

This chapter describes how to configure the first switch (*gateway switch*) in your network and enable it to communicate with the NMS. The gateway switch acts as a master switch and communicates the status of all switches on the Cascade network to the NMS. When the NMS can communicate with the gateway switch, you can configure the second switch (and subsequent switches) on the network.

This chapter also describes the basic steps to configure an ATM direct trunk connection between the gateway switch and another switch. Use these procedures to verify your hardware and software installation. This basic example highlights many of the steps required to configure any switch in your network.

Basic Configuration Procedures

The sections in this chapter describe how to use an ATM direct trunk connection to connect the gateway switch and the second switch in a Cascade network.

These instructions describe switches that have never been initialized (new switches). If your switch contains an existing PRAM configuration, you must first clear the switch PRAM before you can download a new configuration. (Refer to "Erasing Parameter RAM" on page 12-20 for instructions.)

These instructions also assume a typical configuration in which the NMS uses a local Ethernet connection to access the switch. If the NMS connects to the Cascade switch network via remote access (for example, the NMS and the switch are on separate LANs), or through a management VCI/VPI, follow the instructions in Chapter 5 to configure the NMS access.

Before You Begin

Before you set up the gateway switch and NMS, verify that the following tasks are complete:

- ☑ Install the CBX 500 switch hardware and power it on as described in the *CBX 500 Hardware Installation Guide*. (Note the type of switch and the physical configuration of each installed I/O module.)
- ☑ Connect the NMS SPARCstation to the switch through one of the methods described in the *CBX 500 Hardware Installation Guide*. Note whether the NMS is connected via direct Ethernet or indirect Ethernet (on a separate LAN segment).
- ☑ Connect the NMS SPARCstation (either directly or through modems) to the switch through its serial port. This enables you to download the configuration file from the NMS to the switch.
- ☑ Install and configure the NMS software as described in the *Network Management Station Installation Guide*. During the CascadeView/UX installation, make note of the IP address and the network ID number you used to configure the static route. The NMS uses the IP address for the gateway switch and the network number for the network-wide parameters for the map.

Configuring the Gateway Switch and NMS

The procedures in this section describe how to synchronize the gateway switch and NMS SPARCstation so that they are communicating with each other.

Creating the Network Map

To create a new network map:

1. Access HP OpenView and start CascadeView/UX as described in Chapter 2.
2. To log on, from the Misc menu, select CascadeView ⇒ Logon and enter the operator password.

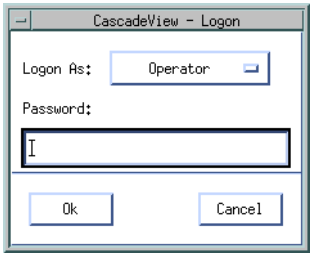


Figure 3-1. Logon Dialog Box

3. From the Maps menu, select Map ⇒ New. The following dialog box appears.

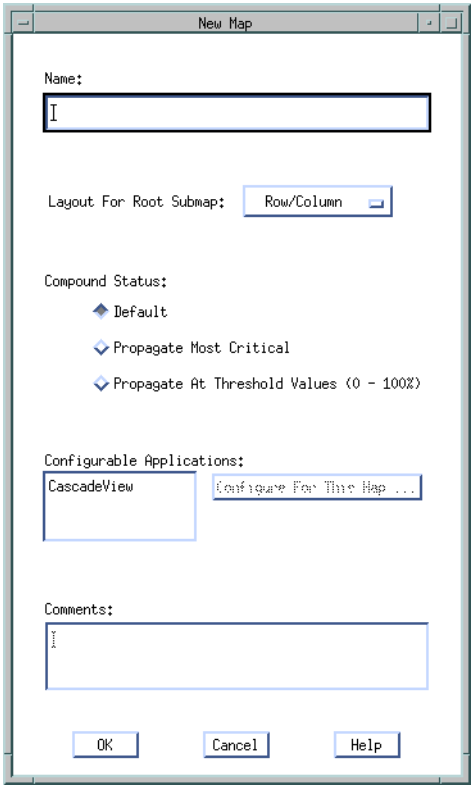


Figure 3-2. New Map Dialog Box

4. Enter a unique alphanumeric name to identify the map.

5. In the Configurable Applications list box, select CascadeView and choose Configure For This Map. The following dialog box appears.

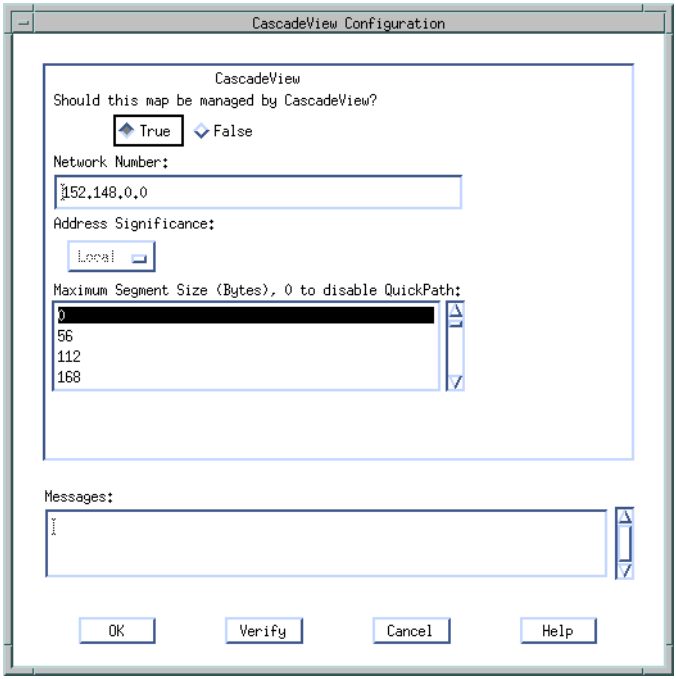


Figure 3-3. Configuration Dialog Box

Once set, you cannot modify these configuration parameters. If you need to change the network number after it is set, you must delete the map and start over. OSPF uses the network number for path selection. Before you change this setting, first check with the Cascade Technical Response Center for recommended guidelines.

6. Configure the following attributes for this map:

   a. "Should this map be managed by CascadeView?" Select True.

   b. The Network Number field displays the number you specified when you installed CascadeView/UX.

   c. Accept the default value for Address Significance.

   d. Set the Maximum Segment Size to 0 (this option is not supported).

   e. Choose Verify.

   f. Choose OK to return to the New Map dialog box.

   g. Choose OK again to exit the dialog box and display the new map.

If the IP Internet icon appears on the map, select the icon, and from the Map menu, select Unmanage Objects. Then from the Edit menu, select Hide ⇒ From All Submaps.

7. To log on to the new network map, from the Misc menu, select CascadeView ⇒ Logon (Figure 3-1 on page 3-3). Enter the operator password.

Creating a Subnet ID

To add a subnet ID:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Subnets. The following dialog box appears.

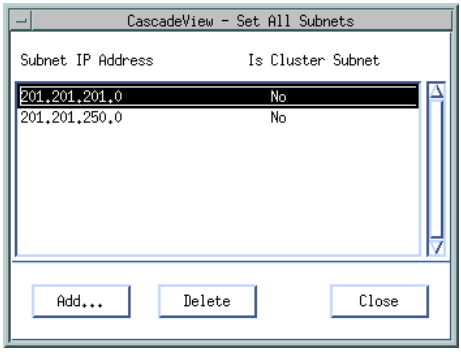


Figure 3-4. Set All Subnets Dialog Box

2. Choose Add. The following dialog box appears.

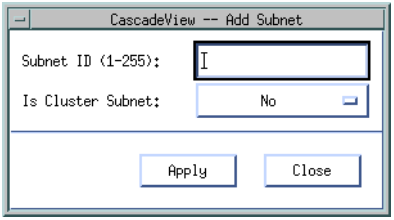


Figure 3-5. Add Subnet Dialog Box

3. Complete the Add Subnet dialog box fields as follows:

   Subnet ID (1-255) — Enter a subnet number between 1 and 255.

   Is Cluster Subnet (*optional*) — If you need to create clusters, select Yes in the Is Cluster Subnet field to make this subnet a cluster subnet. (Refer to page 4-12 for more information on clusters.)

4. Choose Apply to add the subnet ID.

5. Choose Close to exit the Add Subnet dialog box.

Configuring the Gateway Switch

To add the first switch to the map:

1. From the Edit menu, select Add Object.
2. Scroll through the Add Object:Palette dialog box and select Cascade Object. The Symbol Subclasses for Class Cascade Object appear.

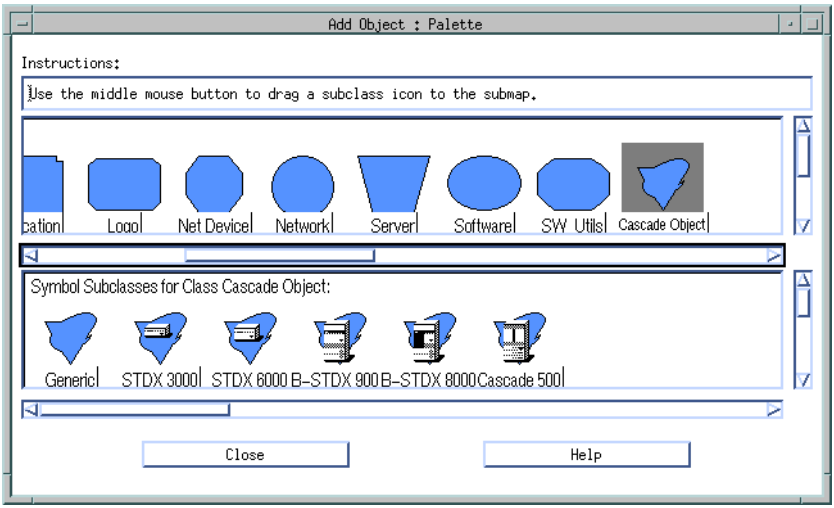


Figure 3-6. Add Object:Palette Dialog Box

3. Select the CBX 500 switch icon. Hold down the middle mouse button, drag the icon to the map, and release. The following dialog box appears.

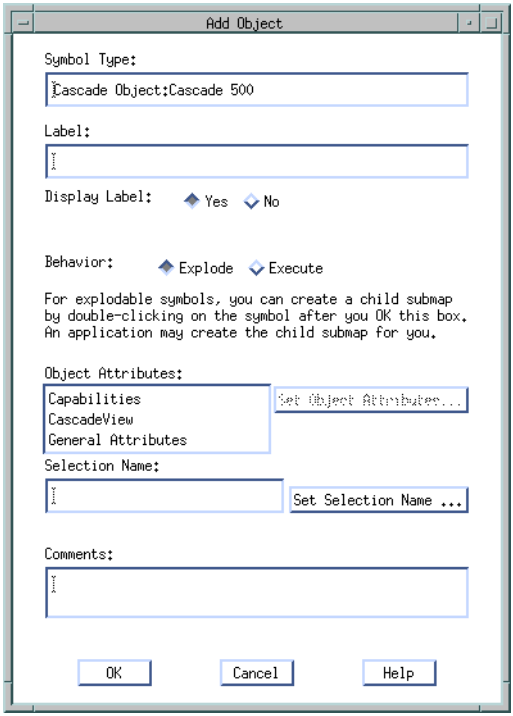


Figure 3-7. Add Object Dialog Box

4. Enter a label for the switch. This must be a unique name within CascadeView/UX.

5. In the Object Attributes box, select CascadeView and choose the Set Object Attributes button. The following dialog box appears.

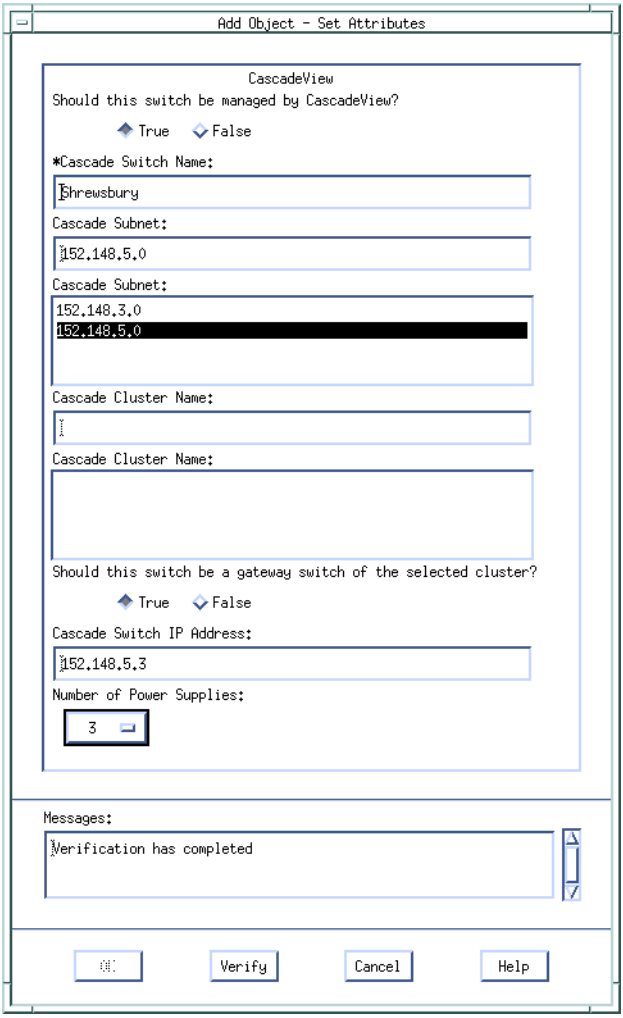


Figure 3-8. Add Object - Set Attributes Dialog Box

6. Complete the Add Object – Set Attributes dialog box as follows:

   a. “Should this switch be managed by CascadeView?” Select True.

   b. Enter the Cascade Switch Name (the same name you entered for the Label).

   c. Select the Cascade Subnet address from the list. The Cascade Cluster Name field displays the cluster to which this subnet belongs.

   d. “Should this switch be a gateway switch of the selected cluster?” Select True if this switch is the gateway switch.

   e. The Cascade Switch IP Address field displays the switch’s IP address.

   f. Make sure the number of power supplies displayed is correct.

   g. Choose Verify. The following message appears in the Messages field: `Verification has completed`.

   h. Choose OK to return to the Add Object dialog box.

7. Choose OK. At the Add Object:Palette dialog box, choose OK to return to the network map. The switch object appears blue and quickly turns red to indicate the NMS cannot access it.

8. To prevent SNMP time-outs, select the switch object, and from the Map menu, select Unmanage Objects. The switch object turns to a wheat color.

9. To configure the switch parameters, select the switch object. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box (Figure 3-9) appears.

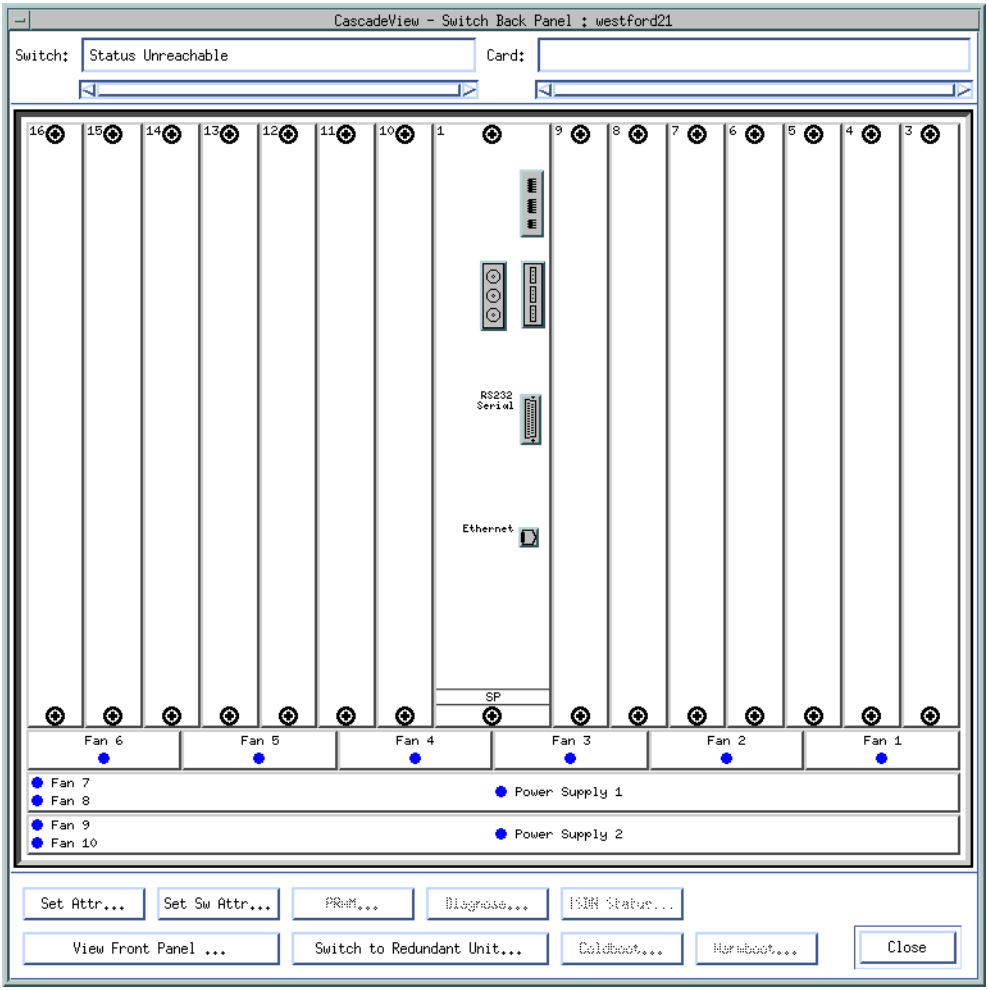


Figure 3-9. Switch Back Panel Dialog Box

10. Choose Set Sw Attr. The following dialog box appears.

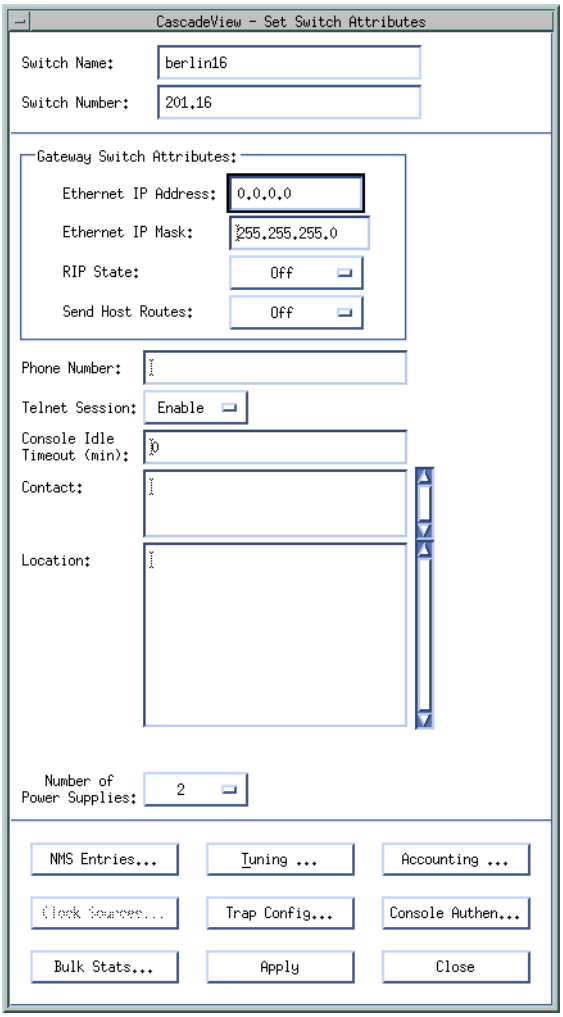


Figure 3-10. Set Switch Attributes Dialog Box

11. Complete the Set Switch Attributes dialog box as follows:

    a. If the NMS is connected to the switch via Ethernet, enter the local (external) IP address of the switch in the Ethernet IP Addr field. (The IP address is the one you specified during the CascadeView/UX installation when you added a static route. This IP address is used as the gateway Ethernet address.)

    b. You do not need to specify any other settings at this time. Choose Apply and then Close to return to the Set Switch Back Panel dialog box.

12. To configure the switch processor (SP) attributes for the Model 10 or Model 20 CBX 500, select SP module (middle slot) and choose Set Attr. The following dialog box appears.

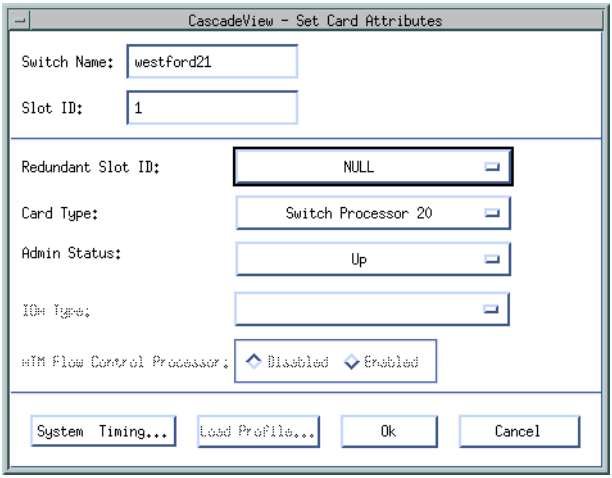


Figure 3-11. Set Card Attributes Dialog Box (for SP Modules)

13. Configure the SP attributes as follows (refer to “Configuring SP Attributes” on page 5-25 for more information):

    a. Select the Redundant Slot ID. The default, NULL, indicates a non-redundant configuration. Select 2 if you have a redundant SP installed in the switch.

    b. If you are configuring a Model 10, select SP10 as the Card Type. If you are using a Model 20, select SP20.

    c. Set the Admin Status to Up (default).

d. Choose System Timing. The following dialog box appears (refer to page 5-27 to change the defaults).

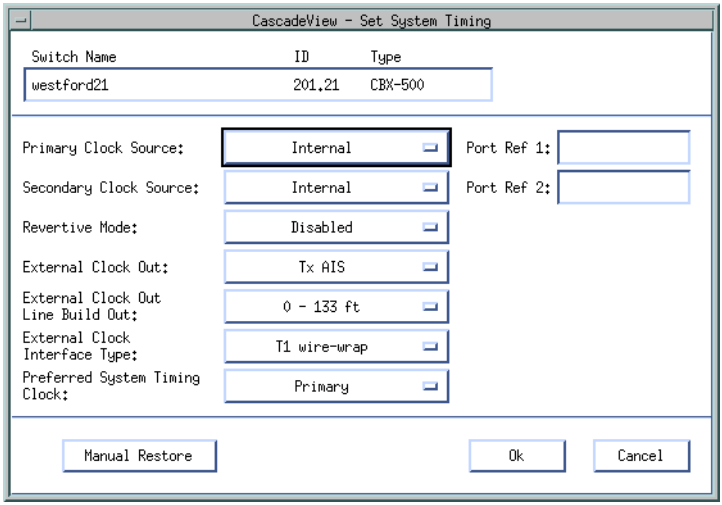


Figure 3-12. Set System Timing Dialog Box (for SP Modules)

e. Choose OK and then OK again to return to the Switch Back Panel dialog box.

14. To configure the first I/O module in the switch, select its representative slot location and choose Set Attr. The following dialog box appears.

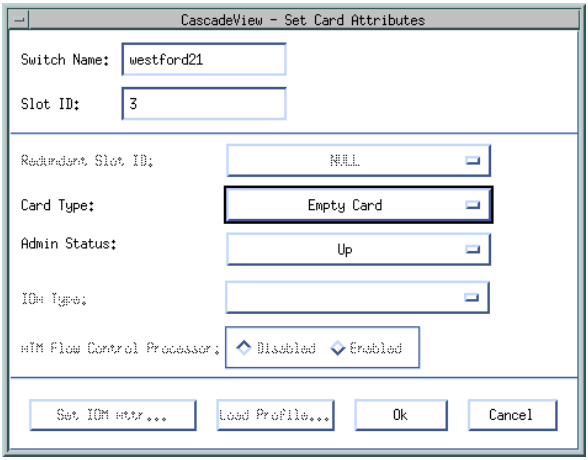


Figure 3-13. Set Card Attributes Dialog Box

15. Select the appropriate card type and verify the Admin Status is Up.
16. Choose Set IOM Attributes. The following dialog box appears.

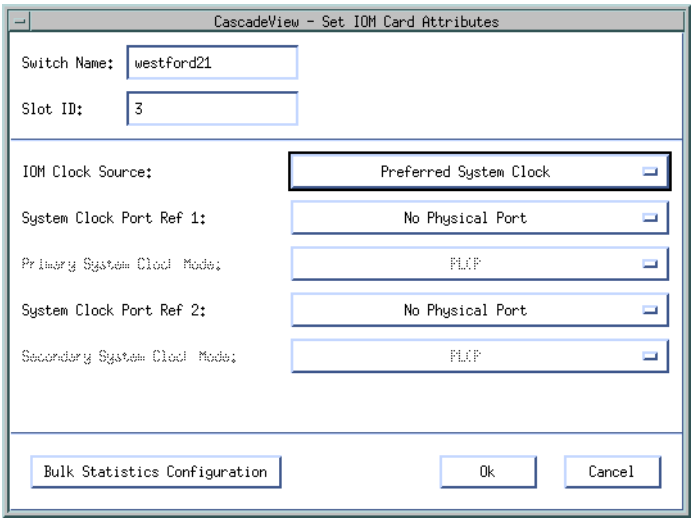


Figure 3-14. Set IOM Attributes Dialog Box (8 port DS3 module example)

17. Configure the IOM attributes for your module (refer to page 6-4 if you need to change the defaults). Choose OK.
18. Choose OK. Repeat Step 14 through Step 17 for each I/O module installed in this switch. When you finish, choose Close to return to the network map.

You must configure each I/O module installed in the switch for the switch to be fully synchronized with the NMS. However, you are not required to configure all physical and logical ports on each I/O module at this time.

19. Select the switch object. Then, from the Administer menu, select Cascade Parameters ⇒ Set NMS Paths. The Set NMS Paths dialog box appears.

20. Choose Add. The following dialog box appears.

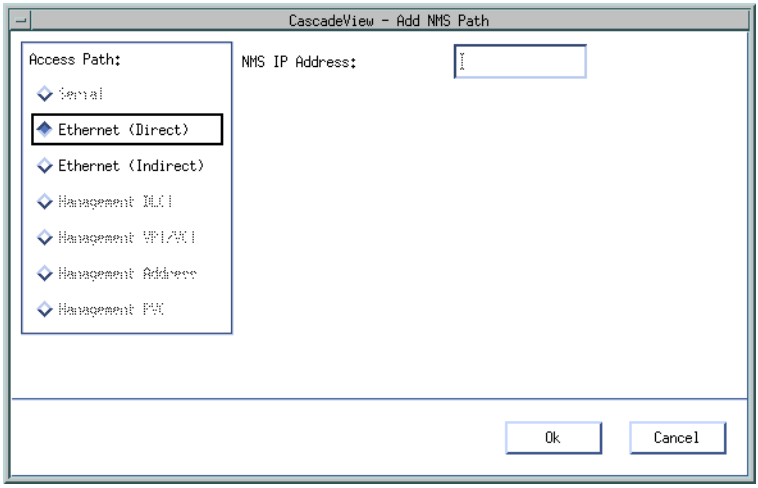


Figure 3-15. Add NMS Path Dialog Box

21. Complete the Add NMS Path dialog box as follows (refer to page 5-22 for more information):

    a. Select the Access Path you used to connect the NMS SPARCstation to the gateway switch.

    b. Enter the NMS IP address.

    c. Choose OK.

    d. Choose Close to return to the network map.

Establishing Switch-to-NMS Communications

Refer to Chapter 12 for procedures you can use to establish NMS-to-switch communications. The method you choose may vary according to your network needs.

Configuring the Second Switch on the Network Map

The following procedure describes the basic steps to get your second switch, and any other switches, synchronized and communicating with each other and the NMS.

Before you set up your next switch, verify the following tasks are complete:

- ☑ Configure the NMS SPARCstation and gateway switch as described in "Configuring the Gateway Switch and NMS" on page 3-3. The gateway switch object should be green on the map.
- ☑ Install the physical connection for the trunk line between this switch and the gateway (or any active switch that is a hop between this switch and the gateway). Refer to the appropriate hardware installation guide.

Adding a Second Switch to the Map

To add the second switch to the map, refer to "Configuring the Gateway Switch" on page 3-8 and follow Step 1 through Step 18. When you finish, the network map displays the second switch object, which is unmanaged (wheat color). The SP and I/O modules are configured.

Configuring the Trunk Physical Port

To configure the trunk physical port on the gateway switch:

1. On the network map, select the gateway switch object. Then, from the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (Figure 3-9 on page 3-12).
2. Select the physical port to use for the trunk connection and choose Set Attr. The Set Physical Port Attributes dialog box (Figure 3-16 on page 3-19) appears. This example shows an ATM DS3 I/O module. Refer to page 6-11 if you need to change the defaults.

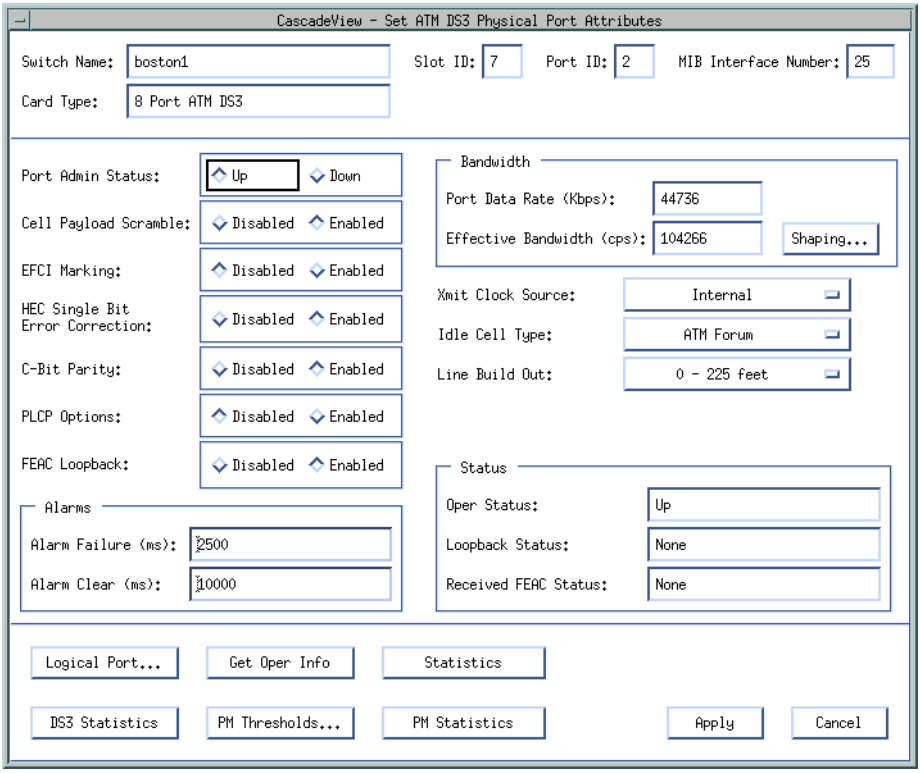


Figure 3-16. Set Physical Port Attributes Dialog Box (ATM DS3 example)

3. Specify the physical port attributes for the trunk connection. Verify that the Port Admin Status is Up.

4. Choose Apply to enter your selections.

Configuring the Trunk Logical Port

To configure the logical port settings for the trunk:

1. Choose the Logical Port command on the Set Physical Port Attributes dialog box. The Set All Logical Ports dialog box appears.
2. Choose Add. The following dialog box appears.

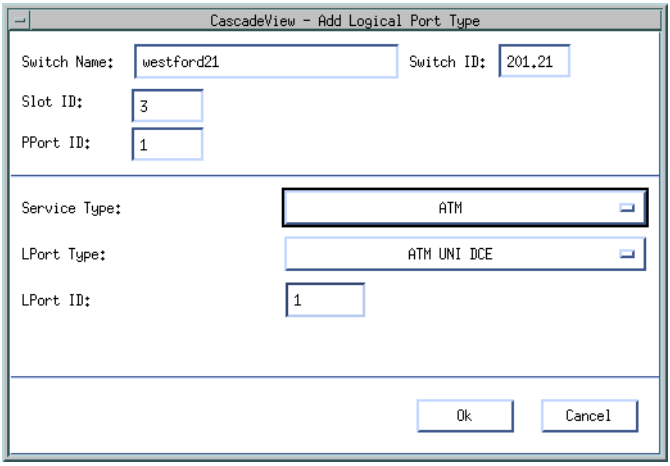


Figure 3-17. Add Logical Port Dialog Box

3. For the logical port type, select ATM Direct Trunk.
4. Choose OK.
5. The Add Logical Port dialog box reappears. Enter a logical port name and specify the bandwidth. (Refer to page 7-54 for more information about ATM direct trunks.)

> *Be sure to set the logical port to the same bandwidth on either end of the trunk connection. The NMS does not allow you to create a trunk if the logical port bandwidth is not identical for the two endpoints.*

6. Choose OK to return to the Set All Logical Ports dialog box. Choose Close, then Cancel to return to the network map.

You now need to set up the physical and logical port at the other end of the trunk. Repeat the steps described in “Configuring the Trunk Physical Port” on page 3-18 and “Configuring the Trunk Logical Port” on page 3-20.

Defining the Trunk Configuration

To configure the trunk between the gateway switch and the second switch:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears.

2. Choose Add. The following dialog box appears.

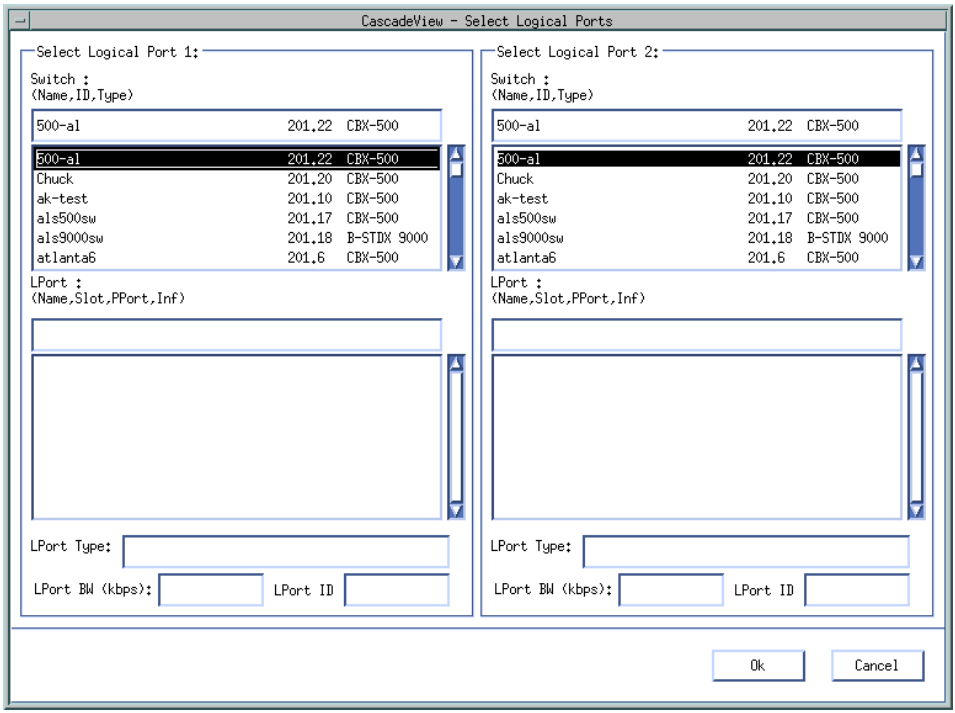


Figure 3-18. Select Logical Ports Dialog Box

3. Select the name of the switch where logical port 1 resides, then select the name of the switch where logical port 2 resides.

4. Select the name of logical port 1, then select the name of logical port 2.

5. Review the LPort Bandwidth field for each endpoint to make sure the bandwidth is identical. Choose OK. The following dialog box appears.

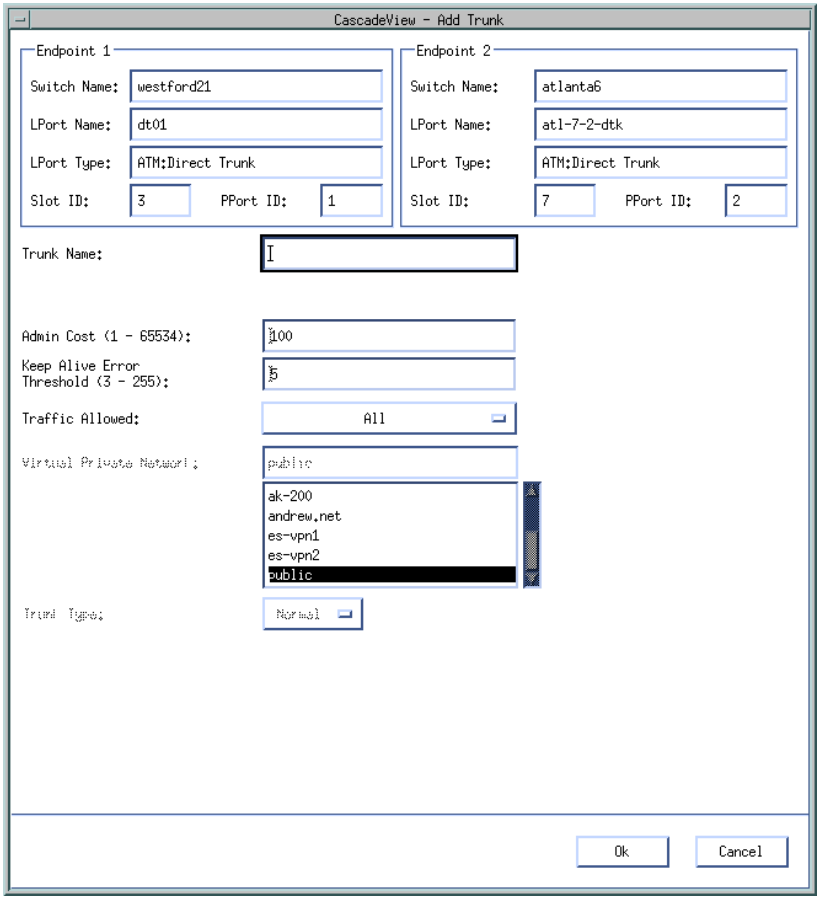


Figure 3-19. Add Trunk Dialog Box

6. Enter a trunk name. (Use this name when you create the trunk line connection in the next section.)

7. Specify the Admin Cost. (For more information about the fields on this screen, refer to page 8-15.)

8. Choose OK and then Close to return to the network map.

Adding a Trunk-Line Connection

To add the trunk line to the network map:

1. From the Edit menu, select Add Connection. The following dialog box appears.

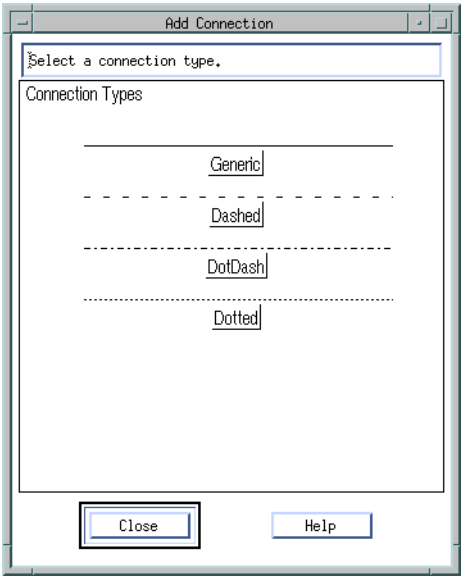


Figure 3-20. Add Connection Dialog Box

2. Select the type of line you want to use to represent the trunk connection.

3. On the network map, click on the first switch object (source symbol) and then click on the second switch object (destination symbol). The following dialog box appears.

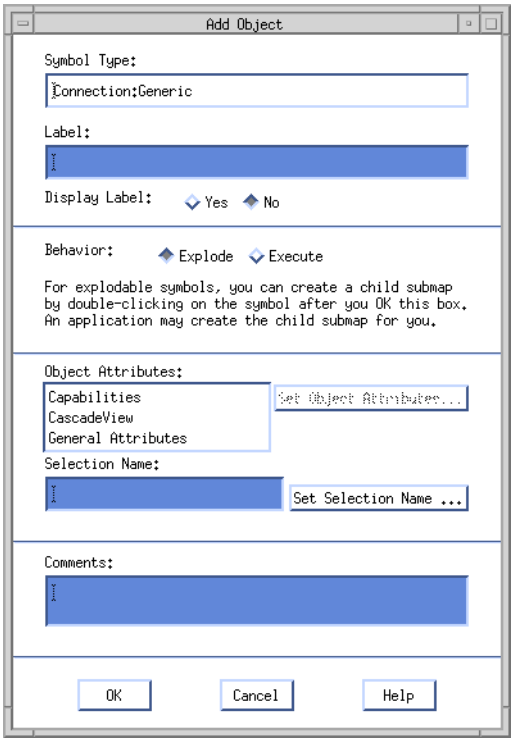


Figure 3-21. Add Object Dialog Box

4. In the Label field, enter the trunk name. This name must be the same one you entered in Step 6 on page 3-22.

5. Select Yes in the Display Label field.

6. In the Object Attributes box, select CascadeView and then choose Set Object Attributes. The following dialog box appears.

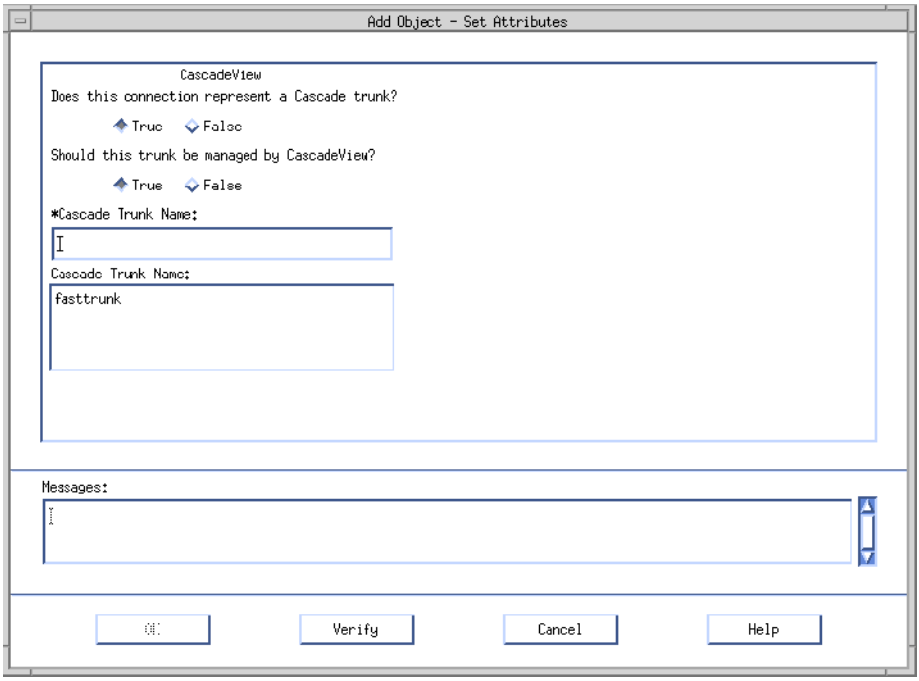


Figure 3-22. Add Object - Set Attributes Dialog Box

7. Complete the Add Object – Set Attributes dialog box as follows:

   a. Select True for both questions.

   b. Select the trunk name from the Cascade Trunk Name list box. The *Cascade Trunk Name field then displays the name you select.

   c. Choose Verify, then choose OK.

8. Choose OK and OK again to return to the network map.

Establishing Switch-to-NMS Communications With the Second Switch

Refer to Chapter 12 for procedures you can use to establish NMS-to-switch communications. The method you choose may vary according to your network configuration.

When you finish, the trunk line and switch objects should be green (on the map), indicating a successful configuration.

If the trunk line is "black", verify that the following environment variable is specified in each user's .profile or .cshrc file.

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

If necessary, log in as root and modify .profile (or .cshrc). Then log out of CascadeView/UX and log back in again to restart the system.

4

Managing Network Maps

This chapter describes IP addressing and subnet addressing. In addition, this chapter describes how to create a network map and add the icons or objects that represent each Cascade switch in your network. Although you use the HP OpenView functions to do this, the CascadeView/UX application manages the network map and switch configuration. Through the network maps, you define the topology of the network and monitor network activity.

IP Address Overview

This section provides an overview of IP addresses and describes the three primary classes of IP addresses (specifically Class B IP).

IP addresses are 32-bit numbers represented by four sequential fields of decimal integers, separated by dots (.); for example, 152.148.225.10. The value of each field (referred to as an *octet* or *byte*) can range from 0 to 255.

The position of the first zero bit in the first four bits determines the class to which an address belongs. The remaining bits specify two subfields - a *network identifier* (netid) and a *host identifier* (hostid). The netid defines what network the system belongs to and the hostid represents the specific location on that network as shown in Figure 4-1.

Figure 4-1. Class B IP Address

Three Primary Classes of IP Addresses

There are three primary classes of IP addresses: Class A, B, and C. Each class uses a different address format to accommodate different size networks. Table 4-1 shows the network ID and host ID formats for each class. Class D addresses (used for multicasting) are not discussed in this guide.

Table 4-1. IP Address Classes

Class	Network ID	Host ID	Format
A	7 bits	24 bits	Class A addresses are used in large networks and allow 16 million host addresses. 0 | Network (7) | Local Address (24)
B	14 bits	16 bits	Class B addresses are used in intermediate size networks and allow 65,534 host addresses. 10 | Network (14) | Local Address (16)
C	21 bits	8 bits	Class C addresses are used in smaller networks and allow 254 host addresses. 110 | Network (21) | Local Address (8)

Class B IP Addresses

Cascade supports Class B IP addresses for internal routing (OSPF), enabling you to expand your network to configure up to 400 switches and 1,000 trunks. Class B addresses use the first two bytes for the network address and the last two bytes for the host address. For example, if your Class B network number is 150.100.0.0, you can start numbering your hosts at 150.100.0.1 and go up to host number 150.100.255.254. Using this example, you have a total of 65,534 host addresses in the Class B network. With Class B IP addresses, you can group single addresses into *subnets* to create several smaller networks.

Subnets

A subnet divides a large network into smaller groups (subnets). Subnets support a three-level hierarchy (as opposed to a two-level hierarchy) in which the host number is divided into two parts, the subnet number and the host number on that subnet (see Figure 4-2).

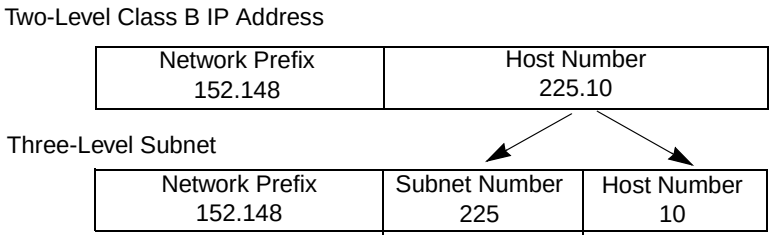


Figure 4-2. Subnet Example

You can use a subnet to:

- Connect different physical networks
- Distinguish between different network LANs
- Isolate parts of the network
- Delegate network administration by assigning administrators to different subnets

The subnet ID represents a smaller group to which individual addresses belong. When you choose a subnet mask, consider the following:

- Number of subnets in your network
- Number of hosts that will attach to each subnet

Before You Begin

Use the following sequence to create a network map and subnet ID:

Step 1. Configure a new map for the CascadeView application. Specify a unique name and network number ("Creating a Network Map" on page 4-6).

Step 2. Create a subnet ("Creating a Subnet ID" on page 4-10).

Step 3. Add the Cascade switch objects to the map ("Adding Cascade Switch Objects to the Map" on page 4-14).

Step 4. (*Optional*) Create virtual private networks (VPNs) and customer names.

These procedures assume you have started CascadeView.

Creating a Network Map

When you create a network map, you configure network-wide parameters, such as the network number. These parameters enable CascadeView to manage the network map from within HP OpenView.

To create a new network map:

1. Access HP OpenView and start CascadeView/UX as described in Chapter 2.
2. To log on, from the Misc menu, select CascadeView ⇒ Logon and enter the operator password.

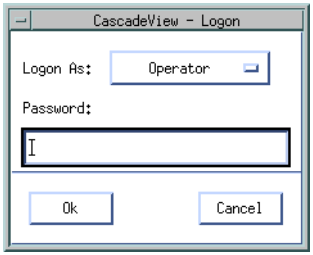


Figure 4-3. Logon Dialog Box

3. From the Map menu, select Maps ⇒ New. The following dialog box appears.

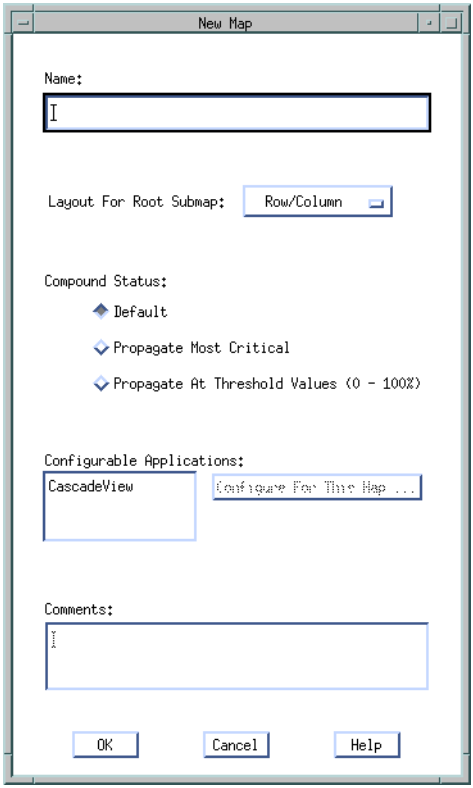


Figure 4-4. New Map Dialog Box

You cannot modify these parameters after they are set. If you need to change the network number, you must delete the map and start over. OSPF uses the network number for path selection. To change this setting, contact the Cascade Technical Response Center for recommended guidelines at one of the following numbers:

1-800-DIAL-WAN (1-800-342-5926) or 1-508-692-2600 (in the United States and Canada)

1-508-952-1299 (outside the U.S., Canada, and United Kingdom)

0-800-96-2229 (in the United Kingdom)

4. Complete the following fields:

   Name — Enter an alphanumeric name that identifies the map.

   Layout For Root Submap — Accept the default Row/Column. This option affects how the objects are arranged on the screen.

   Compound Status — Select the compound status propagation. This field specifies 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*.

   Options include:

   Default – Propagates status according to a predefined algorithm.

   Propagate Most Critical – Propagates the status of the most critical symbol in the child submap, up to the symbols of the parent object.

   Propagate At Threshold Values (0 - 100%) – Enables you to set the following threshold values that determine when HP OpenView propagates status. The numbers represent the default values.

%warning	30
%minor	20
%major	10
%critical	5

   Configurable Applications — *(See Step 5 on page 4-9.)*

   Comments — Enter any additional information for this map.

5. In the Configurable Applications field, select CascadeView and choose Configure For This Map. The following dialog box appears.

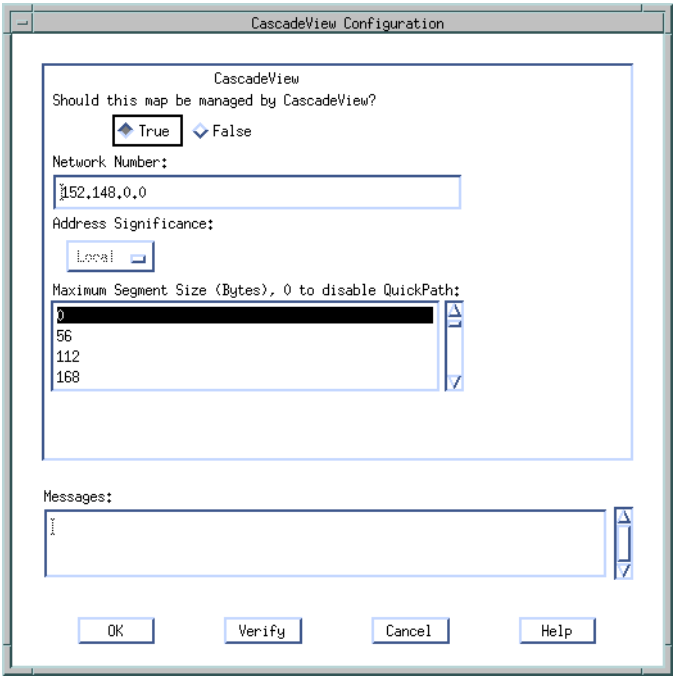


Figure 4-5. Configuration Dialog Box

6. Complete the following fields:

   Should this map be managed by CascadeView? — Select True.

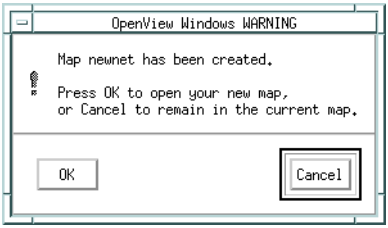
   Network Number — Displays the Internet switch IP Network Number specified when you added a static route during the CascadeView/UX installation (refer to the *Network Management Station Installation Guide*). Contact the Cascade Technical Response Center before you change this number.

   Address Significance — Defaults to Local and cannot be changed.

   Maximum Segment Size (Bytes) 0 to disable Quickpath — This option is not supported.

7. Choose Verify to confirm your settings and then choose OK. The New Map dialog box reappears.

8. Choose OK. The following message indicates you created a new network map.



9. Choose OK to open the new network map.

If the IP Internet icon appears on the map, select the icon and from the Map menu, select Unmanage Objects. Then, from the Edit menu, select Hide ⇒ From All Submaps to hide this icon.

10. To log on to the new network map, from the Misc menu, select CascadeView ⇒ Logon (Figure 4-3 on page 4-6).

11. Enter the logon password (*cascade* is the default) and choose OK.

Creating a Subnet ID

You must create at least one subnet ID between 1 and 255. The subnet ID becomes the third byte of the IP address and the switch ID becomes the last byte of the IP address. For example, an IP address of 152.148.225.10 has a subnet ID of 225 and a switch ID of 10.

To add a subnet ID:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Subnets. The following dialog box appears.

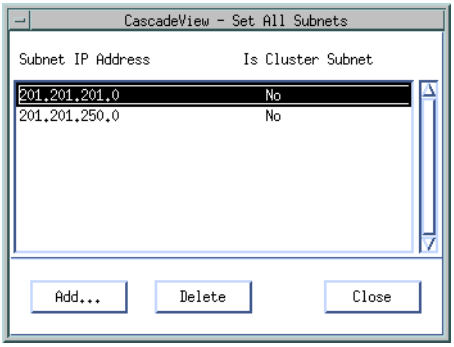


Figure 4-6. Set All Subnets Dialog Box

2. Choose Add.

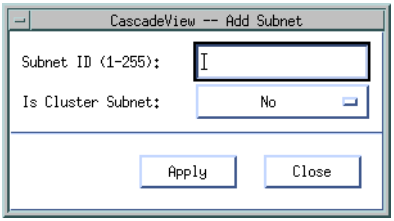


Figure 4-7. Add Subnet Dialog Box

3. Complete the following fields:

   Subnet ID (1-255) — Enter a subnet number between 1 and 255.

   Is Cluster Subnet — (*Optional*) Select Yes to make this subnet a cluster subnet. The default is No.

4. Choose Apply to add the subnet ID.
5. Choose Close to exit the Add Subnet dialog box.
6. To continue, do one of the following:
   - If you selected Yes in Step 3 to make this subnet a cluster subnet, continue with the following section, "Creating Clusters".
   - If you specified No in Step 3 (you do not use subnet clusters), continue with "Adding Cascade Switch Objects to the Map" on page 4-14.

Creating Clusters

After you define a subnet, you can define a cluster. A cluster is a group of switches that run in a single OSPF routing domain. The switch number in the IP address increments according to the cluster ID, as shown in Table 4-2.

Table 4-2. Cluster ID and IP Address Range

Cluster ID	IP Address Range
0	152.148.x.1 - 152.148.x.30
1	152.148.x.33 - 152.148.x.62
2	152.148.x.65 - 152.148.x.94
3	152.148.x.97 - 152.148.x.126
4	152.148.x.129 - 152.148.x.158
5	152.148.x.161 - 152.148.x.190
6	152.148.x.193 - 152.148.x.222
7	152.148.x.225 - 152.148.x.254

If you selected Yes in the Is Cluster Subnet field (Figure 4-7 on page 4-11), you must create a cluster.

To create a cluster:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Clusters. The following dialog box appears.

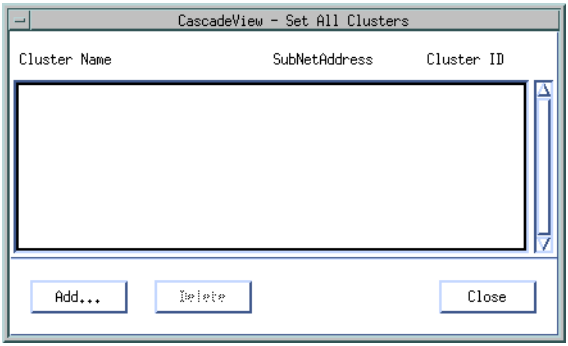


Figure 4-8. Set All Clusters Dialog Box

2. Choose Add to display the Add Cluster dialog box.

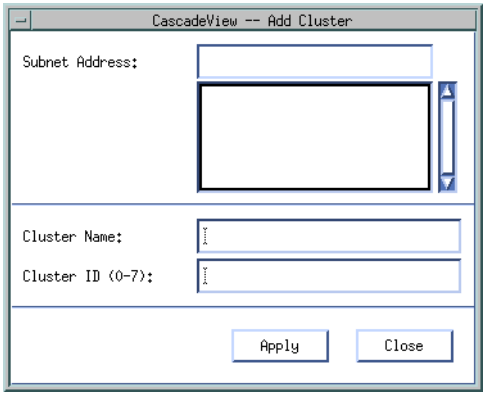


Figure 4-9. Add Cluster Dialog Box

3. Complete the following fields:

   Subnet Address — Select the subnet address to which this cluster belongs.

   Cluster Name — Select a name for this cluster.

   Cluster ID (0-7) — Select an ID between 0-7 for this cluster.

4. Choose Apply to create a cluster. Choose Close to return to the network map.

Adding Cascade Switch Objects to the Map

When you add a CascadeView switch object to the network map, you:

- Select and drag the Cascade switch object to the network map.
- Define the object attributes.

To add a Cascade switch object to the network map:

1. From the Edit menu, select Add Object. The Add Object:Palette dialog box appears.
2. Scroll through the Object Palette to locate the Cascade Object symbol.
3. Select Cascade Object. The Symbol Subclasses for Class Cascade Object appear.

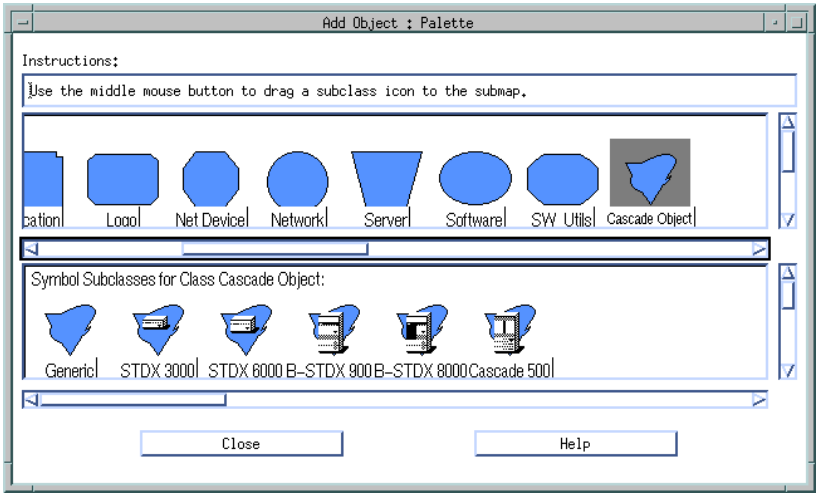


Figure 4-10. Add Object:Palette Dialog Box

4. Add the CBX 500 switch object to the network map. Click on the object, hold down the middle mouse button, drag the object to the map, and release. The following dialog box appears.

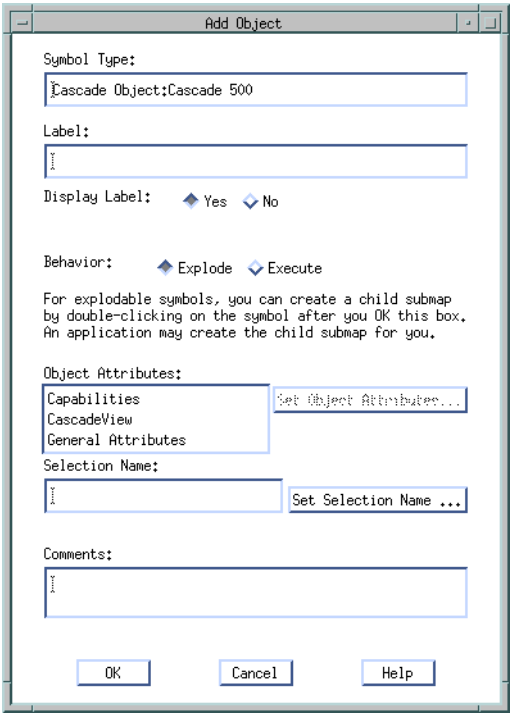


Figure 4-11. Add Object Dialog Box

5. Complete the following fields:

   Symbol Type — Displays the type of Cascade switch (object) you added to the network map.

   Label — Enter a name to identify the object.

   Display Label — Select Yes to display the label beneath the object on the network map. Select No if you do not want the label to appear.

   Behavior — By default, CascadeView sets this field to Explode. Refer to the *HP OpenView User's Guide* for more information about using the Execute function.

Object Attributes — Select CascadeView and then choose Set Object Attributes. The following dialog box appears.

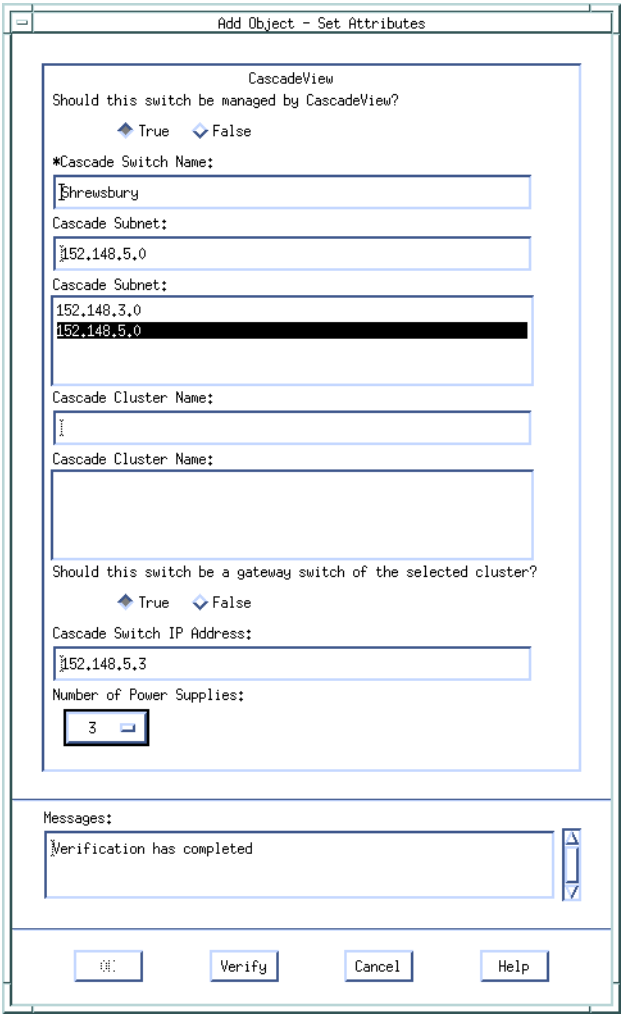


Figure 4-12. Add Object - Set Attributes

6. Complete the following fields:

   Should this switch be managed by CascadeView? — Select True.

   Cascade Switch Name — Enter a unique name for the switch.

   Cascade Subnet — Select the Cascade Subnet from the list.

   Cascade Cluster Name — Displays the name of the cluster to which this subnet belongs. Refer to "Creating Clusters" on page 4-12 for more information.

   Should this switch be a gateway switch of the selected cluster? — Select True to make this a gateway switch, otherwise select False.

   Cascade Switch IP Address — Displays the switch's IP address. Every time you add an object to the map, CascadeView increments the last octet (host id) by 1. If the next host id number is already being used in the network, CascadeView uses the next available number.

   Number of Power Supplies — Select the number of power supplies that this switch supports, either two (2) or three (3).

A chassis that supports three power supplies must have at least two power supplies installed at all times.

7. Choose Verify to confirm your settings. Choose OK to return to the Add Object dialog box.

If the message "access denied" appears, you may not have logged on to the network map. Choose Cancel to return to the network map, then from the Misc menu, select Logon. Enter the default operator logon, cascade.

8. Notice that the Selection Name field on the Add Object dialog box (Figure 4-11 on page 4-15) automatically defaults to the value you entered for the Label name. The Selection Name must be unique throughout all HP OpenView objects. Cascade recommends you leave the selection name as it appears. In the Comments field, enter any additional information you want to describe the object.

9. Choose OK. The Add Object Palette reappears.
10. Choose OK. The network map displays the switch object, which is blue and quickly turns to red. This indicates the NMS cannot access the switch.
11. Select the switch object and from the Map menu, select Unmanage Objects. The switch object turns to a wheat color indicating that the object is in an unmanaged state.
12. To add more Cascade switches to the network map, repeat Step 1 through Step 11.

To turn off the automatic layout feature so you can relocate a switch object, from the View menu, select Automatic Layout ⇒ For All Submaps ⇒ Off for All Submaps.

Virtual Private Networks

Virtual Private Networks (VPNs) enable network providers to dedicate network resources for those customers who require guaranteed performance, reliability, and privacy. A VPN enables you to provide dedicated bandwidth to the customer.

When you add a trunk (described in Chapter 8), you can dedicate trunks to a specific VPN to allow customers to monitor their own networks. However, switch control and configuration stays with the network service 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
```

These lines disable the Administer menu and all its provisioning functions; the NMS user only sees the Monitor menu functions.

Use the following sequence to set up a VPN.

Step 1. Create the VPN (refer to page 4-19).

Step 2. Add customers to a specific VPN (page 4-20).

Step 3. *For SVC traffic*, specify the net overflow parameter for the logical port. This determines whether SVCs originating from this port are restricted to trunks of their own VPN or can use public (shared) trunks during overflow conditions (page 7-27). Then, dedicate the logical port to a specific VPN and customer (page 7-37).

Step 4. *For PVC traffic*, specify the net overflow parameter for the circuit. This determines whether this PVC is restricted to trunks of its own VPN, or uses public (shared) trunks during overflow conditions (page 9-19). Then, dedicate the circuit to a specific VPN and customer (page 9-24).

Step 5. Dedicate a trunk to a specific VPN (refer to Chapter 8).

Creating a Virtual Private Network

Use the following steps to create a VPN and add customers to this network:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Virtual Private Networks.

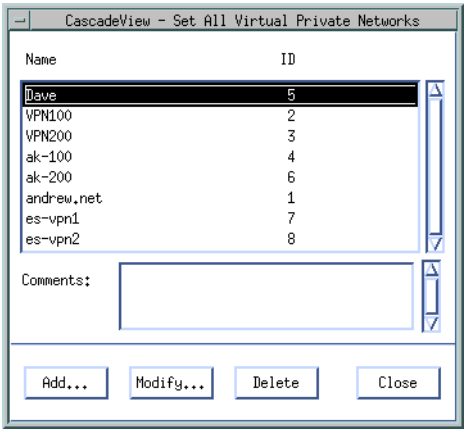


Figure 4-13. Set All Virtual Private Networks Dialog Box

2. Choose Add.

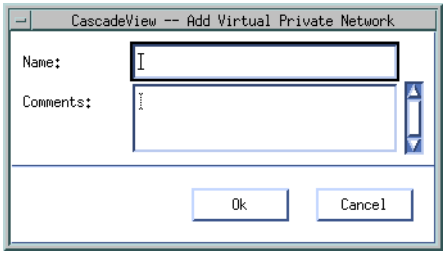


Figure 4-14. Add Virtual Private Network Dialog Box

3. Enter a name for this VPN. Enter any additional comments.
4. Choose Apply.
5. Choose Close to return to the network map.

Adding Customers to the VPN

To add customers to the VPN:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Customers. The following dialog box appears.

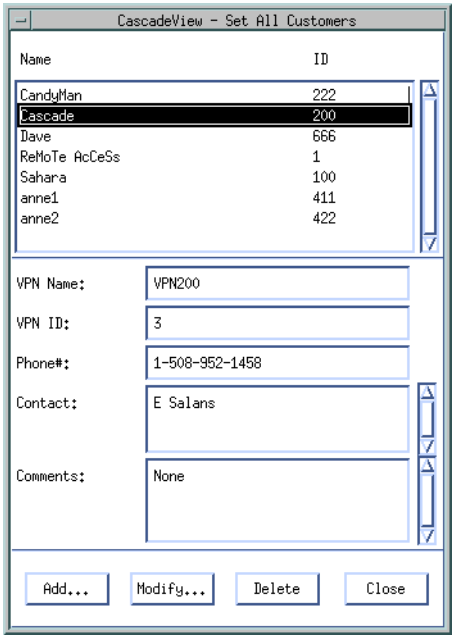


Figure 4-15. Set All Customers Dialog Box

2. Choose Add. The following dialog box appears.

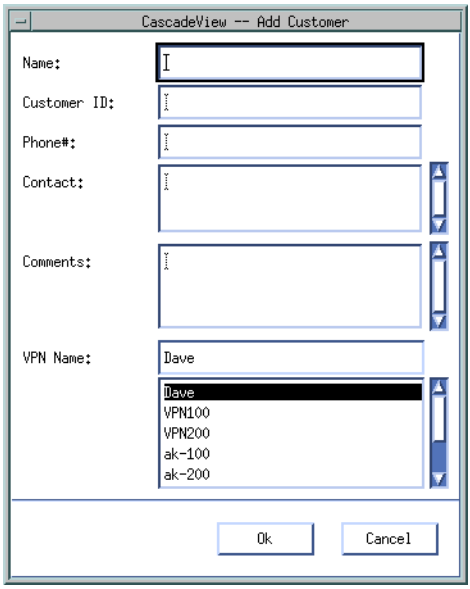


Figure 4-16. Add Customer Dialog Box

3. Enter a customer name.
4. Assign a value from 1 to 65535 for the customer ID.
5. (*Optional*) Enter the phone number, contact name, and any additional comments.
6. Select the VPN name to which this customer belongs.
7. Choose Apply.
8. Choose Close to return to the network map.

Deleting a Network Map Database

Use the following steps to delete a network map. This procedure clears the information from the SYBASE and HP OpenView databases, enabling you to start over.

1. From the Map menu, select Maps ⇒ Open/List Maps. Select the map you want to delete.
2. Delete each object from the map. From the Edit menu, select Delete ⇒ From All Submaps. Use the Delete command to do this. **Do not use Cut**.
3. Delete the map from HP OpenView.
4. From the File menu, select Exit to close HP OpenView.
5. To log in as the root user, enter **su - root**.
6. Enter the root password.
7. To shut down HP OpenView services, enter:

   /usr/OV/bin/ovstop

Step 8 completely removes the database. There is no database recovery process after you execute this command.

8. Enter the following command to completely remove the database.

   rm -rf /usr/OV/databases/openview/*/*

9. Enter the following commands to remove the events and traps alarm logs associated with the database.

   rm /usr/OV/log/xnmevents.[*username*] <Return>

   rm /usr/OV/log/trapd.log <Return>

   rm /usr/OV/log/trapd.log.old <Return>

10. Enter the following command to run the HP OpenView database daemon, register the fields in the database, and start all other OpenView daemons.

    /usr/OV/bin/ovstart ovwdb <Return>

    /usr/OV/bin/ovw -fields <Return>

    /usr/OV/bin/ovstart <Return>

11. Log in as the root user by entering **su - root**.

12. Enter the following command at the # prompt:

    /opt/CascadeView/bin/cv-install.sh

    The system displays the following message:

    ```
    Verifying super user privileges . . .
    Would you like to view (tail -f) the install log (default=y)?
    ```

    (The tail window enables you to view the installation log.)

13. Press Return to view the Tail window.

    The Tail window and CascadeView Installation menu appear. You can exit the script at any time by typing **<Ctrl> c**.

14. At the CascadeView Installation menu, enter 3 to select HP OpenView Integration Only (No DB Action).

    The system displays the message:

    ```
    No Sybase Functionality will be altered.
    ```

15. At the “Do you wish to extract CV/UX Installation media y/n” prompt, press Return.

16. At the “Do you wish to continue” prompt, press Return.

    The system displays the following message:

    ```
    Configuring CascadeView environment.

    Install CascadeView successful.
    ```

The system recreates the cascview database. You now have a clean SYBASE database and HP OpenView database.

5

Managing a Cascade Switch

This chapter describes the front and back panels of a switch, and how to set up network communications between the NMS and a switch object. You will learn how to configure the NMS and the first switch to which it connects, called the *gateway* switch.

Before you configure a switch, verify that the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Create a subnet ID (page 4-10)
- ☑ Add a Cascade switch to the map (page 4-14)

If you need to delete a switch configuration, refer to "Deleting a Switch Configuration from the Database" on page 5-31.

About Console Authentication

Console authentication is a domain security feature that is handled by Remote Access Dial-in User Service (RADIUS) protocol. It allows you to assign a password (other than “cascade”) to each switch in your network. This password is used to authenticate users connecting to a Cascade switch console port via remote dial-up and Telnet access.

RADIUS Authentication Requirements

Before RADIUS authentication can take place, you must have access to an active RADIUS Server that the switch can reach via UDP/IP. If you cannot reach the RADIUS Server when you log on to the switch console port, use the shared secret password for the login name and login password. (You can also use the shared secret password to enter console debug mode.)

The RADIUS Server’s database must contain the following information:

- User authentication information (for example, username and password).
- Switch information for all switches initiating authentication requests (for example, IP address or host name).
- Shared secret (hash key) for each switch initiating authentication requests.

Adding an Authentication Domain

You can add an authentication domain and shared secret for each switch in the network. You set the Radius Server parameters, such as the server domain’s IP address, for each authentication domain server. You can also designate backup servers (Server 2 and Server 3) in the event that Server 1 becomes unreachable or inactive.

To add the authentication domain and configure the shared secret password:

1. From the Administer menu, select Cascade Parameters ⇒ Set Authentication Domains. The following dialog box appears.

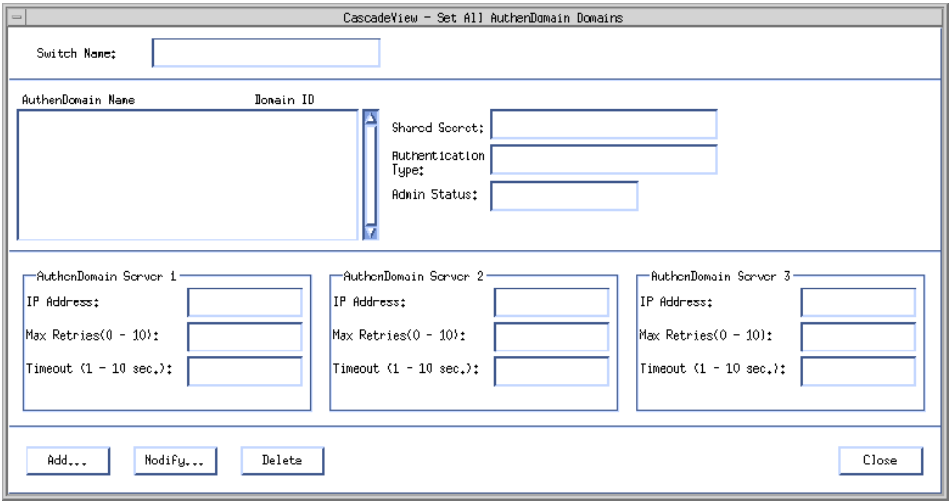


Figure 5-1. Set All AuthenDomains Dialog Box

2. Choose Add. The following dialog box appears.

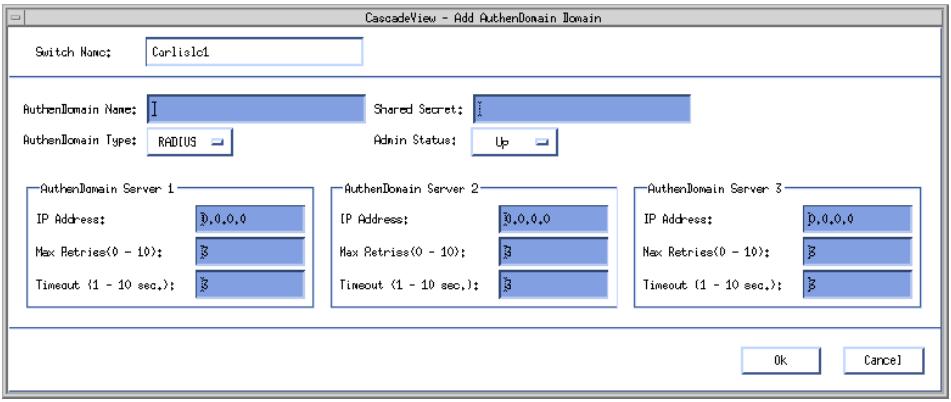


Figure 5-2. Add AuthenDomain Dialog Box

3. Complete the following fields.

Field	Action/Description
AuthenDomain Name	Enter an alphanumeric name (up to 32 characters) for this domain.
AuthenDomain Type	Defaults to RADIUS and cannot be changed.
Shared Secret	Enter an alphanumeric shared secret (hash key) for this switch and all RADIUS Servers in this domain. If you cannot access the radius server from a switch via the switch console port, use the shared secret password as the login and password for console debug mode.
Admin Status	Set the Admin Status to Up to allow immediate access. Set the Admin Status to Down to disable this domain.

4. Complete the AuthenDomain Server fields for Servers 1, 2, and 3.

Field	Action/Description
IP Address	Enter the IP address for this server.
Max Retries (0-10)	Enter the maximum number of attempts (retries) the server should make to authenticate this user. The default is three (3) retries.
Timeout (1-10 sec)	Indicates the number of seconds the server waits before sending an authentication request, if there was no response from the previous request. If a single server is used, it will retry the request. If multiple servers are defined, the request is sent to the next server. Specify the time period (in seconds) of inactivity before trying the next server. The default is three (3) seconds.

5. Choose OK to set the authentication parameters.
6. Choose Close to return to the network map.
7. To enable the console authentication for a specific switch, refer to page 5-17.

About Switch Attributes

You must configure one switch in the network as the *gateway switch* for routing management-protocol requests and responses from the CBX 500 switches to the NMS. The NMS accesses all CBX 500 switches in the network through this gateway switch. The NMS can then control and monitor all other CBX 500 switches in the network through the network trunks.

You can also configure additional NMS workstations for access to the gateway switch. For more information, refer to "Defining Additional Network Management Stations" on page 5-18.

About RIP State and Send Host Route

Routing is the task of finding a path from a sender to a desired destination and sending information. The Routing Information Protocol (RIP) allows hosts and gateways to exchange information for computing routes through the network. The Send Host Routes function determines the RIP packet contents sent by the gateway switch, establishing data transmission routes.

The NMS must be running Routed software for the RIP feature to function. Routed software is a UNIX network routing daemon used to maintain up-to-date kernel-routing table entries.

The RIP feature enables the switch to send and receive RIP packets to and from all routers in the network, and convey information about routes to each destination (switch) in the network. This feature allows the gateway switch to detect failures in the external routing path to the NMS by listening to RIP updates from neighboring routers. It also allows the NMS to detect failures in the gateway switch by listening to RIP updates from the gateway switch. If RIP detects a link failure or loss of connectivity to the gateway switch, it finds an alternate path to reach its destination.

You configure the RIP feature on the gateway switch only. To do this, set the RIP state parameters to *On/Off* to enable and disable the RIP feature. Every switch in the network is updated with a route to the NMS. When the RIP State field is set to *On*, the switch processes received RIP packets and adds the route to the NMS routing table. Refer to page 5-12 for instructions on configuring the RIP state.

Using Figure 5-3 as an example, if Router-1 becomes unreachable, then Gateway-1 deletes the NMS routing table entry from its global routing table. Using Open Shortest Path First (OSPF) metrics, this information is sent to every switch in the network and each switch deletes this path from its routing table. Switches no longer route information through Router-1; instead they use Gateway-2 to Router-2, until Router-1 recovers.

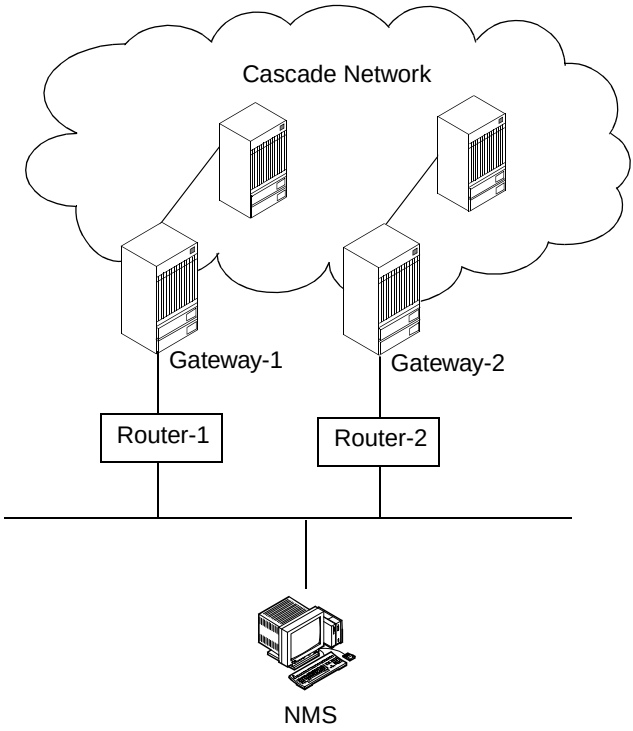


Figure 5-3. Routing Information Protocol Example

About Reroute Time Tuning

You can use the Tuning command to change the parameters associated with PVC rerouting. This feature enables the switch to rapidly redistribute Permanent Virtual Circuits (PVCs) across trunks based on OSPF updates and cost metrics. In large networks with thousands of PVCs, rerouting circuits while re-establishing a trunk is a time-consuming operation.

The Tuning command enables you to tune the rate of reroute requests per switch. The Tuning option defines how many circuits can issue a reroute request during a single reroute batch request. This option also enables you to set the time delay (in seconds) that the switch waits between each batch request.

When you define individual circuits, enable the Reroute Balance parameter (the default) to allow circuits to benefit from the tuning parameters you define for a switch. For more information about reroute balance, refer to *page 9-23**.*

Load balancing enables the switch to route a circuit to a path that provides more bandwidth than the one it is currently using. You can select a load balancing algorithm that configures the switch to perform a more aggressive search for an alternate path with greater bandwidth.

Example

If a switch has four IOMs, each with 50 PVCs, and you set the reroute count to five and the reroute delay to 50 seconds, the switch performs a batch reroute consisting of the first five circuits on each IOM (for a total of 20 circuits). The switch then waits 50 seconds before it begins to reroute the next batch of 20 circuits.

Under normal circumstances, the reroute ratio should be no greater than one circuit (reroute count) in 10 seconds (reroute delay). A higher reroute ratio (e.g., two circuits in 10 seconds) can cause network instability and circuits may bounce from one trunk to the next indefinitely. To balance a set of circuits after a trunk failure, use the above example to set the reroute count to 5, and the reroute delay to 50 seconds.

About the Switch Back Panel Dialog Box

The Switch Back Panel dialog box presents a graphic display of a CBX 500 switch back panel. This dialog box enables you to configure each slot in the CBX 500 with the appropriate I/O module. You can then select each physical port on the module to configure both physical and logical port attributes.

To access the Switch Back Panel dialog box from the network map:

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

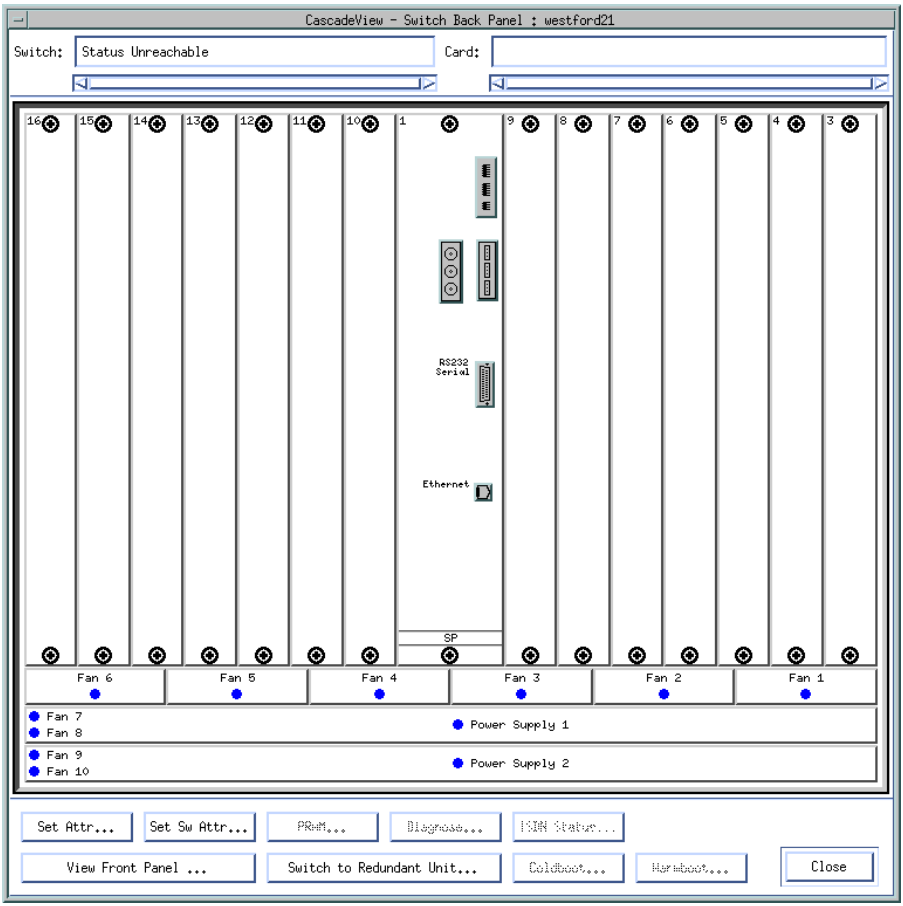


Figure 5-4. Switch Back Panel Dialog Box

The Switch Back Panel dialog box varies according to the type of switch. This dialog box shows a sample CBX 500 configuration.

The following table describes the Switch Back Panel dialog box status indicators and commands.

Table 5-1. Switch Back Panel Dialog Box Command Buttons

Choose	To
Set Attr	Configure 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.
Set Sw Attr	Set the switch attributes, including the local IP address of the switch. For more information about this command, refer to page 5-6.
PRAM	Access the PRAM functions. For information about these functions, refer to Chapter 12.
View Front Panel	Display the front panel of the switch. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for more information.
Switch to Redundant Unit	Switch to a redundant SP. To do this, select the redundant SP module and choose this command to perform the SP switch over.
Diagnose	Access diagnostics for a selected module. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for more information.
Warmboot	Reset the module you select. As it reboots, all physical ports, logical ports, and PVCs on the module stall for approximately 20-30 seconds.
Coldboot	Restart the module as if it were powered off, then on.

Before You Begin

You need to know:

- The local IP address of the gateway switch.
- The community name specified in the *cascadeview.cfg* file in */opt/CascadeView/etc*. To view the contents of this file, enter:

  ```
  cat /opt/CascadeView/etc/cascadeview.cfg
  ```

- The IP address of the SPARCstation (for serial connections) you are using as the NMS.
- The IP address of the router that connects the NMS to the switch (if applicable).

Use the following configuration sequence to configure and manage a switch:

Step 1. (*Optional)* Set up an authentication domain (refer to page 5-2).

Step 2. Set the switch attributes (refer to page 5-9).

Step 3. (*Optional)* Define the reroute tuning parameters (refer to page 5-16).

Step 4. (*Optional)* Define an additional NMS, if necessary (refer to page 5-18).

Step 5. (*Optional)* Enable console authentication (refer to page 5-21).

Step 6. Configure the IP address and access attributes for the NMS or IP host (refer to page 5-20).

Step 7. Set the switch processor (SP) attributes (refer to page 5-20).

Configuring the Switch IP Address

To configure the IP address:

1. From the Switch Back Panel dialog box (Figure 5-4 on page 5-9), choose Set Sw Attr. The following dialog box appears.

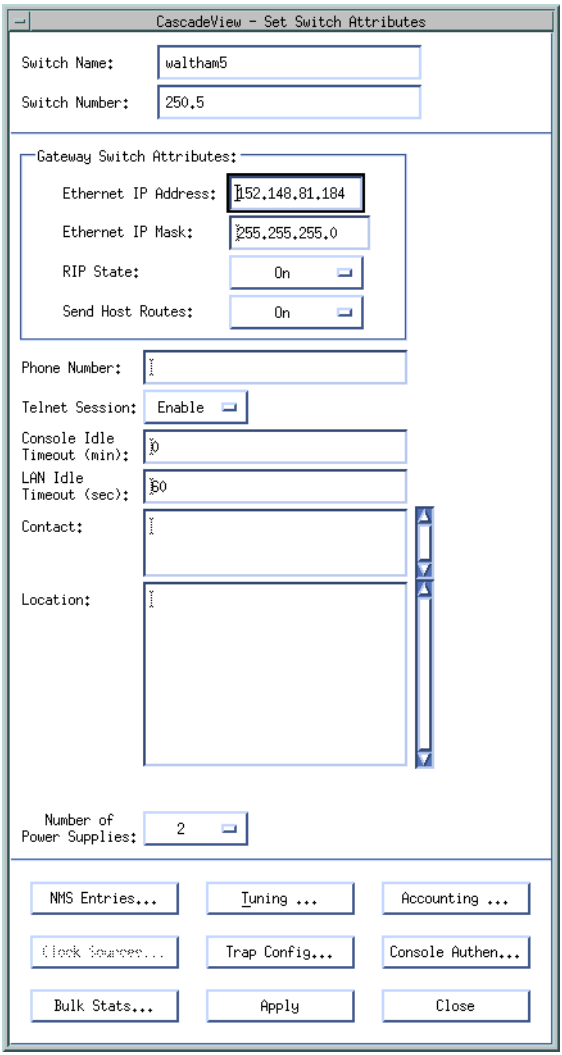


Figure 5-5. Set Switch Attributes Dialog Box

This dialog box displays the switch name (assigned the switch when you added the object to the map) and the unique number of the switch (switch number). If this switch belongs to a cluster subnet, the switch number increments according to the Cluster ID. Refer to “Creating a Cluster” on page 4-13 for more information.

2. Complete the dialog box fields as described in Table 5-2.

Table 5-2. Set Switch Attributes Fields

Field	Action/Description
Ethernet IP Addr (*Gateway switches only*)	If this switch has an Ethernet connection to the NMS Ethernet port, enter the local IP address of the switch. This address is the external Ethernet address of the switch. See your network administrator if you do not know this address.
Ethernet IP Mask (*Gateway switches only*)	Enter the inband (Ethernet) IP Mask for this switch. The default is 255.255.255.0 for class C IP addresses and 255.255.0.0 for class B addresses.
RIP State (*Gateway switches only*)	Set the RIP State parameters: *Off (*default*)* – Disables the RIP State. *On* – Enables the switch to process received RIP packets and send RIP updates to routers connected to the Ethernet.
Send Host Routes (*Gateway switches only*)	Set the Send Host Routes parameters: *Off (*default*)* – RIP update packets contain a single (sub)network address for the entire Cascade network. *On* – RIP update packets contain the host address of all switches in the network.
Phone Number	Enter the phone number of the contact person responsible for the operation of the switch.
Telnet Session	Select either Enable or Disable to specify whether this switch can accept a remote terminal connection.

Table 5-2. Set Switch Attributes Fields (Continued)

Field	Action/Description
Console Idle Timeout (min)	Specify the time period (in minutes) that the console is inactive before you are automatically logged off. The default is five (5) minutes. Enter zero (0) if you never want the console to time-out.
LAN Idle Timeout	Specify the default idle timeout for the switch's external Ethernet interface. The default is 60 seconds. If the gateway switch receives no valid IP traffic during the period you specify, the interface is marked idle and will not be used for outbound traffic. Receipt of valid IP traffic restarts the idle timeout counter and reactivates the interface.
Contact	Enter the name of the person responsible for operating the switch.
Location	Enter a detailed description of the physical location of the switch (city, state, country, building, room, etc.).
Number of Power Supplies	Indicates the number of power supplies in this chassis. The default is two (2). If this chassis uses a third power supply ("N+1 power supply"), select three (3). ***Note:*** *A chassis that supports three power supplies must have at least two power supplies installed at all times.*

3. The Set Switch Attributes dialog box contains the following command buttons described in Table 5-3. If applicable, configure these options now.

Table 5-3. Set Switch Attributes Command Buttons

Choose	To
NMS Entries	Define additional NMS workstations. Refer to page 5-18 for information.
Tuning	Define parameters that enable the NMS to balance circuits between switches. Refer to page 5-16 for information.
Accounting	Access access switch attributes for ATM accounting. Refer to the *Accounting System Administrator's Guide* for information.

Table 5-3. Set Switch Attributes Command Buttons (Continued)

Choose	To
Trap Config	Clear contact alarm relays that are used to notify you of switch malfunctions. You can also use this function to disable the dry contact alarm relay function for this switch. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for information about these alarms.
Console Authen	Set password protection for the switch. Refer to page 5-17.
Bulk Statistics	Access switch attributes for ATM bulk statistics. Refer to the *Bulk Statistics Collector for CBX 500 User's Guide.*

4. When you finish, choose Apply, then Close to return to the Switch Back Panel dialog box (Figure 5-4 on page 5-9).

To continue, do one of the following:

- *If the switch is a gateway switch* and you have not configured the IP address of your NMS workstation(s), continue with "Configuring the IP Address of the NMS" on page 5-21.
- *If the switch is not a gateway switch*, you are ready to configure the switch processor attributes. Refer to "Configuring SP Attributes" on page 5-25.

Defining Circuit Reroute Time Tuning Parameters

To set the tuning parameters:

1. From the Set Switch Attributes dialog box (Figure 5-5 on page 5-12), choose Tuning.

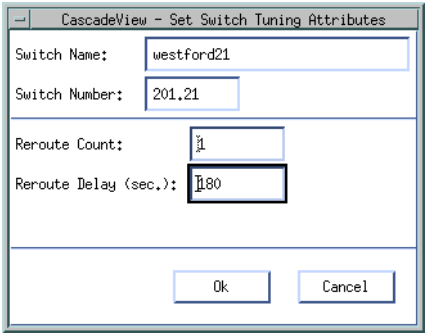


Figure 5-6. Set Switch Tuning Attributes Dialog Box

2. Specify the following parameters:

   Reroute Count — Enter a value between 0 and 64. The reroute count represents the number of circuits that can issue reroute requests in a single batch. The default is one (1).

   Reroute Delay — Enter a value between 1 and 32767. The reroute delay represents the time delay (in seconds) that each IOM in the switch waits between reroute batch requests. This parameter controls the rate at which each IOM polls the virtual circuits for a better route. The default value of 188 seconds is a very conservative setting for normal operation.

3. Choose OK to return to the Set Switch Attributes dialog box.

4. To specify additional switch attributes, proceed to Step 3 on page 5-14.

Enabling Console Authentication

Before you can use Console Authentication, you must first set up the authentication domain server and assign a shared secret password that you will use to access the switch via remote dial-up or Telnet access. Refer to "About Console Authentication" on page 5-2 for more information.

To enable console authentication:

1. From the Set Switch Attributes dialog box (Figure 5-5 on page 5-12), choose Console Authen. The Console Authen dialog box displays all authentication domain names in the Authentication Domain Name list box.

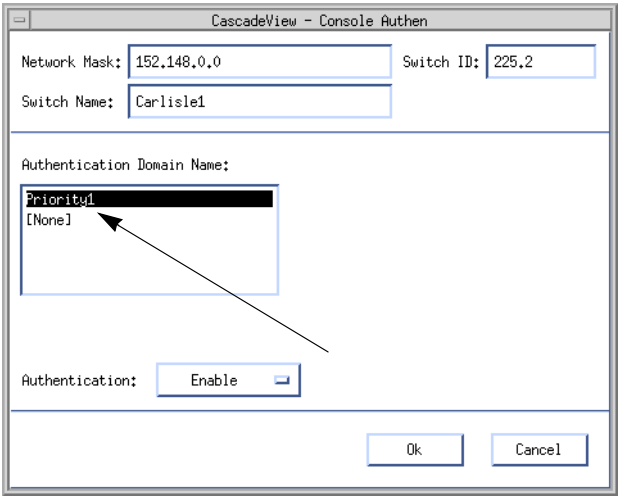


Figure 5-7. Console Authen Dialog Box

2. Select a domain from the list.
3. Set the Authentication parameter to enable or disable (default) authentication.
4. Choose OK to set the authentication parameters. The Set Switch Attributes dialog box reappears.
5. To specify additional switch attributes, proceed to Step 3 on page 5-14.

Defining Additional Network Management Stations

Using the NMS Entries command, you can configure up to 32 additional NMS workstations to have read/write or read-only access to the same switch. Through the NMS workstations, you can communicate with switches on the network via SNMP commands.

To define an NMS entry, enter the IP address of each workstation and use the same community name for each NMS you define. The file *cascadeview.cfg* in */opt/CascadeView/etc* provides the default read/write community name.

To define an additional NMS:

1. From the Set Switch Attributes dialog box (Figure 5-5 on page 5-12), choose NMS Entries. The following dialog box appears, displaying the current NMS entries.

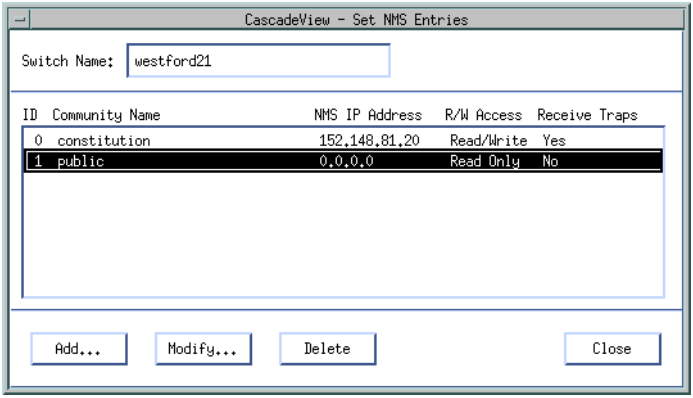


Figure 5-8. Set NMS Entries Dialog Box

Table 5-4 describes the Set NMS Entries dialog box command buttons.

Table 5-4. Set NMS Entries Dialog Box Command Buttons

Choose	To
Add	Add an NMS entry.
Modify	Modify an NMS entry. If you choose this command, continue with Step 3 through Step 6.
Delete	Delete an NMS entry.
Close	Exit this dialog box.

When you add, modify or delete an NMS entry, the changes you make are not automatically updated in the switch. If you use the NMS Entries function on an online and managed switch, you must PRAM Sync the SP module for these changes to take effect.

2. Choose Add. The following dialog box appears.

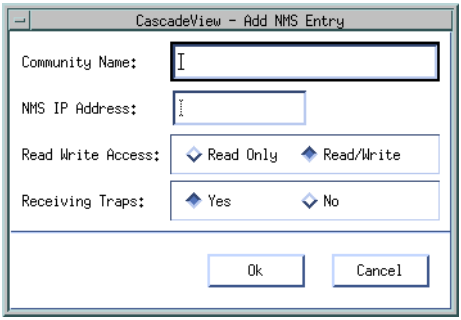


Figure 5-9. Add NMS Entry Dialog Box

3. Enter the community name and NMS IP address for this NMS workstation.

If you need to modify the community name, first edit this dialog box to modify the name, then edit the cascadeview.cfg *file and modify the value for* CV_SNMP_READ_WRITE_COMMUNITY.

4. Select the access rights for this NMS.
   - *Read Only* access allows you to monitor network functions from this NMS.
   - *Read/Write* access allows you to monitor and configure the network map from this NMS.
5. Select the default, Yes, to enable the NMS to receive traps. Trap alarm conditions notify the operator of events taking place on the switch.
6. Choose OK.
7. Repeat Step 2 through Step 6 for each NMS entry.
8. When you finish, choose close to return to the Set Switch Attributes dialog box.
9. To specify additional switch attributes, proceed to Step 3 on page 5-14.

Configuring the IP Address of the NMS

The Set NMS Path function enables you to configure the IP address and access rights of the NMS workstation or IP host that you use to access switches either for configuration or Telnet purposes. If you do not enter the IP address of a particular NMS, that NMS cannot receive switch status information.

The term "NMS" describes the workstation that is used to host the NMS applications. You can use these same procedures to establish communications between the switch and any IP host (i.e., Accounting Server).

The NMS path configuration is node-specific and describes each NMS that attaches via the switch. You only need to define an NMS path for the switch that contains one of the following connections for sending management protocol requests and responses:

Direct Ethernet — The NMS connects to the same LAN as the switch Ethernet connection. You can use Direct Ethernet only if the switch can reach the NMS (address) without going through a gateway router.

Indirect Ethernet — Indicates that the NMS and the switch Ethernet IP Address are on two separate LANs, and are only reachable using a gateway router(s). For this method, enter both the NMS IP address and the associated gateway router IP address. Also, when you installed CascadeView/UX, you entered a "static route" in the gateway router to specify how it is to reach the internal IP network address. This is the Network Number you specified in the Configuration dialog box on page 4-9.

Management PVC — This connection is used when the NMS or IP host connects to the switch via an ATM router or network interface card (NIC). You can use this type of connection for all applications involving a switch and an attached NMS or IP host. Because the management PVC is an actual PVC between the UNI port to which the NMS or IP host connects and the remote switch SP module, the switch to which the NMS or IP host connects is not burdened by the traffic traversing the management PVC.

If you plan to use a management PVC, refer to Chapter 7 to define the logical port. Then refer to "Configuring a Management PVC" on page 9-51.

Management VPI/VCI — This connection is used when the NMS or IP host connects to the switch via an ATM router or network interface card (NIC). This is the preferred method if you only use the attached NMS or IP host to transfer information between the host and the local switch. Even though you can use a management VPI/VCI connection to transfer information between the host and remote switch(es), if you must transfer large amounts of information, use of this method can have a negative impact on the local switch.

If you plan to use Management VPI/VCI, refer to Chapter 7 to define the logical ports. Then refer to "Configuring Management VPI/VCIs" on page 9-46.

Defining the NMS Path

To set the NMS Path:

1. On the network map, select the switch that will contain the NMS path.
2. From the Administer menu, select Cascade Parameters ⇒ Set NMS Paths. The following dialog box appears.

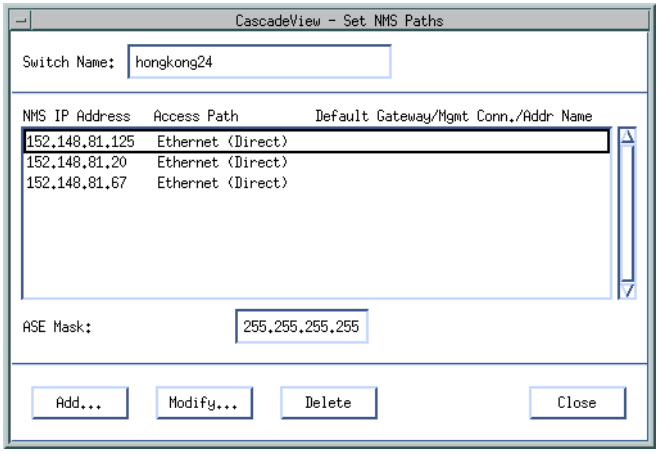


Figure 5-10. Set NMS Paths Dialog Box

3. Choose Add. The following dialog box appears.

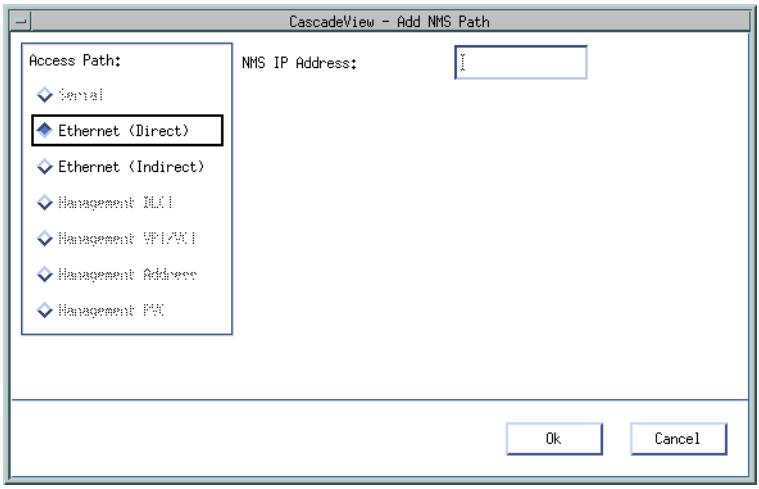


Figure 5-11. Add NMS Path Dialog Box (Management PVC)

4. Complete the following fields:

   a. In the Access Path field, select the connection method you used to connect the NMS to the switch.

   b. Enter the NMS IP address. This is the IP address of the SPARCstation to which this switch connects.

c. The following table describes the fields that appear depending on the type of access path you select:

Access Path	Field(s)	Action/Description
Ethernet (Indirect)	Default Gateway IP Address	Enter the IP address of the gateway router that connects the NMS to the switch.
	ASE Mask	If necessary, enter the ASE mask. The default is 255.255.255.255.
Management VPI/VCI	Management VPI/VCI Name	Select the name of the Management VPI/VCI. To use Management VPI/VCI, first define the logical port as described in Chapter 7. Then, refer to "Adding a New Management VPI/VCI" on page 9-46.
Management PVC	Management PVC Name	Select the name of the Management PVC you defined on page 9-51.

d. Choose OK to save your changes or Cancel to exit without saving.

5. Choose Close to return to the network map.

Configuring SP Attributes

The switch processor attributes enable you to:

- Specify whether or not you have a redundant SP configuration
- Specify the CBX 500 model type
- Set the SP admin status
- Define system timing parameters

To configure SP attributes:

1. From the Administer menu, select Cascade Parameters ⇒ Set Parameters to access the Switch Back Panel dialog box (Figure 5-4 on page 5-9).
2. Select the SP module (middle slot) and choose Set Attr (or, double-click on the SP module) to access the Set SP Attributes dialog box.

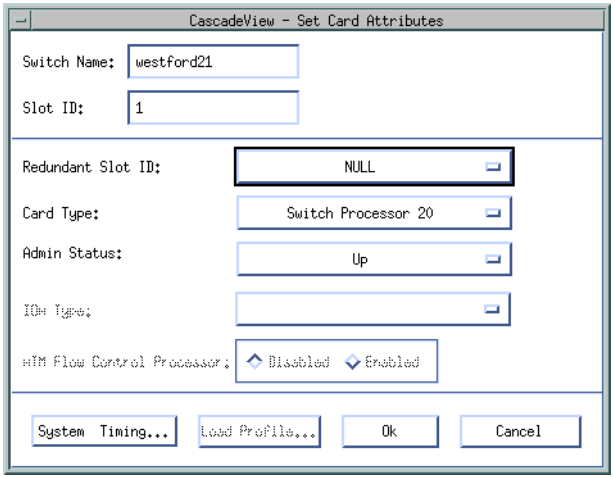


Figure 5-12. Set Card [SP] Attributes Dialog Box

3. Complete the dialog box fields as described in Table 5-5.

Table 5-5. Set Card [SP] Attributes Fields

Field	Action/Description
Redundant Slot ID	Select NULL if you have a non-redundant SP configuration. Select 2 if you have a redundant SP installed in the switch.
Card Type	Select either SP10 for a Model 10 or SP20 for a Model 20.
Admin Status	Select one of the following: *Up (Default)* – The SP module becomes fully operational when you start the switch. To become operational, the module gets its application code from the PCMCIA hard drive card, which resides in the SPA module. *Down* – The SP module does not come online when you start the switch. The configuration is saved in the switch configuration table, but is not downloaded to the switch. Use this option when running foreground diagnostics. *Maintenance* – The SP module does not receive the application code when you start the switch. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that is failing to boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.

To continue, use one of the following methods to define the clock source:

- To use either of the external clock sources or the internal clock as the switch clock source, define the switch clock sources and clock source priorities now. Refer to the following section, "Defining System Timing" for more information.
- To use an IOM's clock source as the switch clock source, you must configure one of the IOM's physical ports as a clock source for the switch. Refer to the section in Chapter 6 that corresponds to the physical port type you are using.

Defining System Timing

The System Timing function enables you to

- Specify the primary and secondary clock sources for the switch.
- Specify whether or not the switch clock source reverts from secondary back to primary in situations where the primary clock has become unavailable, forcing the switch to get its timing from the secondary clock source.
- Enable or disable the external clock output.
- Specify the external line build-out of the external clock output.
- Manually select the active system timing clock.
- Configure an SP for international use.

To view the configured system timing options, refer to the *Diagnostic and Troubleshooting Guide for CBX 500.*

To define System Timing parameters:

1. From the Set SP Attributes dialog box (Figure 5-12 on page 5-25), choose System Timing. The following dialog box appears.

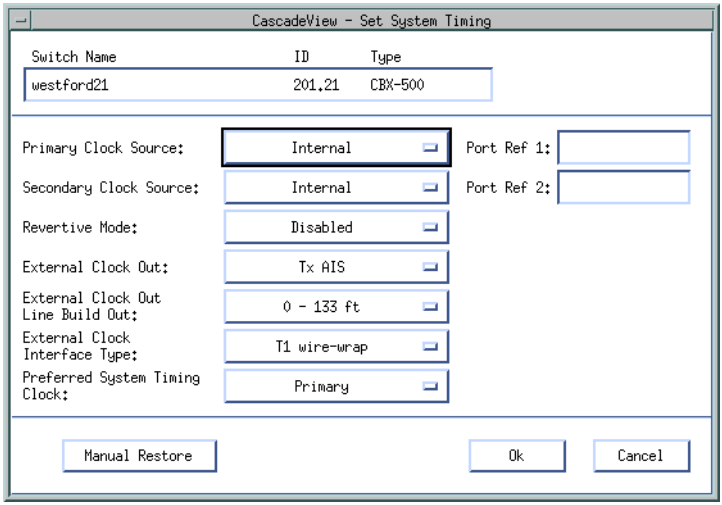


Figure 5-13. Set System Timing Dialog Box

2. Complete the dialog box fields as described in Table 5-6. When you finish, choose OK to apply these settings.

Table 5-6. Set System Timing Fields

Field	Action/Description
Primary/Secondary Clock Source	Select a different option for both the Primary and Secondary clock sources. If the Primary source becomes unavailable, the Secondary source automatically takes control of system timing. Options include: *Internal* (default) – The switch uses the Stratum 3 clock on the SP module as the primary (or secondary) clock source. *External 1* – To use this option, you must connect an external clock source to the primary external clock connection on the SPA module (refer to the *CBX 500 Hardware Installation Guide* for connection instructions). This connection is labeled "In 1." The switch uses this external clock as the primary (or secondary) system timing source. *External 2* – To use this option, you must connect an external clock source to the secondary external clock connection on the SPA module (refer to the *CBX 500 Hardware Installation Guide* for connection instructions). This connection is labeled "In 2." The switch uses this external clock as the primary (or secondary) system timing source. *Port Reference 1* – To use this option, first configure one of the physical ports on the switch as the Primary System Clock Source (refer to Table 6-2 on page 6-5). The switch uses the incoming clock signal on the selected physical port as the primary (or secondary) system timing source. *Port Reference 2* – To use this option, first configure one of the physical ports on the switch as the Secondary System Clock Source (refer to Table 6-2 on page 6-5). The switch uses the incoming clock signal on the selected physical port as the primary (or secondary) system timing source.

Table 5-6. Set System Timing Fields (Continued)

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

Table 5-6. Set System Timing Fields (Continued)

Field	Action/Description
External Clock Interface Type	Select one of the following options: *T1 wire-wrap* (default) – The SP accepts T1 timing inputs and provides T1 timing outputs. The signalling is D4 framed. *E1 BNC* – The SP accepts E1 timing inputs and provides E1 timing outputs.
External Clock Out Line Build Out	If the External Clock Interface Type is T1 wire-wrap, select a value for the External Clock Out Line Build Out field that matches the distance from the external clocking device. The default is 0 – 133 ft.
Preferred System Timing Clock	Select one of the following options: *Primary* – The switch uses the clock source specified in the Primary Clock Source field. *Secondary* – The switch uses the clock source specified in the Secondary Clock Source field. ***Note:*** *If the primary clock source becomes unavailable, the system automatically provides the secondary clock source to the I/O modules.*

Deleting a Switch Configuration from the Database

To delete a switch configuration from the database, first delete the entire configuration associated with the switch to be deleted; for example, logical ports, trunks, and circuits. For complete information, contact the Cascade Technical Response Center.

Use the following sequence to delete a switch configuration from the database:

Step 1. Delete all switched virtual circuits (SVC prefix and addressing information) defined for the switch to be deleted ("this switch").

Step 2. Delete all permanent virtual circuits (PVCs) defined for this switch.

Step 3. Delete all trunk connections involving this switch.

Step 4. Delete all logical ports on this switch.

Step 5. Delete all I/O module configurations on this switch.

Step 6. Delete this switch icon from the map.

6

Configuring I/O Modules and Ports

This chapter explains how to configure each I/O slot with the appropriate module installed in the CBX 500 switch. For each input/output module (IOM), you configure the physical port parameters that determine how a specific port handles clock source and clock rate.

Before you configure the IOM and the physical ports, verify that the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Add the switch object to the map (page 4-14)
- ☑ Specify the attributes for the switch (page 5-12)
- ☑ Configure the IP address of all NMS workstations that need access to the switch (page 5-21)

Configuring CBX 500 IOMs

To configure the IOMs for the CBX 500:

1. On the network map, select the switch whose modules you want to configure.

> *You must log on to CascadeView/UX before you can configure or modify any parameters for the selected switch. If you are not already logged on, select a switch, then select CascadeView ⇒ Logon from the Misc menu and enter the operator password.*

2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box (shown on page 5-9) appears.

3. Double-click on the slot you want to configure, or select the slot, and then choose Set Attr. The following dialog box appears.

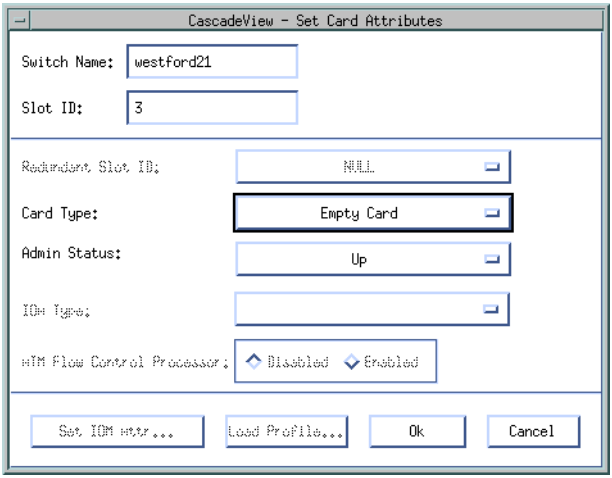


Figure 6-1. Set Card Attributes Dialog Box

4. Complete the dialog box fields as described in Table 6-1.

Table 6-1. Set Card Attributes Fields

Field	Action/Description
Redundant Slot ID	This function is currently not supported.
Card Type	Select the type of IOM installed in this slot.
Admin Status	*Up* – (Default) Activates this IOM at switch start-up. When activated, the module gets its application code from the SP and loads these drivers. *Down* – This IOM does not come online when you start the switch. The configuration is saved in the database but is not downloaded to the switch. Use this option when you run foreground diagnostics. *Maintenance* – Sets this IOM in a state where only its boot flash is running; application code is not running. This setting enables you to reset the PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a hardware problem.
IOA Type	Select the IOA Type that this IOM uses. If select the wrong IOA type, the Switch Back Panel dialog box displays the IOM in yellow to indicate the mismatch. *E1 modules* – Coaxial Pair 75 ohm (default) or DB15 120 ohm. *OC12/STM-4 and OC3/STM-1* – Select one of the following: • Singlemode Optical uses the standard singlemode medium reach fiber optic IOA. This is the default for OC12/STM-4. • Singlemode Optical long reach uses the IOA for long reach singlemode fiber optic transmission. • Multimode (OC3/STM-1 only) uses the multimode fiber optic IOA. This is the default of OC3/STM-1. • STM-1 Copper (OC3/STM-1 only) uses the STM-1 copper IOA that provides a coaxial cable interface instead of fiber optic.

5. Choose the Set IOM Attributes command to specify clocking information for the IOM. Figure 6-2 shows the Set IOM Card Attributes dialog box that appears for a DS3 module.

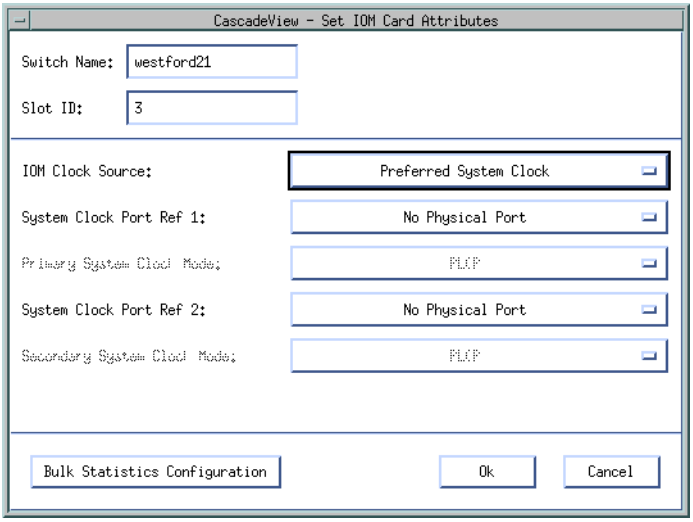


Figure 6-2. Set IOM Card Attributes Dialog Box (8 Port DS3 Modules)

6. Complete the dialog box fields as described in Table 6-2.

Table 6-2. Set IOM Card Attributes Fields

Field	Action/Description
IOM Clock Source	Determines 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* (refer to Table 6-6 on page 6-12). 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. Options include: *Preferred System Clock* – (Default) The preferred system clock provides the IOM clock source, which can be either the primary or secondary system clock (whichever of the two is currently up). *Local Clock* – The local clock on the IOM provides the clock source. *Primary System Clock Only* – The primary system clock source provides the IOM clock source. Specify the primary system clock on the Set System Timing dialog box (refer to "Defining System Timing" on page 5-27). *Secondary System Clock Only* – The secondary system clock source provides the IOM clock source. Specify the secondary system clock on the Set System Timing dialog box.
System Clock Port Ref 1	Determines whether or not the IOM provides the primary system clock source to the SP module. Options include: *No Physical Port* – (Default) Select this option if you do not want the SP to get its primary system clock source from a port on this IOM. *Physical Port* n – Select the physical port that provides the primary system clock source to the SP. When you select this option, the incoming clock signal on the selected port is provided to the SP as the primary system clock source. On a given switch, you can configure a maximum of two physical ports as clock sources (one primary and one secondary).

Table 6-2. Set IOM Card Attributes Fields (Continued)

Field	Action/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. Options include: *PLCP* – The module uses a PLCP frame, which transmits 12 ATM cells every 125 µs. *Line Rate* – The module uses the line rate as the clock mode. The DS3 line rate is 44.5 Mbps.
System Clock Port Ref 2	Determines whether or not the IOM provides the secondary system clock source to the SP module. Select one of the following options: *No Physical Port* – (Default) Select this option if you do not want the SP to get its secondary system clock source from a port on the IOM. *Physical Port* n – Select the physical port that provides the secondary system clock source to the SP. When you select this option, the SP uses the incoming signal on the selected port as the secondary system clock source. On a given switch, you can configure a maximum of two physical ports as clock sources (one primary and one secondary).
Secondary System Clock Mode (*DS3/E3 only*)	This field is available only if you selected a physical port in the Secondary System Clock Source field. Select one of the following options: *PLCP* – The module uses a PLCP frame, which transmits 12 ATM cells every 125 µs. *Line Rate* – The module uses the line rate as the clock mode. The DS3 line rate is 44.5 Mbps.

7. When you finish, choose OK to return to the Set Card Attributes dialog box.
8. Choose OK to return to the Switch Back Panel dialog box. The configured IOM is displayed in the selected slot.

Once you define an IOM, the IOM automatically cold boots. The cold boot process takes about two minutes to complete. When complete, use the instructions on page 12-18 to PRAM Synch the IOM.

To configure the physical ports on the IOM, refer to the following sections:

- "Defining DS3/E3 Physical Ports" on page 6-11
- "Defining OC3c/STM-1 and OC12c/STM-4 Physical Ports" on page 6-22
- "Defining Physical Port Traffic Shaping" on page 6-40

Accessing Physical Port Attributes

Once you define an IOM, you can configure attributes for each of its physical ports. After you define the physical port(s), you configure the logical port attributes (refer to Chapter 7).

To access physical port functions in CascadeView/UX:

1. Select the switch for which you want to configure a physical port.
1. Log in to CascadeView/UX using either a provisioning or operator password.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

3. Select the physical port you want to configure. The Set Physical Port Attributes dialog box appears. Figure 6-3 on page 6-8 displays the dialog box which appears for an ATM DS3 physical port.

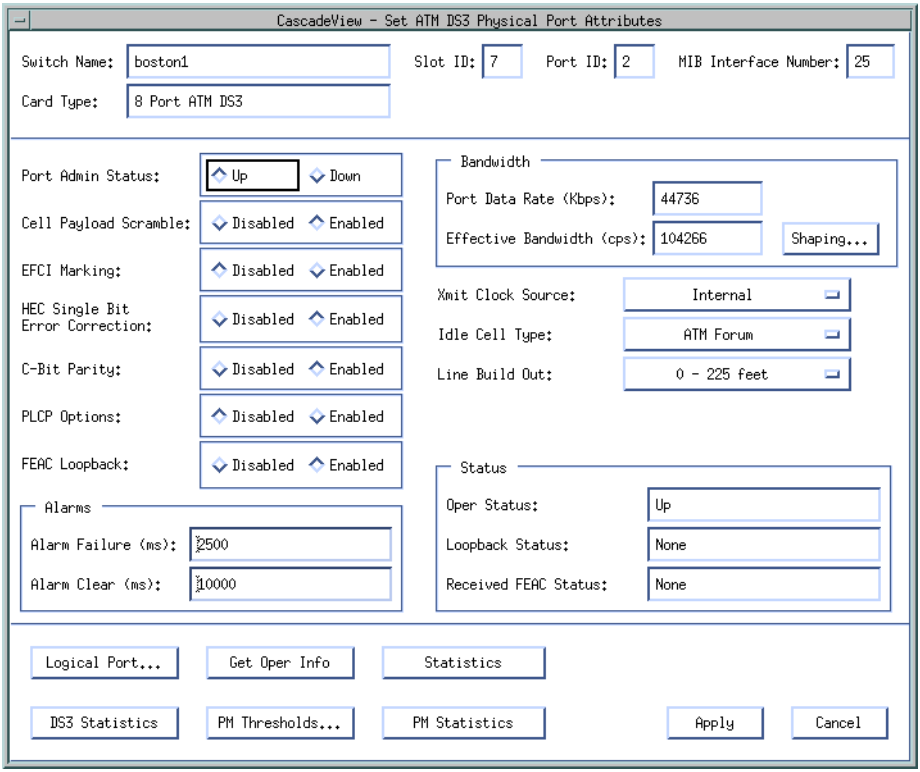


Figure 6-3. Set ATM DS3 Physical Port Attributes Dialog Box

About the Set Physical Port Attributes Dialog Box

The Set Physical Port Attributes dialog box displays the existing physical port configuration which you can modify. It also provides several command buttons that you can use to access additional physical port functions, such as statistics.

Table 6-3 identifies the common command buttons for this dialog box.

Table 6-3. Set Physical Port Attributes Dialog Box Common Command Buttons

Choose	To
Logical Port	Configure logical ports on this physical port (refer to Chapter 7).
Get Oper Info	Update the physical port status message in the Oper Status field. For more information, refer to the section which corresponds to the physical port type you are configuring.
Statistics	Access physical port summary statistics (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).
Apply	Apply your changes to the switch configuration. Once a switch is online, this command updates switch PRAM.
Cancel	Exit the dialog box without saving your changes.

The Set Physical Port Attributes Dialog Box may also display the command buttons described in Table 6-4, depending on the card type you select.

Table 6-4. Port-Specific Dialog Box Command Buttons

Choose	To
Shaping	Access OC3/STM-1 and ATM DS3 traffic shaping parameters. Refer to "Defining Physical Port Traffic Shaping" on page 6-40.
DS3 Statistics	Access ATM DS3 MIB statistics (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).
PM Thresholds	Configure performance monitoring threshold attributes • For ATM DS3 ports, refer to page 6-16. • For OC3/STM-1 and OC12/STM-4 ports, refer to page 6-22. • For T1/E1 ports, refer to page 6-52.
PM Statistics	Access performance monitoring statistics (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).
Sonet Statistics	Access Sonet/SDH MIB statistics for OC3/STM-1 and OC12/STM-4 ports (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).
APS Commands	Access the automatic protection switching (APS) configuration dialog box for OC3/STM-1 and OC12/STM-4 ports (refer to page 6-38).
FDL	Configure facility data link (FDL) control parameters for Extended Superframe T1/E1 circuits types (refer to page 6-50).

To define specific physical port attributes, continue with the section that corresponds to your particular physical port type:

- "Defining DS3/E3 Physical Ports" on page 6-11
- "Defining OC3c/STM-1 and OC12c/STM-4 Physical Ports" on page 6-22
- "Defining T1/E1 Physical Ports" on page 6-42

Defining DS3/E3 Physical Ports

The Asynchronous Transfer Mode (ATM) DS3/E3 module provides eight DS3/E3 ports. To configure the physical ports for a DS3/E3 module:

1. Complete the steps in "Accessing Physical Port Attributes" on page 6-7 to access the Set Physical Port Attributes dialog box for either an ATM DS3 or E3 module.

   Table 6-5 identifies the Oper Status messages for this physical port. Use the Get Oper Info command to update this field.

Table 6-5. DS3/E3 Get Oper Info Messages

Message	Description
red alarm	Receive loss of frame (LOF) signal
yellow alarm	Receive far end LOF signal
blue alarm	Receive alarm indication signal (AIS)
idle	Idle signal condition
looped-back	Physical port in loopback mode
loss-of-signal	Receive loss of signal (LOS)

2. Complete the dialog box fields as described in Table 6-6.

Table 6-6. Set ATM DS3 [E3] 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.
Port Admin Status	Set this option to Up (default) to enable immediate access to the port. Set the Admin Status to Down to save the configuration in the database without activating the port or to take the port offline to run diagnostics. Each time you modify the Port Admin Status, choose Apply and then OK to send the change to the switch.
Cell Payload Scramble	Enable (default) or disable the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (that is, it prevents ATM cell header alienation).
EFCI Marking	The Explicit Forward Congestion Indicator (EFCI) determines if congestion (or impending congestion) exists in a node. This option is disabled by default. If enabled, 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. Disable this option if you do not want to use EFCI marking on this physical port.
HEC Single Bit Error Correction	Enable (default) or disable the single bit header error correction (HEC) on a per port basis. When the framer is operating in the default mode with single bit error correction enabled, the framer corrects the single bit errors but does not count them. Disable this function on the framer to determine how many errors are occurring on the physical port.

Table 6-6. Set ATM DS3 [E3] Physical Port Attributes Fields (Continued)

Field	Action/Description
C-Bit Parity (*DS3 modules only*)	Enable (default) or disable the C-Bit Parity function. The C-Bit Parity function provides a way to monitor the end-to-end performance of T3 circuits. ***Note:*** *This feature requires C-bit parity-compatible customer premise equipment (CPE).*
PLCP Options	Enables or disables the Physical Layer Convergence Protocol (PLCP) option. When Enabled (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 header error correction (HEC) mode.
FEAC Loopback (*DS3 modules only*)	Enable (default) or disable the switch's ability to respond to loopback commands on the Far-End Alarm and Control (FEAC) channel. Select Enable to allow 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. Select Disable to ignore loop up and loop down commands on the FEAC channel.
Alarm Failure (ms)	Enter a value between 0 to 65535 ms to determine how long the switch waits before declaring a physical layer problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch "soaks" the physical layer alarm for 2.5 seconds before declaring the physical port down. A value of 0 ms means the physical port goes down immediately following any physical layer failure. If you set the value lower than the default of 2.5 seconds, the switch takes the physical port down due to any transient failure in the transmission path; for a port that provides trunk connectivity, this may cause unnecessary rerouting of circuits.

Table 6-6. Set ATM DS3 [E3] Physical Port Attributes Fields (Continued)

Field	Action/Description
Alarm Clear (ms)	Enter a value between 0 to 65535 ms to determine how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the physical port up. A value of 0 ms means the physical port comes back up as soon as the physical layer failure alarm clears. If you set the value lower than the default of 10 seconds, the switch may declare the physical port up before the transmission path is stabilized.
Port Data Rate (Kbps)	Represents the raw physical data rate of the port. Due to the bandwidth lost as a result of the ATM layer to physical layer mapping, this number is always greater than the actual cell rate that can be transmitted out the port. The actual rate of cell transmission is dependent on the method of ATM layer mapping used. Refer to Table 7-2 on page 7-8 for additional information.
Effective Bandwidth (cps)	Represents the actual cell transmission rate the physical port uses. By default, the physical port transmits cell traffic at the maximum rate supported on the physical interface. However, you can use the Shaping command to select a transmission rate that is lower than the maximum rate.
Xmit Clock Source	Specify the transmit clock source. *Internal* – (Default) The IOM's internal timing source provides the clock source to this port. The IOM Clock Source setting in the Set IOM Card Attributes dialog box (see page 6-5) determines the internal clock source. *Loop-Timed* – The clock source is derived from the signal coming into this port.
Line Build Out (*DS3 modules only*)	Select 0 – 225 feet (default) for a short cable or 226 – 450 feet for a long cable. This measurement represents the length of the cable that connects the physical port to other network equipment.

Table 6-6. Set ATM DS3 [E3] Physical Port Attributes Fields (Continued)

Field	Action/Description
Idle Cell Type	Allows you to specify the type of cell that is used to fill the gaps between user data cells that are transmitted out of the physical port. The physical port receive function is not affected by this option (both ITU and ATMF are recognized and processed by the physical port receiver). Select one of the following options: *ATM Forum* (default) – The fill cell will have a header of 00 00 00 00 55 and a payload of 6A (for all 48 bytes). *ITU* – The fill cell will have a header of 00 00 00 01 55 and a payload of 6A (for all 48 bytes).
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. Refer to Table 6-5 on page 6-11 for a description of these messages.
Loopback Status	Displays the port loopback status, if you enabled diagnostic loopback tests. The default is None. Refer to the *Diagnostics and Troubleshooting Guide for CBX 500* for more information.
Received FEAC Status (*DS3 only)*	Displays the FEAC (Far-End Alarm and Control) status received by this physical port if C-Bit Parity is enabled. This field indicates the status of the physical port on the other end of the connection.

3. To modify the default physical port performance thresholds for this physical port, continue with the following section.
4. To modify the default physical port traffic shaping parameters, refer to page 6-40.
5. To exit, choose Apply and then OK to save the physical port attributes and send an SNMP SET command to the switch. Choose Cancel to exit the dialog box.

Defining DS3/E3 Performance Thresholds

The NMS allows you to set performance parameter thresholds for the 15-minute and one-day accumulation periods for each DS3/E3 physical port. If you enable threshold crossing, the port generates traps if these thresholds are crossed.

To configure these parameters,

1. From the Set ATM DS3[E3] Physical Port Attributes dialog box (Figure 6-3 on page 6-8), choose PM Thresholds. The following dialog box appears.

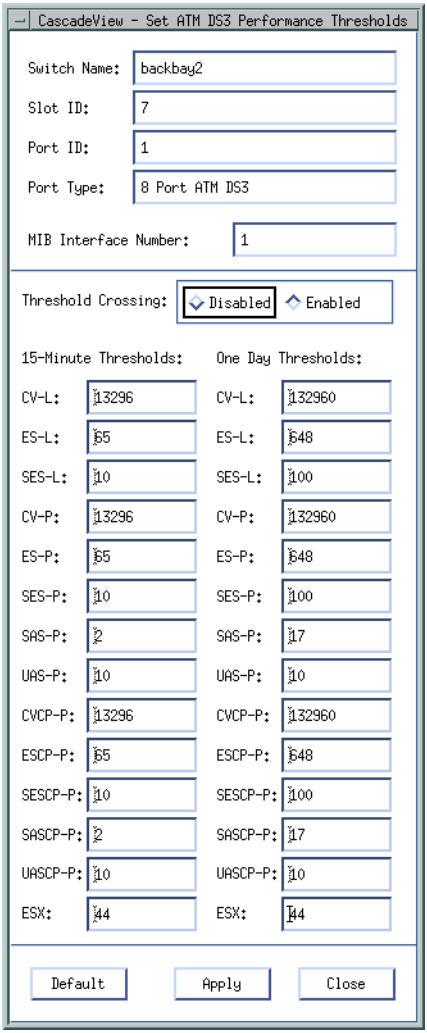


Figure 6-4. Set ATM DS3 Performance Thresholds Dialog Box

2. Threshold Crossing is Disabled by default. Enable it if you want to generate traps for threshold crossing.

3. Use Table 6-7 on page 6-18 to set the 15-minute and one-day threshold values. Use the Default command button to return these values to the default settings.

Table 6-7. DS3/E3 Performance Monitoring Thresholds

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
Near End Line Parameters					
CV-L (Code Violations)	A count of both BPVs and EXZs occurring over the accumulation period.	1 - 16383	1 - 13296	1 - 1048575	132960
ES-L (Errored Seconds)	A count of 1-second intervals containing one or more BPVs, one or more EXZs, or one or more LOS defects.	1 - 900	65	1 - 65535	648
SES-L (Severely Errored Seconds)	A count of 1-second intervals with more than x BPVs plus EXZs, or one or more LOS defects.	1 - 63	10	1 - 4095	100

Table 6-7. DS3/E3 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
Near End Path Parameters					
CV-P (Code Violations)	A count of error events occurring in the accumulation period.	1 - 16383	13296	1 - 1048575	132960
ES-P (Errored Seconds)	A count of 1-second intervals containing the occurrence of one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.	1 - 900	65	1 - 65535	648
SES-P (Severely Errored Seconds)	A count of 1-second intervals containing more than x P-bit parity errors, one or more SEF defects, or one or more AIS defects.	1 - 63	10	1 - 4095	100
SAS-P (AIS Seconds)	A count of 1-second intervals containing one or more AIS defects.	1 - 63	2	1 - 4095	17

Table 6-7. DS3/E3 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
UAS-P (P-bit Unavailable Seconds)	A count of 1-second intervals for which the DS3 path is unavailable.	1 - 63	10	1 - 4095	10
CVCP-P (C-bit Coding Violations)	This error is counted when the three FEBE bits in an M-frame are not all set to one (1).	1 - 16383	13296	1 - 1048575	132960
ESCP-P (C-bit Errored Seconds)	A count of 1-second intervals containing one or more M-frames with the three FEBE bits not all set to one (1); or one or more far-end SEF/AIS defects.	1 - 900	65	1 - 65535	648
SESCP-P (C-bit Severely Errored Seconds)	A count of 1-second intervals containing more than x M-frames with the three FEBE bits not all set to one (1); or one or more far-end SEF/AIS defects.	1 - 63	10	1 - 4095	100

Table 6-7. DS3/E3 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
SASCP-P (C-bit AIS Seconds)	A count of 1-second intervals containing one or more far-end SEF/AIS defects.	1 - 63	2	1 - 4095	17
UASCP-P (C-bit Unavailable Seconds)	A count of 1-second intervals for which the DS3 path is unavailable.	1 - 63	10	1 - 4095	10
ESX (Defects in Errored Seconds)	A count of 1-second intervals containing 1 or more unclassified errors.	1 - 255	44	1 - 65535	44

4. When you finish, choose Apply to save your changes and Close to return to the Set Physical Port Attributes dialog box (Figure 6-3 on page 6-8).

5. Choose Apply and then OK to save the physical port attributes and create an SNMP SET command to send to the switch. Choose Cancel to exit.

Defining OC3c/STM-1 and OC12c/STM-4 Physical Ports

OC3c/STM-1 modules provide physical ports that can operate at 155.52 Mbps. The 1-port OC12c/STM-4 module contains physical ports that can operate at 622 Mbps. You can configure up to 14 OC12c/STM-4 ports per switch.

Once you configure the physical port parameters for either of these modules, you can configure performance monitoring thresholds (refer to page 6-28). For OC12/STM-4 modules, you can also configure the second physical port as a backup. This feature is called *automatic protection switching* (APS). Refer to page 6-33 for more information on this feature.

To configure the physical ports for this module:

1. Complete the steps in "Accessing Physical Port Attributes" on page 6-7 to access the Set Physical Port Attributes dialog box for either an OC3c/STM-1 module or an OC12c/STM-4 module.

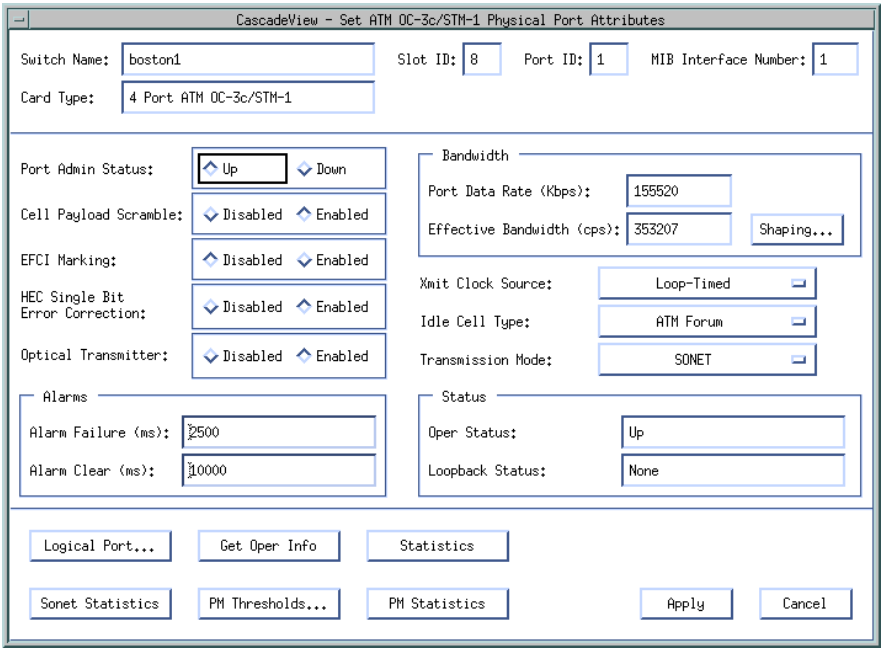


Figure 6-5. Set ATM OC3/STM-1 Ports Physical Port Attributes Dialog Box

Table 6-8 identifies the Oper Status messages for this physical port. Use the Get Oper Info command to update this field.

Table 6-8. OC3c/STM-1 and OC12/STM-4 Get Oper Info Messages

Message	Description
Down with signal label mismatch	Sonet Path signal label mismatch
Down with loss of signal	Receive loss of signal (LOS)
Down with loss of frame	Receive loss of frame (LOF)
Down with cell delination loss	Loss of ATM cell delination
Down with line AIS	Receive Sonet line alarm indication signal (AIS)
Down with path AIS	Receive Sonet path AIS
Down with loss of pointer	Sonet loss of pointer
Down with line RFI	Receive Sonet line remote failure indication (RFI)
Down with path RFI	Receive remote Sonet path RFI
Down with signal label undefined	Sonet Path signal label unequipped

2. Complete the dialog box fields as described in Table 6-9.

Table 6-9. Set ATM OC3/STM-1 [OC12/STM-4] 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.
Port Admin Status	Set this option to Up to enable immediate access to the port. Set the Admin Status to Down to save the configuration in the database without activating the port or to take the port offline to run diagnostics. Each time you modify the Port Admin Status, choose the Apply command to send the change to the switch. ***Note:*** *Changing the Port Admin Status to down sets the physical port operational state to down, but this action does not result in an APS switchover; if you admin down a physical port, user data will be disrupted.*
Cell Payload Scramble	Enables (default) or disables the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (that is, it prevents ATM cell header alienation).
EFCI Marking	The Explicit Forward Congestion Indicator (EFCI) determines if congestion (or impending congestion) exists in a node. The default is disabled. If Enabled, 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's queue. Disable this option if you do not want to use EFCI marking on this physical port.

Table 6-9. Set ATM OC3/STM-1 [OC12/STM-4] Physical Port Attributes Fields (Continued)

Field	Action/Description
HEC Single Bit Error Correction	Enables or disables the single bit header error correction (HEC) on a per-port basis. When the framer is operating in the default mode of single bit error correction enabled, the framer corrects the single bit errors, but does not count them. Disable the single bit error correction function on the framer to determine how many errors are occurring on the physical port.
Optical Transmitter	This field is a safety feature intended to prevent personal injury when you repair/replace the module or connect cables to the module. By default, this option is disabled. This disables the transmit laser or LED for this port, so it cannot transmit incoming traffic. **You must Enable this option to transmit incoming traffic out of this port**. ***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. Disabling the transmit laser does not result in an APS switchover; if you disable the optical transmitter, user data will be disabled.* ***WARNING:*** *Before you remove the optical cable, set this field to disabled. If the optical connectors are exposed, the transmit laser beam can cause personal injury.*
Transmission Mode	Enables you to designate individual ports on this IOM for either SONET (OC3/OC12) or SDH (STM-1/STM-4). For OC3 modules, you can configure OC3 framing on one port and STM-1 framing on another. • Select *SONET* (default) to configure the port for OC3/OC12 (North America) • Select *SDH* to configure the port for STM-1/STM-4 (International)

Table 6-9. Set ATM OC3/STM-1 [OC12/STM-4] Physical Port Attributes Fields (Continued)

Field	Action/Description
Redundancy (*OC12/STM-4 only*)	Select APS 1+1 to enable the Automatic Protection Switching (APS) feature. This feature allows you to use the second port on this module as a backup. If you enable this feature, refer to "Using Automatic Protection Switching" on page 6-33 to configure attributes for this feature. The default is None (no backup port).
Alarm Failure	Enter a value between 0 to 65535 ms to determine how long the switch waits before declaring a physical layer problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch "soaks" the physical layer alarm for 2.5 seconds before declaring the physical port down. A value of 0 ms means the physical port goes down immediately following any physical layer failure. If you set the value lower than the default of 2.5 seconds, the switch takes the physical port down due to any transient failure in the transmission path; for a port that provides trunk connectivity, this may cause unnecessary rerouting of circuits.
Alarm Clear	Enter a value between 0 to 65535 ms to determine how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the physical port up. A value of 0 ms means the physical port comes back up as soon physical layer failure alarm clears. If you set the value lower than the default of 10 seconds, the switch may declare the physical port up before the transmission path is stabilized.

Table 6-9. Set ATM OC3/STM-1 [OC12/STM-4] Physical Port Attributes Fields (Continued)

Field	Action/Description
Port Data Rate (Kbps)	Represents the raw physical data rate of the port. Due to the bandwidth lost as a result of the ATM layer to physical layer mapping, this number is always greater than the actual cell rate that can be transmitted out the port. The actual rate of cell transmission is dependent on the method of ATM layer mapping used. Refer to Table 7-2 on page 7-8 for additional information.
Effective Bandwidth (cps)	Represents the actual cell transmission rate the physical port uses. By default, the physical port transmits cell traffic at the maximum rate supported on the physical interface. However, you can use the Shaping command to select a transmission rate that is lower than the maximum rate.
Idle Cell Type	Allows you to specify the type of cell that is used to fill the gaps between user data cells that are transmitted out of the physical port. The physical port receive function is not affected by this option (both ITU and ATMF are recognized and processed by the physical port receiver). Select one of the following options: *ATM Forum* (default) – The fill cell will have a header of 00 00 00 00 55 and a payload of 6A (for all 48 bytes). *ITU* – The fill cell will have a header of 00 00 00 01 55 and a payload of 6A (for all 48 bytes).
Xmit Clock Source	Specify the transmit clock source. *Internal* – (Default) The IOM internal timing source provides the clock source to this port. The IOM Clock Source setting in the Set IOM Card Attributes dialog box (see page 6-5) determines the internal clock source. *Loop-Timed* – The clock source is derived from the signal coming into this port.

Table 6-9. Set ATM OC3/STM-1 [OC12/STM-4] Physical Port Attributes Fields (Continued)

Field	Action/Description
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. Refer to Table 6-8 on page 6-23 for a description of these messages.
Loopback Status	Displays the port's loopback status if you enabled diagnostic loopback tests. The default is None. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for more information.

3. To modify the default physical port performance thresholds for this physical port, continue with "Defining OC3/STM-1 and OC12/STM-4 Performance Thresholds" on page 6-28.
4. (*OC12/STM-4 only*) To configure the second port on this module as a backup port, refer to "Using Automatic Protection Switching" on page 6-33.
5. (*OC3/STM-1 only*) To modify the default physical port traffic shaping parameters, refer to page 6-40.
6. To exit, choose Apply and then OK to save the physical port attributes and create an SNMP SET command to send to the switch. Choose Cancel to exit.

Defining OC3/STM-1 and OC12/STM-4 Performance Thresholds

The NMS allows you to set performance parameter thresholds for the 15-minute and one-day accumulation periods for each physical port. If you enable threshold crossing, the port generates traps if these thresholds are exceeded.

To configure these parameters:

1. From the Set Physical Port Attributes dialog box (Figure 6-5 on page 6-22), choose PM Thresholds. This example displays the Set ATM OC-12c/STM-4 Performance Threshold dialog box.

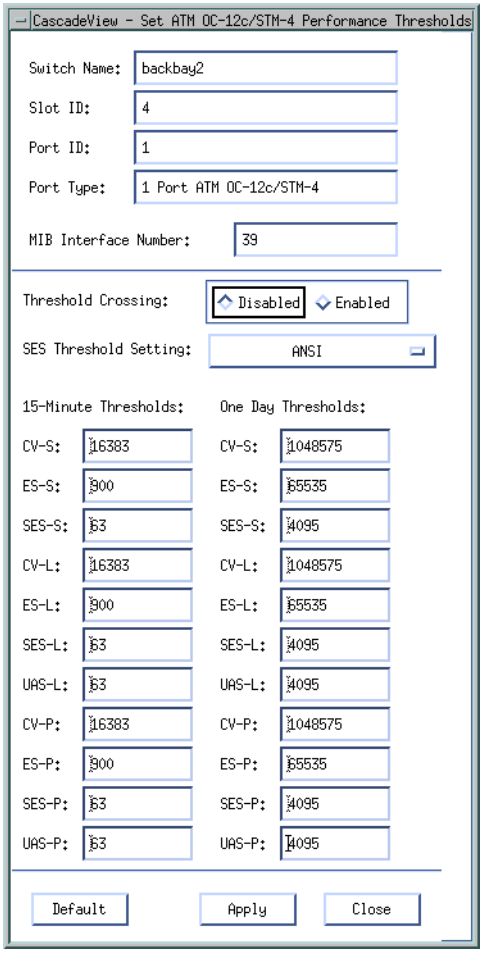


Figure 6-6. Set ATM OC12/STM-4 Performance Thresholds Dialog Box

2. Threshold Crossing is Disabled by default. Enable it if you want to generate traps for threshold crossing.

3. Select the SES Threshold Setting which corresponds to the standard the switch software will use to calculate the severely errored seconds counts. The default is ANSI. Select Bellcore to use the SONET MIB (RFC 1595) thresholds.

Table 6-10 describes the threshold values used for ANSI and Bellcore standards.

Table 6-10. OC3/STM-1 and OC12/STM-4 Severely Errored Seconds Threshold Values

Parameter	ANSI Value	Bellcore Value
Section SES	8800	63
Line SES	10000	124
Path SES	8800	63

4. Use Table 6-11 to set the 15-minute and one-day threshold parameters. Use the Default command button to return these values to the default setting.

Table 6-11. OC3/STM-1 and OC12/STM-4 Performance Monitoring Thresholds

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
CV-S (Section Code Violations)	A count of BIP-8 errors that are detected at the section layer of the incoming signal.	1 - 16383	16383	1 - 1048575	1048575
ES-S (Section Errored Seconds)	A count of 1-second intervals containing one or more BIP-8 errors (B1 byte), one or more SEF defects, or one or more LOS defects.	1 - 900	900	1 - 1048575	1048575

Table 6-11. OC3/STM-1 and OC12/STM-4 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
SES-S (Section Severely Errored Seconds)	A count of 1-second intervals containing x or more BIP-8 errors (B1 byte), one or more SEF defects, or one or more LOS defects.	1 - 63	63	1 - 4095	4095
CV-L (Line Code Violations)	A count of the BIP-8 errors detected at the line layer of the incoming signal.	1 - 16383	16383	1 - 1048575	1048575
ES-L (Line Errored Seconds)	A count of 1-second intervals containing one or more BIP-8 errors (B2 byte), or one or more AIS defects.	1 - 900	900	1 - 1048575	1048575
SES-L (Line Severely Errored Seconds)	A count of 1-second intervals containing x or more BIP-8 errors (B2 byte) or one or more AIS defects.	1 - 63	63	1 - 4095	4095
UAS-L (Unavailable Seconds)	A count of 1-second intervals for which the SONET line is unavailable.	1 - 63	63	1 - 4095	4095

Table 6-11. OC3/STM-1 and OC12/STM-4 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
CV-P (Path Code Violations)	A count of BIP-8 errors that are detected at the STS-path layer of the incoming signal.	1 - 16383	16383	1 - 1048575	1048575
ES-P (Path Errored Seconds)	A count of 1-second intervals containing one or more BIP-8 errors (B3 byte), one or more AIS defects, or one or more LOP-P defects.	1 - 900	900	1 - 1048575	1048575
SES-P (Path Severely Errored Seconds)	A count of 1-second intervals containing x or more BIP-8 errors (B3 byte), one or more LOP-P defects, or one or more AIS defects.	1 - 63	63	1 - 4095	4095
UAS-P (Path Unavailable Seconds)	A count of 1-second intervals for which the SONET STS-path is unavailable.	1 - 63	63	1 - 4095	4095

5. When you finish, choose Apply to save you changes and Close to return to the Set Physical Port Attributes dialog box (Figure 6-5 on page 6-22).

6. Choose Apply and then OK to save the physical port attributes and send an SNMP SET command to the switch. Choose Cancel to exit.

Using Automatic Protection Switching

The OC12/STM-4 modules contain two physical ports. The primary (*working*) port and a backup (*protection*) port. Under normal conditions, traffic passes over the working port. When a failure condition occurs on the OC12 line, traffic automatically transfers over to the protection port. In addition, an APS switchover also occurs when the working line receives LOF, L-AIS, or LOS defects.

To enable this feature, first set the Redundancy field on the OC12/STM-4 Physical Port Attributes dialog box to APS 1+1 (refer to page 6-26). When you view the Switch Back Panel dialog box, the OC12/STM-4 module displays two physical ports. The bottom port is designated as the protection port.

Figure 6-7. OC12/STM-4 APS Port

You can review the physical port parameters for the protection port. Access the Switch Back Panel dialog box (shown on page 5-10) and select the OC12/STM-4 protection port. Choose Set Attr. The following dialog box appears.

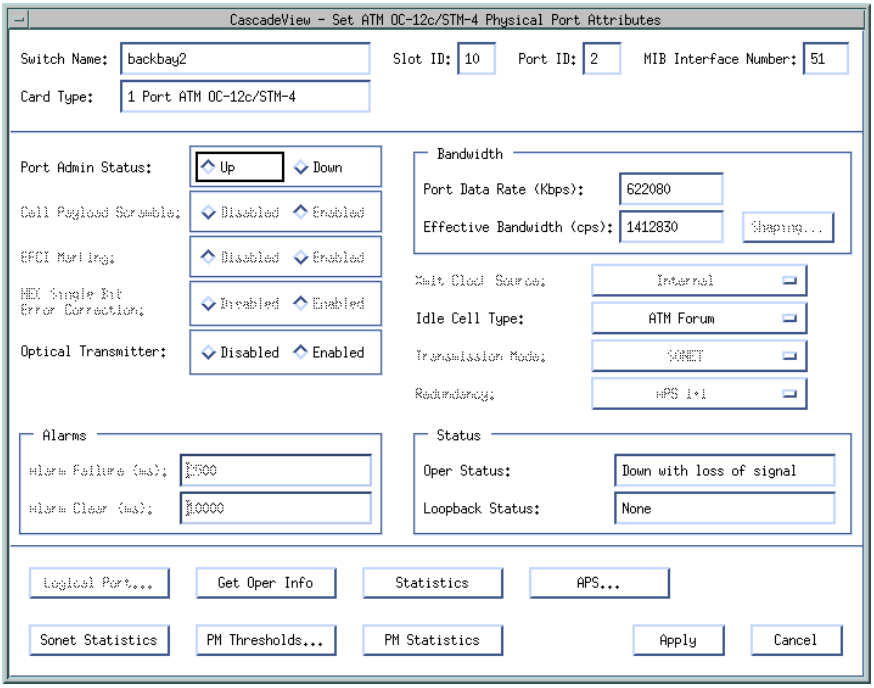


Figure 6-8. Set OC12/STM-4 Physical Port Attributes [Backup Port]

Note that you can only configure the Port Admin Status and Optical Transmitter fields. All other parameters use the values that you defined for the working port. This dialog box also includes command buttons that access the same options used by the working port (refer to Table 6-4 on page 6-10) with one exception: you do not configure logical ports on the protection port.

Configuring APS Parameters

As part of the APS feature, you configure failure thresholds that the working port must exceed before traffic transfers to the protection port. You can configure the APS function to revert back to the working port when the failure condition clears.

> *For more information about APS, refer to the* Bellcore Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria Specification *(GR-253-CORE).*

Use the following steps to configure APS parameters:

1. From the Set Physical Port Attributes dialog box (Figure 6-5 on page 6-22), choose APS. The following dialog box appears.

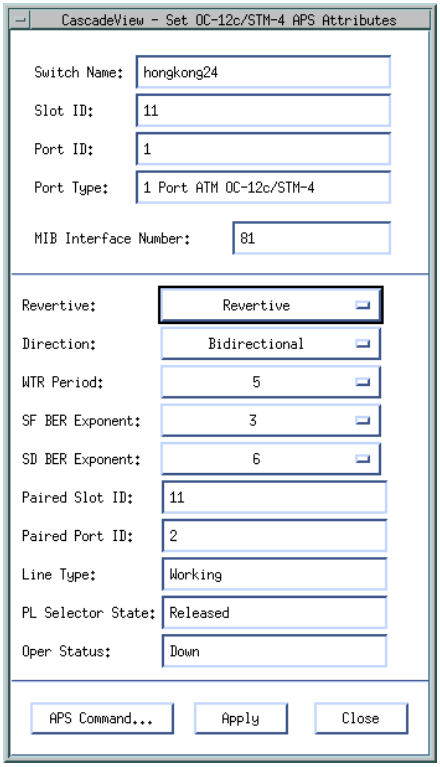


Figure 6-9. Set OC-12c/STM-4 APS Attributes Dialog Box

When you access the Set OC12c/STM-4 APS Attributes dialog box from the protection port, the Line Type field displays Protection. In this case you cannot modify the Revertive, Direction, and WTR Period fields.

2. Complete the APS attributes as described in Table 6-12.

Table 6-12. OC-12c/STM-4 APS Attributes Fields

Field	Action/Description
Revertive	Designates how this port handles traffic once a line failure clears. Select one of the following: *Revertive* (default) – Traffic transfers back to the working port when the wait-to-restore (WTR) time period expires. *Nonrevertive* – Traffic continues to pass over the protection port until you use the APS Command (refer to page 6-38) to transfer back to the working port.
Direction	Determines whether or not one endpoint will switch over independently of the other. (In APS, there is a one-for-one correlation between the ports, and traffic is always transmitted on both working and protection lines.) *Unidirectional* (default) – One end switches independently of the other. *Bidirectional* – When one end detects a line defect, it signals the other end to switch. Thus, both ends switch in tandem.
WTR Period	If this port uses the Revertive option, set the wait-to-restore (WTR) time period (5 to 12 minutes). The default is 5 minutes. This is the period of time the port waits once the automatically initiated switch condition (i.e., SD, SF, LOF, AIS, or LOS) clears before it transfers traffic back to the working port. The port does not use this timer if you used the APS Command to transfer traffic to the protection port (refer to page 6-38).

Table 6-12. OC-12c/STM-4 APS Attributes Fields (Continued)

Field	Action/Description
SF BER Exponent	Set the Signal Fail (SF) Bit Error Rate (BER) exponent. Values can range from 3 to 5; the default is 3. The port uses this value to compute the signal fail threshold. When the BER exceeds $10^{-threshold}$, the port detects the line failure and transfers traffic to the protection port. The port transfers traffic based on how you configured the Direction option (either unidirectional or bidirectional). ***Note:*** *The clear condition for SF BER is a bit error rate of less than* 10^{-7}.
SD BER Exponent	Set the Signal Degrade (SD) Bit Error Rate (BER) exponent. Values can range from 6 to 9; the default is 6. The port uses this value to compute the signal degrade threshold. When the BER exceeds $10^{-threshold}$, the port detects the line failure and transfers traffic to the protection port. The port transfers traffic based on how you configured the Direction option (either unidirectional or bidirectional). ***Note:*** *The clear condition for SD BER is a bit error rate of less than 1/10th the current SD threshold.*

3. Choose Apply to save these settings and Close return to the Set Physical Port Attributes dialog box (Figure 6-5 on page 6-22).

4. To exit, choose Apply and then OK to save the physical port attributes and create an SNMP SET command to send to the switch. Choose Cancel to exit.

Sending APS Commands to the Switch

The Set OC-12c/STM-4 APS Attributes dialog box contains the APS Commands button, which you use to send external commands to the switch. Some of the functions you can perform include manually switching between the working and protection port.

To use the APS commands:

1. From the Set OC-12c/STM-4 APS Attributes dialog box (Figure 6-9 on page 6-35), choose APS Commands. The following dialog box appears.

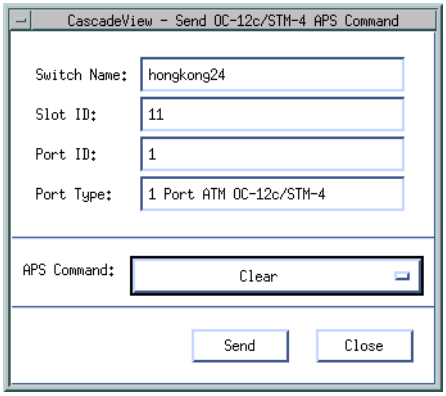


Figure 6-10. Send OC-12c/STM-4 APS Commands

2. Select an APS Command and choose Send. Table 6-13 describes the APS commands that are available to the working or protection port.

Table 6-13. OC12/STM-4 APS Commands

Command	Used to	Port Type Available
Clear	Clear all of the switch commands listed below for the selected port type.	APS and Working
Lockout of Protection	Prevent the working port from switching to the protection port.	Protection
Forced Switch (working -> protection)	Switch from the working port to the protection port. This command does not work if a higher priority request is already in effect.	Working
Forced Switch (protection -> working)	Switch from the protection port to the working port. This command does not work if a higher priority request is already in effect.	Protection
Manual Switch (working -> protection)	Switch from the working port to the protection port. This command does not work if a higher priority request is already in effect. ***Note:*** *If you manually switch to the protection port and then there is a line failure on the working port, the software now prioritizes the port switch as a "forced switch."*	Working

Table 6-13. OC12/STM-4 APS Commands (Continued)

Command	Used to	Port Type Available
Manual Switch (protection -> working)	Switch from the protection port to the working port. This command does not work if a higher priority request is already in effect.	Protection
Exercise	Exercise the protocol for a protection switch to the protection port. This command verifies the response of the protection port. This test clears automatically and returns control to the working port. This command does not work if a higher priority request is already in effect.	Protection

Defining Physical Port Traffic Shaping

For OC3/STM-1 and ATM DS3/E3 physical ports, CascadeView provides the capability to set an ATM physical port traffic shaping parameter. This parameter functions as a pacing mode that enables you to control the effective bandwidth on the physical port.

Use the following formula to compute the effective physical port bandwidth:

```
[1/(n + 1)] * pport clock rate
```

where 360000 cps is the clock rate for an OC3/STM-1 port, 104268 is the clock rate for a DS3/E3 port, and “n” is the pacing mode you specify. The sum of the logical port bandwidth on the physical port cannot exceed the configured effective physical port bandwidth. Likewise, you cannot decrease the effective physical port bandwidth below the sum of the configured logical port bandwidth.

To access physical port traffic shaping:

1. From either the Set OC3/STM-1 Physical Port Attributes (Figure 6-5 on page 6-22) or the Set DS3 [E3] Physical Port Attributes (Figure 6-3 on page 6-8) dialog boxes, choose the Shaping command. The following dialog box appears.

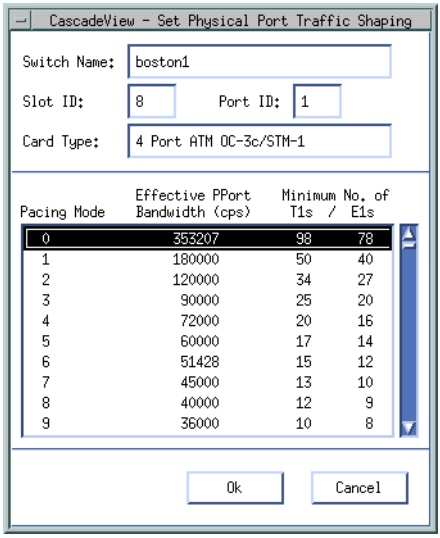


Figure 6-11. Set Physical Port Traffic Shaping Dialog Box

2. Select the pacing mode you need to achieve the desired effective physical port bandwidth or the number of T1/E1s in the inverse MUX. Valid values are 1 to 255.

3. Choose OK to return to the Set Physical Port Attributes dialog box.

Defining T1/E1 Physical Ports

The 8-port T1 and E1 modules contain physical ports that can operate at 1.544 Mbps (T1) or 2.048 Mbps (E1). You can configure up to 112 T1 or E1 ports per switch. Once you configure physical port parameters, configure the performance monitoring thresholds (refer to page 6-52). For a T1 module that uses an extended superframe circuit type, you can also specify the facility data link parameters (refer to page 6-50).

To configure the physical port parameters for these modules:

1. Complete the steps in "Accessing Physical Port Attributes" on page 6-7 to access the Set Physical Port Attributes dialog box for either a T1 or an E1 module.

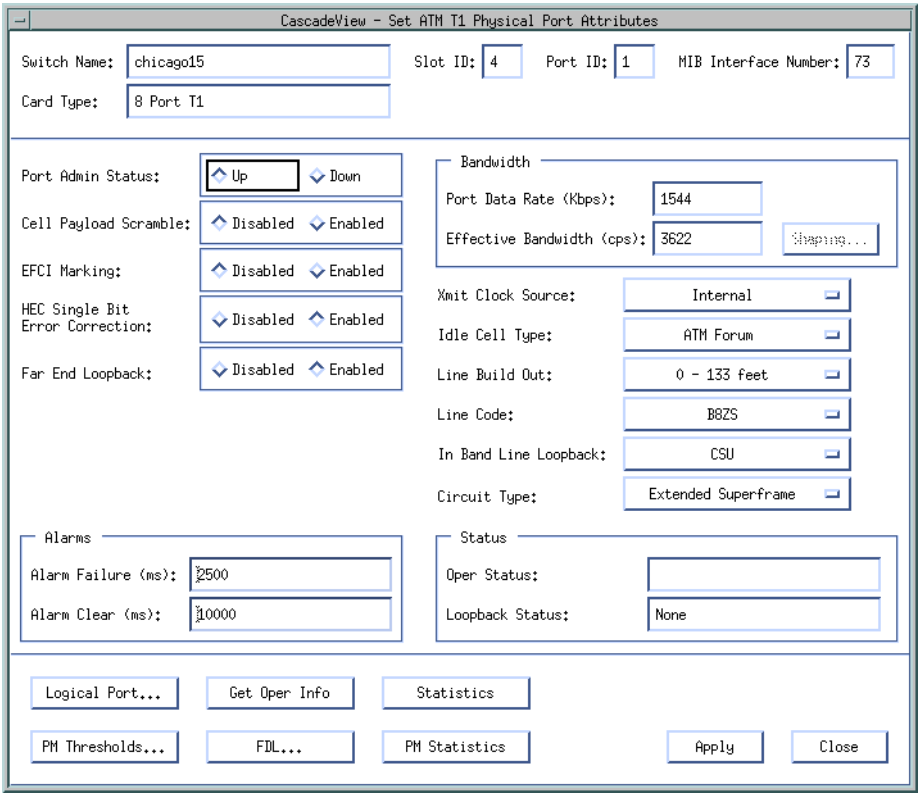


Figure 6-12. Set ATM T1 [E1] Physical Port Attributes Dialog Box

Table 6-14 identifies the Oper Status messages for this physical port. Use the Get Oper Info command to update this field.

Table 6-14. T1/E1 Get Oper Info Messages

Message	Description
admin down	The port's admin status is set to down.
yellow alarm	Receive yellow alarm from far end equipment.
blue alarm	Receive blue alarm indication signal (AIS) from far end equipment.
red alarm	Loss of frame (LOF) detected on the receive signal.
loss-of-signal	Loss of signal (LOS) condition detected on the port.
looped-back	Physical port in loopback mode.
equipment mismatch	Detected physical interface daughter card type (IOA) does not match the configured IOM type. This message means all physical ports on this IOM are down.

2. Complete the dialog box fields as described in Table 6-15.

Table 6-15. Set ATM T1/E1 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	Set this option to Up (default) to enable immediate access to the port. Set the Admin Status to Down to save the configuration in the database without activating the port or to take the port off-line to run diagnostics. If you modify the Port Admin Status, choose Apply.
Cell Payload Scramble	Enable or disable the Cell Payload Scramble function. The Cell Payload Scramble function prevents user data from being misinterpreted (that is, it prevents ATM cell header alienation). For T1 modules, the default is disabled; for E1 modules, it is enabled.
EFCI Marking	The Explicit Forward Congestion Indicator (EFCI) determines if congestion (or impending congestion) exists in a node. This option is disabled by default. If enabled, 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. Disable this option if you do not want to use EFCI marking on this physical port.

Table 6-15. Set ATM T1/E1 Physical Port Attributes Fields (Continued)

Field	Action/Description
HEC Single Bit Error Correction	Enable (default) or disable the single bit header error correction (HEC) on a per-port basis. When the framer is operating in the default mode with single bit error correction enabled, the framer corrects the single bit errors but does not count them. Disable this function on the framer to determine how many errors are occurring on the physical port.
Far End Loopback	Enable (default) or disable the switch ability to respond to loopback commands from far end equipment. Select Enable to allow the switch to respond to loopback commands from far end equipment (loop up and loop down) that can put the port into remote loopback. The loopback signaling can be inband commands, or FDL loopback commands. Select Disable to ignore inband and FDL loop up and loop down commands.
Alarm Failure (ms)	Enter a value between 0 to 65535 ms to determine how long the switch waits before declaring a physical layer problem (i.e., loss of signal) a real failure. The default value of 2500 ms (2.5 seconds) means the switch “soaks” the physical layer alarm for 2.5 seconds before declaring the physical port down. A value of 0 ms means the physical port goes down immediately following any physical layer failure. If you set the value lower than the default of 2.5 seconds, the switch takes the physical port down due to any transient failure in the transmission path; for a port that provides trunk connectivity, this may cause unnecessary rerouting of circuits.

Table 6-15. Set ATM T1/E1 Physical Port Attributes Fields (Continued)

Field	Action/Description
Alarm Clear (ms)	Enter a value between 0 to 65535 ms to determine how long the switch waits once a failure is cleared before declaring a physical layer problem (i.e., loss of signal) resolved. The default value of 10000 ms (10 seconds) means the switch waits 10 seconds after the alarm clears before declaring the physical port up. A value of 0 ms means the physical port comes back up as soon physical layer failure alarm clears. If you set the value lower than the default of 10 seconds, the switch may declare the physical port up before the transmission path is stabilized.
Port Data Rate (Kbps)	Represents the raw physical data rate of the port. Due to the bandwidth lost as a result of the ATM layer to physical layer mapping, this number is always greater than the actual cell rate that can be transmitted out the port. The actual rate of cell transmission is dependent on the method of ATM layer mapping used. Refer to Table 7-2 on page 7-8 for additional information.
Effective Bandwidth (cps)	Represents the actual cell transmission rate the physical port uses. By default, the physical port transmits cell traffic at the maximum rate supported on the physical interface. However, you can use the Shaping command to select a transmission rate that is lower than the maximum rate.
Xmit Clock Source	Specify the transmit clock source. The default is Internal. *Loop-Timed* – The clock source is derived from the clock signal coming into this port. *Internal* – The IOM internal timing source provides the clock source to this port. The IOM Clock Source setting in the Set IOM Card Attributes dialog box (see page 6-5) determines the internal clock source.
Line Build Out (*T1 modules only*)	Select the measurement that represents the length of the cable that connects the physical port to other network equipment, such as a router. The default is 0-133 feet.

Table 6-15. Set ATM T1/E1 Physical Port Attributes Fields (Continued)

Field	Action/Description
Line Code	Indicates the encoding method used on the T1/E1 interface. Line Code specifies the format of the data signal encoding. The signal has three different levels - positive, negative, and ground, which must be referenced from a master clock. The default for T1 ports is B8ZS. ***Note:*** *Refer to your facility service provider for more information about which line code method to use.* *Bipolar with 8 zero substitution (B8ZS)* – (T1 only) This is the ATM Forum standard for ATM cell transmission over a T1 interface. Use this option for optimum performance; the "B8ZS" refers to the use of a specified pattern of normal bits and bipolar violation that is used to replace a sequence of eight zero bits. With B8ZS, a special code is placed in and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment. *HDB3* – (E1 only) This is the ATM Forum standard for ATM cell transmission over an E1 interface. Use this option for optimum performance. *AMI No Bit Stuff* – The AMI No Bit Stuff option allows for ATM cell transmission over AMI interfaces. This mode of operation is not supported by the ATM Forum or ITU and is only provided for users that have transmission equipment that does not support B8ZS operation. *Alternate Mark Inversion (AMI)* – The AMI option (also known as Jammed Bit) is used only for troubleshooting of physical layer interfaces. This mode does not support ATM cell transmission.

Table 6-15. Set ATM T1/E1 Physical Port Attributes Fields (Continued)

Field	Action/Description
Idle Cell Type	Allows you to specify the type of cell that is used to fill the gaps between user data cells that are transmitted out of the physical port. The physical port receive function is not affected by this option (both ITU and ATMF are recognized and processed by the physical port receiver). Select one of the following options. *ATM Forum* (default) – The fill cell will have a header of 00 00 00 00 55 and a payload of 6A (for all 48 bytes). *ITU* – The fill cell will have a header of 00 00 00 01 55 and a payload of 6A (for all 48 bytes).
Circuit Type (*T1 only*)	Configures the T1 interface for a particular framing specification. Framing provides a method of distinguishing between the individual channels. It is accomplished by adding one additional bit to each frame. The default is Extended Superframe. Selections include: *Superframe* – A frame format that consists of twelve frames (also referred to as "*D4 framing"*). It provides end-to-end synchronization and signaling associated with a particular channel. *Extended Superframe* – A framing format that extends the D4 framing format from 12 frames to 24 frames and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of this format over "superframe" is that it enables the Cascade equipment to monitor and respond to network maintenance messages. ***Note:*** *Make sure you configure the customer premise equipment (CPE) to use the same framing specification as the Cascade physical port.* *If you select extended superframe, you can specify the facility data link information (FDL). Refer to* "Defining Facility Data Link (FDL) Parameters" *page 6-50* *for more information.*

Table 6-15. Set ATM T1/E1 Physical Port Attributes Fields (Continued)

Field	Action/Description
In Band Line Loopback	Designates the in-band line loopback code format that is transmitted to the far end to perform far-end inband loopback testing. Also designates the loopback code format the switch will recognize if far-end equipment sets this port into loopback. Selections are CSU or NI (also referred to as smart jack) loopbacks. The default is CSU.
Oper Status	Indicates the operational status of the physical port (Up or Down). If this field is blank, it means the IOM did not respond to a status request.
Loopback Status	Displays the port loopback status, if you enable diagnostic loopback tests. The default is None. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for more information.

3. To modify the default physical port performance thresholds for this physical port, continue with "Defining T1/E1 Performance Thresholds" on page 6-52.

4. To exit, choose Apply and then OK to save the physical port attributes and send an SNMP SET command to the switch. Choose Cancel to exit the dialog box.

Defining Facility Data Link (FDL) Parameters

For T1 modules, if you select Extended Superframe as the Circuit Type (refer to page 6-48), you can specify the facility data line (FDL) control parameters.

To define FDL parameters:

1. From the Set ATM T1 Physical Port Attributes dialog box (Figure 6-12 on page 6-42), choose FDL.

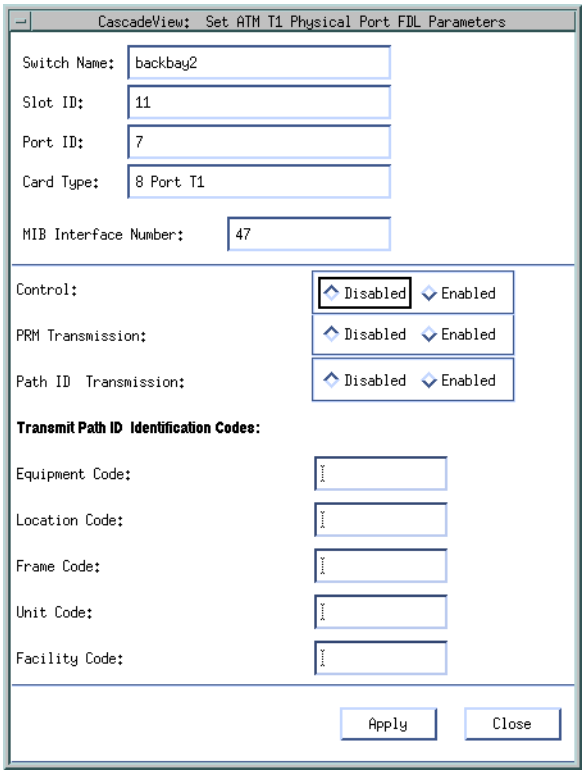


Figure 6-13. Set ATM Physical Port FDL Parameters Dialog Box

2. Complete the dialog box fields as described in Table 6-16.

Table 6-16. Set ATM Physical Port FDL Parameters Fields

Field	Description
Control	Select Enabled to use the FDL control parameters; select Disabled (the default) if the carrier does not use them.
PRM Transmission	The T1 module processes incoming performance report messages (PRM) that provide error count information for far-end equipment. Select Enabled to transmit a similar PRM signal from this port. Select Disabled (the default) if the equipment connected to this port does not process PRM signals.
Path ID Transmission	The T1 module processes the path identification messages it receives from far-end equipment. Select Enabled to transmit a similar Path ID signal from this port. Select Disabled (the default) if the equipment connected to this port does not process path ID information. ***Note:*** *You can disable PRM Transmission and Path ID Transmission signals to save overhead.*
Equipment Code	Enter up to 10 characters to describe this piece of Cascade hardware.
Location Code	Enter up to 11 characters to describe the location of this Cascade hardware.
Frame Code	Enter up to 10 characters to describe the location (within a building) of this Cascade hardware.
Unit Code	Enter up to 6 characters to identify the hardware location (within a bay).
Facility Code	Enter up to 38 characters to identify the specific DS1 path that this physical port uses.

3. Choose Apply and then OK to save your changes. Choose Close to return to the Set Physical Port Attributes screen (Figure 6-12 on page 6-42).

4. Choose Apply and then OK to save the physical port attributes and create an SNMP SET command to send to the switch. Choose Cancel to exit the dialog box.

Defining T1/E1 Performance Thresholds

The NMS allows you to set performance parameter thresholds for the 15-minute and one-day accumulation periods for each physical port. If you enable threshold crossing, the port will generate traps if these thresholds are exceeded.

To configure performance thresholds:

1. From the Set ATM T1 Physical Port Attributes dialog box (Figure 6-12 on page 6-42), choose PM Thresholds. The following dialog box appears.

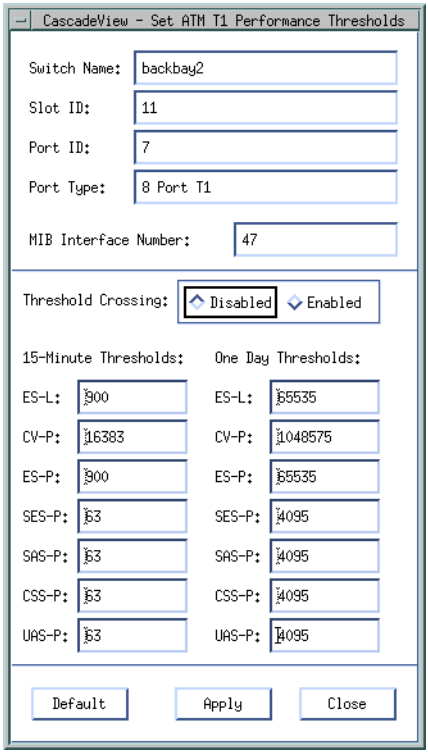


Figure 6-14. Set Performance Thresholds Dialog Box (T1/E1 Ports)

2. Threshold Crossing is disabled by default. Enable it if you want to generate traps for threshold crossing.

3. Use Table 6-17 to set the 15-minute and one-day threshold values. Use the Default command button to return these values to the default settings.

Table 6-17. T1/E1 Performance Monitoring Thresholds

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
ES-L (Line Errored Seconds)	A count of 1-second intervals with one or more BPVs or EXZs.	1 - 900	900	1 - 65535	65535
CV-P (Path Code Violations)	A count of frame synchronization bit errors; i.e., the count of CRC-6 errors in ESF format.	1 - 16383	16383	1 - 1048575	1048575
ES-P (Path Errored Seconds)	A count of 1-second intervals with one or more CRC-6 errors or one or more CS events.	1 - 900	900	1 - 65535	65535
SES-P (Path Severely Errored Seconds)	A count of 1-second intervals with 320 or more CRC-6 errors, or one or more SEF or AIS defects.	1 - 63	63	1 - 4095	4095
SAS-P	A count of 1-second intervals with one AIS defect.	1 - 63	63	1 - 4095	4095

Table 6-17. T1/E1 Performance Monitoring Thresholds (Continued)

Field	Description	15 Min. Range	15 Min. Default	One Day Range	One Day Default
CSS-P	A count of 1-second intervals with one or more controlled slip events.	1 - 63	63	1 - 4095	4095
UAS-P (Path Unavailable Seconds)	A count of 1-second intervals for which the DS1 path is unavailable. The path is unavailable upon detection of 10 contiguous seconds with no SESs.	1 - 63	63	1 - 4095	4095

4. When you finish, choose Apply to save your changes and Close to return to the Set Physical Port Attributes dialog box (Figure 6-12 on page 6-42).

5. Choose Apply and then OK to save the physical port attributes and send an SNMP SET command to the switch. Choose Cancel to exit.

Redefining an IOM

Before you redefine an IOM (e.g., replace a DS3 with an OC3 in the same slot), use the following procedure to redefine an IOM:

1. From the Administer menu, select Cascade Parameters ⇒ Set Parameters to access the Switch Back Panel dialog box (shown on page 5-10).

2. Verify that the IOM is not out-of-sync. The IOM should display in green on the Set Switch Back Panel dialog box.

3. Select the IOM and choose Set Attributes. The Set Card Attributes dialog box appears (Figure 6-2 on page 6-4).

4. In the Card Type field, select Empty, and choose OK.

5. The following warning message appears. Choose OK to acknowledge this message.

   If the IOM is present at the switch, the IOM must not be "out of sync" prior to changing it to Empty.

6. You can now use the Set Card Attributes dialog box to define a new card type.

If the IOM Is Out-of-Synch

If you attempt to redefine IOMs that are installed in the switch, but are "*out of sync*", an SNMP error message appears, prompting you to "abort" or "ignore" the operation. *Cascade strongly recommends* that you do the following:

1. Choose Abort to halt the undefine IOM procedure.

2. PRAM synch the IOM (refer to "Using the Synchronize PRAM Command" on page 12-18).

3. Repeat Step 1 through Step 4 on page 6-55 to redefine the IOM.

If you choose to ignore the SNMP error message, the SP is flagged as "out of sync". When this happens, *Cascade strongly recommends* that you complete the following steps to avoid future logical port and IOM configuration rejections at the switch:

1. PRAM synch the SP (refer to page 12-18).

2. Reboot the "Undefined" card (in its original slot at the switch).

3. After the reboot completes, either latch down the IOM and remove it from the switch, or define a new card in its place.

After you define a new IOM, the Switch Back Panel dialog box should display the new IOM slot in yellow to indicate it is out-of-synch. PRAM Synch the IOM (page 12-18). Note that if you install the card in a slot that already contained PRAM, the new card may not display yellow. However, you still need to PRAM Synch the card.

7

Configuring ATM Logical Ports

This chapter describes how to configure the different types of ATM logical ports on a CBX 500 switch.

About ATM Logical Port Types

This section describes the following types of ATM logical ports.

- UNI DCE and DTE
- NNI
- Direct Trunk
- OPTimum Cell Trunk

ATM UNI DCE and DTE

You use the ATM UNI DCE logical port type to communicate with most ATM customer premise equipment (CPE). An ATM UNI DCE logical port represents the “network side” equipment. This logical port supports all types of PVCs as well as SVCs. You can also use the ATM UNI DCE to connect to other ATM switches on a PVC-only basis, as well as a PVC and IISP basis. For SVC applications, the ATM UNI DCE logical port assumes the role of the network side of the UNI signaling interface.

You can also use the ATM UNI DCE as a feeder port for Cascade OPTimum trunks. When used as a feeder port, you can still use the ATM UNI DCE logical port for PVC and SVC applications.

The ATM UNI DTE logical port type has the identical functionality of the ATM UNI DCE logical port with one exception. For SVC applications, the ATM UNI DTE assumes the role of the “user side” of the UNI signaling interface.

Virtual UNI

Virtual UNIs form an extension of the standard “direct” UNI DCE and DTE logical port types. In an ATM network you can use virtual UNI logical ports to enable VP tunneling or to connect to a VP multiplexer. VP tunneling allows you to connect two switches using UNI signaling via a virtual path through the ATM network. VP multiplexing enables you to connect the CBX 500 switch to a VP multiplexer using a direct UNI logical port on which you have configured several “virtual” UNI ports. The VPI address range you define for each virtual UNI port corresponds to a port on the VP multiplexer.

ATM NNI

The ATM Network-to-Network Interface (NNI) logical port type enables you to connect ATM-based public networks belonging to two different carriers. This logical port type implements the BISDN-Inter-Carrier Interface (B-ICI) protocol, which facilitates the multiplexing of services for inter-carrier (RBOC and IXC) delivery. This initial release only supports PVC connections.

You can also use an ATM NNI logical port as a feeder port for Cascade OPTimum trunks.

ATM Direct Trunk

The ATM Direct Trunk is used to provide trunk connectivity between two directly connected Cascade switches. These switches include the CBX 500 and the B-STDX. The ATM Direct Trunk carries all types of PVC, SVC, and management data.

If the CBX 500 is running release 1.3 (or later) of switch software, and a B-STDX is running release 4.2 (or later) of switch software, you can establish a direct trunk connection between a CBX 500 and a B-STDX switch. If a switch is running an earlier release of switch software, you can only establish a direct trunk connection between switches of the same type.

ATM OPTimum Cell Trunk

You use an ATM OPTimum Trunk logical port type to provide trunk connectivity between two Cascade switches (CBX 500 or B-STDX) that are not directly connected. In this application, some other network elements are separating the two Cascade switches. These network elements usually consist of ATM switches in another network. The network provider operating the other ATM switches provisions a virtual path connection (VPC) to carry the Cascade trunk traffic. This VPC supports the trunk and carries all the associated trunk protocol, management data, PVCs, and SVCs between the two Cascade switches.

Because the ATM OPTimum trunk traverses a VPC through the other ATM network, VPCs from the Cascade switches cannot traverse the OPTimum trunk. OSPF prevents the routing of VPCs over OPTimum trunks.

If the CBX 500 is running release 1.3 (or later) of switch software, and a B-STDX is running release 4.2 (or later) of switch software, you can establish an OPTimum trunk connection between a CBX 500 and a B-STDX switch. If a switch is running an earlier release of switch software, you can only establish an OPTimum trunk connection between switches of the same type.

Virtual Paths and Virtual Channels

To establish connections, ATM uses *virtual channels (VCs)* and *virtual paths (VPs)*. A virtual channel is a connection between two communicating ATM entities. It may consist of a group of several ATM links, CPE to central office switch, and switch-to-switch, or switch-to-user equipment. All communications proceed along this same VC, which preserves call sequence and provides a certain quality of service.

A virtual path is a group of VCs carried between two points. VPs provide a way to bundle traffic headed in the same direction.

Virtual path identifiers (VPIs) and *virtual channel identifiers (VCIs)* are addressing identifiers (similar to Frame Relay's DLCI) that route cell traffic. The ATM cell header contains both a VCI and a VPI, which gives an ATM cell a unique VCI and associates it with a particular virtual path. Every ATM cell uses these VPI/VCI identifiers.

Switching equipment checks the VPI portion of the header to route traffic over certain trunks. It uses the VCI portion of the address to deliver the cell to an individual user within that destination.

The VPI and VCI are used only for establishing connections between two ATM entities, not the end-to-end connection.

Setting the Number of Valid Bits in the VPI/VCI

The Number of Valid Bits setting applies to the VPI and VCI range that you can use for VCCs (both PVCs and SVCs). The default values of VPI = 4 and VCI = 10 mean that you can use VCCs over the range of VPI = 0 – 15 (4 bits of VPI) and a VCI range of VCI = 32 – 1023 (10 bits of VCI). The values have no effect on VPCs, which you can provision anywhere over the VPI = 0 – 255 range; you can provision VPCs over the VPI = 0 – 4095 range if you use the NNI cell header format.

The valid range for the VPI field is 0-8; the valid range for the VCI field is 5-14. You may have to adjust these values in the following situations:

- In cases where the required VPI/VCI(s) of the attached devices are outside the range that the default values provide (VPI = 0 – 15 and VCI 32 – 1023).
- If you will use this logical port as a feeder for OPTimum trunks or virtual UNIs, the VPI value limits the number of OPTimum trunks you can create on this physical port. The VCI value limits the number of circuits you can route over each OPTimum trunk.

  This OPTimum trunk/circuit trade-off is shown by the following formulas, where *P* represents the value in the Valid Bits in VPI field, and *C* represents the value in the Valid Bits in VCI field:

  Maximum virtual paths = $2^P - 1$
  Maximum virtual channels = $2^C - 32$
  $P+C \leq 14$

  For example, if you set the VPI value to 3 and the VCI value to 11, you can have up to 7 virtual paths on the port, and up to 2,016 virtual channels on each path.

Use Table 7-1 as a guide to set these values.

When you configure an OPTimum trunk or virtual UNI between two endpoints, the logical ports must match the VPI of the VPC that provides the connectivity between the two switches. The VPI range for the VPI/VCI valid bits setting for each endpoint must accommodate this VPI.

Table 7-1. Number of Valid Bits in VPI/VCI

[1] If Number of Valid VPI Bits =	Valid VPI Range Is	If Number of Valid VCI Bits =	[2] Valid VCI Range Is
0	0	0	Not Valid
1	0 - 1	1	Not Valid
2	0 - 3	2	Not Valid
3	0 - 7	3	Not Valid
4	0 - 15	4	Not Valid
5	0 - 31	5	Not Valid
6	0 - 63	6	32 - 63
7	0 - 127	7	32 - 127
8	0 - 255	8	32 - 255
Not Valid	–	9	32 - 511
Not Valid	–	10	32 - 1023
Not Valid	–	11	32 - 2047
Not Valid	–	12	32 - 4095
Not Valid	–	13	32 - 8191
Not Valid	–	14	32 - 16383

[1] Only 8 bits of the VPI are available on UNI type interfaces per ATM Forum standards.
[2] VCI 0 - 31 are reserved and cannot be used per ATM Forum standards.

About VCC VPI Start and Stop

The range you define with the VCC VPI start and stop values for a direct UNI must provide enough range for you to define the virtual UNI logical ports you need; the range of VPI start and stop values you define for the first virtual UNI cannot overlap with the range you define for subsequent virtual UNI ports.

For example:

Logical Port	VPI Start	VPI Stop
Direct UNI	0	15
First Virtual UNI	2	5
Second Virtual UNI	6	10

About Logical Port Bandwidth

The maximum amount of logical port bandwidth does not equal the physical port bandwidth due to the overhead associated with packaging ATM cells into the physical layer frames. This overhead is different for each physical media type as well as the different packaging methods. Table 7-2 on page 7-8 provides a guide to map and convert physical layer bandwidth to logical port bandwidth.

Table 7-2. Physical and Logical Port Bandwidth Conversions

Physical Port Media Type	Physical Port Bandwidth (kbs)	Exact Logical Port Bandwidth (kbs)	Exact Logical Port Bandwidth (cps)	NMS Rounded Maximum Logical Port Bandwidth (kbs)	NMS Rounded Maximum Logical Port Bandwidth (cps)
OC-12/STM-4	622080	599040	1412830	599040	1412830
OC-3/STM-1	155520	149760	353207	149760	353207
DS3 (with PLCP)	44736	40704	96000	40704	96000
DS3 (with HCS direct mapping)	44736	44209.694	104268.15	44209	104266
E3 (with HCS direct mapping)	34368	33920	80000	33920	80000
E3 (with G.751 PLCP)	34368	30528	72000	30528	72000
T1	1544	1536	3622.64	1536	3622
E1	2048	1920	4528.3	1920	4528

In some cases, due to the way the switch stores logical port bandwidth, the NMS may have to round down non-integer values of maximum logical port bandwidth values to the nearest kbs value. For most applications, this does not cause any problems. However, if you need to run 100% line rate traffic through a policed PVC where you have rounded values, policing may cause minor cell loss.

Example

If you send 100% line rate traffic over a DS3 interface that uses HCS direct mapping, the cells arrive at a rate equal to 44209.694 kbs or 104268.15 cps. Because of NMS rounding, the maximum PCR you can provision for this PVC is 104266. If you enable UPC on this PVC, approximately two cells every second are lost. For these cases, you may want to either adjust the traffic rate or disable UPC for this circuit.

Allocating Logical Port Bandwidth When Sharing SP Threads

Chassis slots 3-4, 5-6, 7-8, 9-1, 10-2, 11-12, 13-14, and 15-16 are associated with the SP threads. This means that if you have an IOM installed in slots 3 and 4, you are "sharing" an SP thread. If you have an IOM in slot 9 or 10, you are sharing a thread with the SP itself. In this case, there are no thread limitations; the IOM has the full 599.040 Mbps of bandwidth available.

If two IOMs share the same SP thread, the maximum user cell bandwidth available to the two IOMs is 599.040 Mbps (599040 kbs. or 1412830 cps.). The NMS now enforces this limit such that the combined sum of all logical port bandwidths on the two IOMs cannot exceed 599.040 Mbps These bandwidth limitations ensure the QoS guarantees even when you install two IOMs on the same SP fabric thread. Even with this thread bandwidth enforcement, you may still oversubscribe the VBR and UBR service classes on some or all of the IOM ports to utilize the statistical multiplexing gains that are an inherent part of running with two IOMs on one SP thread. However, you should carefully plan such oversubscription according to the intended service offerings and network engineering considerations of the different logical ports that share the thread.

The 599.040 Mbps number is derived from the maximum user cell bandwidth the OC12/STM-4 interface supports. (OC12/STM-4 physical layer bandwidth is 622.080 Mbps, but the maximum user traffic that any OC12/STM-4 port can support is 599.040 Mbps) This 599.040 thread limitation is also derived from the maximum user cell bandwidth the four OC3/STM-1 interfaces support. (OC3/STM-1 physical layer bandwidth is 155.020 Mbps, but the maximum user traffic that any OC3/STM-1 port can support is 149.76 Mbps) Refer to "About Logical Port Bandwidth" on page 7-7, for a detailed description of mapping physical port bandwidth to logical port bandwidth.

The 599.040 Mbps bandwidth value is available exclusively for user cell traffic. Management and internal switch control traffic have the potential for using a maximum of 11 Mbps of thread bandwidth, but this value is already factored into the total available thread bandwidth. The total available thread bandwidth starts at 611 Mbps, and once the NMS reserves 11 Mbps for management and control traffic, 599.040 Mbps remains exclusively for user cell traffic. At no time does management or internal control traffic conflict with the 599.040 Mbps of user cell traffic. If the user cell traffic exceeds 599.040 Mbps, then depending on the QoS class of the user cell traffic, user traffic may be lost if:

- It is a lesser priority than the management and internal control traffic
- It exceeds the overall 611 Mbps thread capacity

This NMS enforcement of SP thread bandwidth only applies when the switch has two IOMs installed on the same SP thread. If the switch only has one IOM on a thread, the maximum possible logical port bandwidth for all ports on the IOM is supported by the 599.040 Mbps limit.

Example

When a switch has two IOMs installed on a SP thread, you will notice the NMS enforcement of the SP thread bandwidth whenever you attempt to provision two OC3 cards on the same SP fabric thread. As you provision logical ports, the NMS subtracts the assigned bandwidth from the 599.040 Mbps total. After you provision four OC3 logical ports on the first OC3 card using the maximum 149.76 Mbps of bandwidth, there will not be any bandwidth left for the other OC3 card and its logical ports.

Consequently, when you have two cards installed on the same fabric thread, Cascade recommends that you allocate the bandwidth accordingly, across all of the IOM ports. In this example, you would allocate approximately 75 Mbps to each of the eight logical ports. This enables each logical port to support 75 Mbps of CBR traffic, and consequently, allows the full utilization of the thread bandwidth.

Even when you use 75 Mbps per logical port, you can still oversubscribe the logical port to overbook the VBR and UBR service classes on the port. For example, by reserving 10% of each logical port's bandwidth (i.e., 75 Mbps) for UBR traffic, and overbooking the UBR bandwidth, hundreds of UBR circuits can be set up. Since UBR circuits are not policed, these best-effort UBR circuits can potentially utilize the full port bandwidth of each logical port, and consequently the full thread bandwidth. However, at periods when the combined UBR traffic exceeds thread bandwidth, the excess UBR traffic is dropped. Refer to the next section for more information.

Modifying Logical Port Bandwidth

You can modify logical port bandwidth on UNI and NNI logical ports even after you configure PVCs on this port. However, if you reduce the logical port bandwidth such that the new value is not sufficient to support all of the PVCs traversing the port, the available bandwidth enters a negative state. The PVC remains active until it has to be reestablished (i.e., trunk reroute, IOM reboot). If at this time the logical port does not have enough bandwidth to support the PVC, the PVC remains inactive due to insufficient bandwidth.

About the Oversubscription Factor

The Oversubscription Factor percentage enables you to optimize the number of permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) you can configure on the network by allowing you to oversubscribe the logical ports. If you configure oversubscription for the VBR classes of service, QoS is no longer guaranteed.

To ensure quality of service, monitor the network closely before you modify oversubscription values to exceed the minimum value of 100%. If you adjust the oversubscription percentage, monitor the cell-loss ratio to be sure the new setting does not impact quality of service.

The port bandwidth is reserved at runtime based on the sum of the effective bandwidth of each VC that uses the port. The CAC (Connection Admission Control) algorithm determines effective bandwidth of a virtual circuit (PVC and SVC). For a VBR circuit, the CAC uses the circuit's PCR, SCR, and MBS values. For CBR circuits, the CAC uses the PCR of the circuit. UBR circuits are assigned zero bandwidth, since it is a "Best Effort" service.

Appendix A describes how to tune the CAC to optimize your network. If you tune the CAC properly, you can optimize network resources without adversely affecting quality of service.

Either an OSPF algorithm or the network administrator (if you manually define the circuit path) determines PVC routing. Each time a PVC attempts to come up after configuration, OSPF reserves the required bandwidth on the port. OSPF deducts the amount of reserved bandwidth from the available virtual bandwidth pool for the applicable class of service.

The available virtual bandwidth can become negative in extreme situations. For the VBR-NRT queue, if a number of trunks fail, PVC rerouting may cause the available virtual bandwidth value to become negative. Existing PVCs can be rerouted over a negative virtual bandwidth trunk. However, *new* PVCs cannot traverse trunks that have a negative virtual bandwidth. Any PVC that fails during the time of the reroute is considered to be a new PVC when it attempts to come up after the trunk is rerouted.

Since inter-LAN traffic is bursty in nature, not all network traffic uses the network resources at precisely the same time. Basically, the higher you set the oversubscription factor, the less guarantee there is that user data will get through on the port; the trade-off is that you can provision more circuits on that port. If, however, 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 even dropped.

If you leave the Oversubscription factor set for the minimum value of 100%, the port delivers all user data for that service class without unanticipated delays or excessive cell loss. A value of 200% effectively doubles the virtual bandwidth available for that service class. (Cascade reserves a certain percentage of bandwidth for network management, routing updates, and other management traffic.)

Version 2.4 of CascadeView/UX and version 2.0 of CBX 500 switch software enable you to provide greater granularity when configuring the oversubscription factor. Using these versions, you can set the oversubscription factor over a range of values from 100% to 1000%, using 1% increments.

Before You Begin

Before you configure a logical port, verify that the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Add the switch object to the map (page 4-14)
- ☑ Specify the switch attributes (page 5-9)
- ☑ Configure the IP address of each NMS workstation for access to the switch (page 5-20)
- ☑ Configure the IOM (page 6-2) and its physical ports (page 6-11) on which the logical port(s) will reside

Accessing ATM Logical Port Functions

To access the Logical Port functions in CascadeView/UX:

1. Select the switch to which you want to add a logical port.
1. Log in to CascadeView/UX using either a provisioning or operator password.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the physical port you want to configure. The Set Physical Port Attributes dialog box appears.

Choose the Logical Port command. The Set All Logical Ports in PPort dialog box appears as shown in Figure 7-1.

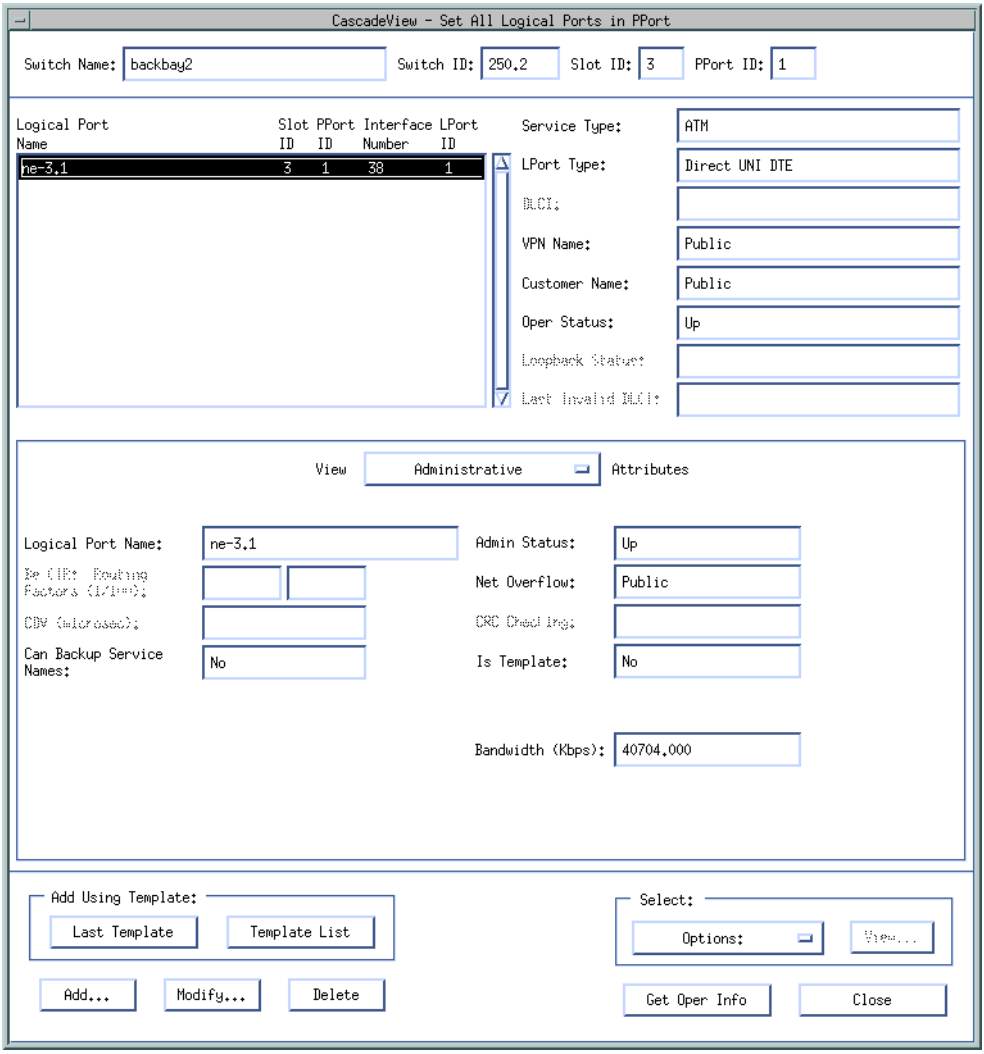


Figure 7-1. Set All Logical Ports in PPort Dialog Box

About the Set All Logical Ports Dialog Box

The Set All Logical Ports In PPort dialog box displays information about an existing logical port or enables you to add a new logical port. It also provides several command buttons that you can use to access additional logical port functions, such as add, modify, and delete logical ports. Table 7-3 describes the dialog box status fields and commands.

Table 7-3. Set All Logical Ports in PPort Dialog Box Status Fields and Commands

Field/Command	Action/Description
Service Type	Displays ATM.
LPort Type	Displays the logical port type: either UNI DCE, UNI DTE, Direct Trunk, or OPTimum Cell Trunk.
VPI/VCI (*OPTimum trunk only*)	Displays the configured VPI/VCI value.
VPN Name	Displays the VPN name to which this logical port belongs.
Customer Name	Displays the name of the customer to which this logical port is dedicated.
Oper Status	Indicates whether this port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.
Loopback Status	Indicates whether loopback testing is enabled on this logical port. The default is None (no testing).
View Attributes (option menu)	Displays the appropriate attributes configured for the selected port. • For ATM UNI logical port types, refer to page 7-26. • For ATM NNI logical port types, refer to page 7-46. • For ATM Direct or OPTimum trunk logical ports, refer to page 7-56.

Table 7-3. Set All Logical Ports in PPort Dialog Box Status Fields and Commands (Continued)

Field/Command	Action/Description
Add	Adds a new logical port.
Modify	Modifies the selected logical port. The Modify command displays dialog boxes which are similar to those displayed when you Add a logical port; however, you cannot modify the logical port name and the logical port type.
Delete	Deletes the selected logical port. For more information about deleting logical ports, refer to page 7-69.
Get Oper Info	Displays a brief status message of the logical port state.
Add Using Template	If you have already defined a logical port configuration and saved it as a template, use this option to define a new logical port using similar parameters. • Choose Last Template to use the last template you defined for this switch. • Choose Template List to display a list of templates previously defined for this map.
Use the Select: Options button to select the following logical port options. Once you select an option from this list, choose View to access the information. 	
Statistics	Displays the summary statistics for the selected logical port. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500.*
Diagnostics	Accesses diagnostic tests for the selected logical port. For more information about diagnostics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.

Table 7-3. Set All Logical Ports in PPort Dialog Box Status Fields and Commands (Continued)

Field/Command	Action/Description
VPN/Customer Info	Assigns a VPN and customer name to the selected logical port.
QoS Parameters	Displays the quality of service parameters (including bandwidth and routing metrics) for the selected logical port. Refer to page 7-59 for more information.
NTM Parameters	Displays the configured network traffic management (NTM) parameters for the selected logical port. For more information about these parameters, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
NTM Statistics	Displays the NTM statistics for the selected logical port. For more information about NTM statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
NDC Statistics	Displays the NDC statistics for the selected logical port. For more information about NDC statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500.*
ATM Accounting	Accesses the ATM accounting functions for a logical port. For more information, refer to the *Accounting System Administrator's Guide.*
Screen Assignments	Displays the port security screen assignments for the selected logical port. Refer to "Viewing Screen Assignments" on page 14-17 for more information.

Defining ATM UNI Logical Ports

This section describes some of the concepts you need to know when defining ATM UNI DCE and ATM UNI DTE logical ports. You can configure a single ATM UNI logical port on a physical port to support standard ATM UNI 3.0 and 3.1 functions. This release of CascadeView/UX also supports ATM Virtual UNI logical ports. Refer to “Defining Virtual ATM UNI Logical Ports” on page 7-45.

Using Fault Tolerant PVCs

You can configure UNI DCE and UNI DTE logical port types to provide backup service if you implement a fault tolerant PVC configuration. A fault tolerant PVC configuration enables a logical port to serve as a backup for any number of active UNI ports. If the primary port fails, you can activate the backup port using CascadeView/UX. Refer to “Configuring Fault Tolerant PVCs” on page 7-62 for more information.

Using Virtual Private Networks for SVC Traffic

Virtual Private Networks (VPNs) enable network providers to have dedicated network resources for those customers who require guaranteed performance, reliability, and privacy. For SVC traffic, you dedicate logical port endpoints to a specific VPN and customer. You specify the net overflow parameters that determine whether SVCs originating from this port are restricted to trunks of their own VPN or use public (shared) trunks during overflow or failure conditions.

Using Interim Local Management Interface (ILMI)

ILMI is a management information base (MIB) that provides status and communication information to ATM UNI devices. ILMI provides status information and statistics about virtual paths, connections, and address registration. It also determines the operational status of the logical port.

If you want to use ILMI, make sure both endpoints of the UNI connection support this MIB. When you enable ILMI on a CBX 500 logical port, the switch polls the attached device every five seconds. Five seconds is the *polling period*. If no response is received after four consecutive polls (*loss threshold)*, the switch considers the ILMI state to be down.

If you enable ILMI, 1% of the available logical port bandwidth is reserved for this purpose. Cascade recommends that you enable ILMI support before you provision circuits. Under certain conditions, enabling ILMI after you provision circuits on a logical port may cause negative bandwidth with the associated QoS classes (including CBR). Note that if you enable ILMI on a logical port, and for some reason the ILMI state is down, the logical port does not go down.

Table 7-4 describes the differences between UNI DCE and DTE logical ports with ILMI enabled and disabled.

Table 7-4. Logical Ports and ILMI Settings

Port Type	Effect On	With ILMI Enabled	With ILMI Disabled
UNI DCE	Logical Port State Determination	Polling – looks for responses; if no responses are received within a given time period, the ILMI state is declared down (time period is based on the polling period x loss threshold).	Based on the physical port state
	Address Registration	• Send node prefixes • Send port prefixes • Accept addresses (qualified against configured prefixes)	None
	Remainder of ILMI MIB	Switch responds to get next commands sent by attached devices.	None
UNI DTE	Logical Port State Determination	Polling – listens for requests; if no requests are received within a given time period, the link is declared down (time period is based on the polling period x loss threshold).	Based on the physical port state
	Address Registration	Accept prefixes (and optionally qualify addresses against configured prefixes).	None
	Remainder of ILMI MIB	Switch responds to get next commands sent by attached devices.	None

Using Logical Port Signaling

This section describes the default signaling tuning parameters for an ATM UNI logical port. In an ATM network, signaling is responsible for establishing and releasing SVCs. Signaling is used only on ingress and egress ports, including user-to-network, network-to-user, and network-to-network ports. If you enable signaling for the logical port, 2% of the available bandwidth is reserved for this purpose.

On ATM UNI DTE or ATM UNI DCE logical ports, if you change the default values and later change the UNI version for the port, the NMS prompts you to overwrite current settings with the default tuning parameters for the new UNI version. Cascade recommends that you set the logical port signaling options before you provision circuits. Under certain conditions, enabling signaling after you provision circuits on a logical port may cause negative bandwidth with the associated QoS classes (including CBR).

ILMI and Signaling Example

To accommodate ILMI and UNI signaling, the CBX 500 implements a bandwidth reservation process for logical ports. If the available logical port bandwidth is 40704 kbps and you enable both ILMI and signaling on the logical port, you have a maximum of 39483 kbps or 93120 cells (97% of 96000 cps) per second available for circuit provisioning.

Under certain conditions, enabling ILMI and/or signaling after you provision circuits on a logical port may cause negative bandwidth for the associated QoS classes. For example, you create a DS3 logical port with both ILMI and signaling disabled. You then create a full bandwidth CBR circuit (PCR=96000 cps) on this logical port. If you later enable ILMI and/or signaling on the logical port, the bandwidth now appears to be negative. If you need to modify the logical port admin status or if you modify the circuit, the circuit will no longer come back up due to insufficient bandwidth.

The Set Attributes Menu

When you configure ATM UNI DCE and DTE logical ports, the Add Logical Port dialog box (Figure 7-3 on page 7-25) contains several parameters, such as bandwidth, which you must set for this logical port type. During this procedure, use the Set Attributes menu on the Add Logical Port dialog box to configure the following:

Administrative — Administrative options, including logical port name, admin status, and bandwidth.

ATM — ATM-specific options, including the number of valid bits in the VCI and VPI and ATM protocol. You can also enable or disable the Call Admission Control (CAC) or Usage Parameter Control (UPC) functions from this display.

ILMI/Signaling/OAM — These selections display options that enable you to fine-tune your ATM service.

ILMI – A management information base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep-alive protocol.

Signaling – A signaling protocol that supports the dynamic creation of ATM virtual circuits. To configure Signaling, you access the Set Logical Port Signaling Tuning Parameters dialog box.

OAM – A parameter that enables this logical port to generate operations, administration, and maintenance (OAM) alarms.

ATM FCP — This selection displays options that enable you to configure logical ports for the ATM flow control processor. For more information, refer to the *ATM Flow Control Processor User's Guide*.

SVC VPI/VCI Range — This selection enables you to configure a separate SVC VPI/VCI address range contained within the PVC VPI/VCI address range. By creating two separate address ranges, you can use one VPI/VCI range for PVCs on a logical port and a different (smaller) VPI/VCI range for SVCs on a logical port. This enables a CBX 500 to interoperate with an SVC-capable CPE that only supports VPI 0 for SVCs. You can set the VPI/VCI range to limit SVCs to VPI 0, while allowing PVCs to utilize the full VPI range.

Adding a Direct ATM UNI Logical Port Type

To add an ATM UNI logical port:

1. Complete the steps in “Accessing ATM Logical Port Functions” on page 7-14.
2. Choose Add to define a new logical port. The following dialog box appears.

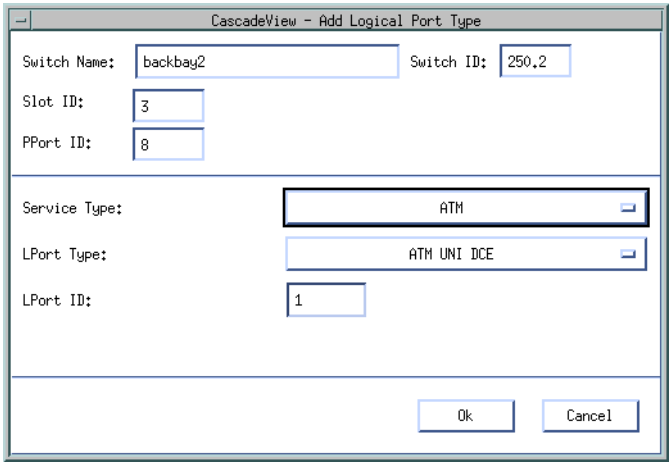


Figure 7-2. Add Logical Port Dialog Box

3. Select the LPort Type, either ATM UNI DTE (user side) or ATM UNI DCE (network side).
4. Choose OK. The Add Logical Port dialog box reappears. The sample dialog box in Figure 7-3 on page 7-25 shows an ATM UNI DCE logical port.

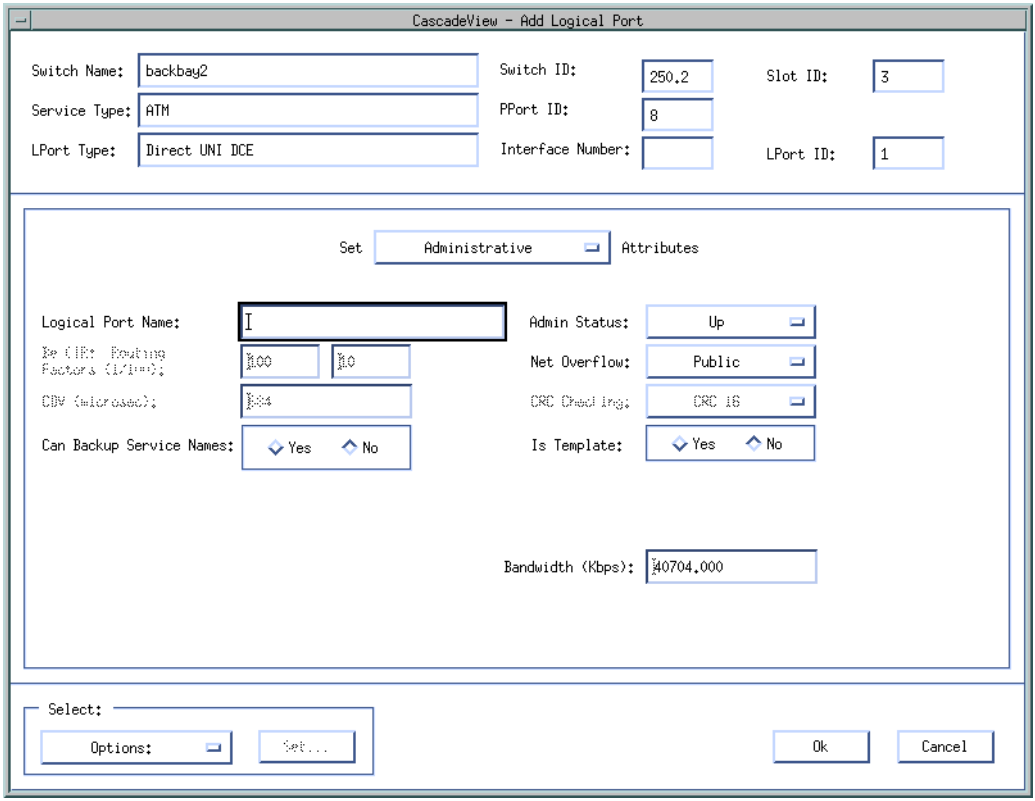


Figure 7-3. Add Logical Port Dialog Box (Direct UNI Logical Ports)

Administrative Attributes

Use the Set [Administrative] Attributes option to complete the fields described in Table 7-5.

Table 7-5. Set Administrative Attributes (UNI Ports) Fields

Field	Action/Description
Logical Port Name	Enter a unique alphanumeric name for this port. CascadeView/UX uses this name to reference the logical port.
Admin Status	Set the Admin Status to Up (the default) to make the port active. Set the Admin Status to Down to make the port inactive.
Can Backup Service Names *(Fault Tolerant PVC only)*	To configure a logical port for backup service in a fault tolerant PVC configuration, select Yes. For more information about fault tolerant PVCs, refer to page 7-62.
Bandwidth	Enter the amount of bandwidth for this logical port. The default is the amount of bandwidth remaining from the physical clock rate less any logical ports already configured. If you are defining an OPTimum cell trunk on this port, configure this UNI logical port with a minimal amount of bandwidth; if you are not configuring an OPTimum Cell Trunk on the logical port, use the remaining bandwidth for the logical port. For specific guidelines on configuring bandwidth with the various physical port types, refer to page 7-7.

Table 7-5. Set Administrative Attributes (UNI Ports) Fields (Continued)

Field	Action/Description
Net Overflow (*VPN only*)	Determines how SVC traffic originating from this logical port is managed during trunk overflow or failure conditions. This feature is used with Virtual Private Networks (VPN). To configure this logical port for a specific VPN and customer, refer to page 7-37. For more information about VPNs, refer to page 7-19. Select one of the following options: *Public (default)* – SVCs originating from this port are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – SVCs originating from this port can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Is Template	*(Optional)* Saves these settings as a template to configure another logical port with similar options. To create a template, choose Yes.

ATM Attributes

Choose the Set [ATM] Attributes option to complete the fields described in Table 7-6.

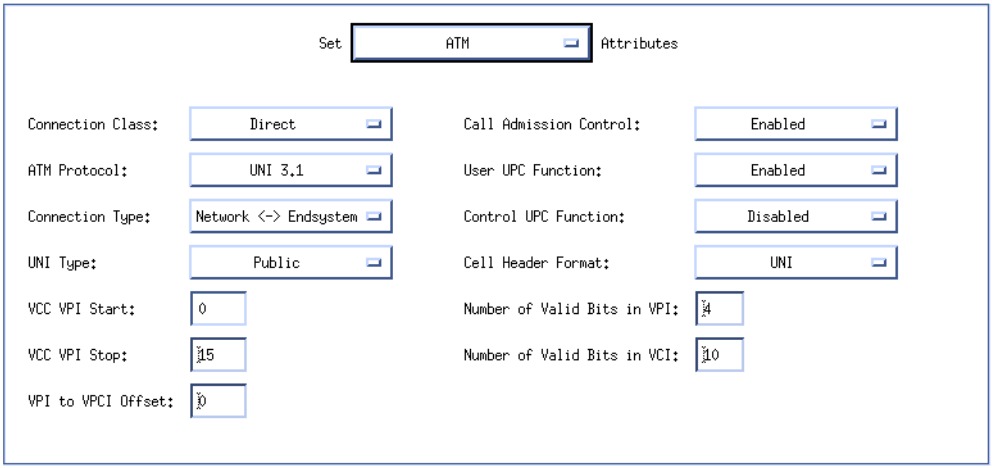


Figure 7-4. Set ATM Attributes (UNI Logical Ports)

Table 7-6. Set ATM Attributes (UNI Ports) Fields

Field	Action/Description
Connection Class	Displays the UNI logical port type, either direct or virtual. This field is set to Direct when you configure the first UNI logical port on this physical port. When you configure subsequent UNI ports on this physical port, this field displays Virtual.
ATM Protocol	Select UNI 3.1 (the default), UNI 3.0, or IISP 3.1. You can use the UNI 3.0 option if IISP 3.0 is the desired protocol. ***Note:*** *The default Signaling Tuning parameters are based on the ATM Protocol you select. If you change the Signaling Tuning parameters for this port and later change the UNI version, the default Signaling Tuning parameters for the ATM Protocol you select overwrite these changes. For more information on Signaling Tuning parameters, refer to page 7-38.*

Table 7-6. Set ATM Attributes (UNI Ports) Fields (Continued)

Field	Action/Description
UNI Type	Select Public if at least one end of this connection attaches to a public network. Select Private if this connection resides completely within a private network.
VCC VPI Start	For direct UNI, this field is set to 0. For virtual UNI, this field represents the VPI of the control channels (i.e., signaling and ILMI).
VCC VPI Stop	To configure this value, use the following formula: `VCC VPI Stop <= (2 numvpibits) – 1` where “numvpibits” equals the value you configure for the Number of Valid Bits in VPI field (page 7-29). Refer to page 7-7 for information on VCC VPI Start and Stop values.
VPI to VPCI Offset	To configure the virtual path connection identifier (VPCI), use one of the following formulas: `VPI – offset = VPCI or VPI= VPCI + offset` where “offset” equals the value you enter in this field. Although you can enter a negative value for the offset, make sure the formula does not produce a negative VPI or VPCI.
Connection Type	This option lets the switch know if it is attached to another switch or an endsystem. • Select Network <–> Endsystem if this port connects to a router or host. (This option is only available for UNI DCE ports.) • Select Network <–> Network if this port connects to another ATM switch.
Number of Valid bits in VPI/VCI	This setting applies to the VPI and VCI range you can use for VCCs (both PVCs and SVCs). The default values of VPI = 4 and VCI = 10 mean you can use VCCs over the range of VPI = 0 – 15 (4 bits of VPI) and a VCI range of VCI = 32 – 1023 (10 bites of VCI). The values have no effect on VPCs, which you can provision anywhere over the VPI = 0 – 255 range. For more information about setting these values, refer to page 7-7.

Table 7-6. Set ATM Attributes (UNI Ports) Fields (Continued)

Field	Action/Description
Call Admission Control	When enabled (the default), the port rejects a circuit creation request if there is not enough available bandwidth. When disabled, the port attempts to create a circuit even if there is not enough available bandwidth (for VBR Non-Real Time queue only). ***Note:*** *If you disable Call Admission Control on a UNI logical port, you are effectively disabling Cascade's Call Master Connection Admission Control (CAC) function on that logical port. For more information about the CAC function, refer to Appendix A.*
User UPC Function	Enables or disables the Usage Parameter Control (UPC) function. You can also enable or disable the UPC function for individual PVCs. If you need to enable the UPC function on a per PVC basis, you must enable the UPC function on the logical port. *Enabled* (default) – Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – All traffic, including non-conforming traffic, passes in through the port. If you disable the UPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. For this reason, *Cascade recommends that you leave the UPC function enabled on all logical ports*. For information on UPC traffic parameters, refer to "About ATM Traffic Descriptors" on page 9-2.

Table 7-6. Set ATM Attributes (UNI Ports) Fields (Continued)

Field	Action/Description
Control UPC Function	Enables or disable policing on a user port for control circuits (signaling and ILMI) independently of user traffic. The default is disable. Enable policing to prevent an attached device from overloading the switch with data on the control circuit. The CBX 500 polices the control circuit to pre-defined default traffic characteristics. The attached device typically needs to support per-VC shaping. ***Note***: *If the attached device is another CBX 500 switch, do not enable policing since the CBX 500 does not support per-VC shaping.*
Cell Header Format	This field controls the number of VPI bits in the ATM cell header for VPCs. Select UNI (default) to use a range of 0 through 8. Select NNI to use a valid bits in VPI range of 0 through 12.

ILMI/Signaling/OAM Attributes

Choose the Set [ILMI/Signaling/OAM] Attributes option to complete the fields as described in Table 7-7.

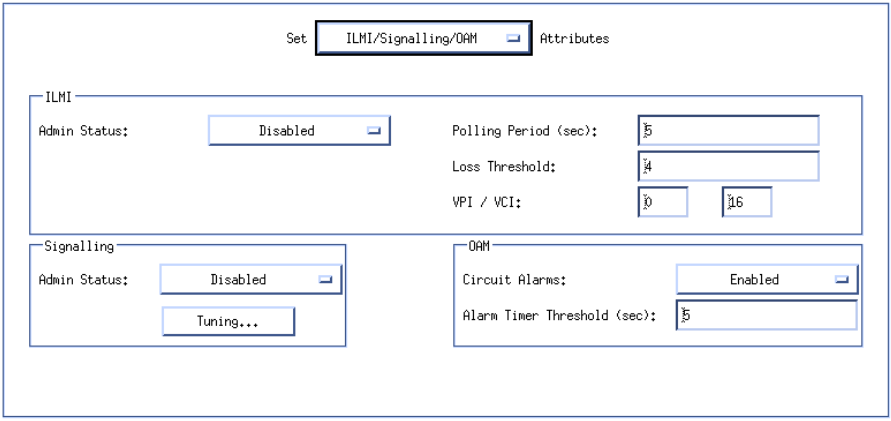


Figure 7-5. Set ILMI/Signaling/OAM Attributes (UNI Logical Ports)

Table 7-7. Set ILMI/Signaling/OAM Attributes Fields

Field	Action/Description
ILMI Attributes	
Admin Status	Choose Enabled to reserve 1% of the bandwidth in the VBR-NRT QoS class for ILMI. If you enable ILMI and the attached device does not respond to ILMI polls, the logical port is brought down. The switch considers the ILMI state to be down. When ILMI is Disabled (default), this bandwidth is not reserved. If the attached device cannot run ILMI, leave ILMI disabled. For information about ILMI support, refer to page 7-20. ***Note:*** *To use line loopback diagnostics, you must disable ILMI support. Refer to the* Diagnostic and Troubleshooting Guide for CBX 500 *for more information.*
DTE Prefix Screen Mode (DTE ports)	When a DTE port receives network prefixes from an external network, you can perform various levels of screening on them against the list of prefixes configured on the node and/or port. Select one of the following options: *Accept All* – No screening occurs; accepts all prefixes. *Node Prefix* – Accepts only network prefixes that partially or fully match a configured node prefix. *Port Prefix* – Accepts only network prefixes that partially or fully match a configured port prefix. *Node or Port Prefix* – Accepts only network prefixes that partially or fully match either a configured node prefix or a configured port prefix. *Reject All* – Rejects all network prefixes received from an external network. For more information about node and port prefixes, refer to Chapter 10.

Table 7-7. Set ILMI/Signaling/OAM Attributes Fields (Continued)

Field	Action/Description
Polling Period	Specify the polling period (T) for an ILMI poll. The switch generates an ILMI poll every (T) seconds. The default is 5 seconds.
Loss Threshold	Specify 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	Enter the ID of the virtual path you want to use for ILMI polling. The default is 0.
VCI	Enter the ID of the virtual channel you want to use for ILMI polling. The default is 16.
Signaling Attributes	
Admin Status	Choose enabled to reserve 2% of the bandwidth in the VBR-NRT QoS class to support the UNI signaling protocol. Use the default setting, disabled, if you will use this logical port only for PVCs (that is, you will not create SVCs on the port).
Tuning	Choose the Tuning command to display the Set Logical Port Signaling Tuning Parameters dialog box. For information about Tuning parameters, refer to page 7-38.
OAM Attributes	
Circuit Alarms	Select enabled (default) to allow this logical port to generate OAM alarms. The switch uses these alarms to signal when the circuits have gone down. Select disabled to disable OAM alarms on this logical port.
Alarm Timer Threshold	Before generating an OAM alarm, the switch waits until the circuit has been down for the time period you specify in this field. The default is 5 seconds.

SVC VPI/VCI Range Attributes

Choose the Set [SVC VPI/VCI Range] Attributes option.

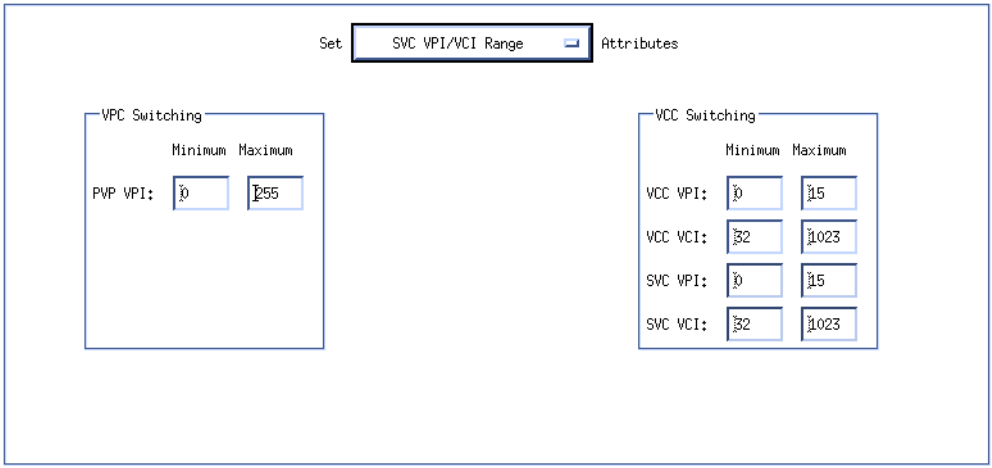


Figure 7-6. Set SVC VPI/VCI Range

The VPI/VCI address range fields allow you to design a PVC VPI/VCI or SVC VPI/VCI address range to match the capability of the equipment attached to this port. Use the following table to configure these ranges:

Field	Minimum/Maximum
VCC VPI	Displays the VPI range for a PVC.
VCC 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.

Defining UNI Logical Port Options

Complete the following steps to select additional options for this new logical port:

1. From the Add Logical Port dialog box, use the Select: Options: menu to review additional options. Choose Set to configure this information.

   The Options button displays the following:

   - QoS Parameters
   - NTM Parameters
   - ATM Accounting
   - Screen Assignments

2. Review the default QoS parameters as shown in Table 7-8. The CBX 500 routes circuits depending on the routing metric you select for the logical port.

Table 7-8. Default Quality of Service Values for ATM UNI Logical Ports

Service Type	Bandwidth Allocation	Routing Metric	Oversubscription Factor
CBR	Dynamic	Cell Delay Variation	100%
VBR-RT	Dynamic	Admin Cost	100%
VBR-NRT	Dynamic	Admin Cost	100%
UBR	Dynamic	Admin Cost	100%

   To modify these settings, from the Select: Options: menu, select QoS Parameters and choose Set. Refer to page 7-59 for details. When you finish, return to this section and proceed to Step 3.

3. *(Optional)* To configure the network traffic management (NTM) parameters for this logical port, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.

4. *(Optional)* To configure accounting parameters for this logical port, refer to the *Accounting System Administrator's Guide*.

5. *(Optional)* To configure screen assignments for port security screening, refer to "Assigning Security Screens to Logical Ports" on page 14-12.

Defining UNI Logical Port Attributes

Use the following steps to complete the logical port configuration.

1. *(Optional)* To configure the ATM flow control processor for this logical port, choose the Set [ATM FCP] Attributes option. For more information about these parameters, refer to the *ATM Flow Control Processor User's Guide*.

2. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 7-1 on page 7-15).

3. (*Optional*) To configure this logical port for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 7-37.

4. Choose Close to return to the Set Physical Port attributes dialog box. Then choose Cancel to return to the Switch Back Panel dialog box.

To continue, do one of the following:

- To configure a virtual UNI logical port, continue with the following section "Defining Virtual ATM UNI Logical Ports".

- Once you configure the logical port endpoints, you can provision PVCs (refer to Chapter 9, "Configuring PVCs").

Selecting the VPN and Customer Name

Use the following sequence to configure this logical port for a VPN:

Step 1. Create the VPN (refer to page 4-19).

Step 2. Add customers to a specific VPN (page 4-20).

Step 3. Create the UNI logical port and specify the net overflow parameter (page 7-27).

Step 4. Associate the logical port to a specific VPN and customer (page 7-37).

To associate this logical port to a specific VPN and customer:

1. From the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15), select the logical port.
2. Using the Select:Options button, select VPN/Customer and choose Set. The following dialog box appears.

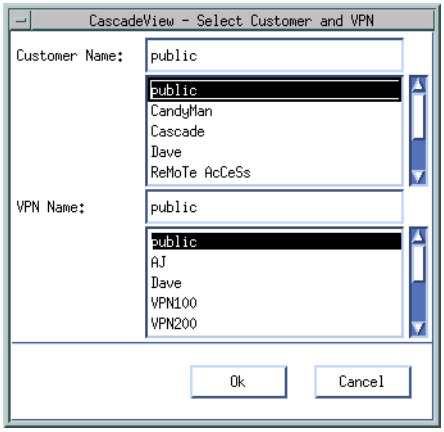


Figure 7-7. Select Customer and VPN Dialog Box

3. Select the customer and VPN name.
4. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 7-1 on page 7-15).
5. Choose Close to exit.

Setting Logical Port Signaling Tuning Parameters

This section describes how to modify the signaling parameters for an ATM UNI logical port. For more information on signaling, refer to "Using Logical Port Signaling" on page 7-22.

To modify the signaling tuning parameters:

1. From the Add Logical Port dialog box (Figure 7-5 on page 7-31), choose the Tuning command in the Signaling box. The following dialog box appears. The fields are the same regardless of the type of logical port you are configuring.

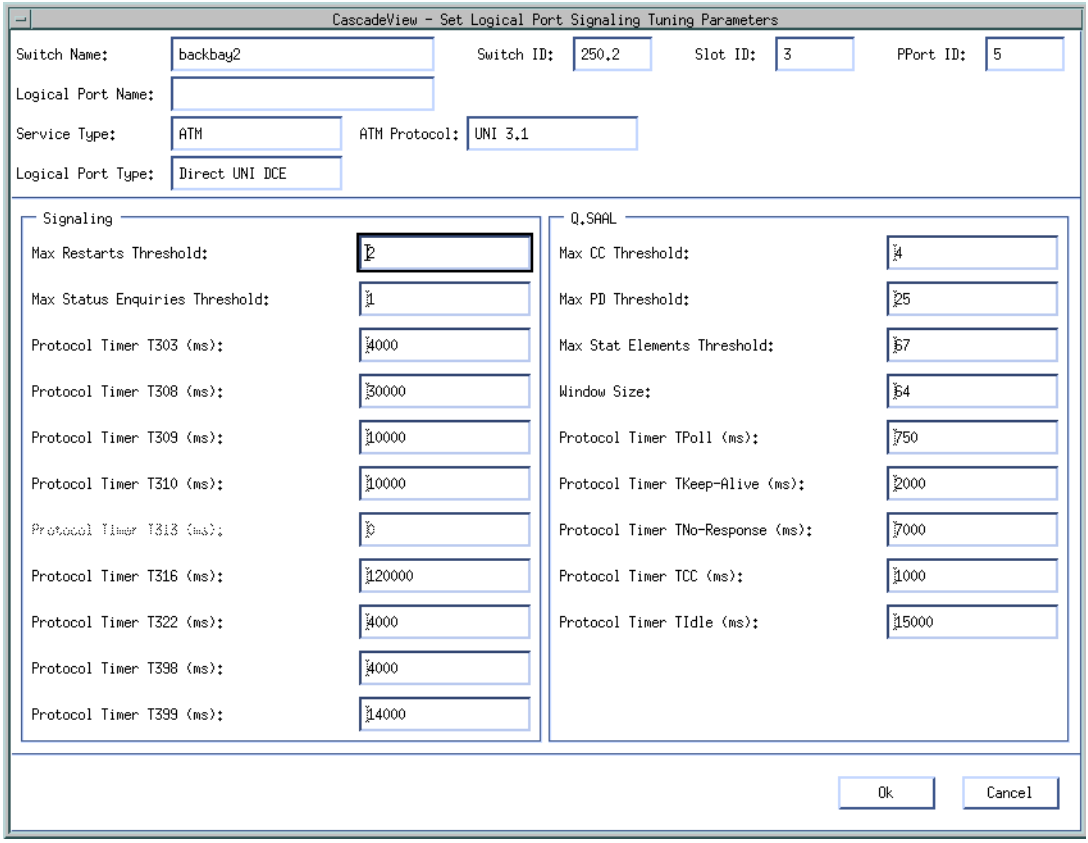


Figure 7-8. Set Logical Port Signaling Tuning Parameters

Use the Set Logical Port Signaling Tuning Parameters dialog box to set the signaling thresholds and timers and the Q.SAAL protocol data unit (PDU) thresholds and timers. In general, you should not change the default values. The displayed defaults are based on the ATM protocol you selected for the logical port (refer to page 7-28).

2. Complete the fields on this screen using the information in Table 7-9. All timer field values are specified in milliseconds (1/1000ths of a second).

Table 7-9. Set Logical Port Signaling Tuning Fields

Field	Description
Signaling	
Max Restarts Threshold	The maximum number of restarts to send without a response. The default is 2.
Max Status Enquiries Threshold	The maximum number of status enquiries that can be unacknowledged before the call is dropped. The default is 1.
Protocol Timer T303	How long to wait for a response after a SETUP protocol data unit (PDU) has been sent. The default is 4000.
Protocol Timer T308	How long to wait for a response after a RELEASE PDU has been sent. The default is 30000.
Protocol Timer T309	If Q.SAAL is down, 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	How long to wait for the next response after a CALL PROCEEDING PDU has been received. The default is 10000.
Protocol Timer T313	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	How long to wait for a response after a RESTART PDU has been sent. The default is 120000.

Table 7-9. Set Logical Port Signaling Tuning Fields (Continued)

Field	Description
Protocol Timer T322	How long to wait for a response after a STAT ENQUIRY PDU has been sent. The default is 4000.
Protocol Timer T398	How long to wait for a response after a DROP PTY PDU has been sent. The default is 4000.
Protocol Timer T399	How long to wait for a response after an ADD PTY PDU has been sent. The default is 14000.
Q.SAAL	
Max CC Threshold	The maximum number of transaction retries for control PDUs. The default is 4.
Max PD Threshold	The maximum number of data PDUs without a POLL. The default is 25.
Max STAT Elements Threshold	The maximum number of missing elements in a STATUS PDU. The default is 67.
Protocol Timer TPoll	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	How often a poll is sent when the Q.SAAL is in the transient state. The default is 2000.
Protocol Timer TNoResponse	The maximum amount of time that can pass without a STATUS PDU being received. The default is 7000.
Protocol Timer TCC	The retry time for control PDUs. The default is 1000.
Protocol Timer TIdle	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 OK to return to the Add Logical Port dialog box (Figure 7-3). Continue with page 7-33 to configure the OAM attributes.

Defining Virtual ATM UNI Logical Ports

You can create a virtual ATM UNI DCE or DTE logical port on any physical port on which you have already defined a direct UNI logical port.

To add a virtual ATM UNI logical port:

1. Complete the steps in “Accessing ATM Logical Port Functions” on page 7-14. Make sure you access a physical port on which you have already defined a UNI logical port.
2. Choose Add to define a new logical port. The Add Logical Port dialog box (Figure 7-2 on page 7-24) appears.
3. Select the LPort Type, either ATM UNI DTE or ATM UNI DCE.
4. Choose OK. The Add Logical Port dialog box reappears. The LPort Type field displays a virtual ATM UNI DCE (or DTE) logical port type.
5. Continue with the instructions beginning with “Administrative Attributes” on page 7-26 to configure attributes for this virtual UNI logical port.

Defining ATM NNI Logical Ports

The ATM NNI logical port type enables you to connect ATM networks from different service providers using the B-ICI 1.1 ATM Protocol. This logical port type is not available for T1 physical ports. You can only configure one NNI logical port per physical port, and NNI logical ports cannot share a physical port with a UNI port.

To configure an ATM NNI logical port:

1. Complete the steps in “Accessing ATM Logical Port Functions” on page 7-14.
2. Choose Add to define a new logical port. The Add Logical Port dialog box appears (Figure 7-2 on page 7-24).
3. Select the LPort Type, ATM NNI. The LPort ID defaults to 1 for this type of configuration and cannot be changed.
4. Choose OK. The Add Logical Port dialog box reappears.

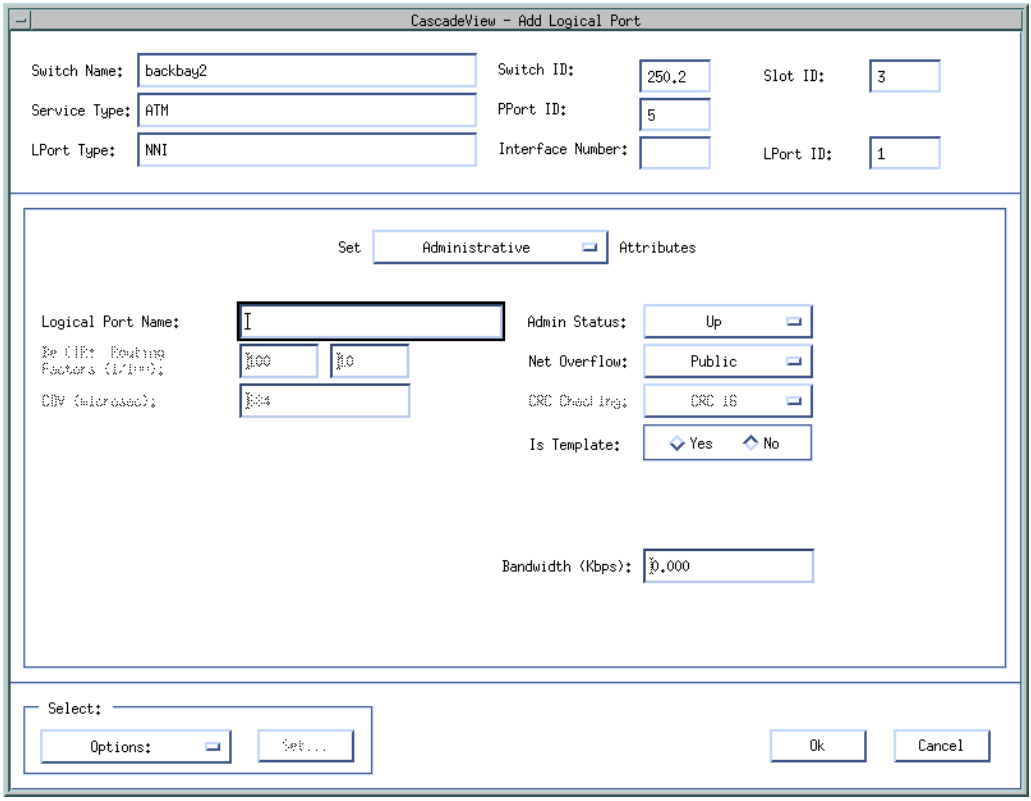


Figure 7-9. Add Logical Port Dialog Box for ATM NNI

Administrative Preference Attributes

Use the Set [Administrative] Attributes option to complete the fields described in Table 7-10.

Table 7-10. Set Administrative Attributes (NNI Ports) Fields

Field	Action/Description
Logical Port Name	Enter a unique alphanumeric name for this port. CascadeView/UX uses this name to reference the logical port.
Admin Status	Set the Admin Status to Up (the default) to make the port active. Set the Admin Status to Down to make the port inactive.
Bandwidth	Enter the amount of bandwidth for this logical port. The default is the amount of bandwidth remaining from the physical clock rate less any logical ports already configured. If you are defining an OPTimum cell trunk on this port, configure this UNI logical port with a minimal amount of bandwidth; if you are not configuring an OPTimum Cell Trunk on the logical port, use the remaining bandwidth for the logical port. For specific guidelines on configuring bandwidth with the various physical port types, refer to page 7-7.
Net Overflow (*VPN only*)	Determines how SVC traffic originating from this logical port is managed during trunk overflow or failure conditions. This feature is used in conjunction with Virtual Private Networks (VPN). To configure this logical port for a specific VPN and customer, refer to page 7-37. For more information about VPNs, refer to page 7-19. Select one of the following options: *Public (default)* – SVCs originating from this port are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – SVCs originating from this port can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Is Template	*(Optional)* Saves these settings as a template to configure another logical port with similar options. To create a template, choose Yes.

ATM Attributes

Choose the Set [ATM] Attributes option to complete the fields described in Table 7-11.

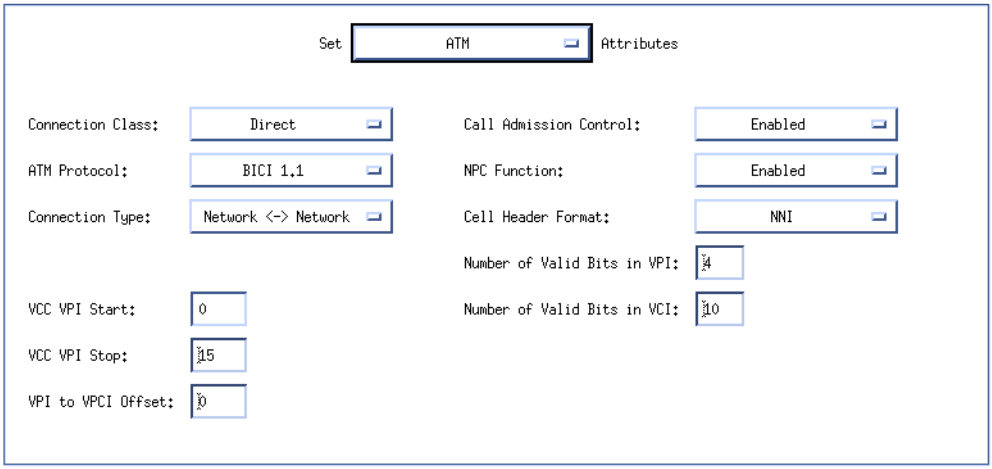


Figure 7-10. Set ATM Attributes (NNI Logical Ports)

Table 7-11. Set ATM Attributes (NNI Ports) Fields

Field	Action/Description
Connection Class	Defaults to BICI 1.1 and cannot be changed.
ATM Protocol	Defaults to BICI 1.1 and cannot be changed.
Connection Type	Defaults to Network <–> Network and cannot be changed.
UNI Type	Select Public if at least one end of this connection attaches to a public network. Select Private if this connection resides completely within a private network.
VCC VPI Start	This field is set to 0 and cannot be modified.

Table 7-11. Set ATM Attributes (NNI Ports) Fields (Continued)

Field	Action/Description
VCC VPI Stop	To configure this value, use the following formula: `VCC VPI Stop <= (2 numvpibits) – 1` where “numvpibits” equals the value you configure for the Number of Valid Bits in VPI field (page 7-51). Refer to page 7-7 for information on VCC VPI Start and Stop values.
VPI to VPCI Offset	To configure the virtual path connection identifier (VPCI), use one of the following formulas: `VPI – offset = VPCI or VPI= VPCI + offset` where “offset” equals the value you enter in this field. Although you can enter a negative value for the offset, make sure the formula does not produce a negative VPI or VPCI.
Call Admission Control	When enabled (the default), the port rejects a circuit creation request if there is not enough available bandwidth. When disabled, the port attempts to create a circuit even if there is not enough available bandwidth (for VBR Non-Real Time queue only). ***Note:*** *If you disable Call Admission Control on a UNI logical port, you are effectively disabling Cascade’s Call Master Connection Admission Control (CAC) function on that logical port. For more information about the CAC function, refer to Appendix A.*

Table 7-11. Set ATM Attributes (NNI Ports) Fields (Continued)

Field	Action/Description
NPC Function	Enables or disables the Network Parameter Control (NPC) function. *Enabled* (default) – Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – All traffic, including non-conforming traffic, passes in through the port. If you disable the UPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. For this reason, *Cascade recommends that you leave the NPC function enabled on all logical ports*.
Cell Header Format	This field controls the number of VPI bits in the ATM cell header for VPCs. Select NNI (default) to use a valid bits in VPI range of 0 through 12. Select UNI to use a range of 0 through 8.
Number of Valid Bits in VPI	Specify a value that is within the range for either the NNI or UNI call header format. The sum of this value and the value you enter for number of valid VCI bits cannot exceed 14.
Number of Valid Bits in VCI	Specify a value that when added to the number of valid VPI bits, does not exceed 14.

OAM Attributes

Use the Set [ILMI/Signaling/OAM] Attributes option to enable this logical port to generate operations, administration, and maintenance (OAM) alarms. NNI logical ports do not support ILMI and Signaling attributes.

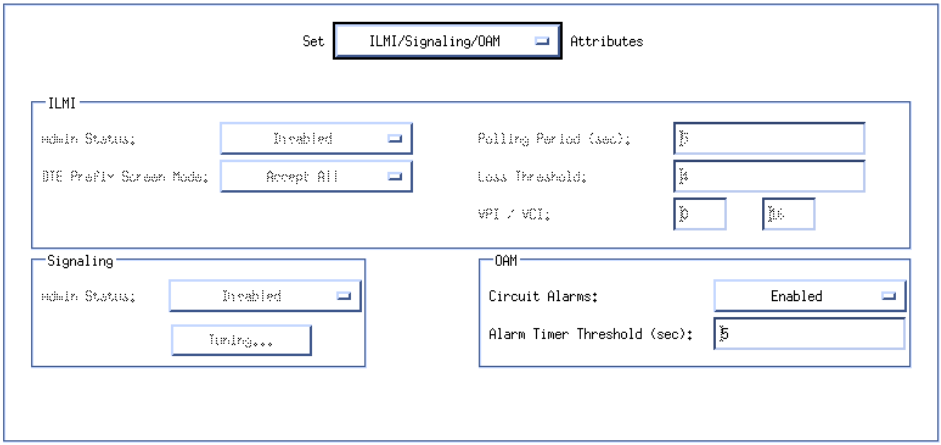


Figure 7-11. Set ILMI/Signaling/OAM Attributes (NNI Logical Ports)

Circuit Alarms — Select Enabled (default) to allow this logical port to generate OAM alarms. The switch uses these alarms to signal when the circuits have gone down. Select Disabled to disable OAM alarms on this logical port.

Alarm Timer Threshold — Before generating an OAM alarm, the switch waits until the circuit has been down for the time period you specify in this field. The default is 5 seconds.

Defining NNI Logical Port Options

Complete the following steps to select additional options for this new logical port:

1. From the Add Logical Port dialog box, use the Select: Options: button to review additional options. Choose Set to configure this information.

   The Options button displays the following options: QoS Parameters and ATM Accounting.

2. Review the default QoS parameters for all four service classes as shown in Table 7-8 on page 7-35. The CBX 500 routes circuits depending on the routing metric you select for the logical port.

   To modify these settings, from the Select:Options: menu, select QoS Parameters and choose Set. Refer to page 7-59 for details.

3. *(Optional)* To configure Accounting parameters for this logical port, refer to the *Accounting System Administrator's Guide.*

Defining NNI Logical Port Attributes

Use the following steps to complete the logical port configuration.

1. *(Optional)* To configure the ATM flow control processor for this logical port, choose the Set [ATM FCP] Attributes option. For more information about these parameters, refer to the *ATM Flow Control Processor User's Guide.*

2. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 7-1 on page 7-15).

3. (*Optional*) To configure this logical port for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 7-37.

4. Choose Close to return to the Set Physical Port attributes dialog box. Then choose Cancel to return to the Switch Back Panel dialog box.

Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports

This section describes how to configure an ATM Direct Trunk or ATM OPTimum Cell Trunk. For information about how these logical port types are used in the network, refer to page 7-3. Before you configure an ATM OPTimum Cell Trunk logical port, make sure you configure an ATM UNI logical port on the same physical port to act as the feeder port.

To configure an ATM OPTimum Cell Trunk or ATM Direct Trunk logical port:

1. Complete the steps in "Accessing ATM Logical Port Functions" on page 7-14.
2. Choose Add to define a new logical port. The Add Logical Port dialog box (Figure 7-2 on page 7-24) appears.
3. Complete the Add Logical Port dialog box fields as follows:

   LPort Type — Select ATM OPTimum Cell Trunk or ATM Direct Trunk.

   Logical Port (*Direct Trunk only*) — Defaults to 1 and cannot be changed.

   Virtual Path ID (*OPTimum Cell Trunk only*) — This is the VPI used for all circuits routed over this OPTimum trunk. The range of valid VPI values depends upon the number of valid VPI bits you set for the ATM UNI feeder port (refer to Table 7-1 on page 7-6).

   Enter a number from 1-*nnnn* to identify the virtual path for the ATM logical port. *nnnn* is equal to 2^{P}-1, where *P* is the value specified in the Valid Bits in VPI field for the UNI feeder port that shares this physical port (refer to page 7-5).

   For example, if you entered 4 in the Valid Bits in VPI field for the UNI feeder port, you can have up to 15 virtual paths on this port (2^{4}-1=15); if you entered 8 in the Valid Bits in VPI field, you can have up to 255 virtual paths on this port (2^{8}-1=255).

The highest value you can enter (and therefore, the number of virtual paths you can configure on the port) depends on the value you entered in the Valid Bits in VPI field for the ATM UNI feeder port (refer to page 7-29). The OPTimum trunk Virtual Path ID must be unique on the port.

Virtual Path ID 0 cannot be used for OPTimum trunks.

The network interfacing with the OPTimum trunk must be configured to accept circuits with this VPI and any of its valid VCIs. You could accomplish this by establishing a VPC with this VPI in the interfacing network.

4. Choose OK. The Add Logical Port dialog box reappears.

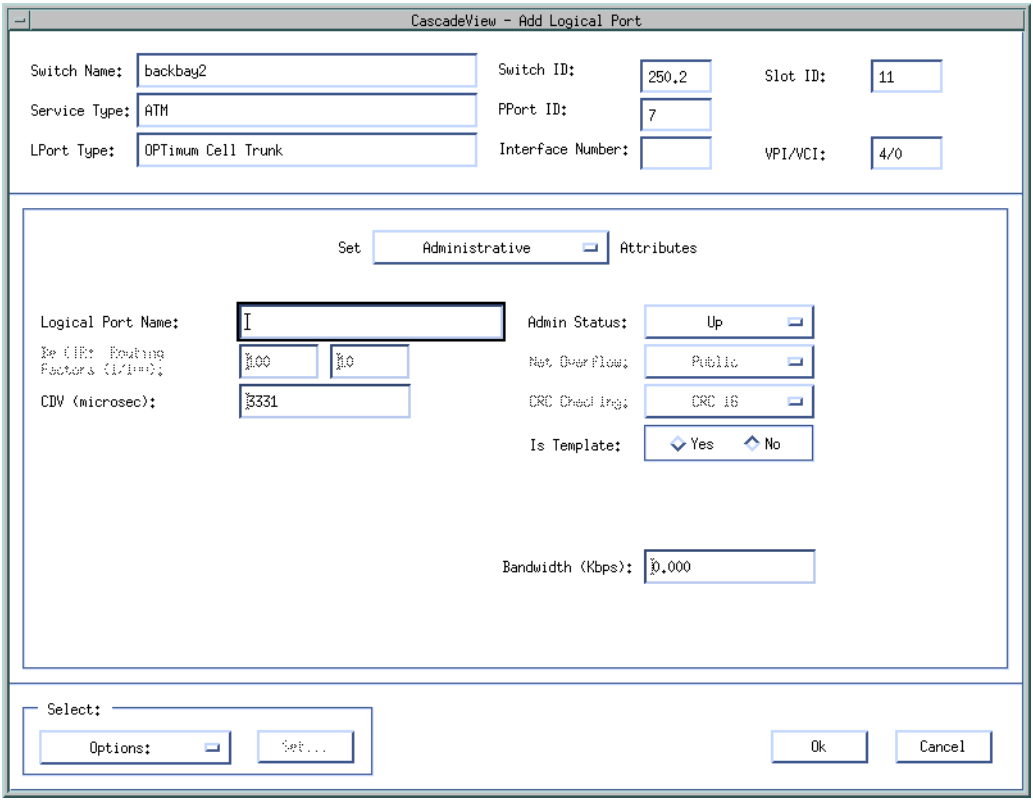


Figure 7-12. Add Logical Port Dialog Box (Trunk Logical Ports)

5. Use the Set [Administrative] Attributes command to configure the following:

   Logical Port Name — Enter a unique alphanumeric name for this port. CascadeView/UX uses this name to reference the logical port.

   Admin Status — Set the Admin Status to Up (the default) to make the port active. Set the Admin Status to Down to make the port inactive.

   Bandwidth — Enter the total amount of bandwidth for this logical port configuration. The default is the amount of bandwidth available on the port. If you are configuring more than one OPTimum Cell Trunk on this logical port, enter the appropriate amount of bandwidth to reserve for the OPTimum trunk you are configuring. Remember to leave bandwidth for any remaining OPTimum trunks you need to configure on this logical port.

There is a limitation for using multiple OPTimum trunks on the same physical port. Although you can provision multiple OPTimum trunk logical ports on a CBX 500 physical port, you can only route one point-to-multipoint PVC leaf over the physical port. This is because you cannot perform multicasting at the port level.

6. (*OPTimum Trunks only*) The CDV field enables you to enter a cell delay variation characteristic (in µsecs) that is different than the Cascade default for each media type, as shown in Table 7-12. This option is useful when the CDV characteristics of the ATM equipment providing the VPC that carries the OPTimum trunk is different than Cascade's CDV characteristic. The CDV value is used in conjunction with the CDV routing metric that is available for the CBR and VBR-RT QoS classes.

Table 7-12 lists the default values.

Table 7-12. CDV Default Values for OPTimum Trunks

Port Type	CDV Default Value
DS3/E3	684µsec
T1	3331µsec
E1	3552µsec
OC12	45µsec
OC3	191µsec

To change the default, you need to know the maximum CDV for PVCs on the port, as well as the hardware traffic requirements on the other end of the connection.

If you want to use the default settings for each service class, you can skip Step 7. By default, Bandwidth Allocation is set to Dynamic and Oversubscription Factor is set to 100%. The Routing Metric setting does not apply to trunks.

7. Use the Select: Options menu to select QoS Parameters. Choose Set to view the Set Logical Port QoS Parameters dialog box. For information about modifying these parameters, refer to page 7-59. When you finish, return to this section and proceed to Step 8.
8. (*Optional*) When you finish, you can save these settings as a template to configure another logical port with similar options. To create a template, select Yes in the Is Template field.
9. Choose OK. The Set All Logical Ports in PPort dialog box reappears.
10. Choose Close to return to the Set Physical Port Attributes dialog box. Then choose Close to return to the Switch Back Panel dialog box.

11. To configure the other trunk logical port endpoint, repeat Step 1 through Step 9 beginning on page 7-54.

    After you configure both logical port endpoints for a trunk, you can add the trunk line connection between them. Refer to Chapter 8, “Configuring Trunks”.

Setting Quality of Service Parameters

This section describes how to set the QoS parameters for a logical port. These parameters enable you to specify the bandwidth and routing metrics (if applicable) for the various traffic service classes. Cascade recommends you set the logical port QoS fixed and dynamic options before you provision circuits. Under certain conditions, if you change the bandwidth from dynamic to fixed after you provision circuits, one or more QoS classes (including CBR) may display negative bandwidth.

The Set Logical Port QoS Parameters dialog box fields (Figure 7-13) are the same regardless of the logical port type. For more information on quality of service, refer to “About the Oversubscription Factor” on page 7-12.

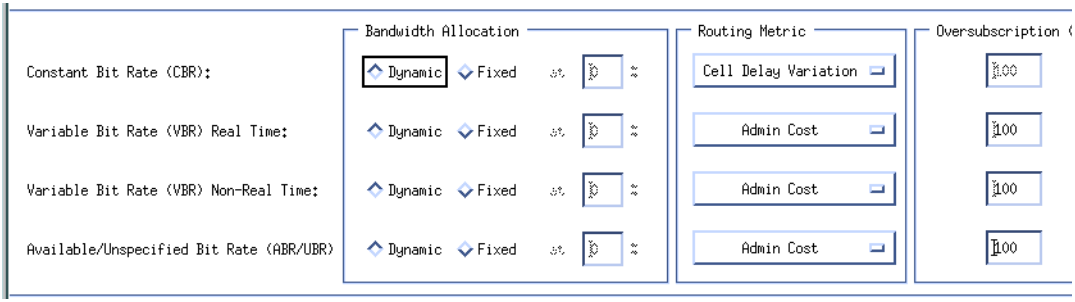


Figure 7-13. Set Logical Port QoS Parameters

The following list briefly describes each class of service:

Constant Bit Rate (CBR) — Handles digital information, such as video and digitized voice that is 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 Bit Rate Unspecified Bit Rate (ABR/UBR) — Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic. You can also use this service class in conjunction with the ATM Flow Control Processor. Refer the *ATM Flow Control Processor User's Guide* for more information.

To set the QoS parameters:

1. Configure the Bandwidth Allocation for each service class as follows:

   Dynamic — Select Dynamic to enable the bandwidth allocation to change dynamically according to bandwidth demands. Dynamic bandwidth allocation pools the remaining bandwidth for this logical port. This includes bandwidth that has not already been allocated to a specific queue or assigned to a connection.

   Fixed — Select Fixed to specify the percentage of bandwidth you want to reserve for that service class. If all four service classes are set to Fixed, ensure that all four values add up to 100% so that you do not waste bandwidth.

   - If you set the CBR or VBR service class bandwidth to Fixed, you are specifying the maximum bandwidth to reserve for this type of traffic; if the network requests a circuit that exceeds the fixed value, the circuit cannot be created.
   - If you set the UBR service class to Fixed, you are guaranteeing that amount of service, at a minimum, for the UBR queue, provided that the VBR queues are not oversubscribed. No bandwidth is actually allocated for UBR connections, so the port admits more connections into the UBR queue than it can service.

If you have service classes set to Dynamic, any remaining bandwidth percentage is allocated to those service classes as needed. For example, if CBR is Fixed at 30%, UBR is Fixed at 25%, and the two VBR classes are set to Dynamic, the remaining 45% of bandwidth will be dynamically allocated between the two VBR service classes.

2. The CBX 500 routes circuits depending on the routing metric you select for the logical port. Routing metrics apply only if the port is configured as UNI DCE, UNI DTE, or NNI logical port. Select one of the following Routing Metrics for each class of service.

   Cell Delay Variation (CDV) — This routing metric is only applicable to the CBR and VBR-RT queues. A circuit originating from a queue with the CDV routing metric will find the lowest CDV path to its destination (this is not necessarily the shortest path or the path with the least number of hops). The CDV route is determined from CDV values that are known for the direct and OPTimum trunks.

   Admin Cost — A circuit originating from a queue with the Admin Cost routing metric looks for the lowest cost route to its destination (this is not necessarily the shortest path or the path with the least number of hops). The switch determines this route by summing the Admin Costs of each of the direct and OPTimum trunks in the route.

   End-to-End Delay — You can configure this routing metric for all service classes. A circuit originating from a queue using the end-to-end delay routing metric finds the path with the lowest end-to-end delay (this is not necessarily the shortest path or the path with the least number of hops). The end-to-end delay is measured between the trunk endpoint interfaces at the time the trunk is initialized.

3. (*Optional*) Specify the Oversubscription Factor percentage for each class of service (except CBR and UBR, which are set to 100% and cannot be modified). This value must be between 100% and 1000%.

   If you leave these values set to 100%, Cascade's Call Master Connection Admission Control (CAC) algorithm ensures that the switch packs circuits on a port without experiencing data loss or losing quality of service. (UBR circuits do not use the CAC algorithm.)

   After monitoring your network, if users of a particular service class are reserving more bandwidth than they are actually using, you can adjust the oversubscription values to suit your needs. By doing so, however, you may adversely impact the quality of service for this and lower priority service classes. For more information on the oversubscription factor, refer to page 7-12.

4. Choose OK to return to the Add Logical Port dialog box.
5. Continue with one of the following:
   - Step 3 on page 7-35 for ATM UNI logical ports.
   - Step 4 on page 7-36 for ATM NNI logical ports.
   - Step 8 on page 7-58 for trunk logical ports.

Configuring Fault Tolerant PVCs

A fault tolerant PVC configuration enables UNI DCE and DTE logical ports to serve as a backup for any number of active UNI ports. If a primary port fails or if you need to take a primary port off-line, you activate the backup port.

Use the following sequence to configure fault tolerant PVCs:

Step 1. Define a UNI-DCE or UNI-DTE logical port. To designate a backup port, choose Yes for the option "Can Backup Service Names" (page 7-26).

Step 2. Specify a service name for the primary port (refer to page 7-64).

Step 3. Configure circuits to use a service name as the endpoint (refer to page 9-15).

Step 4. Activate the backup port (refer to page 7-67).

Cascade does not recommend that you configure SVCs on a logical port that is also designated as a backup port in a fault tolerant PVC configuration.

Creating a Backup Port

To create a backup port, first define a UNI DCE or DTE logical port as a backup. When a backup port is not in use, the port is idle and does not use network resources. For more information about designating a logical port as a backup, refer to page 7-26.

Creating a Primary Port

To create a primary port, you assign a service name to a UNI logical port. (Do not choose a port that you already configured for backup.) When you configure the circuit, choose this service name as the endpoint, instead of a switch and logical port combination. When you activate the backup port, all PVCs on the failed primary port are rerouted, preserving VPI/VCIs in the process.

Cascade's fault tolerant PVC feature is transparent to the end user, meaning that you do not have to configure the CPE to accommodate the new functionality. Therefore, end users can benefit from this feature through the public Cascade-based ATM network, or by combining their private Cascade switches with services provided by their public carrier.

Creating Service Names

The *service name binding* is a name you define to identify the primary port. A circuit recognizes its service endpoint by this name, instead of the logical port name.

To create the service name bindings:

1. From the Administer menu, select Cascade Parameters ⇒ Service Name Bindings. The following dialog box appears, displaying any service names you have already configured.

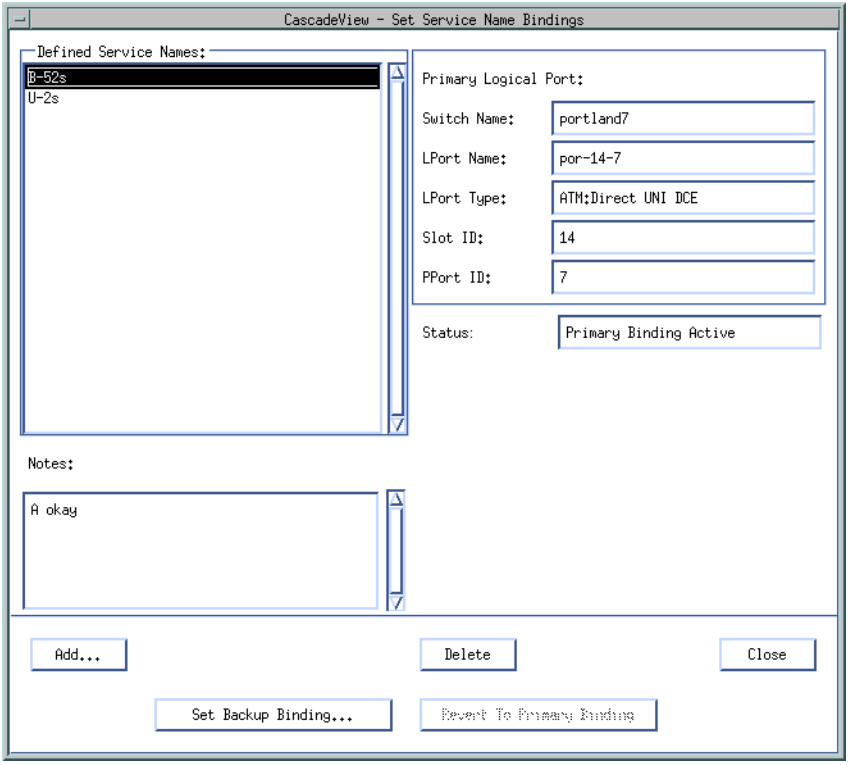


Figure 7-14. Set Service Name Bindings Dialog Box

2. Choose Add. The following dialog box appears.

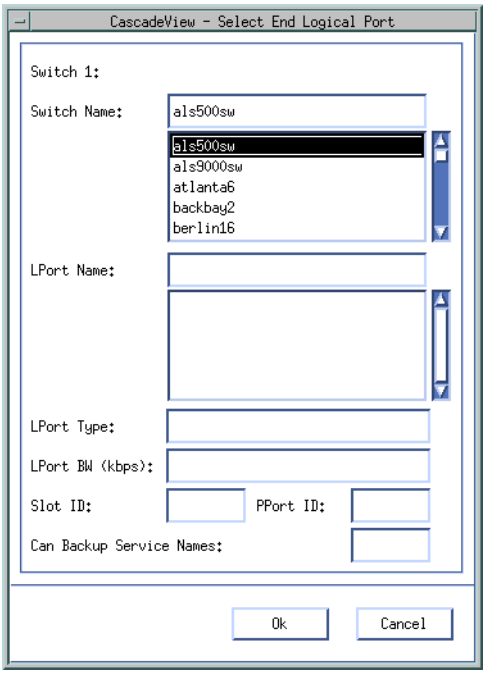


Figure 7-15. Select End Logical Port Dialog Box

3. Select the switch name and the primary logical port name.

Make sure that the Can Backup Service Names field displays No. You cannot configure a Service Name for a logical port you designated as a backup.

4. Choose OK. The following dialog box appears.

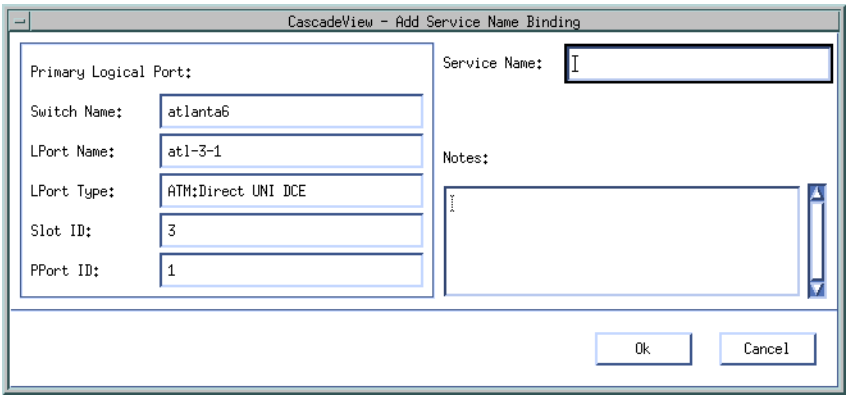


Figure 7-16. Add Service Name Binding Dialog Box

5. Type a service name up to 32 characters. Optionally, you can enter a brief comment or description of the service in the Notes box.

6. Choose OK.

7. Continue with the instructions in "Defining a PVC" on page 9-11 to configure the circuits for fault tolerant PVCs.

When you need to reroute a circuit if a port fails, refer to the following section.

Activating a Backup Binding Port

If a primary port fails, you reassign the service name of the primary port to the backup port. Since circuits use the service name as the endpoint, all circuits configured for the primary port are rerouted to the backup port.

Use the following steps to enable the backup binding:

1. From the Administer menu, select Cascade Parameters ⇒ Service Name Binding. The Set Service Name Bindings dialog box (Figure 7-14 on page 7-64) appears.

2. Choose Set Backup Binding. The following dialog box appears.

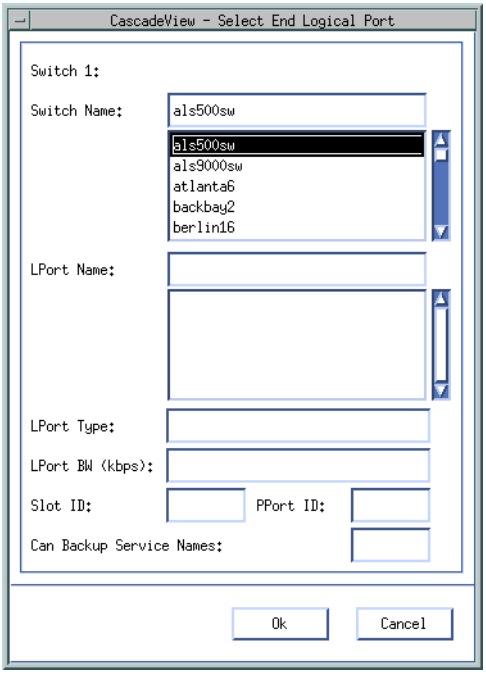


Figure 7-17. Select End Logical Port Dialog Box

3. Select the Switch Name for the backup service name binding you want to use.

4. The LPort Name field displays a list of logical ports configured for this service. Select an LPort Name that has the *same* logical port type as the port you need to backup.

Make sure that the Can Backup Service Names field displays Yes. This indicates you can use this logical port as a backup.

5. Choose OK. The following dialog box appears, displaying the Service Name that corresponds to the switch and logical port names you selected.

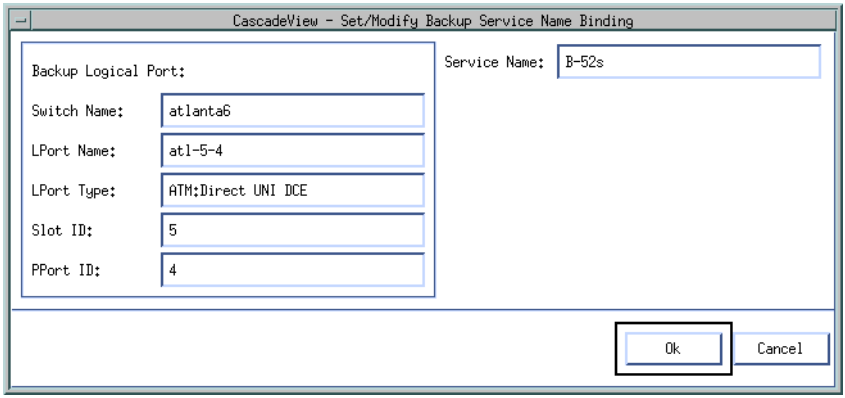


Figure 7-18. Set/Modify Backup Service Name Binding Dialog Box

6. Choose OK. The Set Service Name Bindings dialog box reappears (Figure 7-14 on page 7-64). The Status field should now display the message, Backup Binding Active.

You can also access the following functions from the Set Service Name Bindings dialog box:

- To return the primary logical port to service, select the Service Name and choose Revert to Primary Binding.
- To delete a service name, select the service name and choose Delete.
- To modify a backup service binding, choose Modify Backup Binding.

Deleting ATM Logical Ports

Before you delete an ATM logical port, verify the following:

- ☑ There are no trunks defined on the logical port.
- ☑ This logical port is not defined as the feeder (ATM UNI) for an existing ATM OPTimum Trunk logical port.
- ☑ No SVC addresses or prefixes are defined on the port.
- ☑ No PVCs are defined on the port.
- ☑ No Multipoint PVCs are defined on the port.
- ☑ No Management VPI/VCIs are defined on the port.

To delete a logical port, select the port from the list on the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15) and choose Delete.

8

Configuring Trunks

A Cascade trunk provides the means for two Cascade switches to pass data to each other and exchange internal control messages such as OSPF, SNMP, and others. This chapter describes how to configure a Cascade trunk. In addition, the following sections describe how you can manage trunk traffic:

- "About Administrative Cost" on page 8-2 describes how to configure trunk parameters to route circuits over the trunk with lowest administrative cost.
- "About Link Trunk Protocol" on page 8-3 describes how to configure keep alive (KA) control frames.
- "About Virtual Private Networks (VPNs)" on page 8-5 describes how to dedicate trunks to specific customers to guarantee performance and security.

About Administrative Cost

You can manage trunk traffic by defining the administrative cost for the trunk. Circuits that route data based on administrative cost are created on the path with the lowest administrative cost. You can assign an administrative cost value from 1-65534. The lower the administrative cost of the path, the more likely the path will be chosen when a PVC or SVC routed on administrative cost needs to be created.

The CBX 500 routes circuits based on the routing metric you select for the UNI or NNI logical port endpoint: Admin Cost, CDV (cell delay variation), or End-to-End Delay. Refer to page 7-56 for more information.

The switch manages circuits as follows:

- When you first define a circuit, the circuit looks for a path that has enough available virtual bandwidth to handle the circuit's effective bandwidth.
- If the circuit finds more than one path with enough available virtual bandwidth, the circuit chooses the path with the lowest administrative cost. This assumes that administrative cost is the designated routing metric. For the UNI or NNI logical port endpoint, if you designate CDV or end-to-end delay as the routing metric, the circuit chooses the trunk(s) with the lowest CDV or end-to-end delay.
- If there is more than one path with the same administrative cost (or other designated routing metric), the circuit remains in an inactive state until bandwidth becomes available.

The CBX 500 automatically reroutes circuits around a failed trunk or switch. If a circuit cannot find a path with sufficient bandwidth, the circuit remains in an inactive state until the bandwidth becomes available.

To establish a PVC, the switch establishes the circuit in the direction of higher numbered node to lower numbered node. If the PVC is on the same switch, the switch establishes the circuit in the direction of higher numbered slot (or port) to lower numbered slot (or port). In cases where the logical port endpoints use different routing metrics (not recommended), the PVC uses the routing metric that is associated with the higher numbered element.

About Link Trunk Protocol

Using Link Trunk Protocol (LTP), switches communicate by exchanging keep alive (KA) control frames. Switches send KA requests at regular time intervals (one per second). After a switch receives a KA request, it returns a KA reply. A completed transaction consists of a KA request and a KA reply. The request and reply frame formats are identical.

Trunk Delay

Figure 8-1 illustrates the process of keep alive frames used to measure trunk delay. When Switch A sends a KA request to Switch B, a time stamp is put into the KA request frame. When Switch B receives the KA request, it sends a KA reply to Switch A. Switch A receives the KA reply and calculates the round-trip delay from Switch A to Switch B.

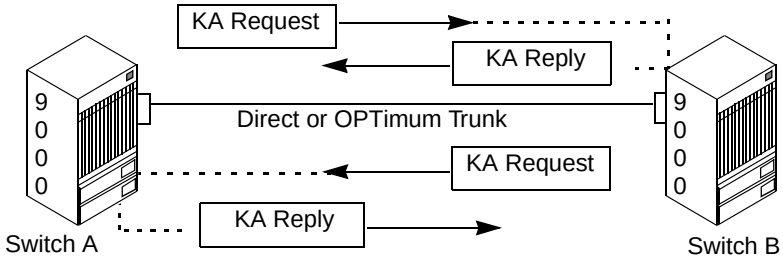


Figure 8-1. Trunk Delay - OSPF Metric and Keep Alive Messaging

Keep Alive Threshold

The Keep Alive Threshold field in the Set All Trunks dialog box represents the number of retries that the trunk protocol attempts before bringing the trunk down. The retry interval is represented in seconds. You can set the keep-alive threshold value between 3 and 255 seconds. The default is 5 seconds.

Static and Dynamic Delay

The Static and Dynamic Delay fields in the Set All Trunks dialog box represent the measured one-way delay in units of 100 microseconds. The static delay is measured upon trunk initialization and is updated only 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 as a means of allowing users to route circuits over trunks with the lowest end-to-end delay.

The dynamic delay is measured 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.

If you use the Set All Trunks dialog box (Figure 8-2 on page 8-6) to view attributes for a selected trunk, and notice that the static and dynamic delay values do not match, you can modify the static delay value to match the dynamic delay. To do this:

1. Choose Modify to access the Modify Trunk dialog box (this is similar to Figure 8-4 on page 8-14).
2. Edit the static delay value.
3. Choose OK to accept the change.

If the trunk reinitializes for any reason, the static delay value you inserted when you modified the trunk is automatically be replaced by whatever static delay value is measured at the time the trunk reinitialized.

About Virtual Private Networks (VPNs)

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

Use the following sequence to configure a trunk for a VPN:

Step 1. Create the VPN (refer to page 4-19).

Step 2. Add customers to a specific VPN (page 4-20).

Step 3. For SVC traffic, specify the net overflow parameter (page 7-27) and dedicate the SVC logical port endpoint to a specific VPN and customer (page 7-37).

Step 4. For PVC traffic, specify the net overflow parameter (page 9-19) and dedicate the PVC to a specific VPN and customer (page 9-24).

Step 5. Specify the trunk parameters (refer to page 8-15).

Accessing Trunk Functions

To access the Set All Trunks dialog box, from the Administer menu, select Cascade Parameters ⇒ Set All Trunks.

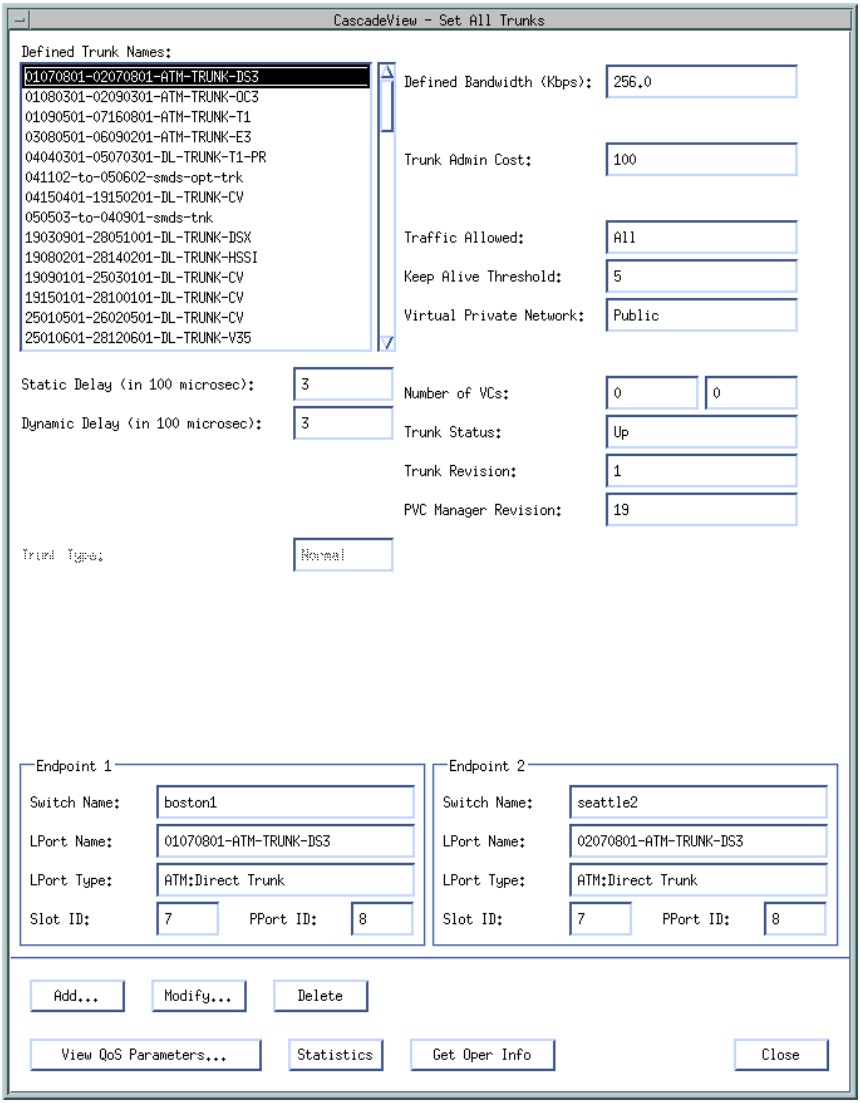


Figure 8-2. Set All Trunks Dialog Box

The Set All Trunks Dialog Box

The Set All Trunks dialog box displays information about the configured options for the trunk you select in the Defined Trunk Names list.

Table 8-1 describes these dialog box status fields and commands.

Table 8-1. Set All Trunks Dialog Box Status Fields and Commands

Field/Command Button	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 "About Administrative Cost" on page 8-2.
Allowed Traffic	Displays one of the following options, which designates the type of traffic allowed on this trunk: *All* – Trunk can carry SVC, PVC, and network management traffic. *Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & Address Restricted* – Trunk can carry PVCs and network management traffic. This trunk does not support SVC addressing information. If this is the only trunk between two nodes and these nodes cannot pass addressing information over other network trunks, then this mode effectively prevents SVCs from traversing this trunk.

Table 8-1. Set All Trunks Dialog Box Status Fields and Commands (Continued)

Field/Command Button	Description
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.
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: *Unknown* – The NMS cannot communicate with one or both switch endpoints that make up this trunk. *Down* – The switches cannot establish a communication link. *Attempt* – A switch is attempting to contact another switch but has not yet received a response. *Init* – A one-way communication exists between the two switches. *Two-way* – A bi-directional communication exists between the two switches. *Exchange Start* – The two switches are about to exchange the network topology. *Exchange* – The two switches are exchanging network topology. *Loading* – The two switches are requesting the most recent link state information. *Up* – The trunk is up and operational between the two switches.

Table 8-1. Set All Trunks Dialog Box Status Fields and Commands (Continued)

Field/Command Button	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 8-1. Set All Trunks Dialog Box Status Fields and Commands (Continued)

Field/Command Button	Description
Add	Defines a new trunk.
Modify	Modifies a trunk definition.
Delete	Deletes a trunk.
View QoS Parameters	Displays the Show Logical Port QoS Parameters dialog box for each logical port endpoint of the trunk. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
Statistics	Displays the summary statistics for the selected trunk. For more information, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*. ***Note:*** *Trunk statistics are not available for CBX 500 OPTimum trunks.*
Get Oper Info	Displays the status of the selected trunk. A message appears in the Trunk Status field. Refer to page 8-8 for a description of these messages.
Close	Exits the Set All Trunks dialog box.

Before You Begin

Before you define a trunk connection, verify that the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Add switch objects to the map (page 4-14)
- ☑ Specify the attributes for these switches (page 5-9)
- ☑ Configure the NMS path information for all NMS workstations that need access to the switches (page 5-21)
- ☑ Configure the I/O modules and physical ports on which the logical ports for the trunk will reside (Chapter 6)
- ☑ Configure the logical ports on which the trunk will reside (Chapter 7)

Defining a Trunk

The Set All Trunks function specifies the two endpoints for the Cascade-to-Cascade switch trunk line. When you configure a trunk, you select endpoints that use the same logical port type (such as ATM:Direct Trunk) and the same bandwidth.

The trunk definition is a three-step sequence:

Step 1. Configure a trunk logical port type. Refer to "Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports" on page 7-50.

Step 2. Define a trunk configuration between the two switches. Refer to page 8-11.

Step 3. Create a trunk line connection on the network map to represent the trunk. Refer to page 8-16.

To define a trunk between two Cascade switches:

1. Refer to "Accessing Trunk Functions" on page 8-6 for instructions on accessing the Set All Trunks dialog box (Figure 8-2 on page 8-6).

2. Choose Add. The following dialog box appears.

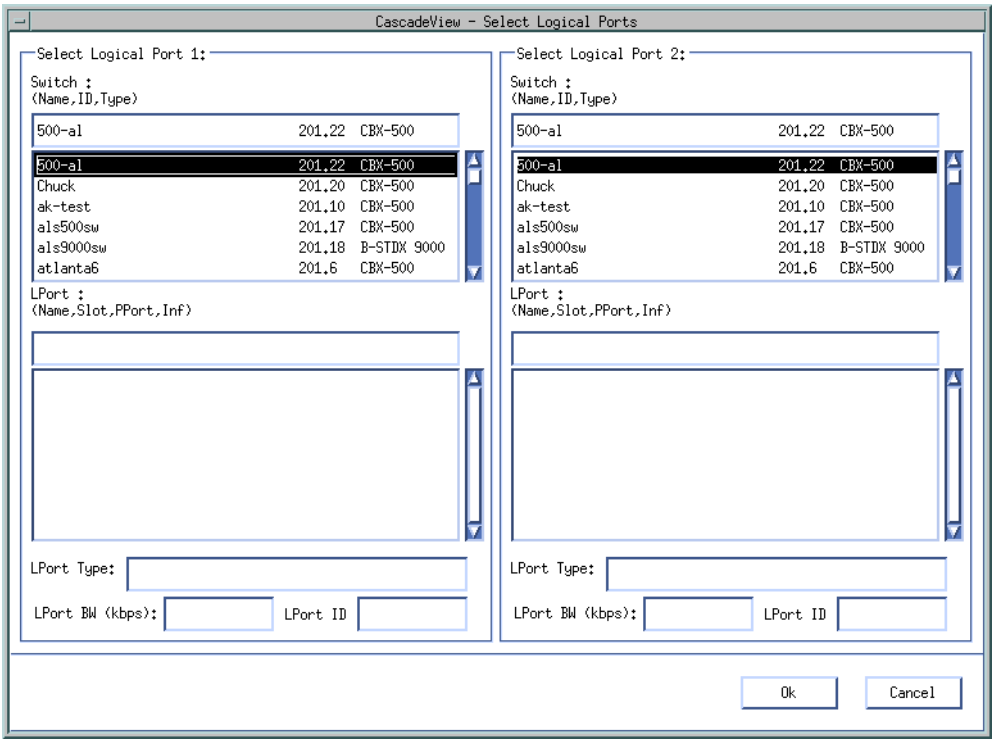


Figure 8-3. Select Logical Ports Dialog Box

3. Provide the following information for both Logical Port 1 and Logical Port 2:

   a. Select the name of the switch where logical port 1 resides, then select the name of the switch where logical port 2 resides. You can create a trunk between either two CBX 500 switches or a CBX 500 and B-STDX switch.

   b. Select the name of logical port 1, then select the name of logical port 2.

   c. Review the LPort Type field. Both endpoints must use the same logical port type. The CBX 500 supports both ATM:Direct Trunk and ATM:OPTimum Cell Trunk configurations.

When you configure an OPTimum trunk or virtual UNI between two endpoints, the logical ports must match the VPI of the VPC that provides the connectivity between the two switches. The VPI range for the VPI/VCI valid bits setting for each endpoint must accommodate this VPI.

   d. Review the LPort BW field. The bandwidth for each logical port endpoint must be the same.

4. Choose OK. The Add Trunk dialog box appears, displaying the parameters for both logical ports in the trunk configuration.

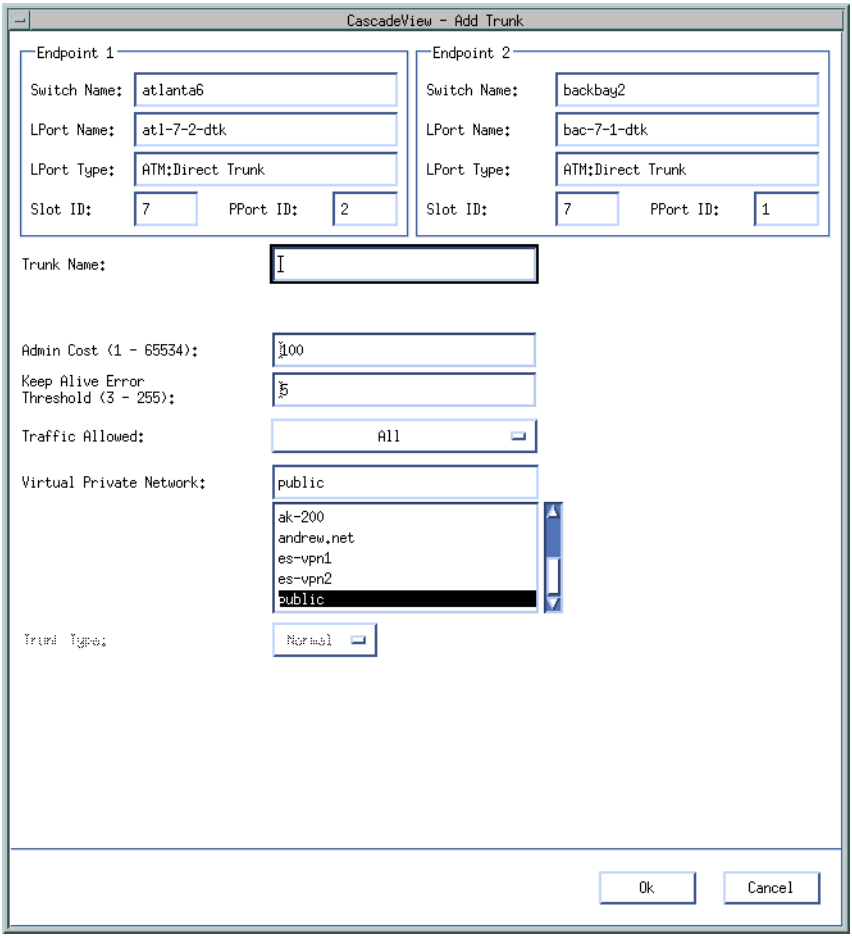


Figure 8-4. Add Trunk Dialog Box

5. Use Table 8-2 to complete the Add Trunk dialog box. If you are creating a trunk between a B-STDX and CBX 500 and have questions about B-STDX features (such as trunk backup), refer to the *Network Configuration Guide for B-STDX/STDX*.

Table 8-2. Add Trunk Dialog Box Fields

Field	Action/Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk.
Admin Cost	Enter a value (from 1 - 65534) that defines the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch. For guidelines, refer to "About Administrative Cost" on page 8-2.
Keep Alive Error Threshold	Enter a value between 3 and 255 seconds to define the keep alive threshold. The default is 5 seconds. Service is disrupted if you modify this value once the trunk is online. For more information about this parameter, refer to page 8-4.
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – Trunk can carry SVC, PVC, and network management traffic. *Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & Address Restricted* – Trunk can carry PVCs and network management traffic. This type of 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.
Virtual Private Network	Select a VPN name. The default is Public. For more information about VPNs, refer to page 8-5.

6. When you finish defining the trunk attributes, choose OK to complete the trunk configuration. Choose Close to return to the network map.

Continue with the next section to create the trunk line connection.

Creating a Trunk Line Connection

After you define the trunk configuration between two switches, you can create the trunk line connection on the network map. The Add Connection function enables you to draw a line to connect the two switches on the network map.

To add a trunk line connection:

1. From the Edit menu, select Add Connection. The following dialog box appears.

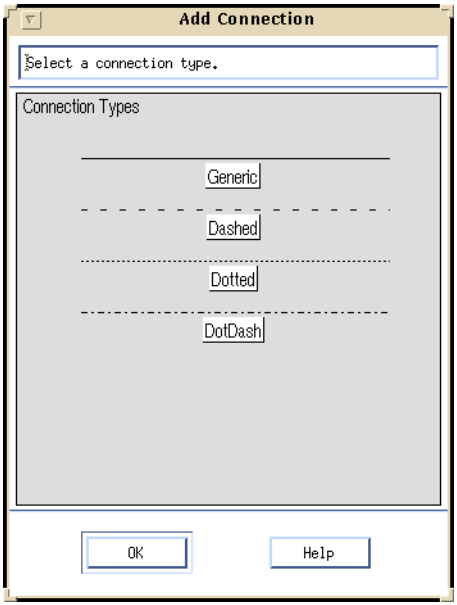


Figure 8-5. Add Connection Dialog Box

2. Select a connection symbol from the palette.
3. With the Add Connection dialog box open, create a trunk line between the two Cascade switches on the network map by clicking on the first switch object (source symbol) and then the second switch object (destination symbol).
4. The following dialog box appears.

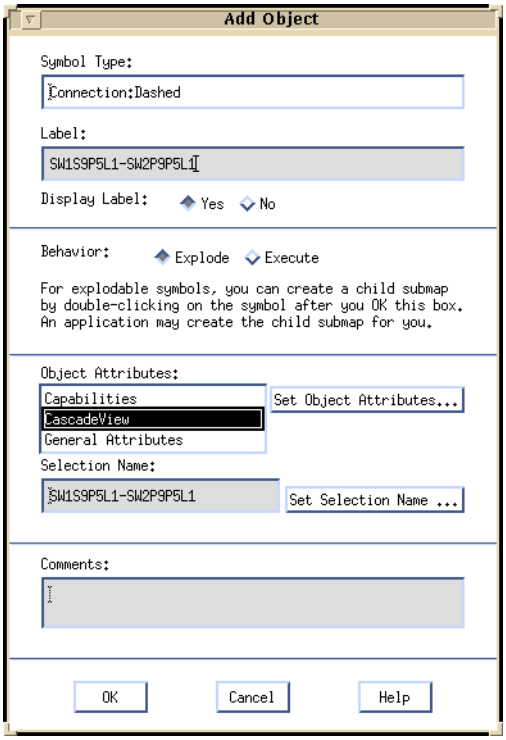


Figure 8-6. Add Object Dialog Box

5. Complete the Add Object dialog box fields as follows:

   Symbol Type — Displays the type of connection you are adding to the network map.

   Label — Enter the trunk name you specified on the Add Trunk dialog box.

   Display Label — Select Yes to have the label (name) appear beneath the switch object on the network map. Select No if you do not want the label to appear on the map.

   Behavior — Select Explode to create the basic CascadeView network configuration. Refer to the *HP OpenView User's Guide* for more information about the Execute function.

Object Attributes — Select CascadeView. Then choose Set Object Attributes. The following dialog box appears.

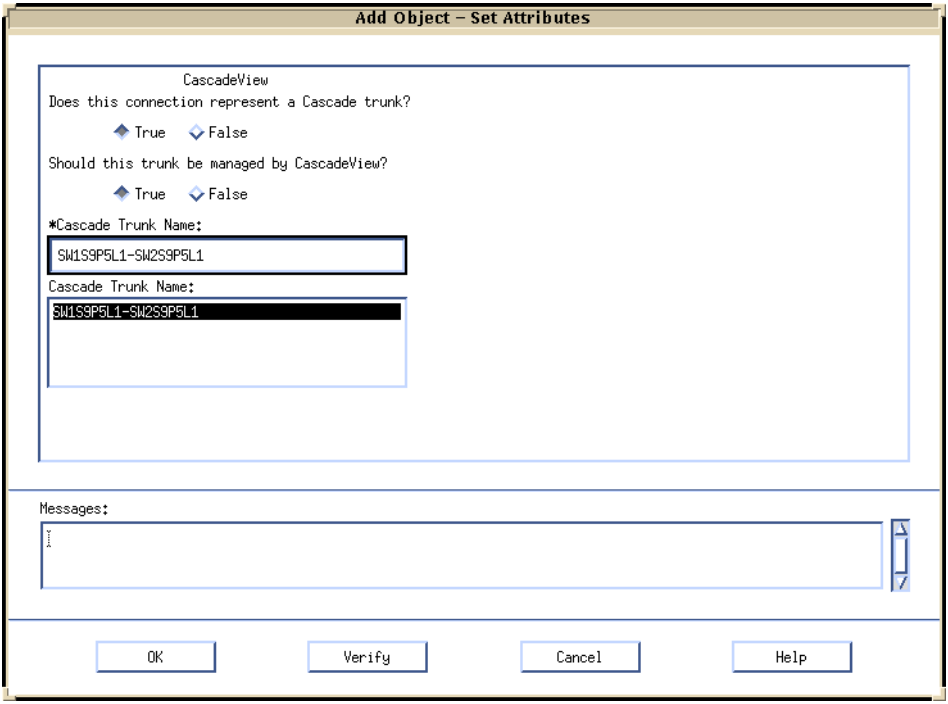


Figure 8-7. Add Object - Set Attributes Dialog Box

6. Complete the Add Object – Set Attributes dialog box fields as follows:

   Does this connection represent a Cascade Trunk? — Select True.

   Should this trunk be managed by CascadeView? — Select True.

   Cascade Trunk Name — Select the trunk name from the Cascade Trunk Name list. The selected trunk name appears in the *Cascade Trunk Name field.

7. Choose Verify to confirm your selections and then choose OK to return to the Add Object dialog box.

8. Choose OK to return to Add Connection dialog box. Then choose OK to return to the network map. A trunk line appears between the two switches on the map.

9

Configuring PVCs

This chapter describes how to configure the following types of Permanent Virtual Circuits (PVCs):

- Point-to-Point
- Point-to-Multipoint
- Management PVC
- Management VPI/VCI

In addition, this chapter provides information on ATM traffic descriptors. This chapter explains how to manually define PVCs and use the Move Circuit function.

About ATM Traffic Descriptors

This section describes network traffic parameters and their associated ATM traffic descriptor combinations. When you create either a PVC or a point-to-multipoint circuit, you select one of several traffic descriptor combinations. The traffic descriptor combination specifies which traffic parameters are used for traffic control. It also determines the number and type of cells that are admitted into a congested queue, and whether or not high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds.

Table 9-1 describes the traffic parameters, the traffic descriptor combinations, and their impact on cell traffic.

Table 9-1. Traffic Parameter Descriptions

Traffic Parameter	Description
CLP=0	Specifies the high-priority cell stream (cells whose Cell Loss Priority bit is set to 0).
CLP=1	Specifies the low-priority cell stream (cells whose Cell Loss Priority bit is set to 1).
CLP=0+1	Specifies the aggregate cell stream (all cells in this circuit whose Cell Loss Priority bit is either 0 or 1).
PCR (Peak Cell Rate)	Peak Cell Rate is the maximum allowed cell transmission rate (expressed in cells per second). It defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
SCR (Sustained Cell Rate)	Sustained Cell Rate is the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. It allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR traffic; it does not apply to CBR or UBR/ABR traffic.

Table 9-1. Traffic Parameter Descriptions (Continued)

Traffic Parameter	Description
MBS (Maximum Burst Size)	Maximum Burst Size is the maximum number of cells that can be received at the Peak Cell Rate. This allows a burst of cells to arrive at a rate higher than the SCR. If the burst is larger than anticipated, the additional cells are either tagged or dropped. This parameter applies only to VBR traffic; it does not apply to the CBR or UBR traffic.
Tagging	Tagging refers to the method of changing a high-priority cell (CLP=0) to a low-priority cell (CLP=1), as opposed to simply dropping the cells from cell stream, when the CLP=0 cell stream is non-conforming.
Best Effort	This option means that the network attempts to deliver traffic that exceeds the limits of the traffic contract. However, there are no guarantees that traffic will be delivered.

When you choose the Forward (or Reverse) Traffic Descriptor combination, select the combination that best describes the traffic characteristics of the circuit. The UPC function uses the traffic parameters to determine the conforming cells of an ATM connection, based on the threshold values for PCR, SCR, and MBS as specified in the service contract. If a traffic descriptor combination is not valid for the service class specified in the Forward (or Reverse) QoS class field, you cannot select it.

For more information on how each traffic descriptor combination affects the cell streams under different traffic conditions, refer to Appendix D.

Accessing the Set All PVCs On Map Dialog Box

The Set All PVCs On Map dialog box displays status information for the circuit you select from the Defined Circuit Name list. To access this dialog box, from the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Point.

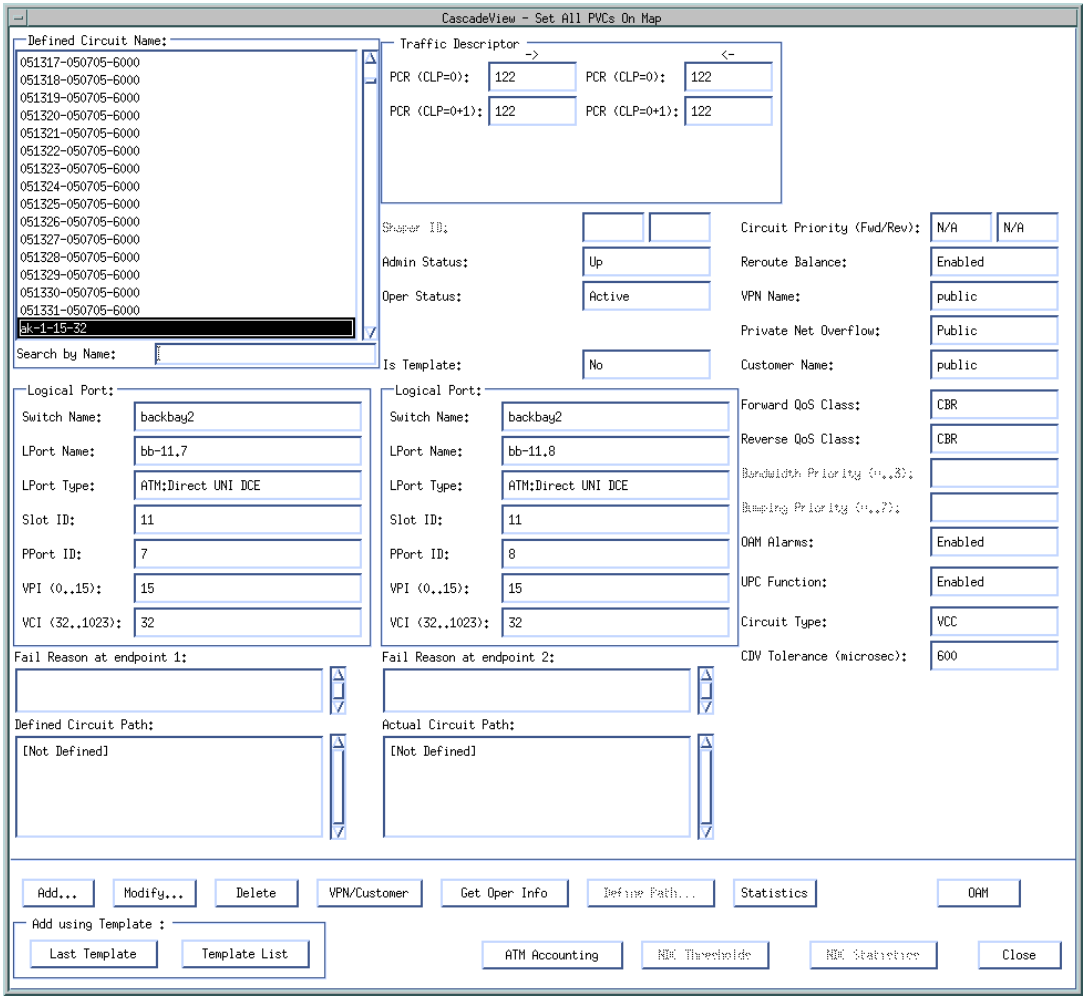


Figure 9-1. Set All PVCs On Map Dialog Box

To view a list of configured circuits, position the cursor in the Search by Name field and press Return. To use a wildcard search to find a specific circuit name, you can

- 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 \\

The Set All PVCs On Map Dialog Box

The Set All PVCs On Map dialog box displays information about the configured options for the circuit name you select. Table 9-2 describes these dialog box status fields and commands.

Table 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands

Field/Command	Description
Defined Circuit Name	Displays a listing of the circuits configured in the network. Use a wildcard search to find a specific circuit name.
Traffic Descriptor	Specifies the settings for forward and reverse traffic, where forward traffic is traffic from Endpoint 1 to Endpoint 2 (→), and reverse traffic is from Endpoint 2 to Endpoint 1 (←). For information on traffic descriptor combinations and parameters, refer to page 9-2.
Admin Status	Displays whether the selected circuit is online (Up) or offline (Down).

Table 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands (Continued)

Field/Command	Description
Oper Status	Displays the current operational status of the selected circuit. Messages include: *Active* – The circuit is operational through the network end-to-end. *Inactive* – The circuit is not operational. Check the Reason field for possible reasons. *Unknown* – The NMS cannot reach the higher numbered node for status. (If the circuit is an intra-switch PVC, then the NMS cannot reach the highest numbered LPort.) *Invalid* – The circuit definition is not found in the higher-numbered node. You may need to return to the Set Circuits dialog box and choose Apply to save the circuit definition.
Is Template	Displays Yes if you can use this circuit as a template to create other circuits using similar parameters.
Circuit Priority	Displays the values used to control both forward and reverse circuit priority for VBR-RT and VBR-NRT circuits. The following list specifies the possible values: 1 = high priority 2 = medium priority 3 = low priority (lowest VBR-NRT priority) 4 = lowest priority (lowest VBR-RT priority)
Reroute Balance	When enabled, the PVC conforms to the configured reroute tuning parameters (refer to page 5-16). This means that when the PVC reroutes during trunk failure, it will migrate back to the original trunk at a rate and time determined by the configured reroute tuning parameters.

Table 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands (Continued)

Field/Command	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. For a description of the QoS classes, refer to page 7-54.
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.* For information about UPC traffic parameters, refer to "About ATM Traffic Descriptors" on page 9-2.
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 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands (Continued)

Field/Command	Description
Logical Port	The dialog box displays the following logical port information for each circuit endpoint: *Switch Name* – Displays the name of the switch at each endpoint of the circuit. *LPort Name* – Displays the name of the logical port at each endpoint of the circuit. *LPort Type* – Displays the configured type of the selected logical port. *Slot ID* – Indicates the physical slot number where the I/O module containing the selected port is installed. *PPort ID* – Displays the ID number of the physical port for which the selected logical port is configured. *VPI (0..nnnn)* – Displays the VPI for the selected circuit at this endpoint. *VCI (32..nnnn)* – Displays the VCI for the selected circuit at this endpoint. For more information on the Valid Bits in VPI/VCI fields, refer to page 7-4.
Fail Reason at endpoint 1 (2)	Displays the reason a selected circuit failed (if any) for a given endpoint. Refer to the *Diagnostic and Troubleshooting Guide for CBX 500* for a description of these fail reasons.
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.
Add	Adds a new PVC.

Table 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands (Continued)

Field/Command	Description
Modify	Modifies the selected circuit. The Modify command displays dialog boxes that are similar to those displayed for Add circuit; however, you cannot modify the circuit name, logical port endpoints, circuit type, or VPI/VCI values from this dialog box.
Delete	Deletes the selected circuit.
VPN/Customer	Assigns the selected circuit to a specific VPN and customer name.
Get Oper Info	Displays the current operational status of the selected circuit in the Oper Status field. Refer to page 9-6 for an explanation of these status messages.
Defined Path	Manually defines a circuit path (refer to page 9-26).
Statistics	Displays the summary statistics for the selected circuit. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
OAM	Runs the Operations, Administration, and Management loopback diagnostics for the selected circuit. For more information about these diagnostics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
Add using Template	If you have already defined a circuit configuration and saved it as a template, use this command to define a new circuit using similar parameters. • Choose Last Template to use the last template you used to establish a circuit in this NMS session. • Choose Template List to display a list of templates previously defined for this map.
ATM Accounting	Accesses the ATM accounting functions for a PVC. For more information, refer to the *Accounting System Administrator's Guide*.

Table 9-2. Set All PVCs On Map Dialog Box Status Fields and Commands (Continued)

Field/Command	Description
NDC Thresholds	Displays the configured network data collection (NDC) thresholds for the selected circuit. For more information about these thresholds, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
NDC Statistics	Displays the NDC statistics for the selected circuit. For more information about NDC statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500.*
Close	Exits this dialog box and return to the network map.

Before You Begin

Before you configure a PVC, verify that the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Add the switch object(s) to the map (page 4-14)
- ☑ Specify the attributes for the switch (page 5-9)
- ☑ Configure the IP address of all NMS workstations that need access to the switch (page 5-20)
- ☑ Configure the I/O modules (IOMs) and physical ports on which the PVC's logical ports will reside (Chapter 6)
- ☑ Configure the logical ports on which to define the PVC (Chapter 7)

Defining a PVC

This section describes some of the concepts and information you need to know when defining PVCs, including:

- Using Virtual Private Networks for Circuit Traffic
- Setting VPI/VCI Values for PVCs
- Using the Set Attributes Menu

Using Virtual Private Networks for Circuit Traffic

Virtual Private Networks (VPNs) enable network providers to have dedicated network resources for those customers who require guaranteed performance, reliability, and privacy. For PVC traffic, you dedicate circuits to a specific VPN and customer. You specify the net overflow parameters that determine whether these PVCs are restricted to trunks of their own VPN or use public (shared) trunks during overflow or failure conditions.

The logical port endpoints you use to configure a PVC do not have to belong to the same VPN or customer ID. How you set the net overflow parameter for the PVCs logical port endpoints does not effect this PVC.

Using the VPN/Customer View Function

When you need to create PVCs for a specific VPN or customer, use the Select Customer/VPN function. This function allows you to enable a network map view for a specific VPN or customer. As you configure logical ports, use the instructions on page 7-37 to assign the port to a VPN or customer. When you create PVCs, the Select End Logical Ports dialog box (Figure 9-3 on page 9-15) only displays the logical ports that belong to the VPN or customer you select.

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
```

These lines disable the Administer menu and all its provisioning functions; the NMS user only sees the Monitor menu functions.

To use VPN/Customer view:

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

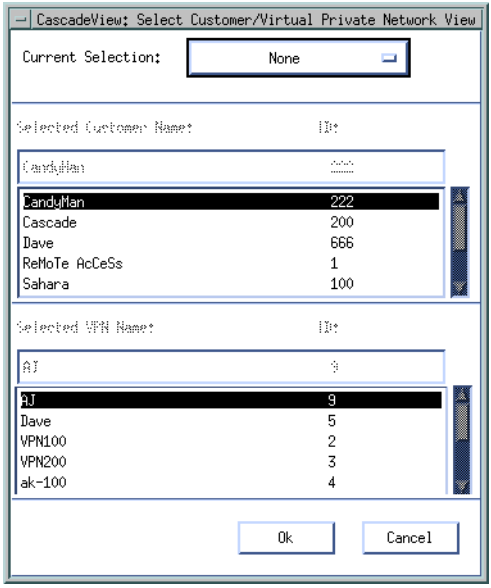


Figure 9-2. Select Customer/Virtual Private Network Dialog Box

2. Use the Current Selection button to select either Customer or VPN. Use None (default) to disable VPN/Customer view.

With the VPN/Customer view disabled, you can configure PVCs using logical port endpoints that belong to any VPN or customer.

3. Depending on the option you select, review either the Selected Customer Name or Selected VPN Name list.
4. Select the Customer or VPN name.
5. Choose OK.

Setting the VPI/VCI Values for PVCs

For each PVC you configure, you must specify a value from 0-*nnnn* to represent the Virtual Path Identifier (VPI) for the PVC circuit (refer to page 9-18). The maximum value is based on the Valid Bits in VPI that is configured for the logical port, as follows:

Maximum value = $2^P - 1$

where *P* is the value in the Valid Bits in VPI field. For example, if you entered 5 in the Valid Bits in VPI field, the maximum value is 31 ($2^5 - 1 = 31$) which would give you up to 32 virtual paths (numbered 0-31). Refer to page 7-4 for details on setting the Valid Bits in VPI.

If you are defining a Virtual Channel Connection (VCC), you must also specify a value to represent the Virtual Channel Identifier (VCI) for an ATM circuit (refer to page 9-18). The maximum value is based on the Valid Bits in VCI value that is configured for the logical port, as follows:

Maximum value = $2^C - 1$

where C is the value in the Valid Bits in VCI field. For example, if you entered 6 in the Valid Bits in VCI field, the maximum VCI value you can enter is 63 (which would give you 32 virtual channels, numbered 32 to 63).

These VPI/VCI range restrictions only apply to VCCs. You can provision VPCs to any value in the VPI=0-255 range. In addition, if the logical port uses the NNI cell header format, you can provision VPCs over the 0 - 4095 range. For more information on the Valid Bits in VPI/VCI fields, refer to Table 7-1 on page 7-6.

The VPI/VCI combination must be unique at each circuit endpoint (including multipoint circuits). As a result, since a VPC has access to all valid VCIs, a VCC or multipoint circuit that uses a VPI already in use by a VPC cannot be established, nor can a VPC be established if the selected VPI is already in use by a VCC or multipoint circuit.

The Set Attributes Menu

When you configure a PVC, the dialog box provides detailed parameters that you need to specify for each endpoint. During this procedure, you use the Set Attributes menu on the Add PVC dialog box to configure the following information:

Administrative — Defines administrative information, such as circuit name, administrative status, and circuit type.

Traffic Type — Defines the traffic descriptor settings for forward and reverse traffic.

User Preference — Defines PVC features that deal with port congestion and traffic policing.

NDC — Defines Network Data Collection (NDC) functions, which can detect any violation of PVC service subscription parameters, and establish trends in network traffic patterns and loads.

Configuring a PVC

You create a PVC between two ATM UNI or NNI logical port endpoints. These ATM logical ports can reside on either a CBX 500 or a B-STDX.

To define a new PVC connection between two logical ports:

1. Refer to page 9-4 for instructions for accessing the Set All PVCs On Map dialog box (Figure 9-1 on page 9-4).
2. From the Set All PVCs On Map dialog box, choose Add. The following dialog box appears.

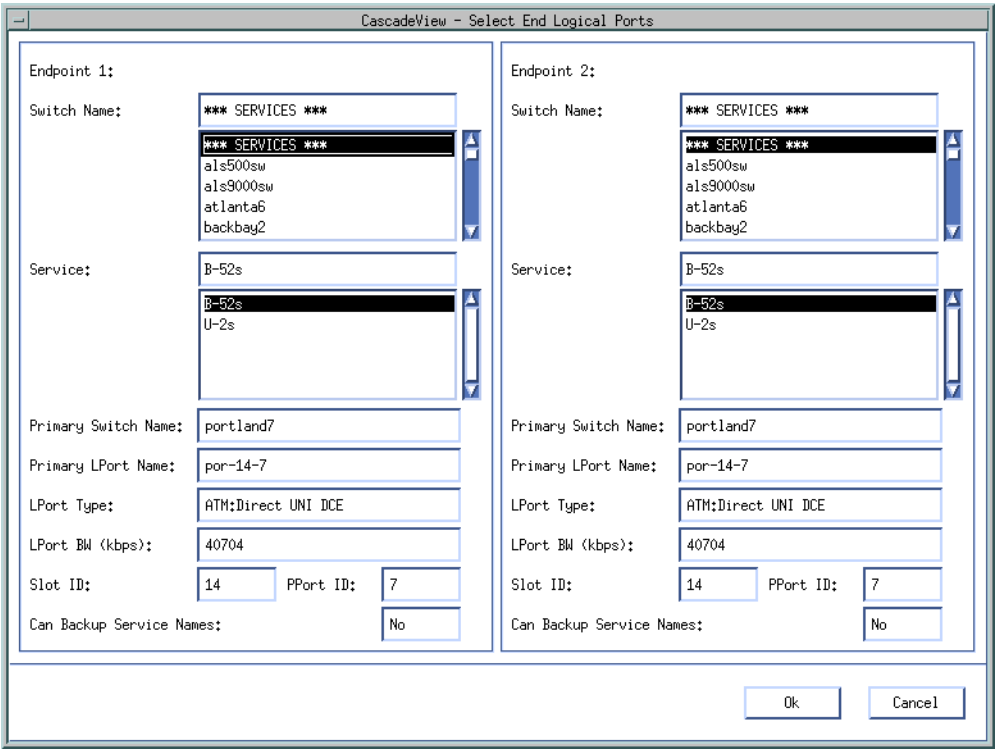


Figure 9-3. Select End Logical Ports Dialog Box

3. Configure Endpoint 1 and Endpoint 2 as follows:

For a Fault Tolerant PVC configuration

a. Choose *** SERVICES *** to configure a fault tolerant PVC.

b. Select a service name from the list. You can only configure a fault tolerant PVC for ATM UNI DCE and UNI DTE logical port types. For more information about fault tolerant PVCs, refer to “Configuring Fault-Tolerant PVCs” on page 7-44.

c. Continue with Step 4.

For a standard circuit configuration

a. Select the name of the switch where Endpoint 1 resides, then select the name of the switch where Endpoint 2 resides. You can create a PVC between either two CBX 500 switches or a CBX 500 and B-STDX switch.

b. Select the name of the logical port for Endpoint 1, then select the name of the logical port for Endpoint 2. Note that if you enable the VPN/Customer view function (refer to page 9-11), only logical ports that belong to the VPN or customer you select appear in this list.

c. Continue with Step 4.

4. The Select End Logical Ports dialog box displays the following information for both Endpoint 1 and Endpoint 2:

   LPort Type — Displays the logical port type for the selected logical ports.

   LPort Bandwidth — Displays the logical port bandwidth for the selected logical ports. At each endpoint, logical ports may have different bandwidth.

   Slot ID — Displays the I/O slot (number) where the IOMs for the selected logical ports reside.

   PPort ID — Displays the port ID numbers for the selected logical ports.

5. Choose OK. The following dialog box appears.

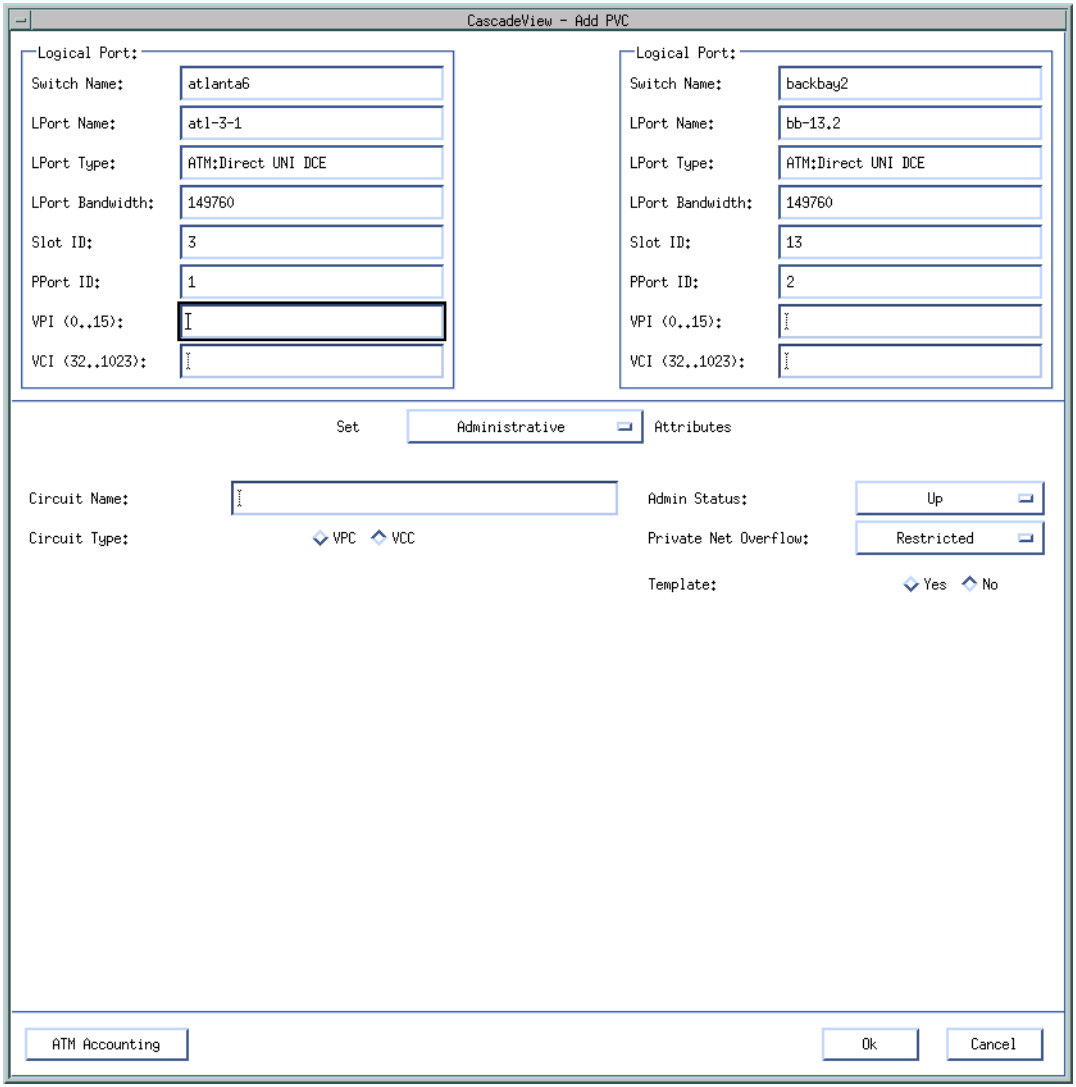


Figure 9-4. Add PVC Dialog Box

6. Define the following parameters for each of the circuit's two endpoints. If you are configuring a PVC between a CBX 500 and a B-STDX and have questions about B-STDX features (i.e., priority routing), refer to Chapter 11 of the *Network Configuration Guide for B-STDX/STDX*.

   VPI (0 .. nnn) — Enter a value from 0-*nnnn* to represent the Virtual Path Identifier for the PVC. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. Refer to page 9-13 for information about setting this value.

   VCI (32..nnnn) — (*for VCCs only*) Depending on the circuit configuration, enter a value to represent the Virtual Channel Identifier for an ATM PVC. Refer to page 9-13 for information about setting this value.

Administrative Attributes

Use the Set [Administrative] Attributes option to configure the fields defined in Table 9-3.

Table 9-3. Set Administrative Attributes Fields

Field	Action/Description
Circuit Name	Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the circuit at switch startup, or Down if you do not want to activate the circuit at switch startup.
Circuit Type	Specify whether the circuit is a Virtual Path Connection (VPC) or Virtual Channel Connection (VCC, the default). If you select VPC, the VCI field is set to 0 and cannot be changed.

Table 9-3. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Private Net Overflow	Determines whether this PVC is restricted to trunks of its own VPN or can use public (shared) trunks during overflow conditions. To configure this circuit for a specific VPN and customer, refer to page 9-24. For more information about VPNs, refer to page 9-11. Select one of the following options: *Public – (Default)* PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restrict* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template *(Optional)*	You can save these settings as a template to configure another PVC with similar options. To create a template, choose Yes in the "Is Template" field.

Traffic Type Attributes

Choose the Set [Traffic Type] Attributes option to specify Traffic Descriptor settings for forward and reverse traffic.

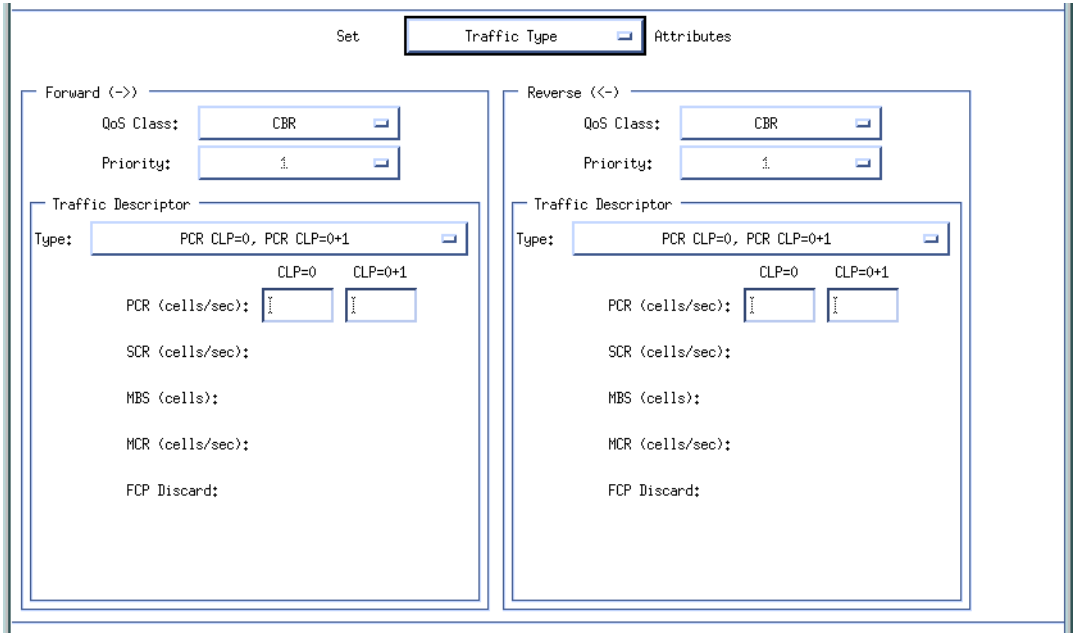


Figure 9-5. Set Traffic Type Attributes

For more information on standard traffic descriptor combinations and parameters, refer to page 9-2. For information about the ABR QoS class, and MCR and FCP Discard traffic parameters, refer to the ATM Flow-Control Processor User's Guide.

Forward traffic is traffic from Endpoint 1 to Endpoint 2, and reverse traffic is from Endpoint 2 to Endpoint 1. Refer to Table 9-4 for details.

Table 9-4. Set Traffic Type Attributes Fields

Field	Action/Description
QoS Class (Fwd/Rev)	Select the Quality of Service class for forward and reverse traffic. The forward and reverse QoS classes do not have to match. For a description of the QoS classes, refer to page 7-12. Note that the QoS class determines which traffic descriptors you can select.
Priority (Fwd/Rev) *(VBR-NRT and VBR-RT QoS classes only)*	Select both the forward and reverse circuit priority, where 1 is high priority, 2 is medium priority, 3 is low priority, and 4 is lowest priority (only available for VBR-RT traffic). The forward and reverse circuit priority values do not have to match.
Traffic Descriptor Type	Select from the following traffic descriptor options: *PCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (i.e., the CLP=0 cell stream). *PCR CLP=0+1 (cells/sec)* – Specify the PCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (i.e., the CLP=0 cell stream). *SCR CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream).

Table 9-4. Set Traffic Type Attributes Fields (Continued)

Field	Action/Description
Traffic Descriptor Type (*continued*)	*MBS CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (i.e., the CLP=0 cell stream). *MBS CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (i.e., the CLP=0+1 cell stream).

User Preference Attributes

Choose the Set [User Preference] Attributes option.

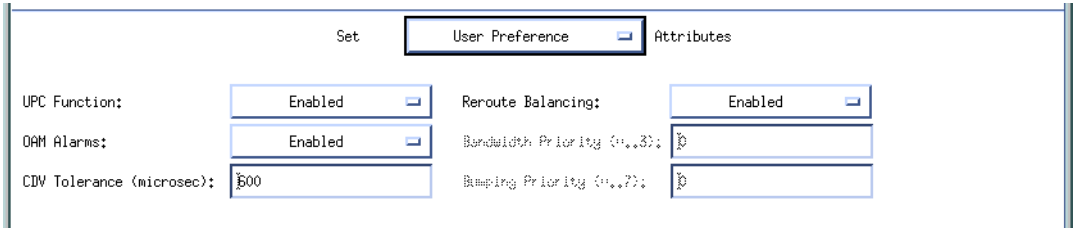


Figure 9-6. Set User Preference Attributes

To configure these fields, refer to Table 9-5. (If you are configuring a PVC between a B-STDX and the CBX 500, refer to the *Network Configuration Guide for B-STDX/STDX* for details on bandwidth and bumping priority.)

Table 9-5. Set User Preference Attributes

Field	Action/Description
UPC Function	Enables (default) or disables the Usage Parameter Control (UPC) function. When you enable UPC, the circuit tags or drops cells that do not conform to the traffic parameters as they come into the port. When you disable UPC, the circuit allows all traffic, including non-conforming traffic, into the port. As a result, when you disable UPC, quality of service is no longer guaranteed for circuits in the network due to the potential for increasing the cell loss ratio because of port congestion. For this reason, *Cascade recommends that you enable the UPC function on all circuits.* For information about UPC traffic parameters, refer to "About ATM Traffic Descriptors" on page 9-2. ***Note:*** *To use the UPC function for individual circuits, verify that the UPC function is enabled for both logical port endpoints on which you will define the circuit. Enabling UPC at the circuit level has no effect if you did not enable UPC at the logical port level. UPC is enabled by default for both logical ports and circuits.*
Reroute Balancing	When enabled (default), the PVC conforms to the configured reroute tuning parameters. This means that when the PVC reroutes during trunk failure, it will migrate back to its original trunk at a rate and time determined by the configured reroute tuning parameters. When disabled, the PVC ignores the switch tuning parameters. For more information, refer to "Defining Circuit Reroute Time Tuning Parameters" on page 5-16.
CDV Tolerance	Configure the Cell Delay Variation Tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. Valid values are between 1 - 65535 µs. The default is 600 µs.
OAM Alarms	Set to Enabled (default) to use OAM alarms on this circuit. Set to Disabled to disable OAM alarms on this circuit. When enabled, the switch sends OAM F5 or F4 AIS (alarm indicator signal) cells out of each UNI logical port endpoint, to indicate that the circuit is down.

Defining Circuit Attributes

Use the following steps to complete the circuit configuration.

1. *(Optional)* To configure Network Data Collection parameters for this circuit, choose the the Set [NDC] Attributes option button. For more information, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
2. *(Optional)* To configure accounting parameters for this circuit, choose the Accounting command button. For more information, refer to the *Accounting System Administrator's Guide.*
3. Choose OK to define the circuit parameters. The Set All PVCs on Map dialog box reappears (Figure 9-1 on page 9-4).
4. (*Optional*) To configure this PVC for a specific VPN and customer, refer to the following section, "Selecting the VPN and Customer Name".
5. To add more PVCs, repeat the steps in "Configuring a PVC" on page 9-14.
6. When you finish, choose Close to return to the network map.

Selecting the VPN and Customer Name

Complete the following sequence before you configure this PVC for a VPN:

Step 1. Create VPN names (refer to page 4-19).

Step 2. Add customers to a specific VPN (page 4-20).

Step 3. For SVC traffic, create a UNI logical port and specify the net overflow parameter (page 7-27). Dedicate the logical port to a specific VPN and customer (page 9-24).

Step 4. Dedicate a trunk to a specific VPN (Chapter 8).

Step 5. Specify the PVC net overflow parameter (page 9-19) and dedicate the PVC to a specific VPN and customer.

To associate this circuit with a specific VPN and customer:

1. From the Set All PVCs on Map dialog box (Figure 9-1 on page 9-4), select the circuit and choose VPN/Customer. The following dialog box appears.

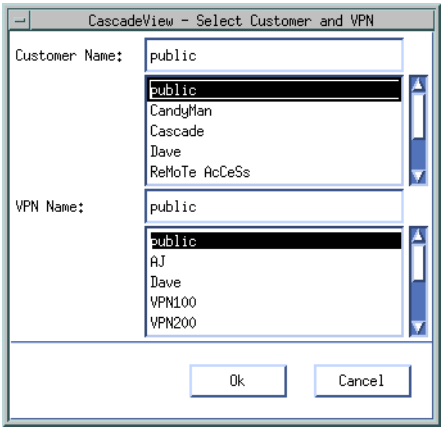


Figure 9-7. Select Customer and VPN Dialog Box

2. Select the customer and VPN name.

3. Choose OK to return to the Set All PVCs on Map dialog box (Figure 9-1 on page 9-4).

Manually Defining the Circuit Path

The Define Path function enables you to manually define a circuit path and the OSPF algorithm's circuit routing decisions. You cannot manually route a circuit that is configured with both endpoints in the same switch.

To manually define the circuit path:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All Circuits on Map dialog box (Figure 9-1 on page 9-4) appears.

2. Select the circuit for which you want to manually define the circuit path. Choose Define Path. The following dialog box appears.

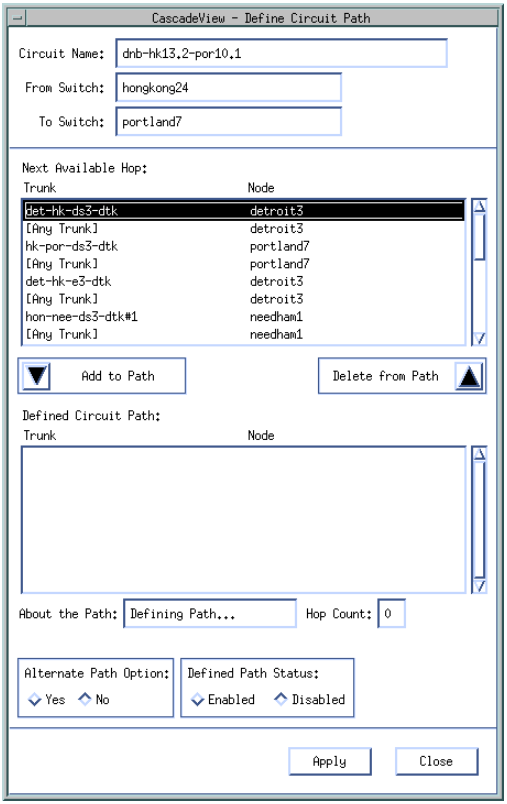


Figure 9-8. Define Circuit Path Dialog Box

3. Complete the dialog box fields as described in Table 9-6.

Table 9-6. Define Circuit Path Fields

Field	Action/Description
Next Available Hop	Displays a listing of the available hops (e.g., trunk-node pairs). • Select the trunk-node pair through which you want to route the circuit. When there are multiple trunks between two nodes, select Any Trunks to cause OSPF to decide which is the best path to use at any given time. • Choose Add to Path. The trunk-node selection is added to the Trunk/Node field, which displays all selected hops.
Alternate Path Option	Select either Yes or No to define whether OSPF should route the circuit if the manual route fails. • Select Yes to enable OSPF to route the circuit based on the best available path. • Select No to disable the circuit from being rerouted; the circuit remains down until the defined path becomes available.
Defined Path Status	Select Enabled to route the circuit based on the manual route defined. Select Disabled to route the circuit based on the network's OSPF algorithm.

4. Choose Apply and then choose OK.

Moving Circuits

The Move Circuit function enables you to move a circuit endpoint defined for one logical port (the source) to another logical port (the destination). If you are upgrading a switch or replacing an IOM and do not want to lose PVC connections, you can use this function to move circuits to another switch or IOM.

This function has the following restrictions:

- You should not move a circuit that is currently in use because it may lose traffic.
- You cannot move a circuit for which you have manually defined a circuit path.
- The VPI/VCI must be unique to the destination logical port.
- The Move Circuit function fails if the number of circuits moved exceeds the maximum allowed for the IOM.

To move a circuit:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Move Circuit Endpoint. The following dialog box appears.

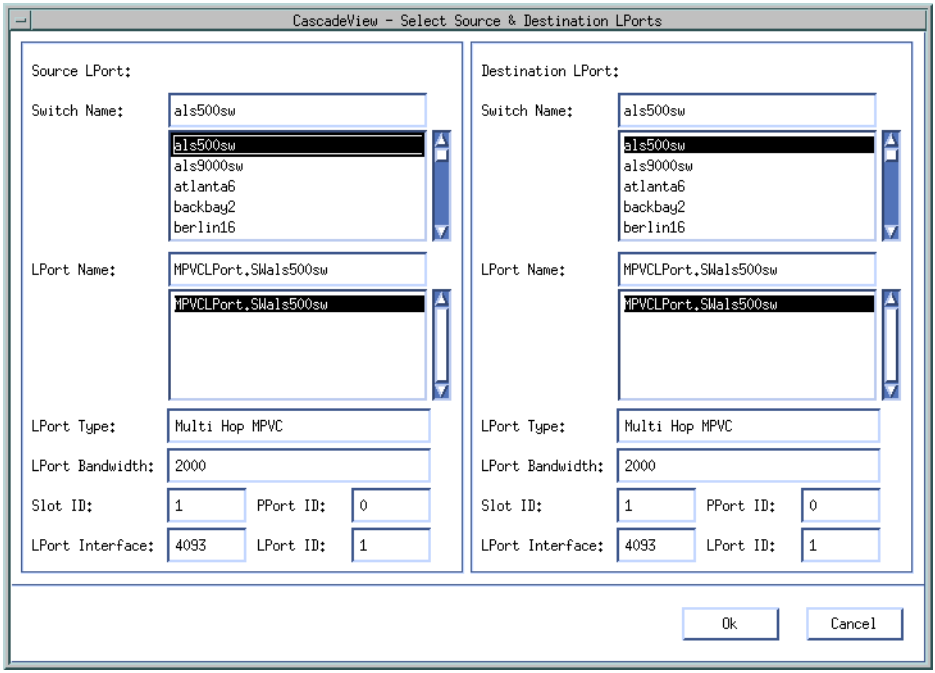


Figure 9-9. Select Source & Destination LPorts Dialog Box

2. To select the Source LPort that contains the circuit you want to move:
   a. Select the Switch Name.
   b. Select the LPort Name.
3. To select the Destination LPort to which you want to move the circuit:
   a. Select the Switch Name.
   b. Select the LPort Name.

4. Choose OK. The following dialog box appears. This dialog box displays the circuits that have the source logical port as an endpoint.

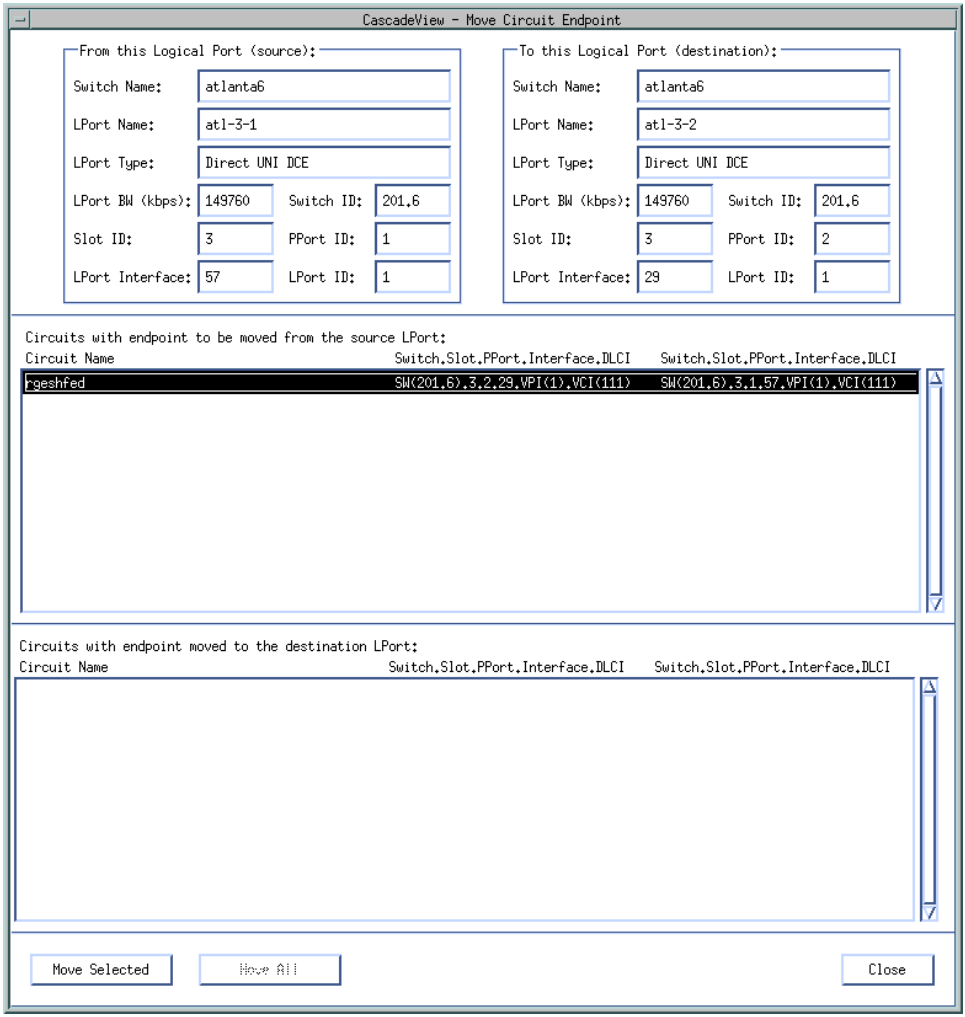


Figure 9-10. Move Circuit Dialog Box

5. From the *Circuits with endpoint to be moved from the source LPort* list, select the circuit(s) you want to move.

6. Choose Move Selected (or Move All to move more than one circuit). The selected circuit appears in the *Circuits with endpoint moved to the destination LPort* list.

7. When you finish, choose Close.

Configuring Point-to-Multipoint Circuits

A point-to-multipoint (PMP) circuit consists of the originating point (circuit root), and endpoints (circuit leafs). The endpoints of a given PMP circuit can be on any switch in the network map, and on any number of switches (that is, the endpoints do not have to terminate on the same switch).

To access the Set All Point-to-Multiple-Point Circuit Roots dialog box, from the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Multipoint Circuits. The following dialog box appears (Figure 9-11 on page 9-32).

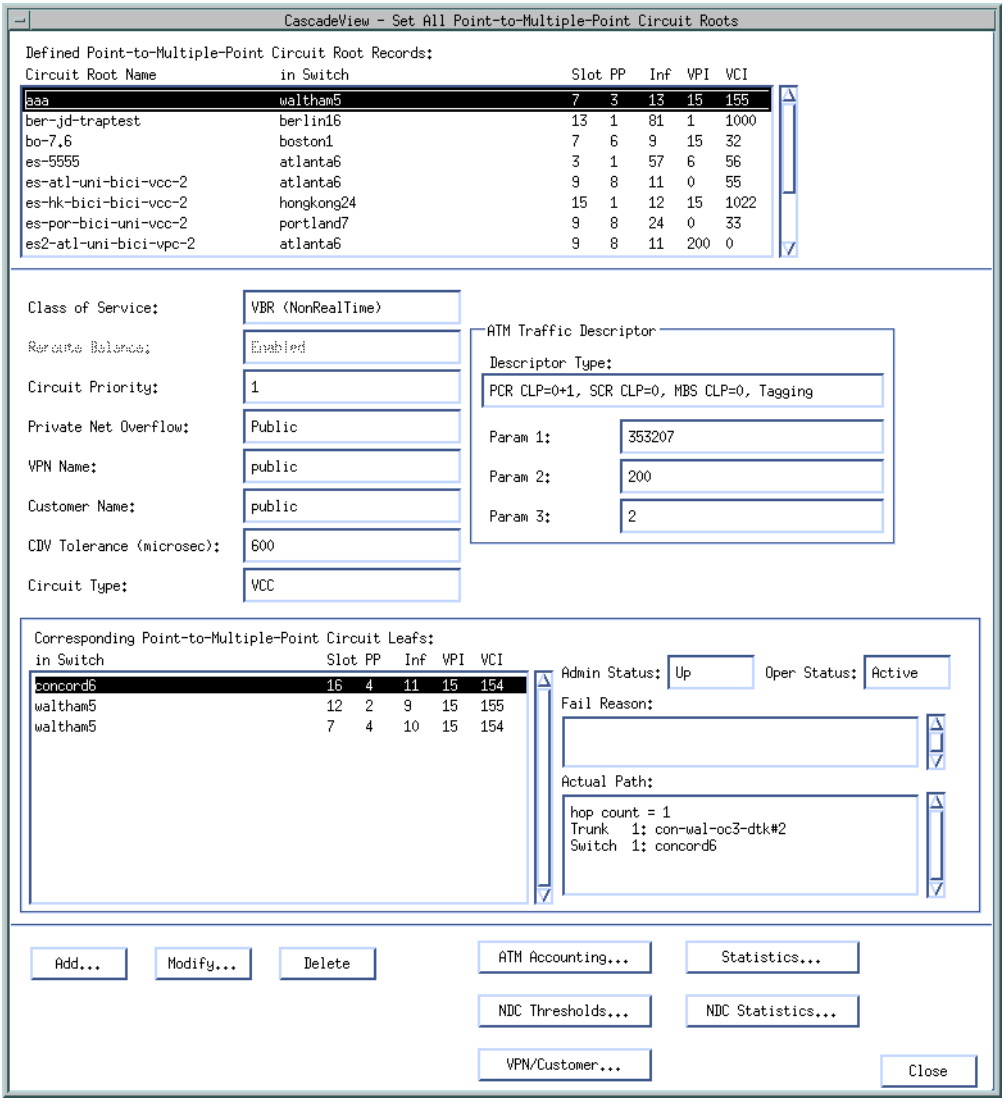


Figure 9-11. Set All Point-to-Multiple-Point Circuit Roots Dialog Box

The *Defined Point-to-Multiple-Point Circuit Root Records* box at the top of the screen lists any existing PMP circuit roots. The *Corresponding Point-to-Multiple-Point Circuit Leafs* box at the bottom of the screen lists any existing circuit leafs (endpoints) for the selected circuit root.

Table 9-7 displays the following information for each root and leaf:

Table 9-7. Set All Point-to-Multipoint Dialog Box Fields and Command Buttons

Field/Command	Action/Description
in Switch	The switch ID and switch name on which the root or leaf resides.
Slot	The physical slot for the IOM on which the root or leaf was created.
PP	The number of the physical port on which the root or leaf was created.
Inf	The MIB interface number for the logical port on which the root or leaf was created.
VPI	The Virtual Path ID of the logical port assigned to the root or leaf.
VCI	The Virtual Channel ID of the logical port assigned to the root or leaf.
Class of Service	Displays the QoS class (CBR, VBR-RT, VBR-NRT, or UBR) for the PMP circuit.
Reroute Balance	Shows whether reroute balancing is Enabled (default) or Disabled for this PMP circuit. Refer to page 9-23 for information about reroute balancing.
Circuit Priority	Displays the priority of the circuit: 1 (High), 2 (Medium), 3 (Low), or 4 (Lowest). Refer to page 9-21 for more information on circuit priority.

Table 9-7. Set All Point-to-Multipoint Dialog Box Fields and Command Buttons (Continued)

Field/Command	Action/Description
Circuit Type	Displays whether the circuit is a VCC (Virtual Channel Connection) or VPC (Virtual Path Connection).
ATM Traffic Descriptor	Displays the circuit's traffic descriptor(s) settings. The number of values displayed depends on the traffic descriptor combination that was selected for the circuit. For example, if you selected the combination PCR CLP=0+1, SCR CLP=0, and MBS CLP=0, three values are displayed: • The first value (Param 1) is the PCR for CLP=0+1 • The second value (Param 2) is the SCR for CLP=0 • The third value (Param 3) is the MBS for CLP=0 If, however, you selected the PCR CLP=0+1 combination, only one value is displayed: the PCR for CLP=0+1.
Add	Adds a new point-to-multipoint circuit.
Modify	Modifies the selected point-to-multipoint circuit root. The Modify command displays dialog boxes that are similar to those displayed for Add point-to-multipoint; however, you cannot modify the circuit name, logical port endpoints, circuit type, or VPI/VCI values from this dialog box.
Delete	Deletes the selected point-to-multipoint circuit root.
ATM Accounting	Accesses the ATM accounting functions for a PVC. For more information, refer to the *Accounting System Administrator's Guide*.

Table 9-7. Set All Point-to-Multipoint Dialog Box Fields and Command Buttons (Continued)

Field/Command	Action/Description
Statistics	Displays the summary statistics for the selected point-to-multipoint circuit. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
NDC Thresholds	Displays the configured network data collection (NDC) thresholds for the selected circuit. For more information about these thresholds, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
NDC Statistics	Displays the NDC statistics for the selected circuit. For more information about NDC statistics, refer to the *Diagnostic and Troubleshooting Guide for CBX 500*.
VPN/Customer	Assigns the selected point-to-multipoint circuit root to a specific VPN and customer name. You must do this before you create PMP circuit leafs.

Defining a Point-to-Multipoint Circuit Root

The following procedure describes how to configure the originating point (circuit root) for a point-to-multipoint circuit.

1. Choose Add. The following dialog box appears.

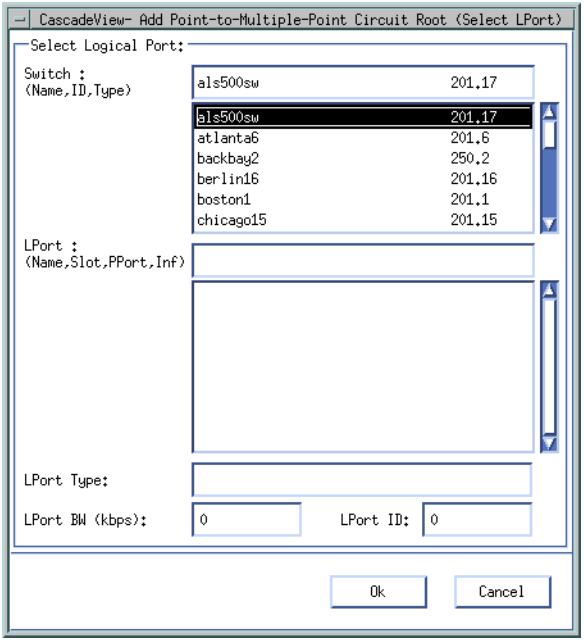


Figure 9-12. Add Point-to-Multiple-Point Circuit Root (Select LPort) Dialog Box

2. In the Switch list box, select the switch on which the originating point of the circuit will reside. The list contains the switch name and switch ID for all switches the NMS can currently access. The selected switch name appears in the text box above the list.

3. In the LPort list box, select the logical port on which the originating point of the circuit will reside. The selected logical port appears in the text box above the list. The list box displays the logical port name, slot ID, physical port number, and MIB interface number (Inf) for all logical ports on the selected switch.

The LPort list box displays following information for the selected port:

LPort Type — Displays the type of logical port.

LPort BW (Kbps) — Displays the total logical port bandwidth for the selected logical port, in kilobits per second (Kbps).

LPort ID — Displays the logical port ID for the selected logical port.

4. Choose OK to display the Add Point-to-Multiple-Point Circuit Root dialog box.

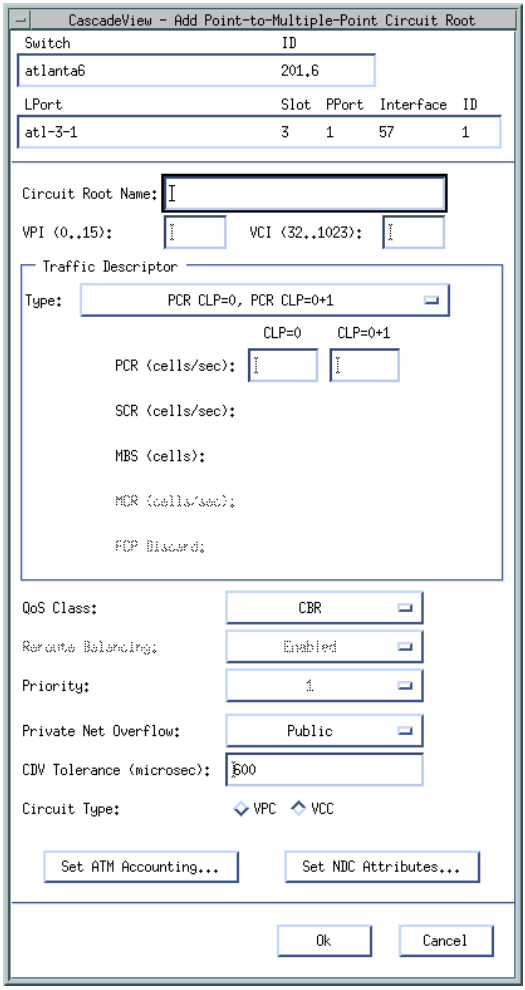


Figure 9-13. Add Point-to-Multiple-Point Circuit Root Dialog Box

5. In the Circuit Root Name field, enter an alphanumeric name for the circuit root.
6. In the VPI and VCI fields, enter the Virtual Path ID and Virtual Channel ID for this circuit root.
7. Configure the remaining fields as described in Table 9-8. Note that your choice of QoS class affects which traffic descriptors are available. For more information about traffic descriptor combinations and traffic parameters, refer to "About ATM Traffic Descriptors" on page 9-2.

Table 9-8. Add Point-to-Multiple-Point Circuit Root Fields

Field	Action/Description
PCR CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (i.e., the CLP=0 cell stream).
PCR CLP=0+1 (cells/sec)	Specify the PCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream).
SCR CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (i.e., the CLP=0 cell stream).
SCR CLP=0+1 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream).
MBS CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (i.e., the CLP=0 cell stream).
MBS CLP=0+1 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (i.e., the CLP=0+1 cell stream).
QoS Class	Select the Quality of Service class for traffic on this PMP circuit.

Table 9-8. Add Point-to-Multiple-Point Circuit Root Fields (Continued)

Field	Action/Description
Reroute Balance	When enabled, circuits use the tuning parameters you defined for the switch. When disabled, switch tuning parameters are ignored for the circuit. For more information, refer to "Defining Circuit Reroute Time Tuning Parameters" on page 5-16.
Circuit Priority	Select circuit priority, where 1 is high priority, 2 is medium priority, 3 is low priority, and 4 is lowest priority. (*VBR-NRT and VBR-RT QoS classes only*)
CDV Tolerance	Enter a value between 1 - 65535 µs to define the Cell Delay Variation Tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. The default is 600 µs.
Private Net Overflow	Determines whether this PVC is restricted to trunks of its own VPN or can use public (shared) trunks during overflow conditions. To configure this circuit for a specific VPN and customer, refer to page 9-24. For more information about VPNs, refer to page 9-11. Select one of the following options: *Public – (Default)* PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restrict* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Circuit Type	Specify whether the circuit is a Virtual Path Connection (VPC) or Virtual Channel Connection (VCC, the default). If you select VPC, the VCI field is set to 0 and cannot be changed.

8. (*Optional*) Choose the Set [NDC] Attributes option and continue the instructions on page 9-40. When you finish, continue with Step 9.

9. Choose OK to return to the Set All PMP Circuit Roots dialog box (Figure 9-11 on page 9-32).

For information about the Set ATM Accounting command, refer to the Accounting System Administrator's Guide.

10. To assign this PMP Circuit to a VPN or customer, choose the VPN/Customer command and refer to "Selecting the VPN and Customer Name" on page 9-24.

11. Continue with "Configuring Point-to-Multipoint Circuit Leafs" on page 9-42.

NDC Attributes for a Point-to-Multipoint Circuit Root

You can only configure network data collection (NDC) attributes for a point-to-multipoint circuit when you initially define a circuit root. Once you create the root, you *cannot* enable or modify NDC.

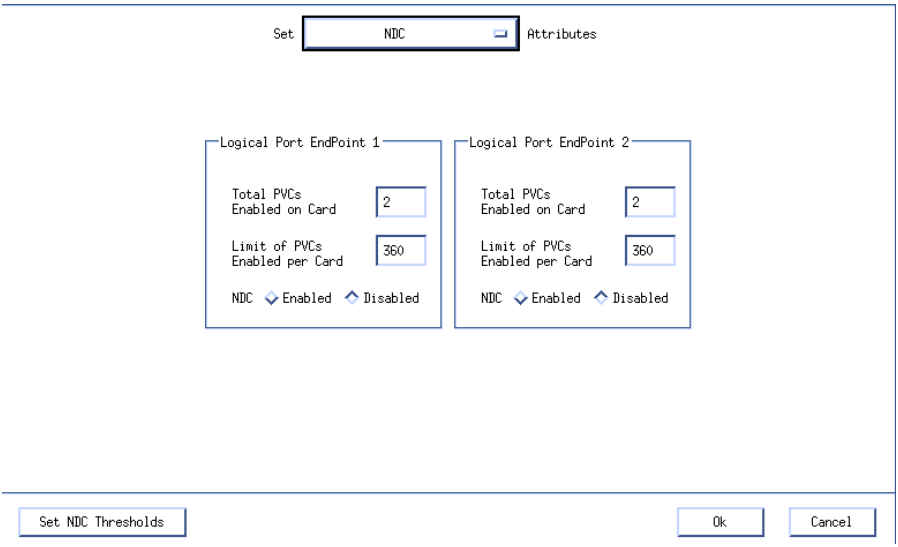


Figure 9-14. Set NDC Attributes

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.

Use the following steps to configure NDC:

1. Enable NDC to collect NDC statistics for a point-to-multipoint circuit.
2. Choose the Set NDC Thresholds command button. The following dialog box appears.

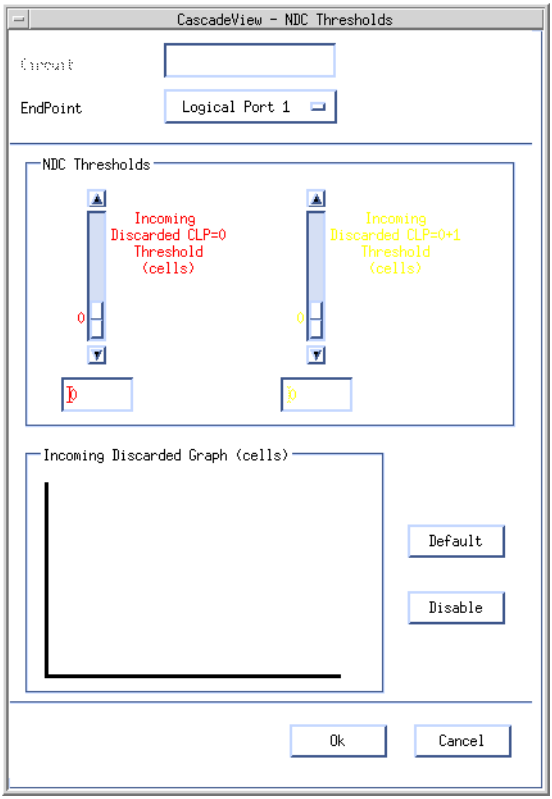


Figure 9-15. NDC Thresholds Dialog Box

3. Configure the NDC Threshold. Choose Default to use the default threshold. To configure the threshold you can:

   - Use the scroll bar and arrows.
   - Type a cell value below each scroll bar and press Enter/Return.

   These thresholds apply to the number of incoming CLP=0 and CLP=0+1 cells that have been discarded. If the number of discarded cells for this endpoint exceeds the value you configure, a trap is generated.

4. Choose OK to set these thresholds and return to the Add Point-to-Multiple Point Circuit roots dialog box (Figure 9-13 on page 9-37). Continue with Step 9 on page 9-40.

Configuring Point-to-Multipoint Circuit Leafs

The following procedure describes how to add endpoints to the root circuit.

1. To configure the multiple endpoints of the PMP circuit, choose Modify. The following dialog box appears.

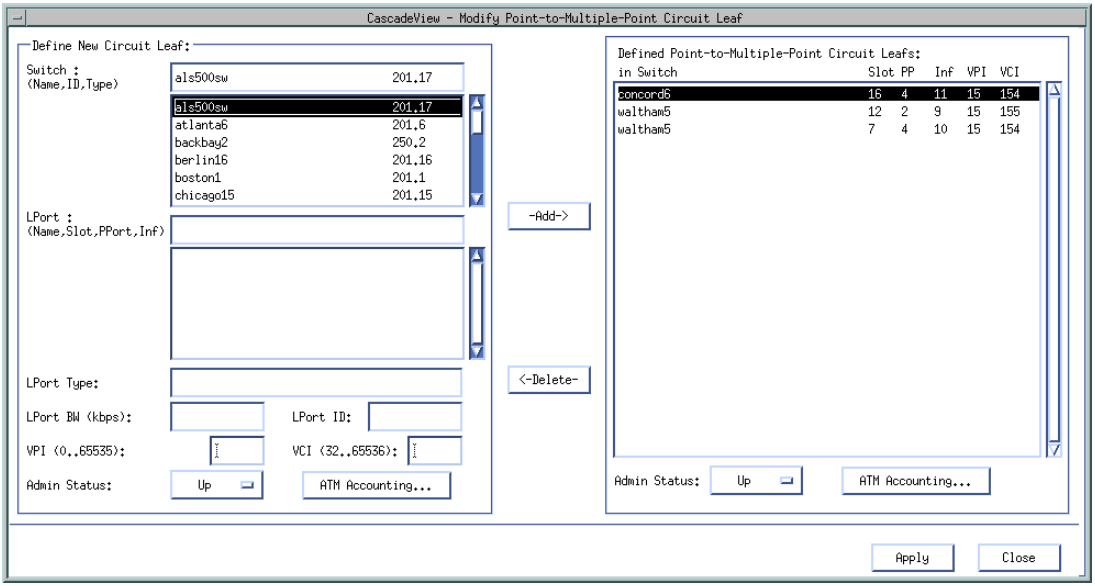


Figure 9-16. Modify PMP Circuit Leaf Dialog Box

The left side of this box enables you to define the endpoints of the PMP circuit. The list on the right shows the endpoints that have already been defined for the selected originating point.

2. To add a new endpoint:

   a. From the Switch list box, select the switch on which to configure the new endpoint. The LPort list box changes to show the logical ports that are configured on the selected switch.

   b. In the LPort list box, select the logical port for the new endpoint.

   c. In the VPI and VCI fields, enter the Virtual Path ID and Virtual Channel ID for the PMP circuit as appropriate (i.e., VPCs do not require a VCI).

   d. Set the Admin Status to Up if you want to activate this circuit when the switch comes online. Set the Admin Status to Down if you do not want to activate this circuit when the switch comes online.

   e. Choose -Add-> to add the circuit to the PMP Circuit Leaf list.

   f. Repeat Step 2 for each endpoint you want to create for this PMP circuit. When done, go to Step 3.

Do not configure more than one circuit leaf for a given root on the same physical port. If you configure more than one OPTimum trunk on a physical port, only one OPTimum trunk can be used for routing one of the leafs for a given root.

For information about the Accounting command, refer to the Accounting System Administrator's Guide*.*

Figure 9-17 illustrates invalid and valid configuration examples that show how multiplexing cannot occur at the port level.

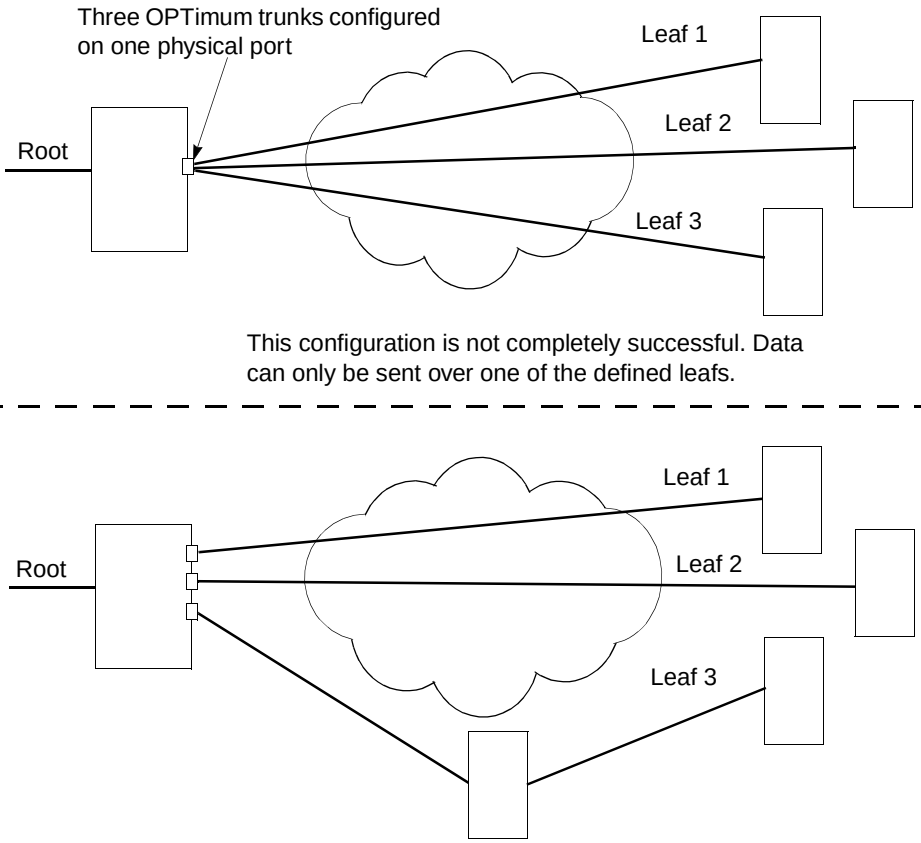


Figure 9-17. Point-to-Multipoint Circuit Example

3. Choose Apply, then choose Close to return to the Set All Point-to-Multiple Point Circuits dialog box.

To define additional PMP circuits and endpoints, repeat Step 1 through Step 3. When you are done adding PMP circuits and endpoints, choose Close to return to the network map.

Deleting a PMP Circuit Root and Leafs

Before you delete the root of a circuit, you must delete all of the circuit's leafs.

The following procedure describes how to delete a PMP circuit root and/or one or more of the circuit's leafs, as well as the entire circuit.

1. From the Administer menu, select Cascade Parameters ⇒ Set All Point-to-Multipoint Circuits. The Set All Point-to-Multiple Point Circuit Roots dialog box appears (Figure 9-11 on page 9-32).
2. From the Circuit Root Name list, select the PMP circuit root you want to delete.
3. Choose Modify. The Modify PMP Circuit Leaf screen appears.
4. From the Defined PMP Circuit Leafs list, select the leaf you want to delete. Then choose Delete. A confirmation box appears. Choose OK to continue.
5. Repeat Step 4 for each circuit leaf you want to remove from the PMP circuit. If you are deleting the circuit, delete all leafs.
6. When done, choose Apply and then Close.
7. In the Circuit Root Name list, verify that the circuit you want to delete is selected. Also, in the Corresponding PMP Circuit Leafs list, verify that no leafs are listed (that is, they have all been deleted).
8. Choose Delete. A confirmation box appears. Choose OK to delete the circuit root. The circuit is now deleted from the network.
9. Choose Close to return to the network map.

Configuring Management VPI/VCIs

You use a Management VPI/VCI when the NMS connects to the gateway switch via an ATM router or ATM network interface card (NIC). The NMS accesses the gateway switch through this connection. This method of access enables you to monitor the network without the use of an Ethernet module in the switch.

After configuring the Management VPI/VCI, remember to add an NMS Path for the Management VPI/VCI (refer to "Defining the NMS Path" on page 5-22). Also, enter a static route in the router or workstation to access the internal IP network.

Adding a New Management VPI/VCI

To configure a Management VPI/VCI:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Management VPI/VCIs. The following dialog box appears.

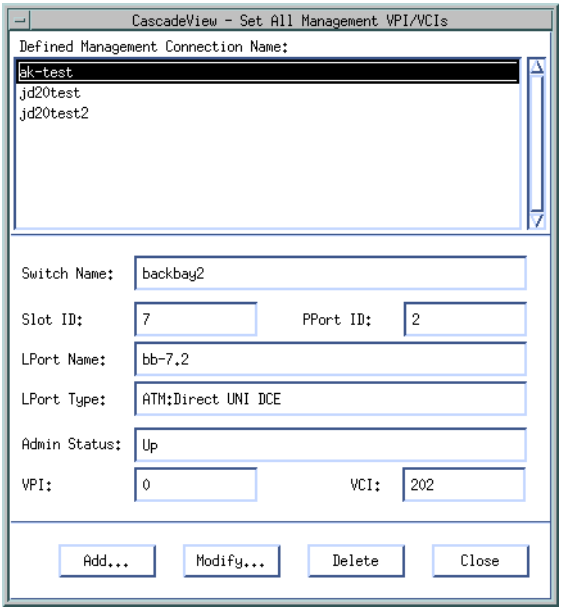


Figure 9-18. Set All Management VPI/VCIs Dialog Box

If you have already configured a Management VPI/VCI, the dialog box displays this information. From the Set All Management VPI/VCI dialog box, you can use the Modify *or* Delete *commands to modify or delete Management VPI/VCI configurations.*

2. Choose Add. The following dialog box appears.

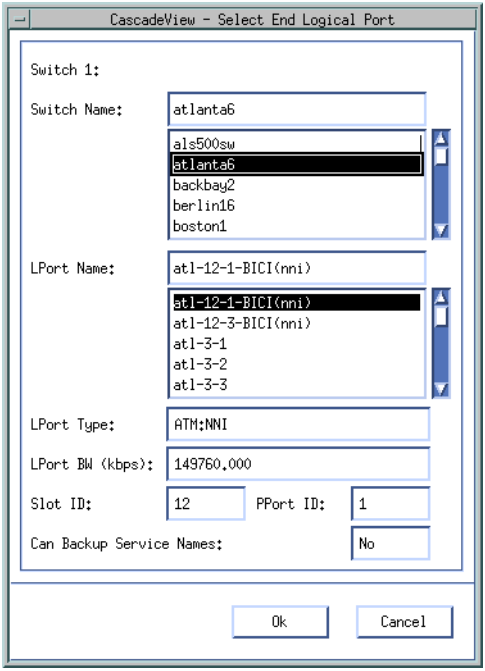


Figure 9-19. Select End Logical Port Dialog Box

3. Complete the dialog box fields as described in Table 9-9.

Table 9-9. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the name of the switch that connects to the router or NIC which serves as the interface for the Network Management VPI/VCI.
LPort Name	Select the name of the logical port configured to access the router or NIC.
LPort Type	Displays the logical port type.
LPort Bandwidth	Displays the logical port bandwidth.
Slot ID	Displays the I/O slot number in which the module resides.
PPort ID	Displays the port number for the port you are configuring.

4. Choose OK. The following dialog box appears.

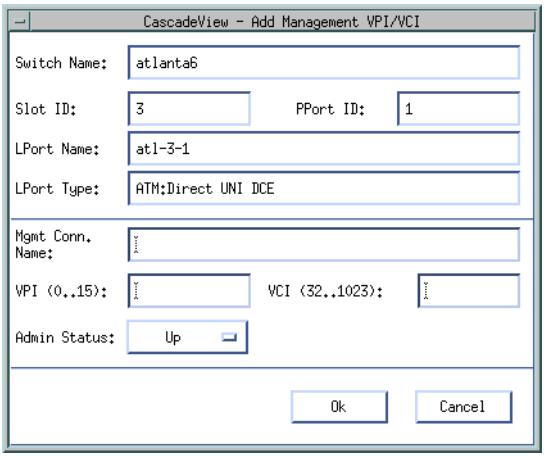


Figure 9-20. Add Management VPI/VCI Dialog Box

5. Complete the Add Management VPI/VCI dialog box fields as described in Table 9-10.

Table 9-10. Add Management VPI/VCI Fields

Field	Action/Description
Switch Name	Displays the name of the switch that connects to the router which 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 configured for the router.
LPort Type	Displays the logical port type.
Management Conn. Name	Enter a unique, continuous, alphanumeric name to identify the connection. Do not use hyphens, dashes, parentheses, and asterisks.
VPI	Enter the VPI that is used for the connection.
VCI	Enter the VCI that is used for the connection.
Admin Status	Select either Up or Down to define whether the Management VPI/VCI connection is activated when the switch or port comes online.

6. Choose OK to complete the configuration.

Configuring a Management PVC

You create a management PVC to access the CBX 500 management port. A management PVC (MPVC) is a data path providing an access point to the CBX 500 network management plane. You terminate the MPVC on an internal logical port that is designated as MPVCLPort.SW[*switch name*]. You then connect this endpoint to any UNI or NNI logical port type to create the circuit.

To define a management PVC connection:

1. Refer to page 9-4 for instructions for accessing the Set All PVCs On Map dialog box (Figure 9-1 on page 9-4).
2. From the Set All PVCs On Map dialog box, choose Add. The Select End Logical Ports dialog box (Figure 9-3 on page 9-15) appears.
3. Configure Endpoint 1 and Endpoint 2 as follows:
   a. Select the name of the CBX 500 switch where the management port (Endpoint 1) resides.
   b. Select the logical port name "MPVCLPort.SW[*switchname*]" for Endpoint 1. The [*switchname*] should correspond to the name of the switch on which the management port endpoint resides. The LPort Type field should display Others:Multi Hop MPVC.
   c. Select the name of the switch where Endpoint 2 resides. This endpoint can be on either a CBX 500 or a B-STDX switch.
   d. Select the name of the logical port for Endpoint 2.
   e. Continue with Step 4.
4. The Select End Logical Ports dialog box displays the following information for both Endpoint 1 and Endpoint 2:

   LPort Bandwidth — Displays the logical port bandwidth for the selected logical ports. At each endpoint, logical ports may have different bandwidth.

   Slot ID — Displays the I/O slot (number) where the IOMs for the selected logical ports reside.

   PPort ID — Displays the port ID numbers for the selected logical ports.

5. Choose OK. The following dialog box appears.

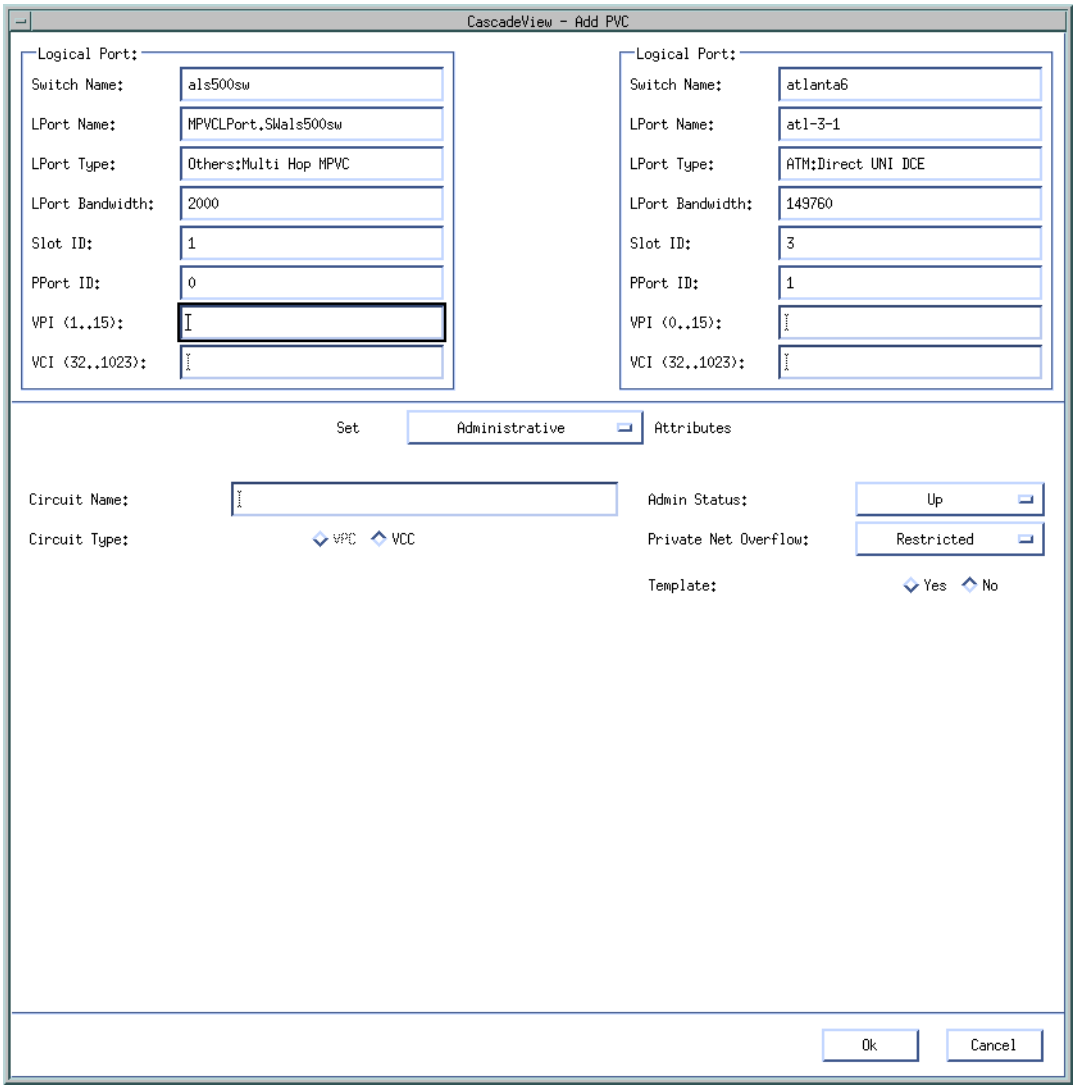


Figure 9-21. Add PVC Dialog Box

6. Define the following parameters for each of the circuit's two endpoints. If you are configuring a PVC between a CBX 500 and a B-STDX, and have questions about B-STDX features (i.e., priority routing), refer to Chapter 11 of the *Network Configuration Guide for B-STDX/STDX*.

   VPI (0 .. nnn) — Enter a value from to represent the Virtual Path Identifier for the PVC. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. Zero is not a valid value for a management PVC. Refer to page 9-13 for information about setting this value.

   VCI (32..nnnn) — Depending on the circuit configuration, enter a value to represent the Virtual Channel Identifier for an ATM PVC. Refer to page 9-13 for information about setting this value.

Set Administrative Attributes

Use the Set [Administrative] Attributes option to configure the fields described in Table 9-11.

Table 9-11. Set Administrative Attributes Fields

Field	Action/Description
Circuit Name	Enter any unique alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the circuit at switch startup, or Down if you do not want to activate the circuit at switch startup.
Circuit Type	Defaults to VCC (Virtual Channel Connection) for a management PVC.

Table 9-11. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Private Net Overflow	Determines whether this PVC is restricted to trunks of its own VPN or can use public (shared) trunks during overflow conditions. To configure this circuit for a specific VPN and customer, refer to page 9-24. For more information about VPNs, refer to page 9-11. Select one of the following options: *Public – (Default)* PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restrict* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template *(Optional)*	You can save these settings as a template to configure another PVC with similar options. To create a template, choose Yes in the "Is Template" field.

Set Traffic Type Attributes

Choose the Set [Traffic Type] Attributes option.

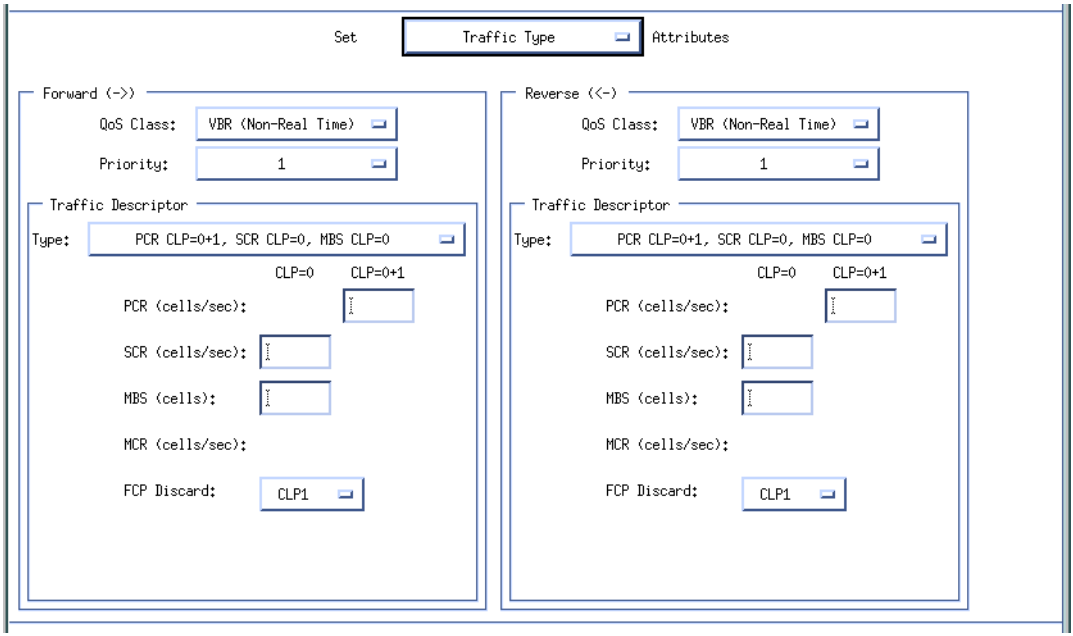


Figure 9-22. Set Traffic Type Attributes

For more information on standard traffic descriptor combinations and parameters, refer to page 9-2. For information about the ABR QoS class, and MCR and FCP Discard traffic parameters, refer to the ATM Flow-Control Processor User's Guide.

Specify Traffic Descriptor settings for forward and reverse traffic as described in Table 9-12. Forward traffic is traffic from Endpoint 1 to Endpoint 2, and reverse traffic is from Endpoint 2 to Endpoint 1.

Table 9-12. Set Traffic Type Attributes

Field	Action/Description
QoS Class (Fwd/Rev)	Select the Quality of Service class for forward and reverse traffic, either VBR-NRT or UBR. The forward and reverse QoS classes do not have to match. For a description of the QoS classes, refer to page 7-12. Note that the QoS class determines which traffic descriptors you can select.
Priority (Fwd/Rev) *(VBR-NRT QoS classes only)*	Select both the forward and reverse circuit priority, where 1 is high priority, 2 is medium priority, and 3 is low priority. The forward and reverse circuit priority values do not have to match.
Traffic Descriptor Type	Select from the following traffic descriptor options: *PCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (i.e., the CLP=0 cell stream). *PCR CLP=0+1 (cells/sec)* – Specify the PCR in cells per second, for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (i.e., the CLP=0 cell stream). *SCR CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (i.e., the CLP=0+1 aggregate cell stream).

Table 9-12. Set Traffic Type Attributes (Continued)

Field	Action/Description
Traffic Descriptor Type (*continued*)	*MBS CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (i.e., the CLP=0 cell stream). *MBS CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (i.e., the CLP=0+1 cell stream).

Set User Preference Attributes

Choose the Set [User Preference] Attributes option.

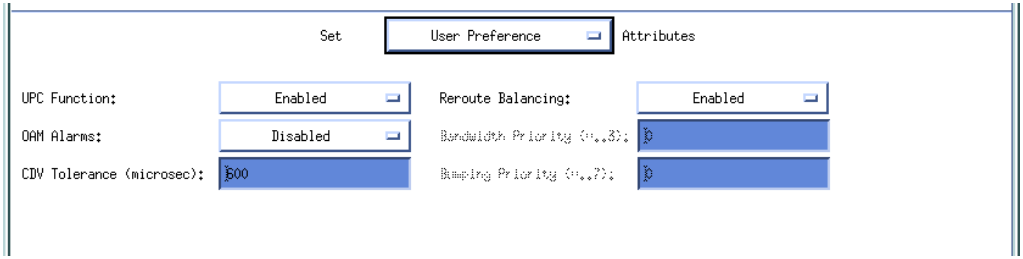


Figure 9-23. Set User Preference Attributes

Configure these fields as described in Table 9-13. (For details on bandwidth and bumping priority parameters, refer to Chapter 11 of the *Network Configuration Guide for B-STDX/STDX*.)

Table 9-13. Set User Preference Attributes

Field	Action/Description
UPC Function	Enables (default) or disables the Usage Parameter Control (UPC) function. When you enable UPC, the circuit tags or drops cells that do not conform to the traffic parameters as they come into the port. When you disable UPC, the circuit allows all traffic, including non-conforming traffic, into the port. As a result, when you disable UPC, quality of service is no longer guaranteed for circuits in the network due to the potential for increasing the cell loss ratio because of port congestion. For this reason, *Cascade recommends that you enable the UPC function on all circuits.* For information about UPC traffic parameters, refer to "About ATM Traffic Descriptors" on page 9-2. ***Note:*** *To use the UPC function for individual circuits, verify that the UPC function is enabled for both logical port endpoints on which you will define the circuit. Enabling UPC at the circuit level has no effect if you did not enable UPC at the logical port level. UPC is enabled by default for both logical ports and circuits.*
Reroute Balancing	When enabled (default), switch tuning parameters take effect. When disabled, switch tuning parameters are ignored for the circuit. For more information, refer to "Defining Circuit Reroute Time Tuning Parameters" on page 5-16.
CDV Tolerance	Configure the Cell Delay Variation Tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. Valid values are between 1 - 65535 µs. The default is 600 µs.
OAM Alarms	Set to Disabled and cannot be changed.

Defining Circuit Attributes

Complete the following steps to apply the attributes you have defined and send the configuration file to the switch (provided the switch is communicating with the NMS).

1. Choose OK to define the circuit parameters. The Set All PVCs on Map dialog box reappears (Figure 9-1 on page 9-4).

2. Choose Close to return to the network map.

10

Configuring SVC Parameters

This chapter describes how to use switched virtual circuits (SVCs). With SVCs, connections are not predefined as they are for PVCs. Instead, end stations use a signaling protocol to indicate to the ATM network the endpoint to which it should route the call (*called party*). To support SVC services, each user endpoint is assigned a unique address which identifies the endpoint and enables the network to route the call.

The procedures in this chapter describe the following tasks:

- Configure node and port prefixes to route calls to a specific node or logical port. With node and port prefixes, you may take advantage of address registration.
- Configure the port user part of an address (DTE ports only). Address registration combines the port user part with a node or port prefix to route the call.
- Configure SVC port addresses to route calls to a specific logical port when the attached network device does not support address registration.
- Configure the various SVC call screening and call handling parameters for a selected logical port.

Address Formats

Before you can begin to configure your network for SVCs, you must decide which of the following address format types to use:

ATM End System Address (AESA) formats — AESA formats give service providers using a private ATM network the flexibility to develop an addressing scheme that best suits their network needs; for example, you may find that most CPEs in your network only support a specific AESA address format.

Native E.164 address format — E.164 addresses are phone numbers. This address format provides a simple and familiar format; native E.164 addresses are a convenient choice for service providers using a public ATM network (e.g., RBOCs) that already "owns" E.164 address space.

The following sections describe these address formats.

ATM End System Address (AESA) Formats

The CBX 500 supports four AESA formats:

Data Country Code (DCC) — For DCC AESA addresses, the initial domain identifier (IDI) is a two-byte data country code field that identifies the country in which this address is registered. These country codes are standardized and defined in ISO reference 3166.

International Country Designator (ICD) — For ICD AESA addresses, the IDI field contains the international country designator that uniquely identifies an international organization. The British Standards Organization administers these values.

E.164 — For E.164 AESA addresses, the IDI field contains an eight-byte E.164 address. This E.164 address uses the international format and consists of up to fifteen decimal digits.

Custom — Custom AESA addresses enable you to use a customized octet structure and a customized Authority and Format Identifier (AFI).

All AESA address formats consist of 20 octets. Each of these address formats contain the following components:

Initial Domain Part (IDP) — Defines the type of address and the regulatory authority responsible for allocating and assigning the Domain Specific Part. There are two subfields: the AFI and IDI fields.

Authority and Format Identifier (AFI) – The AFI part of the AESA address identifies the authority that allocates the DCC, ICD, or E.164 part of the AESA address, as well as the syntax of the rest of the address. The following are valid AFIs:

Address Type	AFI
DCC	0x39
ICD	0x47
E.164	0x45
Custom	A user-specific code for custom prefixes/addresses. (You must know the appropriate code to enter when defining custom prefixes/addresses.)

Initial Domain Identifier (IDI) – A hex code that identifies the sub-authority that has allocated the address. The format depends on the following address types:

Address Type	IDI Description
DCC	Consists of 2 octets (4 hex digits) that identifies the country in which this address is registered.
ICD	Consists of 2 octets (4 hex digits) that identifies an international organization to which this address is registered.
E.164	Consists of 8 octets in BCD format. (1-15 hex digits, plus a trailing Fh; if less than 15 digits are entered, enter leading zeros to fill the 8 octets.) Represents an international E.164 address.

Domain Specific Part — Consists of the HO-DSP, EDI, and SEL fields.

High-Order Domain-Specific Part (HO-DSP) – The authority specified in the AFI/IDI octets determines the format of this field. It identifies a segment of address space that is assigned to a particular user or subnetwork. It should be constructed to facilitate routing through interconnected ATM subnetworks. The general format for each address type is as follows:

Address Type	HO-DSP Description
DCC, ICD	Consists of 10 octets (20 hex digits)
E.164	Consists of 4 octets (8 hex digits)
Custom	Consists of 12 octets (24 hex digits)

End System Identifier (ESI) – A 6-octet (12 hex digit) field that uniquely identifies the end system within the specified subnetwork. This is typically an IEEE MAC address.

Selector (SEL) – A 1-octet (2 hex digit) field that is not used for ATM routing, but may be used by the end system.

In summary, the combination of IDP + HO-DSP + ESI must be unique. To ensure interoperability and equipment portability, it is desirable to use an ESI that is globally unique. For instance, if the ESI is not globally unique, and you move the ATM end system from one network to a different network, there could be address conflicts.

Figure 10-1 shows how the octets are assigned for each AESA address format. Each octet is equivalent to two hex digits.

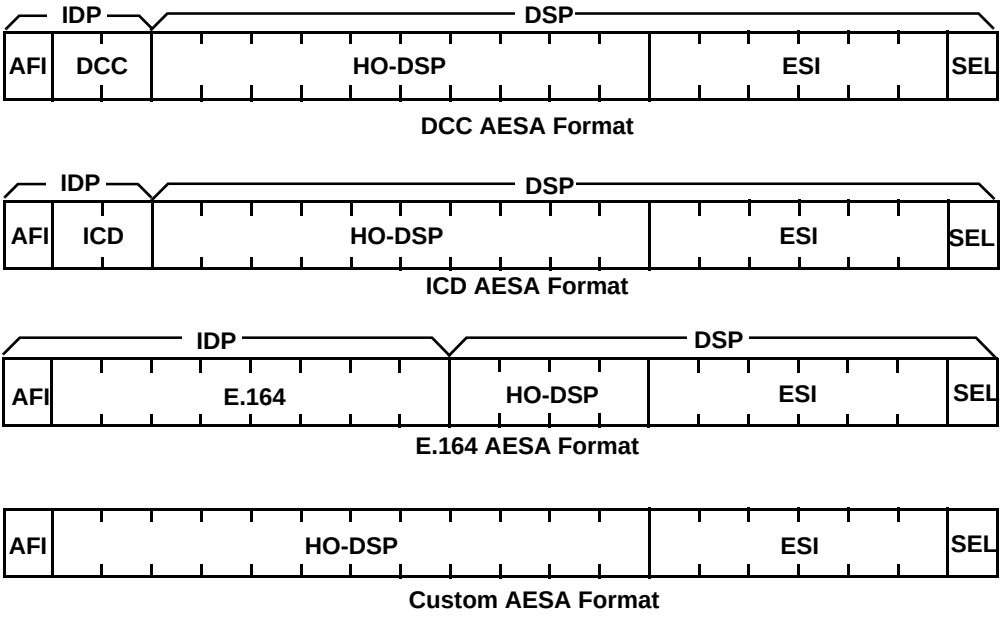


Figure 10-1. AESA Address Formats

Native E.164 Address Format

Native E.164 addresses are the standard Integrated Services Digital Network (ISDN) numbers, including telephone numbers. Native E.164 addresses consist of 1-15 ASCII digits. For example, standard 10-digit United States telephone numbers, such as 508-555-1234, are native E.164 addresses.

Unlike AESA address formats, native E.164 addresses are not broken down into an AFI, HO-DSP, ESI, and SEL portion. When a native E.164 address is translated to E.164 AESA format, the native E.164 address is stored in octets 2-9 of the 20-octet AESA address, while the HO-DSP, ESI, and SEL portions are filled with zeros. Conversely, when an E.164 AESA address is translated to native E.164 address format, the AFI, HO-DSP, ESI, and SEL portions, as well as any leading zeros in the 8-octet AESA E.164 address, are stripped off to produce the native E.164 address.

Designing an Address Format Plan

The SVC address formats you select must support the equipment and services your network needs to provide. Keep in mind that some CPEs may not support certain address formats. To avoid address conflicts, apply for globally-recognized address space in the ATM formats you need to use.

Address formats provide a means to develop a network numbering plan. Using an AESA address, you can design the IDP portion of an address to target a specific network; then use the HO-DSP portion of the address to identify subnetworks within that network, and use the ESI to identify a specific end system.

Regardless of the address format you choose, the network numbering plan should satisfy the following goals:

- Intelligently assign network addresses
- Simplify network topology using a hierarchal organization
- Minimize the size of network routing tables
- Uniquely identify each endpoint
- Provide a high level of network scalability

About Address Registration

Address information in a switch is used to determine call routing and for calling party screening. When used for route determination, the switch advertises an appropriate subset of its configured node prefixes, port prefixes, and port addresses to all other switches in the network. When used for calling party screening, the switch uses the configured node prefixes, port prefixes, and/or port addresses to determine whether or not a call should be accepted by the network.

To perform these two functions at a UNI, both the user and the network need to know the ATM addresses that are valid at the UNI. Address registration provides a mechanism for address information to be dynamically exchanged between the user and the network, enabling them to determine the valid ATM addresses that are in effect at a UNI. Address registration applies only to UNI ports on which ILMI is enabled (refer to page 7-31 for instructions on how to enable ILMI on a UNI logical port). Any ILMI-eligible node or port prefix will be transferred from all ILMI-enabled private UNI-DCE ports and all ILMI-enabled public end-system UNI-DCE ports to their peer DTE devices.

Node prefixes are not exchanged from "network-to-network" UNI-DCE ports. Only port prefixes are exchanged from these ports.

For address registration to work, attached UNI devices must support ILMI.

ILMI-eligible prefixes include:

- All native E.164 node prefixes
- All 13-octet (104-bit) AESA node prefixes
- All native E.164 port prefixes
- All 13-octet (104-bit) AESA port prefixes

The network side of the UNI provides the network prefix, which consists of the IDP and HO-DSP portions. The user side of the UNI provides the remaining portion of the address, which consists of the IEEE MAC address (the ESI portion) and the SEL portion of an ATM address; this forms the user part of the address. Figure 10-2 shows this addressing scheme.

Native E.164 prefixes sent by the network are concatenated with a NULL user part by the user, and returned to the network as native E.164 addresses. (The prefix and address are identical.)

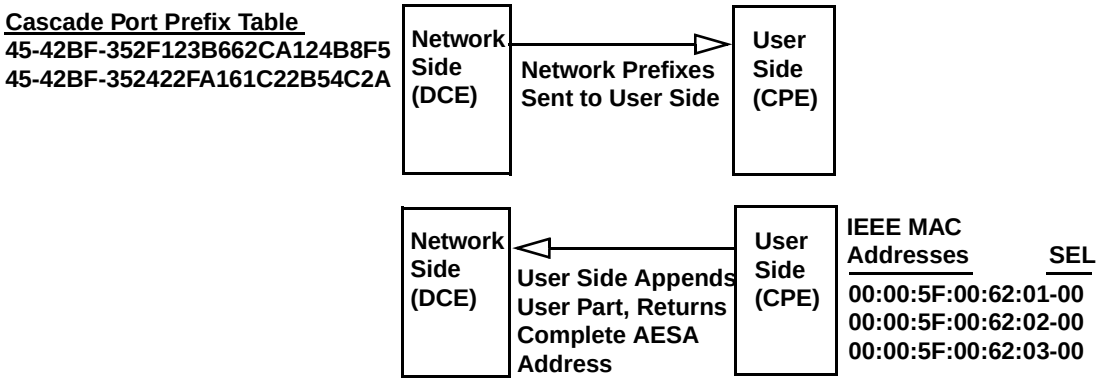


Figure 10-2. Address Registration

About Route Determination

The node prefixes, port prefixes, and port addresses that are configured on network nodes are used to determine the route for a given SVC. The route is determined by a "best match" hierarchy, starting from the left-most digit of the called party address.

Keep in mind that you use node prefixes to summarize the common address parts of the node. For example, if all addresses on the node contain the digits: 15085551, you would define this as the node prefix. To allow for address routing, node prefixes should be unique to a switch; you will have address conflicts if more than one node in the network uses the same node prefix.

The following example shows three nodes configured with a combination of native E.164 node prefixes, port prefixes, and port addresses:

	Node 1	**Node 2**	**Node 3**
Node Prefixes	508 6	None	508 603
Port Prefixes	508551 508552 508553	5085 508553 6035	508554 508555
Port Addresses	5085511111 5085511112 5085511113 5085555555 5085555556	None	None

The following table shows the node to which a call is routed for certain called-party addresses, and why the call is routed to that node:

Called Party Address	Node	Reason
5085511234	1	Port prefix 508551 on Node 1 is a longer match than port prefix 5085 on Node 2 and node prefix 508 on Node 3.
5085555555	1	This calling party address exactly matches a port address defined on Node 1. This is a longer match than port prefix 5085 on Node 2 and port prefix 508555 on Node 3.
5085555557	3	Port prefix 508555 on Node 3 is a longer match than port prefix 50855 on Node 2 and node prefix 508 on Node 1.
5085561111	2	Port prefix 5085 on Node 2 is a longer match than node prefix 508 on Node 1 and node prefix 508 on Node 3.
6175551111	1	Node prefix 6 on Node 1 is the only match.
6035551111	2	Port prefix 6035 on Node 2 is a longer match than node prefix 6 on Node 1 and node prefix 603 on Node 3.
6038558888	3	Node prefix 603 on Node 3 is a longer match than node prefix 6 on Node 1. There is no matching prefix or address on Node 2.
5085531111	1 or 2	Since the longest match occurs on both Nodes 1 and 2, the Admin Cost value assigned to port prefix 5085 on each node determines where the call is routed. The call is routed to the node with the lowest Admin Cost value for port prefix 5085.
5145551234	None	The call is not routed to any of these nodes because there are no matching node prefixes, port prefixes, or port addresses. If, however, you set up a default route on a port being used for network-to-network connections, all non-matching calls are routed to that port (refer to “Defining Default Routes for Network-to-Network Connections” on page 10-35).

Before You Begin

Before you define SVC configuration parameters, verify the following tasks are complete:

- ☑ Create a network map (page 4-6)
- ☑ Add the switch(es) for which you will define the SVCs (page 4-14)
- ☑ Specify the switch attributes for these switches (page 5-9)
- ☑ Configure the IP address of all NMS workstations that access the switch(es) (page 5-21)
- ☑ Configure the IOMs and physical ports associated with the logical ports for which you define SVCs (Chapter 6)
- ☑ Configure the logical ports for which you define SVCs (Chapter 7)

Configuring Node Prefixes

Node prefixes apply to all ports on the switch and are used for routing aggregation, source address validation, and address registration. You can configure multiple node prefixes on a switch; however, you do not need to configure any if you have port prefixes or port addresses defined on the node.

At the very least, a node prefix consists of the two AFI digits of the AESA address, or at least one digit of the 1-15 digit native E.164 address. You can define the node prefix to be part or all of the AESA or E.164 address. For example, for E.164 addresses that begin with 508555, you can configure the node prefix as 5 (at a minimum), 50, 508, 5085, etc. The level of granularity you need to define depends on your network.

Node prefixes do not have to be unique to a particular node. For example, you can define node prefix 508 on multiple nodes. However, if you do so, you may need to define port prefixes or port addresses to provide more granularity for routing determination. For example, you may define port prefixes 508551, 508552, and 508553 on one of these nodes, and port prefixes 508554, 508555, and 508556 on the second of these nodes.

About Address and Routing Options

The Add Node Prefix dialog boxes contain fields that allow you to enable or disable the address and routing options.

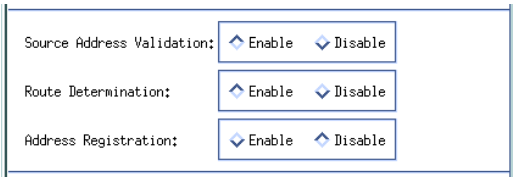


Figure 10-3. Add Node Prefix Address and Routing Fields

Use Table 10-1 to configure these options.

Table 10-1. Add Node Prefix Address and Routing Fields

Field	Description
Source Address Validation	Select enable to validate the calling party address against the node prefix associated with the UNI logical port that received the call setup message. If you disable this option, this node prefix is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this node prefix for routing aggregation. If disabled, OSPF does not use it. Enable this option to use PVC/PVP termination (refer to page 11-2).
Address Registration	If enabled, this node prefix is used for ILMI address registration for all UNI-DCE “network-to-endsystem” logical ports that support ILMI. You cannot enable this option for AESA node prefixes that are not 13 octets long.

Defining a Node Prefix

To define a node prefix:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All Node Prefixes. The following dialog box appears.

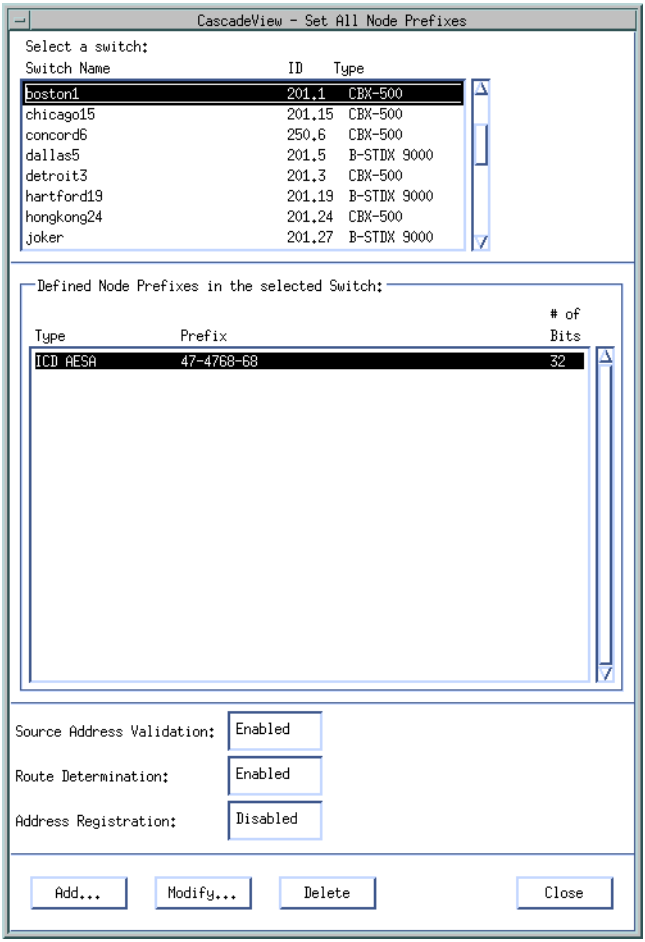


Figure 10-4. Set All Node Prefixes Dialog Box

The top list box (*Select a switch:*) displays all switches that are accessible from this NMS. The bottom list box (*Defined Node Prefixes in the selected Switch:*) displays all the node prefixes configured on the selected switch. You can display the address and routing options for each node prefix.

2. From the top list box, select the switch for which to configure node prefixes.
3. Choose Add. The Add Node Prefix dialog box appears.
4. To define a node prefix for a specific format, select one of the following address formats and refer to the corresponding section:

Format	Description	Refer to
E.164 Native	Standard 1-15 digit Integrated Services Digital Network (ISDN) number, which includes telephone numbers.	“Native E.164 Node Prefix Format” on page 10-15
DCC AESA	Data Country Code ATM End System Address, which identifies the country in which the address is registered.	“DCC and ICD AESA Node Prefix Format” on page 10-16
ICD AESA	International Country Designator ATM End System Address, which identifies the international organization to which the address applies.	“DCC and ICD AESA Node Prefix Format” on page 10-16
E.164 AESA	E.164 ATM End System Address, which encapsulates a standard 1-15 digit ISDN number, including telephone numbers.	“E.164 AESA Node Prefix Format” on page 10-18
Custom AESA	ATM End System Address with customized octet structure and customized Authority and Format Identifier (AFI).	“Custom AESA Node Prefix Format” on page 10-20

Native E.164 Node Prefix Format

Complete the following information for the E.164 (Native) format:

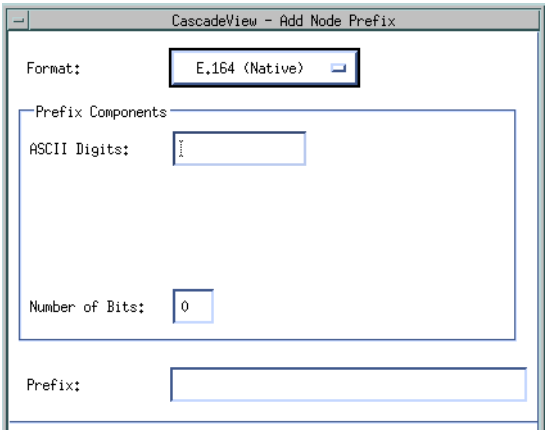


Figure 10-5. Add Node Prefix Dialog Box (E.164 Native Format)

1. In the ASCII Digits field, enter all or part of the 1-15 ASCII digits that represent the E.164 address.

   For example, enter 5085552600 (a standard 10-digit U.S. phone number), or enter a partial number (such as 508). The value you enter is converted to the ASCII hex values that represent each digit in the number (this value is displayed in the Address in Hex field). If you entered 5085552600, it converts to 35308353535323630 30. This value is also displayed in the Address in Hex column on the Set All Node Prefixes dialog box (Figure 10-4 on page 10-13).

2. Refer to page 10-12 to configure the address and routing options.

3. Choose OK to return to the Set All Node Prefixes dialog box.

DCC and ICD AESA Node Prefix Format

Complete the following information for the DCC or ICD AESA format:

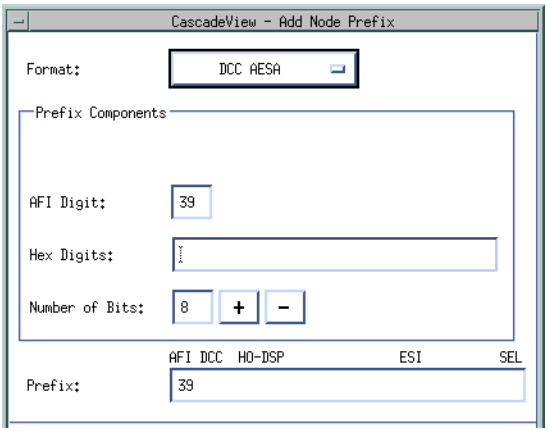


Figure 10-6. Add Node Prefix Dialog Box (DCC or ICD AESA Format)

1. In the Hex Digits field, enter the Data Country Code (DCC) of the country in which the address is registered, or the International Country Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.

2. (*Optional*) Enter the HO-DSP, ESI and SEL portions of the address.

   For information on the appropriate format to use for DCC and ICD addresses, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the address registration option set to enabled (refer to page 10-12).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you type). Click on the — icon to decrease the number of address bits that are checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 39-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**39-43BF12AC**
Address in binary (40 bits):	**00111001-01000011110011110001001010111100**
Address in binary (38 bits):	**00111001-01000011110011110001001010111**

Address you entered:	**39-43BF12A8**
Address in binary (40 bits):	**00111001-01000011110011110001001010111000**
Address in binary (37 bits):	**00111001-0100001111001111000100101011**

4. Refer to page 10-12 to configure the address and routing options.

5. Choose OK to return to the Set All Node Prefixes dialog box (Figure 10-4 on page 10-13). The new entry appears, along with the preceding AFI (39 or 47), in the bottom list box (*Defined Node Prefixes in the selected Switch*).

E.164 AESA Node Prefix Format

Complete the following information for the E.164 AESA format:

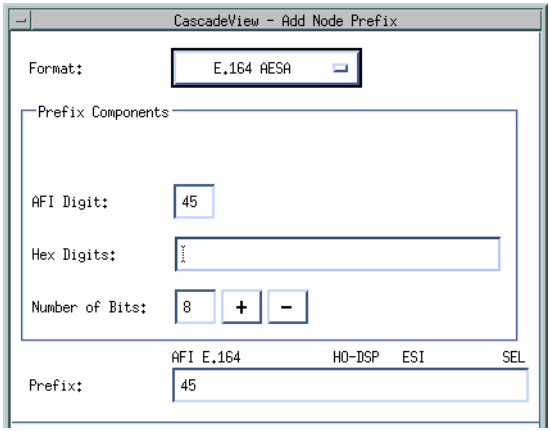


Figure 10-7. Add Node Prefix Dialog Box (E.164 AESA Format)

1. In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh.

   If you do not enter all 15 digits of the IDI portion, you must enter leading zeros to fill in the octets. For example, enter 508 as 000000000000508F; enter 508555 as 000000000508555F.

2. If you enter the IDI portion of the address, you can optionally enter the HO-DSP, ESI, and SEL portions. For example, if you enter 000005085551234F, you can then enter all or some of the remaining parts. For information about the appropriate format to use for E.164 AESA addresses, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the address registration option set to enabled (refer to page 10-12).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you enter). Click on the — icon to decrease the number of address bits that are checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 45-00000504 (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**45-00000504**
Address in binary (40 bits):	**01000101-0000000000000000000000010100000100**
Address in binary (38 bits):	**01000101-0000000000000000000000101000001**

4. Refer to page 10-12 to configure the address and routing options.

5. Choose OK to return to the Set All Node Prefixes dialog box (Figure 10-4 on page 10-13). The new entry appears, along with the preceding AFI (45), in the bottom list box (*Defined Node Prefixes in the selected Switch*).

Custom AESA Node Prefix Format

Complete the following information for the Custom AESA format:

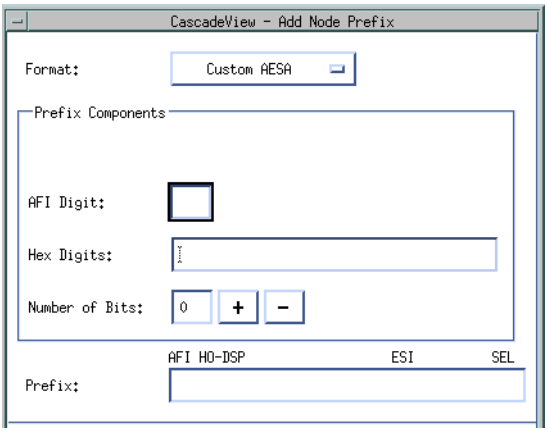


Figure 10-8. Add Node Prefix Dialog Box (Custom AESA Format)

1. In the AFI Digits field, enter the custom AFI you want to use.
2. In the Hex Digits field, enter in the customized address format, starting with the HO-DSP, and followed by the ESI and SEL values (in that order).

   This address can be up to 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. You do not have to enter the entire address; the HO-DSP, ESI, and SEL entries are optional. However, you must enter the AFI digits. For information about these items, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the address registration option set to enabled (refer to page 10-12).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you type). Click the — icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 51-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing, click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**51-43BF12AC**
Address in binary (40 bits):	**01010001-01000011110011110001001010111100**
Address in binary (38 bits):	**01010001-01000011110011110001001010111**

Address you entered:	**51-43BF12A8**
Address in binary (40 bits):	**01010001-01000011110011110001001010111000**
Address in binary (37 bits):	**01010001-0100001111001111000100101011**

4. Refer to page 10-12 to configure the address and routing options.

5. Choose OK to return to the Set All Node Prefixes dialog box (Figure 10-4 on page 10-13).

Configuring SVC Port Prefixes

The Set All Prefixes function enables you to define how calls are routed to the port. Port prefixes are also used for calling party screening.

When you add a port prefix, the Add Prefix dialog box contains fields which allow you to enable or disable the following options, as shown in Figure 10-9.

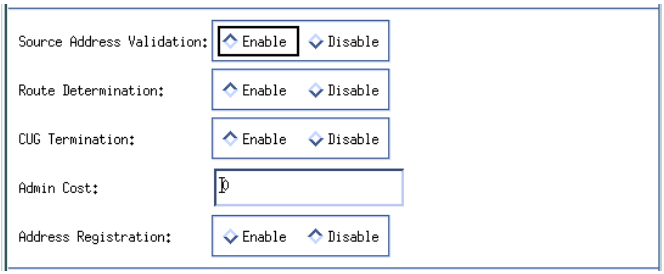


Figure 10-9. Add Port Prefix Option Fields

Use Table 10-2 to configure these options.

Table 10-2. Add Port Prefix Option Fields

Field	Action/Description
Source Address Validation	Select enable to validate the calling party address against the port prefix associated with the UNI port that received the call setup message. If you disable this option, this port prefix is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this port prefix for route determination. If disabled, OSPF registration is not used. Enable this option to use PVC/PVP termination (refer to page 11-2).

Table 10-2. Add Port Prefix Option Fields (Continued)

Field	Action/Description
CUG Termination	Select enable to use this prefix 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 Chapter 13.
Admin Cost	Enter 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	If enabled, 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 13 octets long.

Defining a Port Prefix

To define a port prefix:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All Port Prefixes. The following dialog box appears.

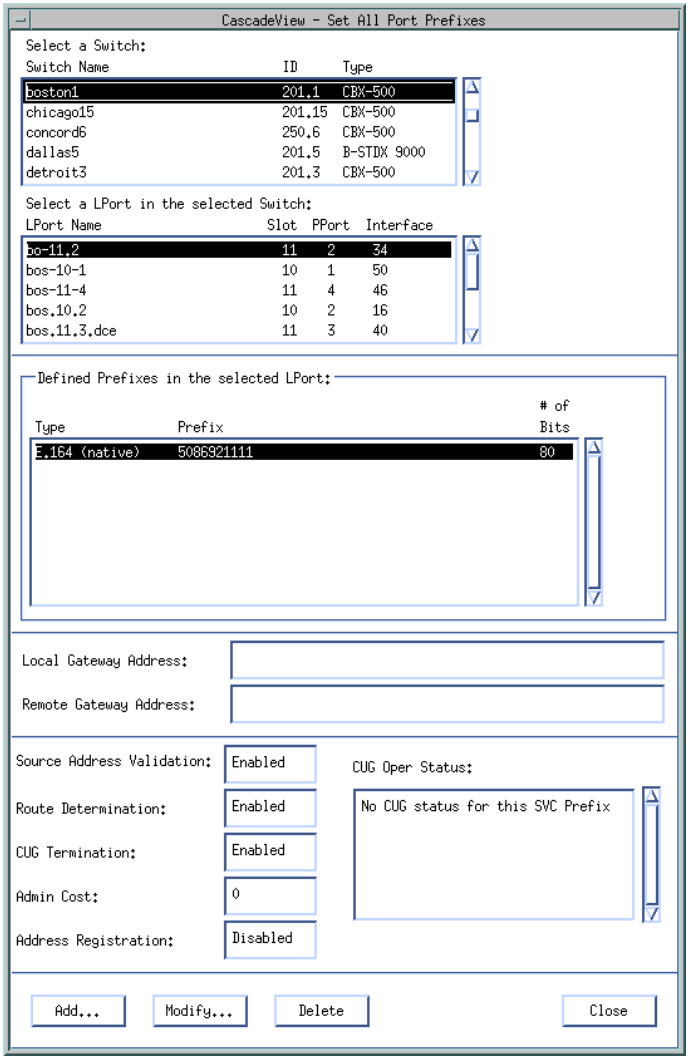


Figure 10-10. Set All Port Prefixes Dialog Box

- The *Select a Switch:* list box displays all switches that this NMS can access.
- The *Select a LPort in the selected Switch:* list box displays the logical ports that are configured for the selected switch, along with the slot, physical port, and MIB interface number for the logical port.
- The *Defined Prefixes in the selected LPort:* list box displays all port prefixes that have already been defined on the selected logical port. You can display configured options for each of these prefixes.

2. Select the switch for which to configure port prefixes.
3. Select the logical port for which to configure port prefixes.
4. Choose Add. The Add Prefix dialog box appears.
5. Select an address format and refer to one of the following sections:

Format	Refer to
E.164 Native	page 10-26
DCC AESA	page 10-27
ICD AESA	page 10-27
E.164 AESA	page 10-29
Custom AESA	page 10-31
Default Route	page 10-35

E.164 Native Prefixes Port Prefix Format

Complete the following information for the E.164 native prefix format:

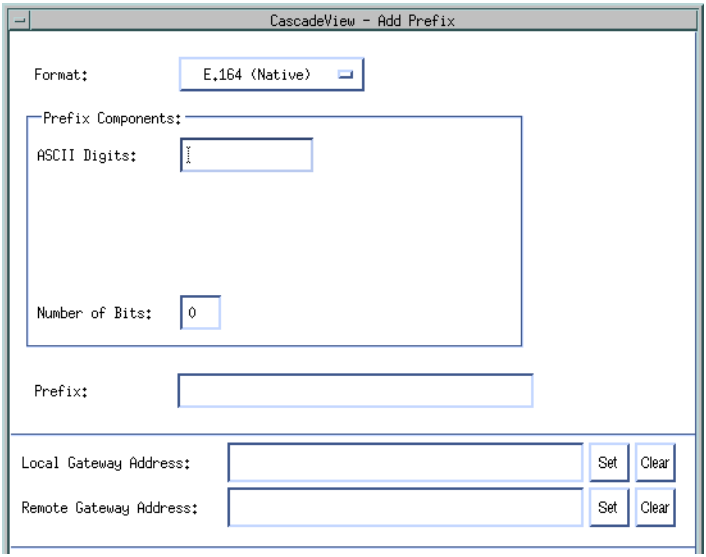


Figure 10-11. Add Prefix Dialog Box (E.164 Native Format)

1. In the ASCII Digits field, enter all or part of the 1-15 ASCII digits that represent the E.164 address.

   For example, enter 5085552600 (a standard 10-digit U.S. phone number), or enter a partial number (such as 508). The value you enter is converted to the ASCII hex values that represent each digit in the number (this value is displayed in the Address in Hex field). If you entered 508555260, it converts to 35303835353532363030. This value is also displayed in the Address in Hex column on the Set All Port Prefixes screen.

2. If the port provides a network-to-network connection, refer to "Setting the Local and Remote Gateway Address for Port Prefixes" on page 10-33 for instructions. When done, proceed to Step 3.

3. Refer to Table 10-2 on page 10-22 to configure additional port prefix options.

4. Choose OK to return to the Set All Port Prefixes dialog box (Figure 10-10 on page 10-24).

DCC and ICD AESA Port Prefix Format

Complete the following information for the DCC or ICD AESA prefix format:

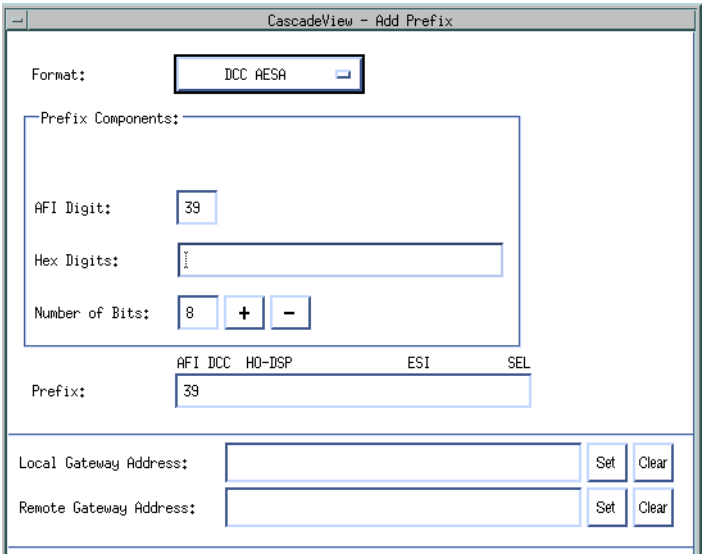


Figure 10-12. Add Prefix Dialog Box (DCC and ICD AESA Format)

1. In the Hex Digits field, enter the Data Country Code (DCC) of the country in which the address is registered, or the International Country Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.

2. (*Optional*) Enter the HO-DSP, ESI and SEL portions of the address.

   For information on the appropriate format to use for DCC and ICD addresses, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening and call routing. (The value increases by eight with each address digit you type). Click the — icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 39-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two digits are binary 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**39-43BF12AC**
Address in binary (40 bits):	**00111001-01000011110011110001001010111100**
Address in binary (38 bits):	**00111001-0100001111001111000100101011111**

Address you entered:	**39-43BF12A8**
Address in binary (40 bits):	**00111001-01000011110011110001001010111000**
Address in binary (37 bits):	**00111001-0100001111001111000100101011**

4. If the port provides a network-to-network connection, refer to "Setting the Local and Remote Gateway Address for Port Prefixes" on page 10-33 for instructions. When done, proceed to Step 5.

5. Refer to Table 10-2 on page 10-22 to configure additional port prefix options.

6. Choose OK to return to the Set All Port Prefixes dialog box (Figure 10-10 on page 10-24). The new entry appears, along with the preceding AFI (39 or 47), in the *Defined Prefixes in the selected LPort* list box on the bottom half of the screen.

E.164 AESA Port Prefix Format

Complete the following information for the E.164 AESA prefix format:

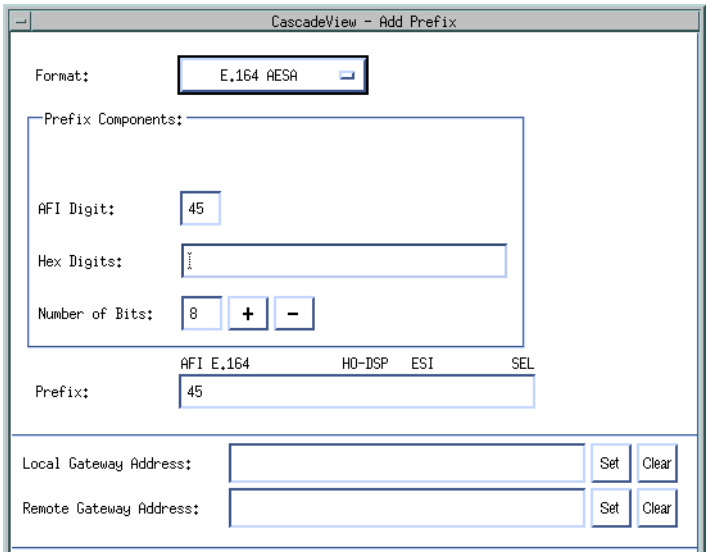


Figure 10-13. Add Prefix Dialog Box (E.164 AESA Format)

1. In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh.

   If you do not enter all 15 digits of the IDI portion, you must enter leading zeros to fill in the octets. For example, enter 508 as 000000000000508F; enter 508555 as 000000000508555F.

2. If you enter the IDI portion of the address, you can optionally enter the HO-DSP, ESI, and SEL portions. For example, if you enter the IDI portion, such as 000005085551234F, you can then enter all or some of the remaining parts. For information on the appropriate format to use for E.164 addresses, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening and call routing. (The value increases by eight with each pair of address digits you type). Click the — icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 45-00000504 (which uses 40 bits) as the port prefix, but you only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**45-00000504**
Address in binary (40 bits):	**01000101-0000000000000000000000010100000100**
Address in binary (38 bits):	**01000101-0000000000000000000000101000001**

4. If the port provides a network-to-network connection, refer to "Setting the Local and Remote Gateway Address for Port Prefixes" on page 10-33 for instructions. When done, proceed to Step 5.

5. Refer to Table 10-2 on page 10-22 to configure additional port prefix options.

6. Choose OK to return to the Set All Port Prefixes dialog box (Figure 10-10 on page 10-24). The new entry appears, along with the preceding AFI (45), in the *Defined Prefixes in the selected LPort* list box.

Custom AESA Port Prefix Format

Complete the following information for the Custom AESA prefix format:

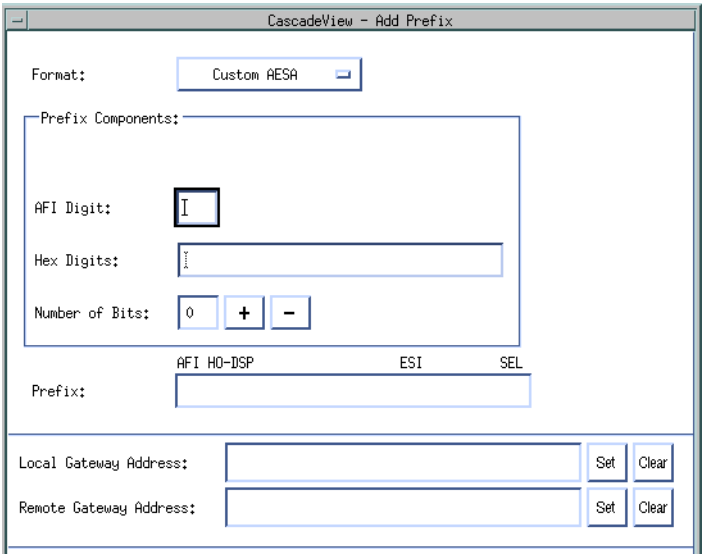


Figure 10-14. Add Prefix Dialog Box (Custom AESA Format)

1. In the AFI Digits field, enter the custom AFI you want to use.
2. In the Hex Digits field, type in the customized address format, starting with the HO-DSP, and followed by the ESI and SEL values (in that order). This address can be up to 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. You do not have to enter the entire address; the HO-DSP, ESI, and SEL entries are optional. However, the AFI digits are required. For information on these items, refer to "ATM End System Address (AESA) Formats" on page 10-2.

To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening/call routing. (The value increases by eight with each address digit you type). Click the — icon to decrease the number of address bits, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial address 51-43BF12AC (which uses 40 bits) as the port prefix, but you only need to check the first 38 bits of the port prefix for call screening and call routing, click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**51-43BF12AC**
Address in binary (40 bits):	**01010001-01000011110011110001001010111100**
Address in binary (38 bits):	**01010001-0100001111001111000100101011111**

Address you entered:	**51-43BF12A8**
Address in binary (40 bits):	**01010001-01000011110011110001001010111000**
Address in binary (37 bits):	**01010001-0100001111001111000100101011**

4. If the port provides a network-to-network connection, refer to “Setting the Local and Remote Gateway Address for Port Prefixes” on page 10-33 for instructions. When done, proceed to Step 5.

5. Refer to Table 10-2 on page 10-22 to configure additional port prefix options.

6. Choose OK to return to the Set All Port Prefixes dialog box (Figure 10-10 on page 10-24).

Setting the Local and Remote Gateway Address for Port Prefixes

This section describes how to set the optional local and remote gateway addresses for ports that are providing a network-to-network connection. Local and remote gateway addresses are used in conjunction with the egress address translation feature (refer to page 10-56).

Figure 10-15 shows which addresses to enter as the local and remote gateway addresses for each end of the network-to-network connection.

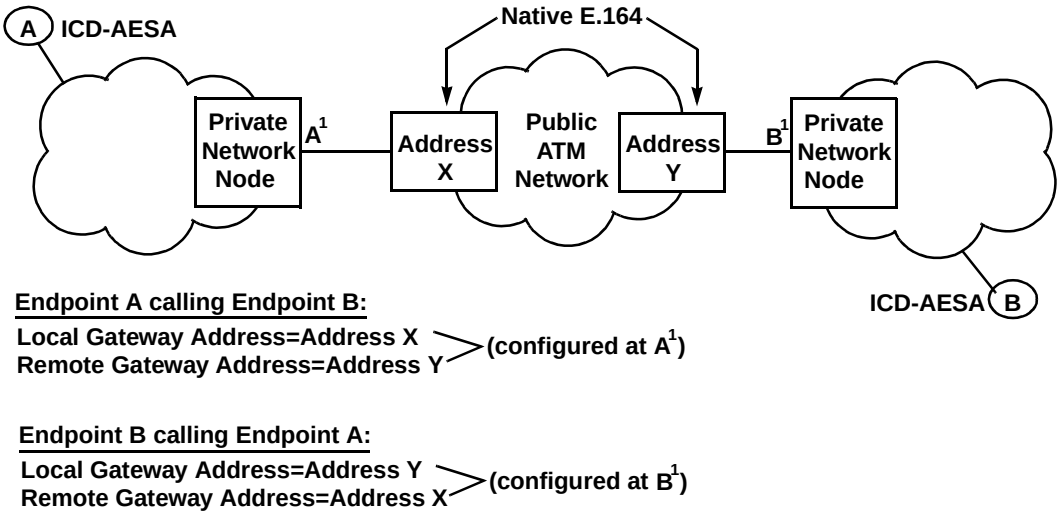


Figure 10-15. Setting Local and Remote Gateway Addresses

You can configure prefixes on a network-to-network port with the following:

- Null local and remote gateway addresses
- Only a local gateway address
- Only a remote gateway address
- Both a local and a remote gateway address

You need to define gateway addresses for address translation only. For more information on egress address translation, refer to "About Address Translation" on page 10-60.

To set the local (or remote) gateway address:

1. From the Add Prefix dialog box, choose the Set command. The Set Local (or Remote) Gateway Address dialog box appears.

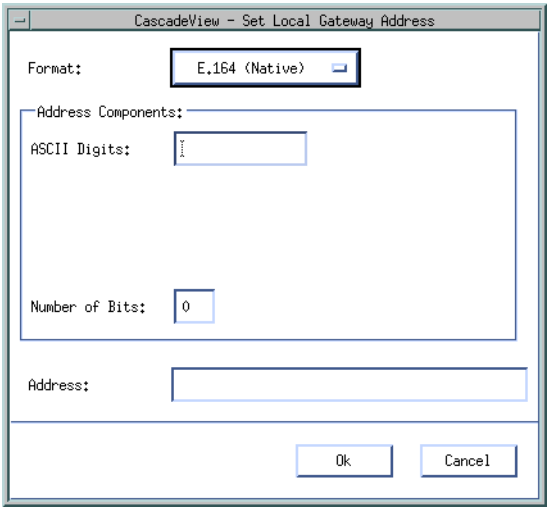


Figure 10-16. Set Local Gateway Address Dialog Box

2. Select the local (or remote) gateway address format.

3. If you specify the local gateway address, enter the address of the public network gateway used to enter the public network. If you specify the remote gateway address, enter the address of the public network gateway used to exit from the public network back to the private network.

4. When done, choose OK to return to the Add Prefix dialog box.

5. To continue, do one of the following:

   - If you are defining a DCC or ICD AESA prefix format, proceed to Step 5 on page 10-28.
   - If you are defining an E.164 AESA prefix format, proceed to Step 5 on page 10-30.
   - If you are defining a Custom AESA prefix format, proceed to Step 5 on page 10-32.

Defining Default Routes for Network-to-Network Connections

If you are using ports for network-to-network connections, you can define a default route (which is automatically assigned 0x00 as its address, with a length of 0 bits).

If the network receives a call and the calling party address does not match any port prefixes or addresses, it routes the call to the port on which the default route is defined. If more than one port has a default route defined, then the administrative cost value is used to determine the port to which the call is routed.

You can define multiple default routes within a node or the network. The default route typically applies to network-to-network logical ports (IISP or public UNI DTE).

Complete the following information for a default route:

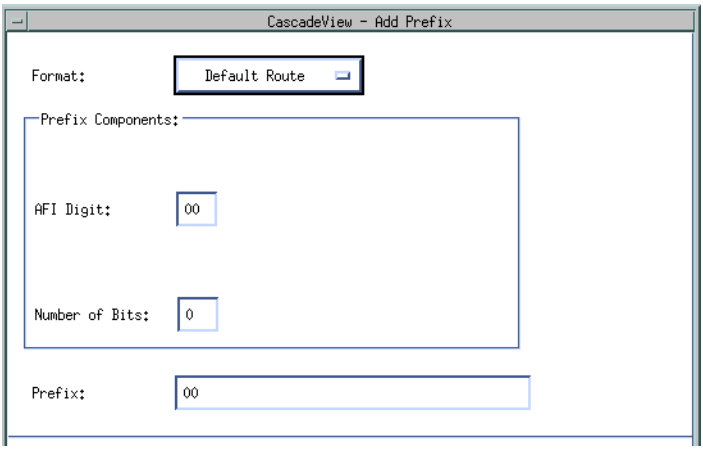


Figure 10-17. Add Prefix Dialog Box (Default Route)

1. In the Format field, select Default Route.
2. Refer to Table 10-2 on page 10-22 to configure additional port prefix options.
3. Choose OK to return to the Set All Port Prefixes dialog box.

Configuring the Port User Part of the Address

The port user part of an AESA address consists of the ESI and SEL portions of the address. It is used for the DTE (user) ports on a Cascade switch and provides information for the address table on the DCE device attached to the UNI on the public network side (refer to “About Address Registration” on page 10-7). When the attached DCE device receives prefixes, the user part(s) are concatenated to form full addresses. The full addresses are then written back to the DCE device’s ILMI address table.

However, when you configure the port user part to complete an address connection with the attached DCE device, you can supply any 7-octet value as the user part (it does not have to be a real IEEE MAC address and SEL combination). Also, you should enter any user addresses in your network that you want to make known to the attached public network. To do this, collect Media Access Control (MAC) addresses from attached devices and enter them as user parts at the public UNI port.

You may have to define user parts only on UNI-DTE ports where the device attached to that port expects address registration completion. That is, the attached device is broadcasting its network prefixes to the Cascade port, and expects the Cascade switch to respond with the user part of the address.

Defining a Port User Part

To define the port user part of the address:

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

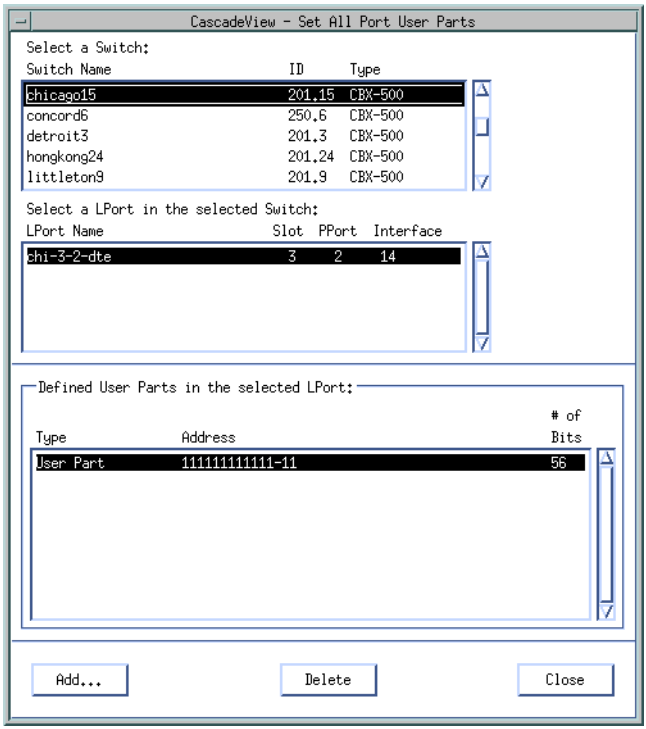


Figure 10-18. Set All Port User Parts Dialog Box

- The *Select a Switch* list box shows all switches that this NMS can access.
- The *Select a Logical Port* list box shows the UNI-DTE logical ports that are configured for this switch.
- The *Defined User Parts* list box displays any user parts you already defined for this logical port.

2. In the Switch Name list box, select the switch on which you want to configure port user parts. The logical ports configured on the selected switch appear in the Lport Name list box.

3. In the Lport Name list box, select the logical port on which you want to configure user parts. If any user parts are already configured on this logical port, they appear in the list box at the bottom of the dialog box.

4. Choose Add. The Add User Part dialog box appears.

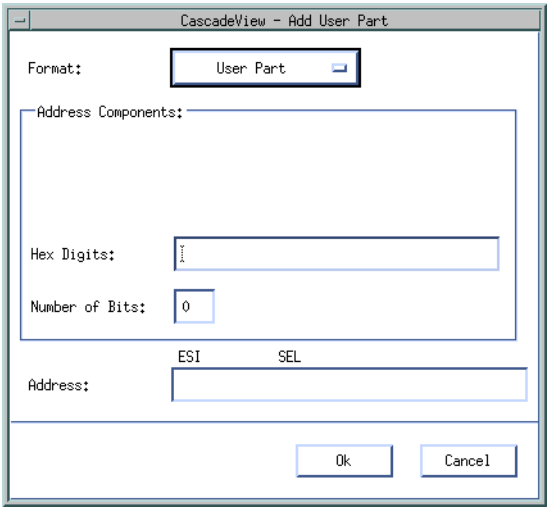


Figure 10-19. Add User Part Dialog Box

5. Enter the 7-octet (14-digit) user part in the Hex Digits field.

6. When done, choose OK to return to the Set All Port User Parts dialog box (Figure 10-18 on page 10-38).

Configuring SVC Port Addresses

If the device attached to a given physical port does not support ILMI address registration, or to fully specify an address to be used for calling party screening, you can define SVC addresses on all the logical ports on that physical port. The AESA formats must have full-length address definitions and include all 20 octets (40 hex digits). That is, you must enter the AFI, IDI, HO-DSP, ESI, and SEL portions of the address. (Since ATM routing does not use the SEL portion, you can enter any value for that part of the address.) For native E.164 addresses, you enter the 1-15 digit E.164 address.

About SVC Port Address Options

The Add Address dialog boxes contain fields that allow you to enable or disable the following options.

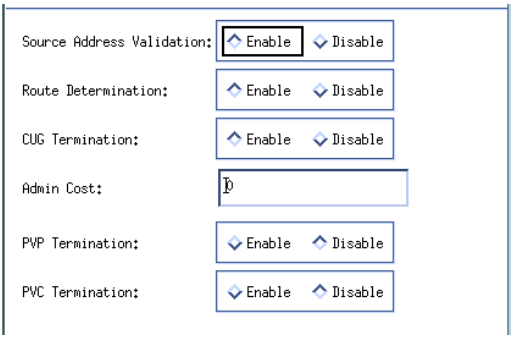


Figure 10-20. Add SVC Port Address Option Fields

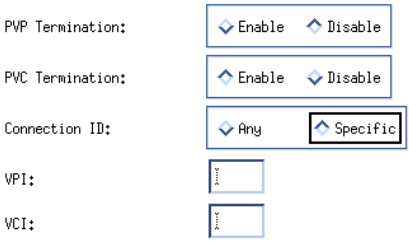
Use Table 10-3 to configure the options shown in Figure 10-20.

Table 10-3. Add SVC Port Address Option Fields

Field	Description
Source Address Validation	Select enable to validate the calling party address against the port address associated with the UNI port that received the call setup message. If you disable this option, this address is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this address for route determination. Enable this option to use PVC/PVP termination (refer to page 11-2).
CUG Termination	Select enable to use this address as part of a Closed User Group (CUG). Incoming and outgoing calls with a calling or called party address that match this address are subject to CUG security checks. For more information about CUGs, refer to Chapter 13.
Admin Cost	Enter the administrative cost associated with the port address. When an SVC is being created, if more than one port in the network is found with the same port address, the call is routed to the port in the network that has the lowest administrative cost associated with the port address.
PVP Termination	Enable this option to terminate an SPVC to this address on this logical port. *Connection ID* – Select Any if you want the network to allocate a VPI for the SPVPC. Select Specific to supply a VPI. Note that if you enable PVC termination, this field is set to Any and cannot be changed. *VPI* – Enter the VPI of the logical port where you want the switch to terminate this SPVPC. The logical port cell header type limits the range of values you can enter: UNI = 255, NNI = 4095. For more information about SPVCs, refer to "Using PVC/PVP Termination" on page 11-2.

Configuring PVC Termination

You can enable this option to terminate an SVC (spoofing) or SPVCC to this address on this logical port. If you enable this option, the Connection ID field appears.



Complete the following fields:

Connection ID — Select Any if you want the network to allocate a VPI/VCI for the spoofed SVC or terminated SPVCC. Select Specific to supply a VPI/VCI value. Note that you cannot select specific if you also enable PVP termination.

VPI/VCI — Enter the VPI/VCI of the logical port where you want the switch to terminate this SPVCC.

Defining an SVC Port Address

To define SVC addresses:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All Port Addresses. The following dialog box appears.

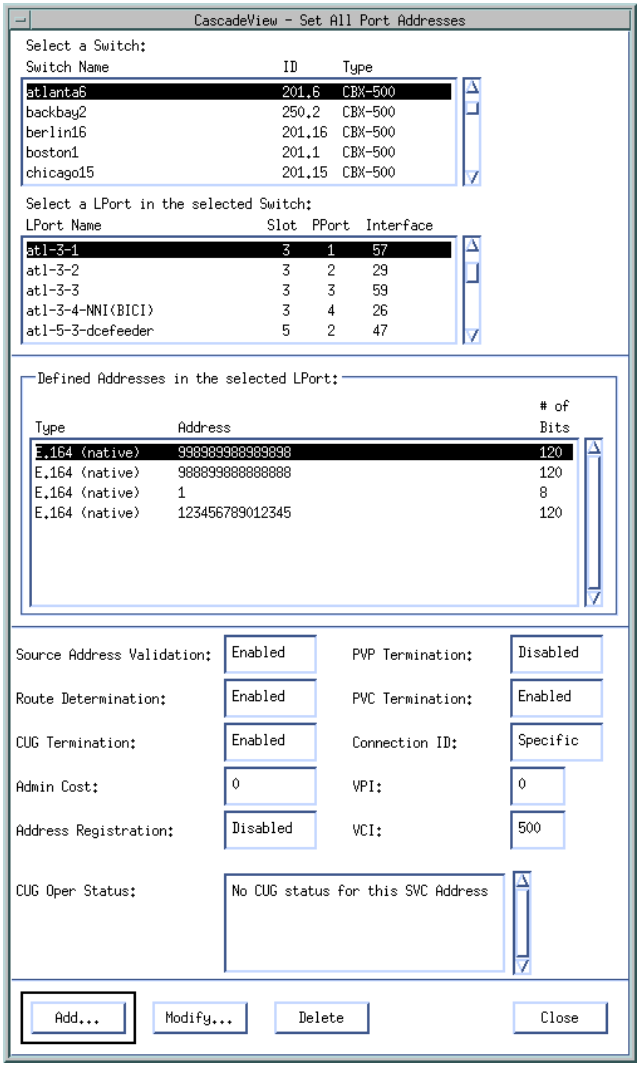


Figure 10-21. Set All Port Addresses Dialog Box

The top list box (*Select a Switch*) displays all switches that the NMS can access. The center list box (*Select a LPort*) displays the logical ports that are configured on the selected switch. The bottom list box (*Defined Addresses*) displays any SVC addresses that you already defined on the selected logical port.

2. Select the switch for which to configure SVC addresses.
3. Select the logical port for which to configure SVC addresses.
4. Choose Add. The Add Address dialog box appears.
5. Select one of the following formats and refer to the applicable section:

Format	Refer to
E.164 Native	page 10-45
DCC AESA	page 10-46
ICD AESA	page 10-46
E.164 AESA	page 10-47
Custom AESA	page 10-48

Native E.164 SVC Addresses

Complete the following information for E.164 (Native) format:

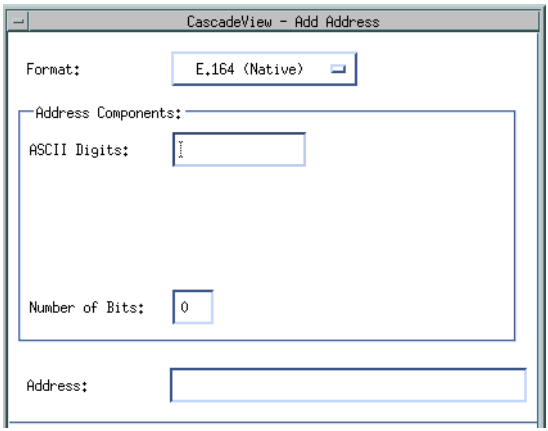


Figure 10-22. Add Address Dialog Box (Native E.164 SVC Address Format)

1. In the ASCII Digits field, enter all of the 1-15 ASCII digits that represent the E.164 address. For example, enter 5085552600 (a standard 10-digit U.S. phone number). The value you enter is converted to the ASCII hex values that represent each digit in the number (this value is displayed in the Address in Hex field).

   For example, 5085552600 converts to 35303835353532363030. The Address in Hex column on the Set All Port Addresses dialog box also displays this value.

2. Refer to Table 10-3 on page 10-41 to configure additional fields.

3. Choose OK to return to the Set All Port Addresses dialog box (Figure 10-21 on page 10-43).

DCC and ICD AESA SVC Addresses

Complete the following information for DCC or ICD AESA format:

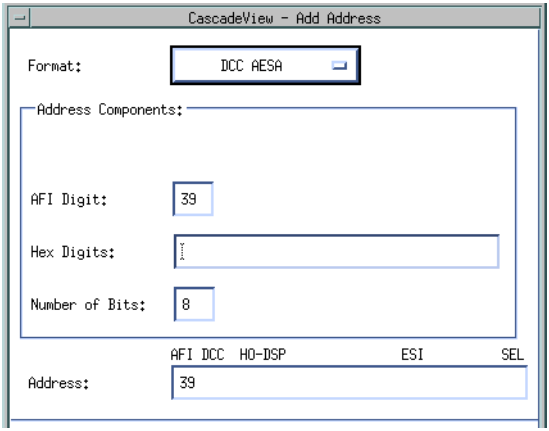


Figure 10-23. Add Address Dialog Box (DCC or ICD AESA Format)

1. In the Hex Digits field, enter the Data Country Code (DCC) of the country in which the address is registered, or the International Country Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.

2. Enter the appropriate HO-DSP, ESI and SEL values. For information on these items, and the appropriate format to use for DCC and ICD AESA addresses, refer to “ATM End System Address (AESA) Formats” on page 10-2.

3. Refer to Table 10-3 on page 10-41 to configure additional fields.

4. Choose OK to return to the Set All Port Addresses dialog box (Figure 10-21 on page 10-43).

E.164 AESA SVC Addresses

Complete the following information for the E.164 AESA format:

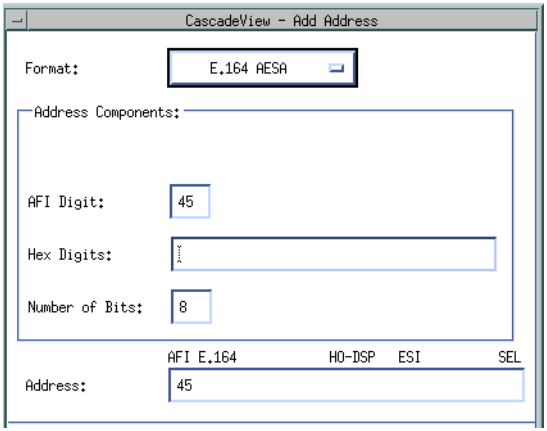


Figure 10-24. Add Address (E.164 AESA Format)

1. In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh. For example, enter 5085551234 as 000005085551234F.

2. After you type the IDI portion of the address, enter the appropriate HO-DSP, ESI, and SEL portions to complete the address. For information on the appropriate format to use for E.164 AESA addresses, refer to "ATM End System Address (AESA) Formats" on page 10-2.

3. Refer to Table 10-3 on page 10-41 to configure additional fields.

4. Choose OK to return to the Set All Port Addresses dialog box (Figure 10-21 on page 10-43).

Custom AESA SVC Addresses

Complete the following information for the Custom AESA format:

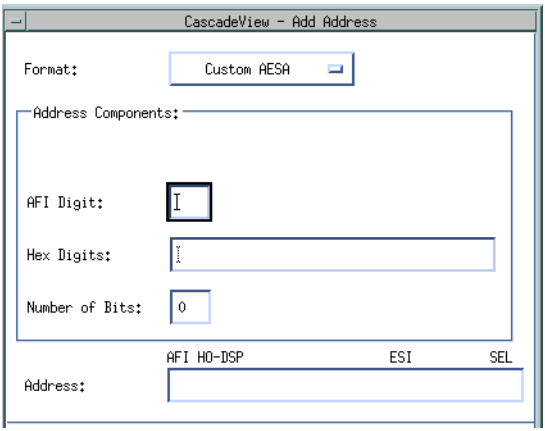


Figure 10-25. Add Address Dialog Box (Custom AESA Format)

1. In the AFI Digits field, enter the custom AFI.
2. In the Hex Digits field, enter the customized address format, starting with the HO-DSP, and followed by the ESI and SEL values (in that order).

   This address must be the full 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. For information on these items, refer to "ATM End System Address (AESA) Formats" on page 10-2.
3. Refer to Table 10-3 on page 10-41 to configure additional fields.
4. Choose OK to return to the Set All Port Addresses dialog box (Figure 10-21 on page 10-43).

Setting All SVC Configurations on the Node

The Set All SVC Configurations function enables you to define various call screening and call handling parameters for each logical port on the switch, including:

- Calling Party Insertion Mode and Address
- Calling Party Screening and Presentation Mode
- Egress/Ingress Address Translation Mode
- SVC Hold Down Timer
- SVC Load Balance Control
- CDV Tolerance
- CUG State

To define the SVC call screening and call handling parameters:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All Port SVC Configurations. The following dialog box appears.

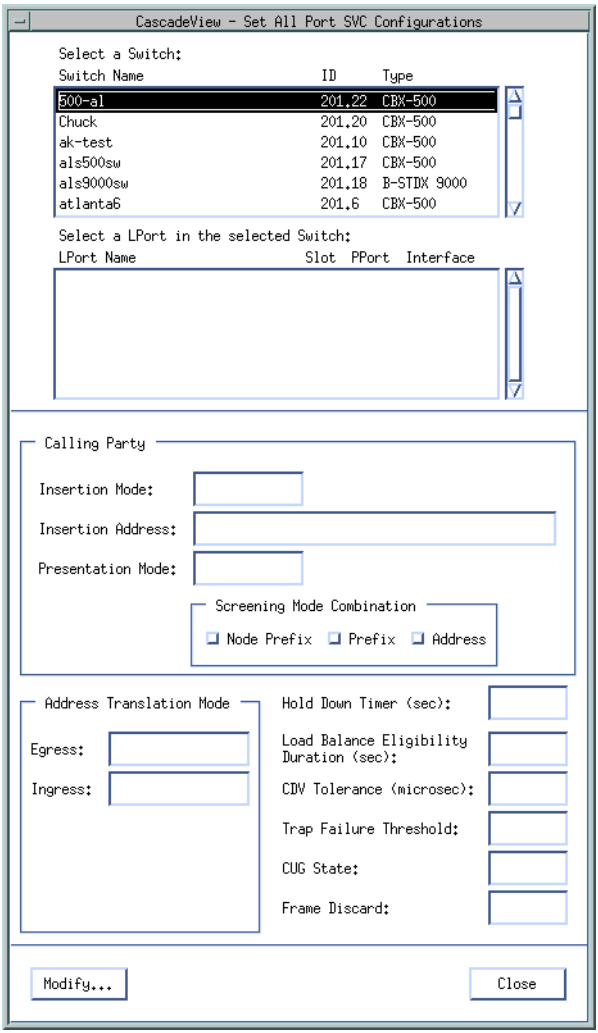


Figure 10-26. Set All Port SVC Configurations Dialog Box

2. Select the switch on which to configure call screening/call handling parameters.
3. Select the logical port on which to configure SVC configuration parameters.

4. Choose Modify. The Modify SVC Configurations dialog box appears.

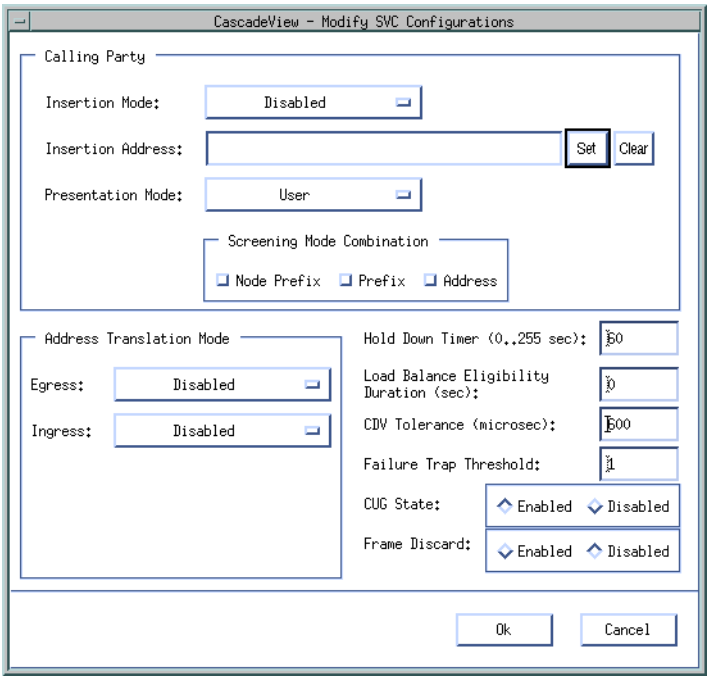


Figure 10-27. Modify SVC Configurations Dialog Box

5. Proceed to the following section to define the calling party insertion address.

Defining Calling Party Insertion Address

1. Select one of the following Insertion Mode options:

For calling party screening to occur, set this field to Disable or Insert. If you select Replace, calling party screening is effectively disabled because the Calling Party Insertion Address is always considered valid. Also, if you select Insert, calling party screening occurs only when the caller signals the calling party address; if the caller does not signal the calling party address, the Calling Party Insertion Address, which is always considered valid, is used.

Disabled — The logical port does not insert or replace the calling party address. If you set the Insertion Mode field to Disable, skip to Step 3 on page 10-53.

Insert — If the logical port receives a call that does not have a calling party information element, it inserts the address that is specified in the Calling Party Insertion Address field.

Replace — When the logical port receives a call:

- If there is no calling party address, it inserts the calling party address specified in the Calling Party Insertion Address field.
- If there is a calling party address, it overwrites the existing calling party information element with the address specified in the Calling Party Insertion Address field.

2. Choose the Set button to the right of the Insertion Address field. The Set Insertion Address dialog box appears.

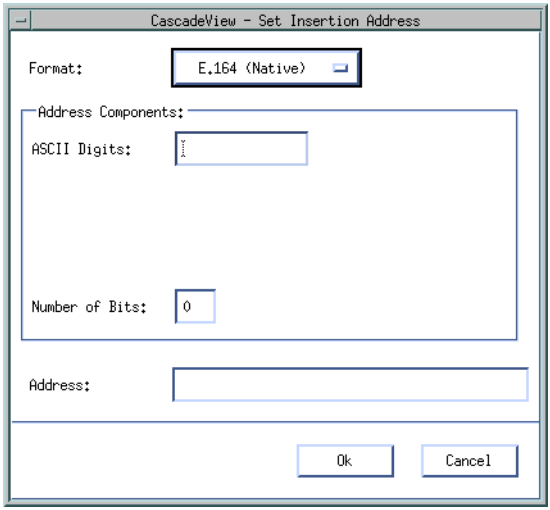


Figure 10-28. Set Insertion Address Dialog Box

The calling party insertion address is not used to route calls to this port. To use the calling party insertion address to route calls to this port, configure the address (or a prefix corresponding to the address) on this port. For more information, refer to "Defining an SVC Port Address" on page 10-43.

3. Select the appropriate SVC Port Address Format. Refer to the applicable section for instructions. Then proceed to the following section to define the calling party presentation mode.

   - For Native E.164 Addresses, refer to page 10-45.
   - For DCC or ICD AESA addresses, refer to page 10-46.
   - For E.164 AESA addresses, refer to page 10-47.
   - For Custom AESA addresses, refer to page 10-48.

Defining Calling Party Presentation Mode

In the Modify SVC Configurations dialog box (Figure 10-27 on page 10-51), select one of the following Presentation Mode options to specify whether or not to include the calling party address on outgoing calls:

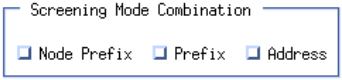
User — Include the calling party address based on the Presentation Indicator in the SETUP message of the user's call.

Always — Always include the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's call.

Never — Never include the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's call.

Defining Calling Party Screening Mode Combination

In the Modify SVC Configurations dialog box (Figure 10-27 on page 10-51), select one or more of the Screening Mode options to specify the level of screening this port performs on the calling party address.



Screening determines whether or not to process an ingress call at this logical port. Select none of these items to disable call screening and accept all calls. If you select more than one item, the ingress call is processed if it meets one or more of the selected criteria (for example, if you select both Node Prefix and Address, the calling party address must match either a valid node prefix or a valid port address).

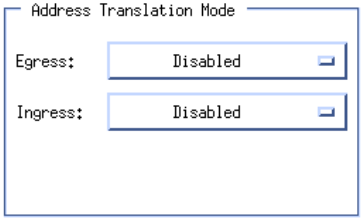
If you enable screening at any level, and the calling party has no calling party address, the call fails unless you set the Calling Party Insertion Mode to Insert or Replace, and configure a Calling Party Insertion Address.

Select one of the following Screening Modes and refer to the corresponding section:

Mode	Description	Refer to
Node Prefix	Screens the calling party against all of the configured node prefixes. If a match is found, the screen is successful.	“Configuring Node Prefixes” on page 10-11
Prefix	Screens the calling party against all of the configured port prefixes. If a match is found, the screen is successful.	“Configuring SVC Port Prefixes” on page 10-22
Address	Screens the calling party against all of the configured port addresses. If a match is found, the screen is successful.	“Configuring SVC Port Addresses” on page 10-40

Defining the Egress and Ingress Address Translation Mode

1. In the Modify SVC Configurations dialog box (Figure 10-27 on page 10-51), select one of the following Egress Address Translation Mode options:



Disabled — No address translation occurs on egress from the logical port.

Tunnel — Select this option if the call is being routed through another network that is using a different address domain (see Figure 10-29). If the calling party address matches a port prefix and the port prefix has a gateway address defined, substitute the local gateway address for the calling party address, and substitute the remote gateway address for the called party address on egress from the logical port. The original addresses are then carried as a sub-address. If you select this option, you should also select Tunnel for the Ingress Address Translation Mode.

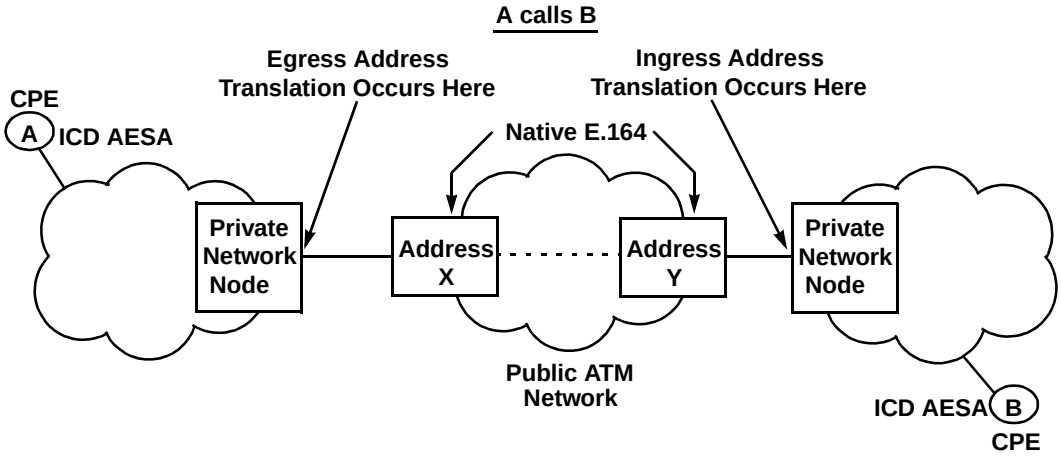


Figure 10-29. Tunnelling Through a Public Network

E.164 Native to AESA — Select this option to convert native E.164 addresses to E.164 AESA format. With this option, the HO-DSP, ESI, and SEL octets of the AESA address are filled with zeros at the network's egress logical port. Also, leading zeros and the trailing Fh are added to the IDP portion. For example, the native E.164 address 5085551234 would be converted to AESA E.164 address 45-000005085551234F-00000000-000000000000-00.

E.164 AESA to Native — Select this option to convert E.164 AESA addresses to native E.164 format. If you select this option, the AFI, HO-DSP, ESI, and SEL octets of the address are removed at the network's egress logical port. Also, all leading zeros and the trailing Fh in the IDP portion of the address are removed. For example, the E.164 AESA address 45-000005085551234F-1A2B3C-0000050F0601-00 would be converted to the native E.164 address 5085551234.

Replace — Select this option if the call is being routed into an attached network that is using a different address domain (see the following illustration). With this option, the calling party address is replaced with the local gateway address and the called party address is replaced with the remote gateway address at the network's egress logical port.

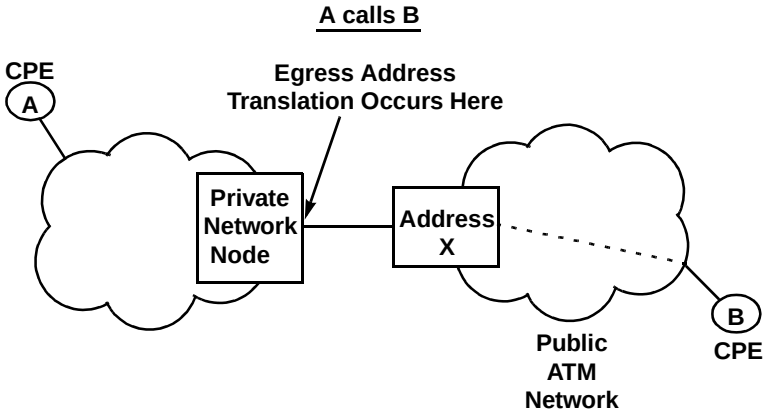


Figure 10-30. Calling Into a Public Network

For more information on egress address translation, refer to "About Address Translation" on page 10-60.

2. Select one of the following Ingress Address Translation Mode options. These options should match those specified for the Egress Address Translation Mode.

   Tunnel — Select this option if a sub-address is present in the SETUP message, to promote it to the address information element at the ingress port.

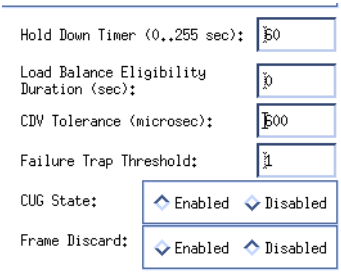
   E.164 Native to AESA — Select this option if you selected E.164 AESA to Native as the Egress Address Translation Mode. If you select this option, the AFI, HO-DSP, ESI, and SEL octets of the address are removed at the network's ingress logical port. Also, all leading zeros and the trailing Fh in the IDP portion of the address are removed. For example, the E.164 AESA address 45-000005085551234F-1A2B3C- 0000050F0601-00 would be converted to the native E.164 address 5085551234.

   E.164 AESA to Native — Select this option if you selected E.164 Native to AESA as the Egress Address Translation Mode. With this option, the HO-DSP, ESI, and SEL octets of the AESA address are filled with zeros at the network's ingress logical port. Also, leading zeros and the trailing Fh are added to the IDP portion. For example, the native E.164 address 5085551234 would be converted to AESA E.164 address 45-000005085551234F-00000000-000000000000-00.

   For more information on ingress address translation, refer to "About Address Translation" on page 10-60.

Defining Additional SVC Configuration Options

The Modify SVC Configuration dialog box (Figure 10-27 on page 10-51) provides additional SVC options.



Use Table 10-4 to review the remaining Modify SVC Configuration dialog box options. When you finish, choose OK to return to the Set All Port SVC Configurations dialog box (Figure 10-26 on page 10-50).

Although you can modify these fields, Cascade recommends you use the default parameters.

Table 10-4. Modify SVC Configuration Options

Field	Action/Description
Hold Down Timer	Enter the number of seconds to wait before the network initiates call clearing when a circuit has gone down (for example, a trunk has gone down, and no reroute is available). If you enter 0, the network clears the SVC immediately upon detection of a trunk outage.
Load Balance Eligibility Duration	Enter the number of seconds an SVC must be established before a call is eligible for load balance rerouting. The default is 3600 seconds. This feature is useful for those SVCs that are long term, and may encounter a forced reroute due to trunk failure.
CDV Tolerance	Configure the Cell Delay Variation Tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. Enter a value between 1 - 65535 µs which represents cell delay tolerance. The default is 600 µs.
Failure Trap Threshold	Enter the threshold crossing alarm value for SVC failure traps. The switch generates a trap if the internal SVC failure counter crosses this threshold during the current 15 minute time period. The internal counter is reset every 15 minutes. The default value of 1 means that if one SVC failure occurs on a logical port, a trap is issued and no additional traps are issued until the next 15-minute period expires. If you change the threshold value to 100, it means that to trigger a trap, 100 SVC failures must occur in a 15-minute window. If you enter 0, the switch never generates a failure trap.
CUG State	Select enable to allow CUG processing for this logical port.

Table 10-4. Modify SVC Configuration Options (Continued)

Field	Action/Description
Frame Discard	(*For CBX 500s equipped with Flow Control Processors only.*) The network performs early packet discard (EDP) for SVCs originating on the logical port only if you enable frame discard and the SVC connection attempt indicates the use of AAL5. Otherwise, the network performs CLP1 discard on SVCs originating on the logical port.

About Address Translation

This section describes how address translation occurs in various situations and at various points along a network connection. This information applies only if you enable address translation. Also, egress address translation requires matching a called party address to a configured prefix on the egress port.

Calling party and called party addresses are stored as information elements in the SETUP message which is sent to initiate call setup. In some situations, calling party and called party sub-addresses are also stored as information elements in the SETUP message.

Calling Party Address	**Called Party Address**
Calling Party Subaddress	**Called Party Subaddress**

Egress address translation, when enabled on a network-to-network port, functions as described in Table 10-5 and Table 10-6. The following factors determine how address translation occurs:

- Whether or not local and/or remote gateway addresses are defined on the egress port
- The type of translation (tunnel or replace) selected as the egress address translation mode
- The numbering plan of the signalled calling and called addresses

Calling party and called party processing are independent. Note that in the SETUP message, the called party address is mandatory, while the calling party address is optional. In the case of a native E.164 called party or calling party address, the related sub-address field is always be set to null, since the sub-address field cannot carry native E.164 addresses (note that in the tables, if the signalled calling party address is native E.164 format, the calling party sub-address field is always set to null).

Using ingress address translation, the calling party sub-address (if it is not null) overwrites the calling party address at the ingress port, and the called party sub-address (if it is not null) overwrites the called party address.

Table 10-5 shows how calling party addresses are translated at the egress port.

Table 10-5. Calling Party Address Translation at Egress Port

Signalled Address	SETUP Information Element	No Local Gateway Address	Local Gateway Address, with Tunnel Option	Local Gateway Address, with Replace Option
No calling party	Calling Party Address	Null	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Null	Null
AESA calling party	Calling Party Address	Signalled AESA Calling Party Address	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Signalled AESA Calling Party Address	Null
Native E.164 calling party	Calling Party Address	Signalled Native E.164 Calling Party Address	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Null	Null

Table 10-6 shows how called party addresses are translated at the egress port.

Table 10-6. Called Party Address Translation at Egress Port

Signalled Address	SETUP Information Element	No Remote Gateway Address	Remote Gateway Address, with Tunnel Option	Remote Gateway Address, with Replace Option
AESA called party	Called Party Address	Signalled AESA Called Party Address	Remote Gateway Address	Remote Gateway Address
	Called Party Sub-address	Null	Signalled AESA Called Party Address	Null
Native E.164 called party	Called Party Address	Signalled Native E.164 Called Party Address	Remote Gateway Address	Remote Gateway Address
	Called Party Sub-address	Null	Null	Null

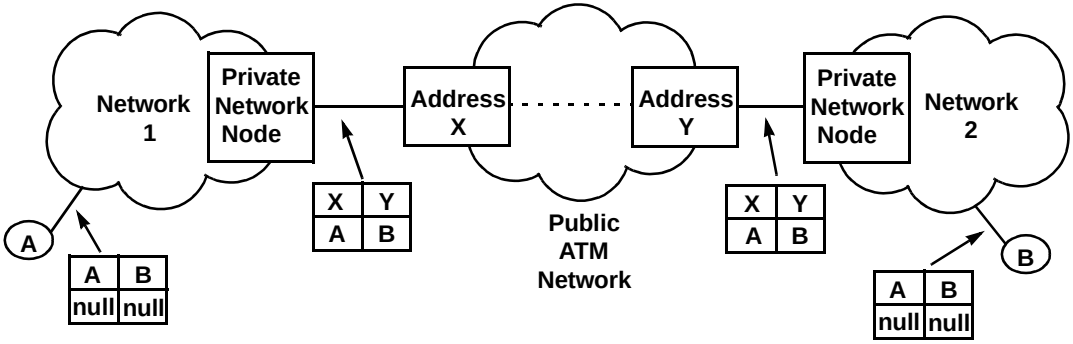
Examples

The following diagrams show some examples of the state of the calling party/called party address and sub-address elements of the SETUP message at various points along the connection.

The example diagrams represent the calling party and called party address and sub-address elements as follows:

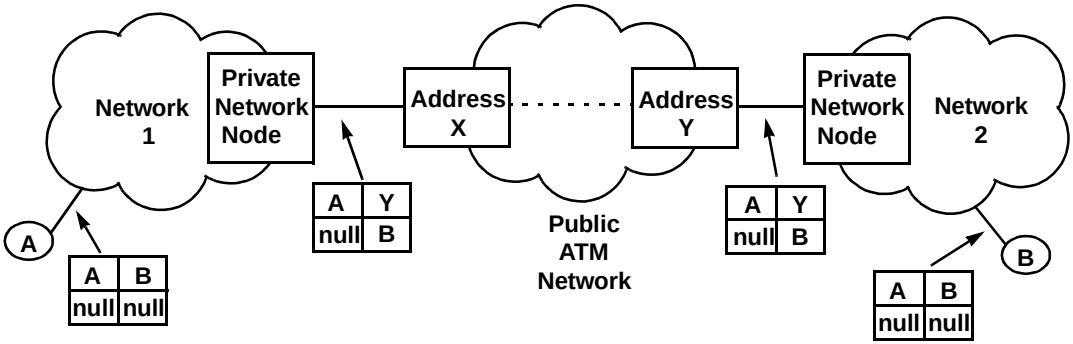
Calling Party Address	Called Party Address
Calling Party Subaddress	Called Party Subaddress

Example 1
- **Egress tunnelling enabled on Network 1's egress port**
- **Ingress tunneling enabled on Network 2's ingress port**
- **Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B**
- **Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B**



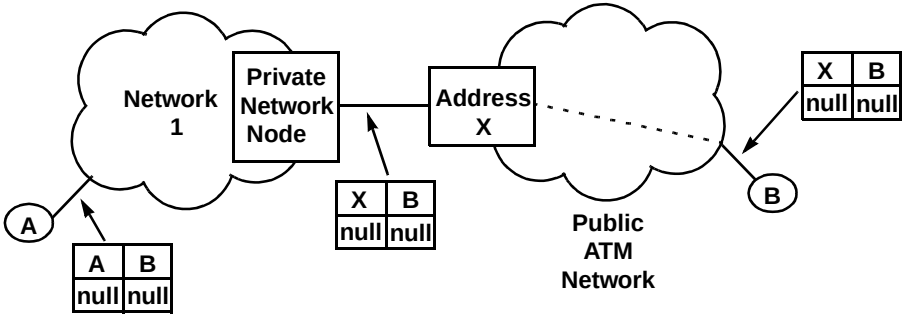
Example 2

- Egress tunnelling enabled on Network 1's egress port
- Ingress tunneling enabled on Network 2's ingress port
- No Local Gateway address defined on egress port
- Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B



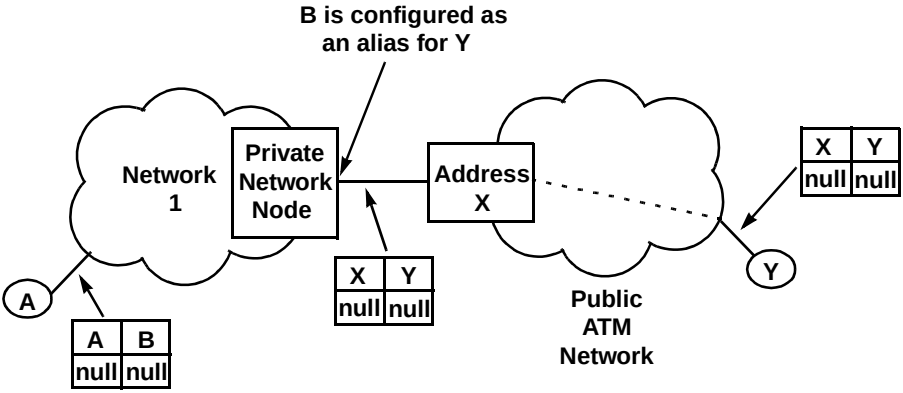
Example 3

- Replace option selected on egress port of Network 1
- Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B



Example 4

- **Replace option selected on egress port of Network 1**
- **Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B**
- **Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B**



11

Configuring SPVCs

A Permanent Virtual Circuit (PVC) is established administratively (i.e., by network management) rather than on demand (i.e., using signaling across the UNI). A soft PVC (SPVC) is established by the network using signaling. Once the SPVC configuration is in place, the switch at one end of the SPVC initiates the signaling.

The network management system provisions one end of the SPVC with the address identifying the egress interface from the network. The calling end has the responsibility for establishing, releasing, and re-establishing the call.

About SPVCs

There are two types of ATM virtual connections: Virtual Channel Connections (VCCs) and Virtual Path Connections (VPCs). These virtual connections are made up of a series of virtual links which form a path between two endpoints. Based on the type of virtual connections you are using (VCC or VPC), you can create either a soft virtual channel connection (SPVCC) or a soft virtual path connection (SPVPC).

When working with SPVCs, you can configure a connection that is point-to-point or point-to-multipoint. In a point-to-multipoint configuration, the CBX 500 endpoint defined as the root can access several terminating endpoints (configured as “leafs”).

When you create an SPVC, you configure one endpoint (known as the *originating endpoint*) as you would a PVC. You select the logical port on which the endpoint will reside, and assign a VPI/VCI address. You configure the other endpoint(s) (*terminating endpoints*) with addresses, as you would an SVC. The originating endpoint uses signaling to access the terminating endpoints.

Using PVC/PVP Termination

Before you can configure SPVCs, you must first configure the SVC address or prefix you want to assign to the SPVC terminating endpoint. This endpoint may not actually terminate the SPVC. When you configure an SVC port address, you enable or disable PVC/PVP termination. If you disable termination, the egress logical port signals the SPVC on as a regular SVC.

If you enable PVC termination, you can optionally specify a VPI/VCI or allow the network to choose a VPI/VCI. The switch terminates the SPVCC on the logical port that is associated with the VPI/VCI, and the traffic then continues on the local PVC segment. If you enable PVP termination, you can optionally specify a VPI or allow the network to choose a VPI, and the CBX 500 terminates the SPVPC on the associated logical port. PVC and PVP termination enables you to send traffic through the network to a non-SVC endpoint, using an SVC. In previous releases, you needed to provision PVCs through the network to access an endpoint that did not support SVCs.

For more information about configuring PVC/PVP Termination on the SVC, refer to page 10-40.

About ATM Traffic Descriptors for SPVCs

When you create an SPVC, you need to configure a set of traffic descriptors. You select a class of service and the traffic parameters which are used to control SPVC traffic. The traffic descriptor combination you configure determines the number and type of cells that are admitted into a congested queue, and whether or not high priority cells are tagged as low priority cells when traffic exceeds the traffic parameter thresholds. For more information about ATM traffic descriptors, refer to page 9-2.

You can configure up to 512 traffic descriptors per switch. When you configure an SPVC, you assign traffic descriptors to the forward and reverse direction of the SPVC. The following table lists the traffic descriptors that are available for each QoS class.

Table 11-1. SPVC QoS Class Traffic Descriptors

QoS Class	Traffic Descriptor	Description
Constant Bit Rate (CBR) (specified/ unspecified)	PCR CLP=0, PCR CLP=0+1, tagging	Traffic conformance is based on the Peak Cell Rate (PCR) of both the CLP=0 and CLP=0+1 cell streams with Tagging enabled.
	PCR CLP=0, PCR CLP=0+1, no tagging	Traffic conformance is based on the PCR of both the CLP=0 and CLP=0+1 cell streams with no Tagging.
	PCR CLP=0+1	Traffic conformance is based only on PCR of the CLP=0+1 aggregate cell stream with no Best Effort.

Table 11-1. SPVC QoS Class Traffic Descriptors (Continued)

QoS Class	Traffic Descriptor	Description
VBR-RT/ VBR-NRT (specified/ unspecified)	PCR CLP=0+1, SCR CLP=0, MBS CLP=0, tagging	Traffic conformance is based on PCR of the CLP=0+1 aggregate cell stream, as well as the Sustained Cell Rate (SCR) and Maximum Burst Size (MBS) of the CLP=0 cell stream with Tagging enabled.
	PCR CLP=0+1, SCR CLP=0, MBS CLP=0, no tagging	Traffic conformance is based on PCR of the CLP=0+1 aggregate cell stream, as well as the SCR and MBS of the CLP=0 cell stream with no Tagging.
	PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1	Traffic conformance is based on PCR, SCR, and MBS of the CLP=0+1 cell stream with no Tagging.
UBR	PCR CLP=0+1	Traffic conformance is based only on PCR of the CLP=0+1 aggregate cell stream with no Best Effort.
Unspecified “Best Effort”	None	A “best effort” attempt is made to deliver all traffic, but there is no guarantee the switch will not drop cells due to congestion.

Configuring ATM Traffic Descriptors

To configure the traffic descriptors:

1. From the Administer menu, choose Cascade Parameters ⇒ Set All ATM Traffic Descriptors. The following dialog box appears.

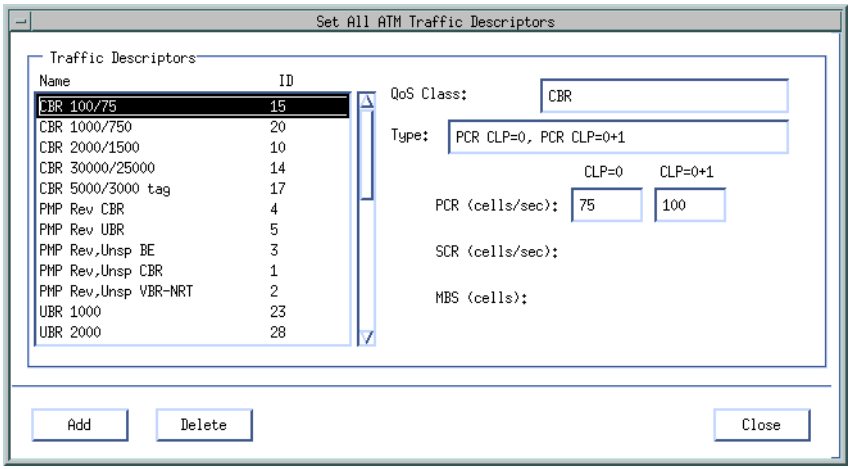


Figure 11-1. Set All ATM Traffic Descriptors Dialog Box

This dialog box displays information about previously configured traffic descriptors. If you need to delete a traffic descriptor, select the name from the list and choose Delete.

2. Choose Add to add a traffic descriptor. The following dialog box appears.

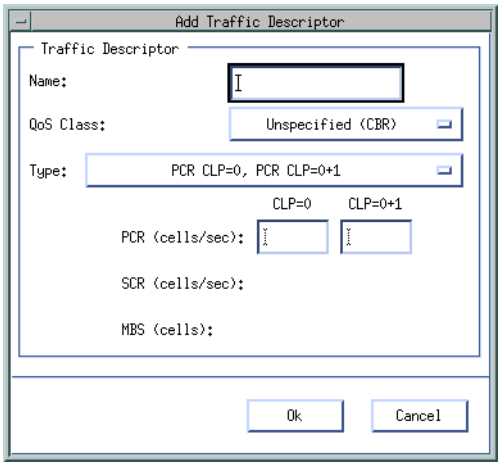


Figure 11-2. Add Traffic Descriptor Dialog Box

3. Enter a name (up to 20 characters) for this character descriptor type.

4. Select the QoS class. The QoS class determines which traffic descriptors you can select. If the attached equipment does not support QoS classes other than 0, select only the unspecified service classes.

Table 11-2 describes each class of service.

Table 11-2. SPVC Traffic Descriptor QoS Classes

Type	Description	QoS Class
CBR	Handles digital information, such as video and digitized voice, that is represented by a continuous stream of bits. CBR traffic requires guaranteed throughput rates and service levels.	1
CBR unspecified	Same as CBR.	0
VBR-RT	For packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.	2
VBR-RT unspecified	Same as VBR-RT.	0
VBR-NRT	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.	3
VBR-NRT unspecified	Same as VBR-NRT.	0
UBR	Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic.	4
UBR unspecified	Same as UBR.	0

5. Select one of the following traffic descriptor types and specify the required values in cells per second.

Table 11-3. SPVC Traffic Descriptor Types

Type	Description
PCR CLP=0+1	Specify the PCR for the CLP=0+1 aggregate cell stream (i.e., high- and low-priority traffic).
PCR CLP=0, PCR CLP=0+1 (tagging or no tagging)	Specify the PCR for the CLP=0 cell stream (i.e., high-priority traffic) and the PCR for the CLP=0+1 aggregate cell stream (i.e., combined high- and low-priority traffic).
PCR CLP=0+1, SCR CLP=0, MBS CLP=0 (tagging or no tagging)	Specify the PCR for the CLP=0+1 aggregate cell stream (i.e., combined high- and low-priority traffic), the Sustained Cell Rate (SCR) for the CLP=0 cell stream (i.e., the combined high-priority traffic), and the Maximum Burst Size (MBS) for the CLP=0 stream.
PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1 (no tagging)	Specify the PCR for the CLP=0+1 aggregate cell stream (i.e., combined high- and low-priority traffic), the SCR for the CLP=0+1 cell stream, and the MBS for the CLP=0+1 stream.
UBR	Specify the PCR for the CLP=0+1 aggregate cell stream (i.e., combined high- and low-priority traffic).

6. Choose OK to set the ATM traffic descriptor. The Set All ATM Traffic Descriptors dialog box appears (Figure 11-1 on page 11-5).

7. Choose Add to repeat these steps to create additional ATM traffic descriptors or choose Close to return to the network map.

About Point-to-Point SPVCs

To access the Set All Point-to-Point SPVCs dialog box, from the Administer menu, select Cascade Parameters ⇒ Set All Soft PVCs ⇒ Point-to-Point. The following dialog box appears.

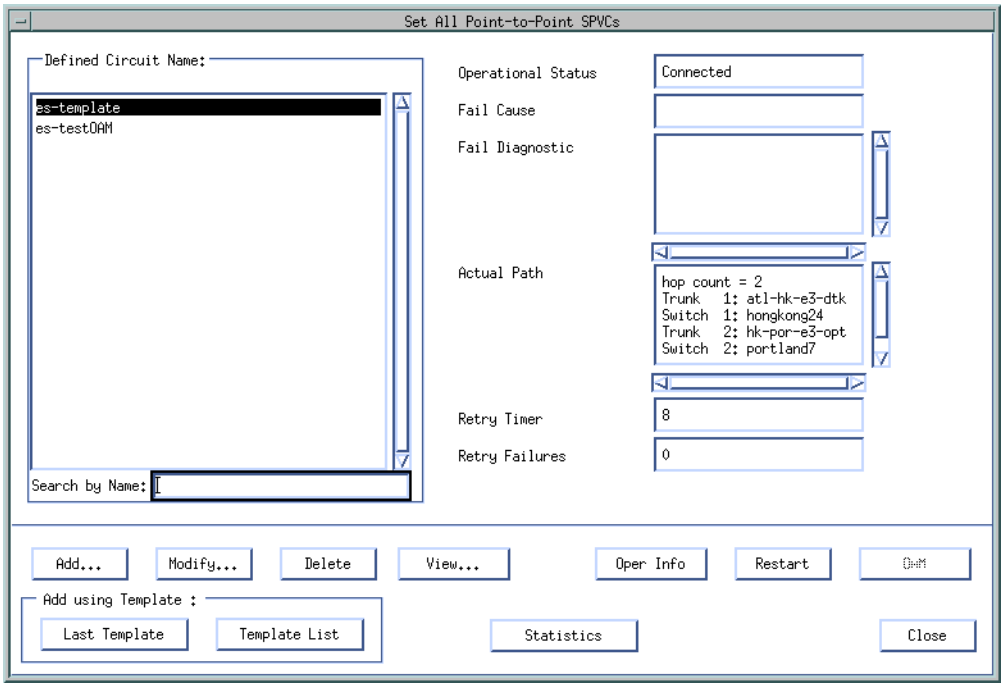


Figure 11-3. Set All Point-to-Point SPVCs

To view a list of configured SPVCs, position the cursor in the Search by Name field and press Return. To use a wildcard search to find a specific SPVC name, you can:

- 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 \\

The Set All Point-to-Point SPVCs dialog box displays information about the configured options for the Defined Circuit Name you select. Table 11-4 describes the dialog box status indicators and commands.

Table 11-4. Set All Point-to-Point SPVCs Dialog Box Status Indicators and Commands

Field/Command	Action/Description
Operational Status	Displays a status message: Establishing, Connected, Failed, or Other.
Fail Cause ID	Displays the ID of the last release failure.
Fail Diagnostic	Displays an eight-character diagnostic of the last release failure (as applicable).
Actual Path	Displays a character string that represents the actual path the SPVC used.
Retry Timer	Displays the current value of the retry timer in seconds.
Retry Failures	Displays the number of failed attempts to establish a connection.
Add	Enables you to add an SPVC.
Modify	Enables you to modify an SPVC.
Delete	Enables you to delete an SPVC.
View	Enables you to view the configured attributes for the selected SPVC.

Table 11-4. Set All Point-to-Point SPVCs Dialog Box Status Indicators and Commands (Continued)

Field/Command	Action/Description
Oper Info	Updates the information in the following Operational Status fields: • Fail Cause ID • Fail Diag • Actual Path • Retry Time • Retry Failure
Restart	Restarts the selected SPVC no matter what condition it is in. If the SPVC is not established, it restarts the process to establish the connection. If it is established, this command clears the existing connection and establishes it again.
OAM	Runs the Operations, Administration, and Management loopback diagnostics for the selected circuit.
Statistics	Displays the summary statistics for the selected SPVC.
Add using Template	If you have already defined an SPVC configuration and saved it as a template, use this command to define a new circuit using similar parameters. • Choose Last Template to use the last template you used to establish a circuit in this NMS session. • Choose Template List to display a list of templates previously defined for this map.
Close	Exits this dialog box and return to the network map.

Setting the VPI/VCI Values for SPVCs

For each SPVC you configure, you must specify a value from 0 – *nnnn* to represent the Virtual Path Identifier (VPI) for the SPVC. The maximum value is based on the Valid Bits in VPI that is configured for the logical port, as follows:

Maximum value = $2^P - 1$

where *P* is the value in the Valid Bits in VPI field. For example, if you entered 5 in the Valid Bits in VPI field, the maximum value is 31 ($2^5 - 1 = 31$) which would give you up to 32 virtual paths (numbered 0-31).

If you are defining a Soft Permanent Virtual Channel Connection (SPVCC), you must also specify a value to represent the Virtual Channel Identifier (VCI) for an ATM circuit. The maximum value is based on the Valid Bits in VCI value that is configured for the logical port, as follows:

Maximum value = $2^C - 1$

where *C* is the value in the Valid Bits in VCI field. For example, if you entered 6 in the Valid Bits in VCI field, the maximum VCI value you can enter is 63 (which would give you 32 virtual channels, numbered 32 to 63).

These VPI/VCI range restrictions only apply to SPVCCs. You can provision SPVPCs to use the following values:

For UNI, use the VPI=0-255 range.
For NNI cell header format, use the VPI=0-4095

For more information on the Valid Bits in VPI/VCI fields, refer to *Table 7-1 on page 7-6**.*

Adding an SPVC

To add an SPVC:

1. From the Set All Point-to-Point SPVCs dialog box (Figure 11-3 on page 11-9), choose Add. The following dialog box appears.

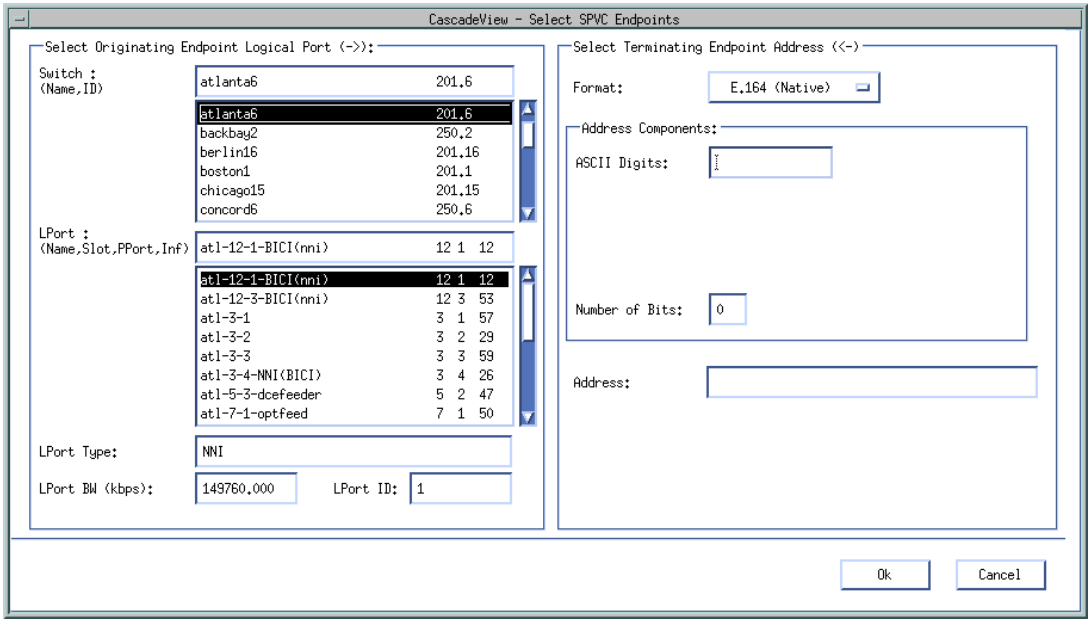


Figure 11-4. Select SPVC Endpoints Dialog Box

2. Configure the originating endpoint logical port:
   a. Select the name of the switch on which the endpoint will reside.
   b. Select the name of the logical port that will be used as the endpoint.

      The dialog box displays the logical port type, bandwidth, and ID for this endpoint.

3. Use Table 11-5 to select the address format and configure the terminating endpoint address.

For more information on AESA address formats, refer to page 10-2.

Table 11-5. Configuring the SPVC Terminating Endpoint Address

Address Format	Address Components
E.164 (Native)	In the ASCII Digits field, enter all of the 1-15 ASCII digits that represent the E.164 address. The value you enter is then converted to the ASCII hex values that represent each digit in the number (this value is displayed in the Address).
DCC and ICD AESA	In the Hex Digits field, enter the Data Country Code (DCC) of the country in which the address is registered, or the International Country Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets. Then enter the appropriate HO-DSP, ESI and SEL values.

Table 11-5. Configuring the SPVC Terminating Endpoint Address (Continued)

Address Format	Address Components
E.164 AESA	• In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh. For example, 5085551234 should be entered as 000005085551234F. • After typing in the IDI portion of the address, enter the appropriate HO-DSP, ESI, and SEL portions to complete the address.
Custom AESA	• In the AFI Digits field, enter the custom AFI you want to use. • In the Hex Digits field, enter the customized address format you want to use, starting with the HO-DSP, and followed by the ESI and SEL values (in that order). This address must be the full 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL.

4. Choose OK. The following dialog box appears.

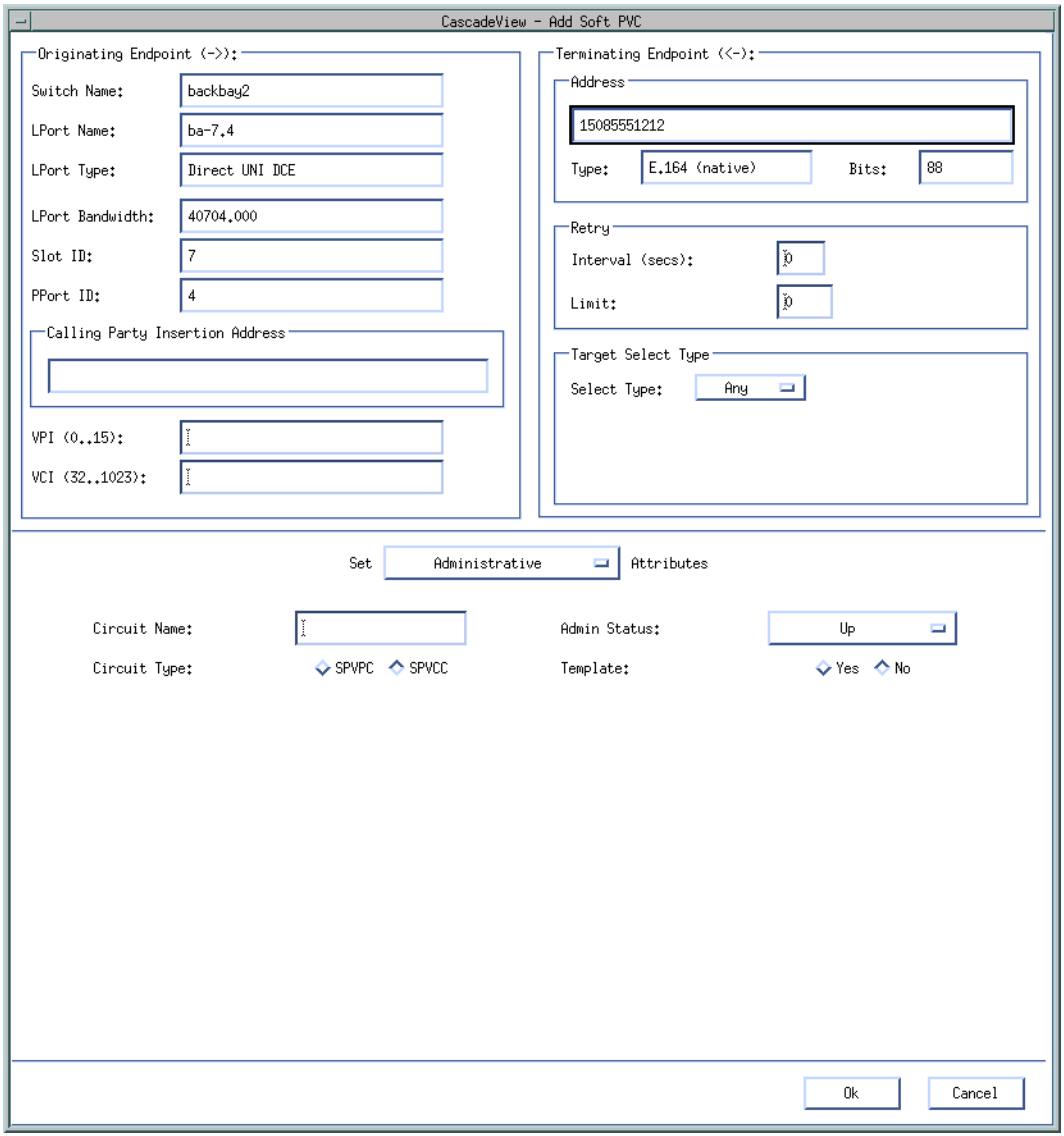


Figure 11-5. Add Soft PVC Dialog Box

5. For the Originating endpoint, define the VPI/VCI values. (Refer to page 11-12 for more information.)

Field	Description
VPI	Enter a value from 0 – *nnnn* to represent the VPI for the SPVC. The maximum value you can enter is based on the Valid Bits in VPI that is configured for the logical port. (Enter a value from 0 – 4095 if you use the NNI cell header format.)
VCI (*SPVCCs only*)	If you are configuring a Soft Permanent Virtual Channel Connection (SPVCC), enter a value to represent the VCI for the SPVCC.

6. Configure the Terminating Endpoint.

Field	Description
Retry Interval	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying to reestablish a connection. Specify this interval in seconds (1 – 3600), or enter 0 (default) for no retries.
Retry Limit	This value indicates the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535), or enter 0 (default) for an unlimited number of retries.
Target Type	In this release, this field is set to Any which indicates the terminating endpoint uses any available VPI/VCI value. This method supports the current IISP signaling protocol, which can only propagate the SVC address through the network. If you want to specify a VPI/VCI for the terminating endpoint, you must enable PVC Termination on the SVC Address dialog box. Refer to "About SVC Port Address Options" on page 10-40.

7. Set the Administrative Attributes.

Field	Description
Circuit Name	Enter any unique, alphanumeric name to identify the SPVC. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (the default) to activate the SPVC at switch start-up, or Down if you do not want to activate the SPVC at switch start-up.
Circuit Type	Specify whether the circuit is a Soft Permanent Virtual Path Connection (SPVPC) or Soft Permanent Virtual Channel Connection (SPVCC, the default). If you select SPVPC, the VCI field is set to 0 and cannot be changed.
Template *(Optional)*	You can save these settings as a template to configure another SPVC with similar options. To create a template, choose Yes in the “Is Template” field.

8. Choose Set [Traffic Type] Attributes to select the traffic descriptors for this SPVC. The following dialog box appears.

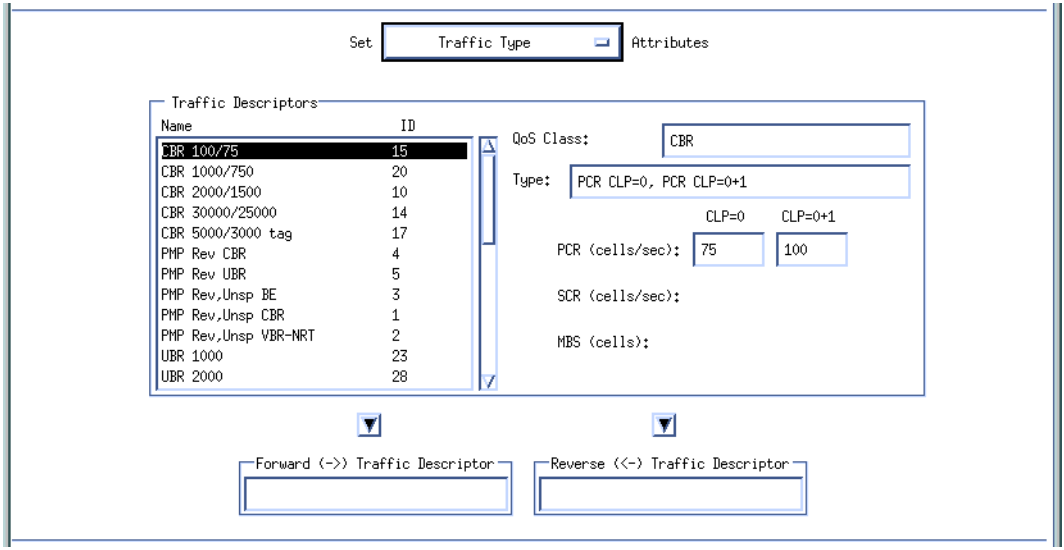


Figure 11-6. Add Soft PVC Dialog Box - [Set Traffic Type]

9. To create a new traffic descriptor definition, complete Step a and Step b. To use an existing definition, continue with Step 10:

   a. Choose the Add Traffic Descriptor command to display the Add Traffic Descriptor dialog box (Figure 11-2 on page 11-6).

   b. Use Step 3 through Step 6 starting on page 11-6 to configure the traffic descriptor.

10. Select a traffic descriptor name from the list and click on the arrow to assign this as either the forward or reverse traffic descriptor. You must assign a traffic descriptor in both the forward and reverse directions.

11. Choose OK to create the new SPVC and return to the Set All Point-to-Point SPVCs dialog box (Figure 11-3 on page 11-9).

12. Choose Close to return to the network map.

Configuring Point-to-Multipoint SPVCs

To access the Set All Point-to-Multipoint SPVCs dialog box, from the Administer menu, select Cascade Parameters ⇒ Set All Soft PVCs ⇒ Point-to-Multipoint. The following dialog box appears.

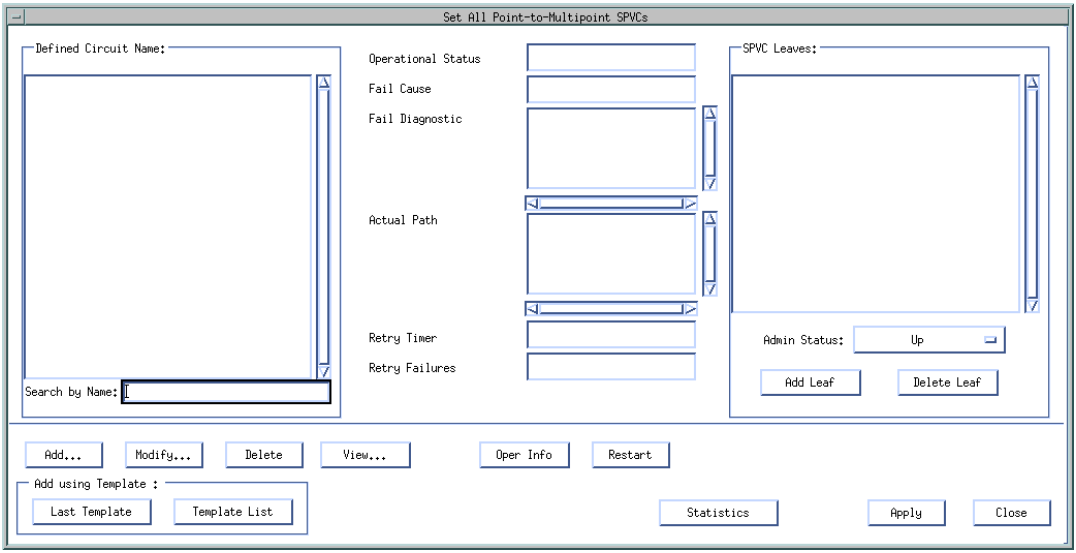


Figure 11-7. Set All Point-to-Multipoint SPVC Dialog Box

To view a list of configured Point-to-Multipoint SPVCs, position the cursor in the Search by Name field and press Return. To use a wildcard search to find a specific SPVC name, you can do any of the following:

- 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 \\

The Set All Point-to-Multipoint SPVCs dialog box displays information about the configured options for the Defined Circuit Name you select. Table 11-4 on page 11-10 describes the dialog box status indicators and commands.

Adding a Point-to-Multipoint SPVC

When you configure a Point-to-Multipoint SPVC, you first define an SPVC consisting of a root (originating endpoint) and one leaf (terminating endpoint). This procedure is similar to the one for creating Point-to-Point SPVCs. Once you define the initial root/leaf combination, you can create additional leafs.

Defining the Point-to-Multipoint SPVC Root

1. From the Set All Point-to-Multipoint SPVC dialog box, choose Add. The Select SPVC Endpoints dialog box appears (Figure 11-4 on page 11-13).
2. Configure the originating endpoint logical port (root):
   a. Select the name of the switch on which the endpoint will reside.
   b. Select the name of the logical port that will be used as the endpoint.

      The dialog box displays the logical port type, bandwidth, and ID for this endpoint.
3. Use Table 11-5 on page 11-14 to select the address format and configure the terminating endpoint address for this leaf.

For more information on AESA address formats, refer to page 10-2.

4. Choose OK. The Add Soft PVC dialog box appears (Figure 11-5 on page 11-16).

5. For the originating endpoint (root), define the VPI/VCI values. (Refer to page 11-12 for more information.)

Field	Description
VPI	Enter a value from 0 – *nnnn* to represent the VPI for the SPVC. The maximum value you can enter is based on the Valid Bits in VPI that is configured for the logical port. (Enter a value from 0 – 4095 if you use the NNI cell header format.)
VCI (*SPVCCs only*)	If you are configuring a Soft Permanent Virtual Channel Connection (SPVCC), enter a value to represent the VCI for the SPVCC.

6. Configure the terminating endpoint (leaf).

Field	Description
Retry Interval	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying again to establish a connection. Specify this interval in seconds (1 – 3600), or enter 0 (default) for no retries.
Retry Limit	This value indicates the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535), or enter 0 (default) for an unlimited number of retries.
Target Type	In this release, this field is set to Any which indicates the terminating endpoint uses any available VPI/VCI value. This method supports the current IISP signaling protocol, which can only propagate the SVC address through the network. If you want to specify a VPI/VCI for the terminating endpoint, you must enable PVC Termination on the SVC Address dialog box. Refer to "About SVC Port Address Options" on page 10-40 for more information.

7. For the SPVC, set the Administrative Attributes.

Field	Description
Circuit Name	Enter any unique, alphanumeric name to identify the SPVC. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (the default) to activate the SPVC at switch start-up, or Down if you do not want to activate the SPVC at switch start-up.
Circuit Type	Specify whether the circuit is a Soft Permanent Virtual Path Connection (SPVPC) or Soft Permanent Virtual Channel Connection (SPVCC, the default). If you select SPVPC, the VCI field is set to 0 and cannot be changed.
Template *(Optional)*	You can save these settings as a template to configure another SPVC with similar options. To create a template, choose Yes in the "Is Template" field.

8. Choose Set Traffic Type Attributes (Figure 11-6 on page 11-19) to select the traffic descriptors for this SPVC.

9. To create a new traffic descriptor definition, complete Step a and Step b. To use an existing definition, continue with Step 10:

   a. Choose the Add Traffic Descriptor command to display the Add Traffic Descriptor dialog box (Figure 11-2 on page 11-6).

   b. Use Step 3 through Step 6 starting on page 11-6 to configure the traffic descriptor.

10. Select a traffic descriptor name from the list and click on the arrow to assign this as either the forward or reverse traffic descriptor.

11. Choose OK to create the new SPVC and return to the Set All Point-to-Multipoint SPVCs dialog box.

Defining Additional SPVC Leafs

1. Once you configure the circuit root and initial leaf, choose Add Leaf to configure additional SPVC leafs. The following dialog box appears.

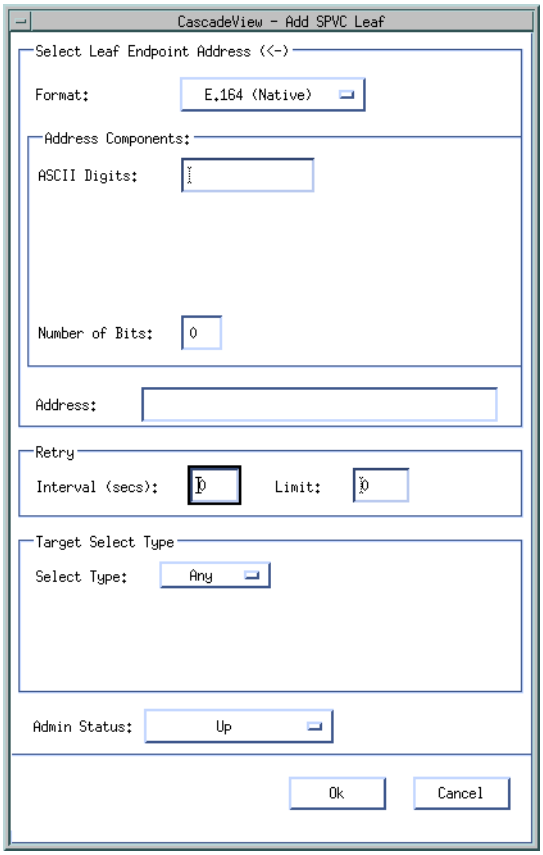


Figure 11-8. Add SPVC Leaf Dialog Box

2. Use Table 11-5 on page 11-14 to select the address format and configure the address components for this leaf. For more information on AESA address formats, refer to page 10-2.

3. Define the retry attributes.

Field	Description
Retry Interval	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying again to establish a connection. Specify this interval in seconds (1 – 3600), or enter 0 (default) for no retries.
Retry Limit	This value indicates the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535), or enter 0 (default) for an unlimited number of retries.
Target Type	In this release, this field is set to Any which indicates the terminating endpoint uses any available VPI/VCI value. This method supports the current IISP signaling protocol, which can only propagate the SVC address through the network. If you want to specify a VPI/VCI for the terminating endpoint, you must enable PVC Termination on the SVC Address dialog box. Refer to "About SVC Port Address Options" on page 10-40 for more information.

4. Choose OK to return to the Set All Point-to-Multipoint SPVC dialog box (Figure 11-7 on page 11-20).

12

Downloading the Configuration

This chapter describes the procedures you can use to establish NMS-to-switch communications. You can use these procedures to activate a new switch or to reconfigure an existing switch. This chapter also describes the following PRAM functions:

Synchronize PRAM — Sends the specific configuration information (for logical ports, circuits, and so on.) to the switch. Refer to page 12-18 for details.

Erase PRAM — Enables you to clear a configuration file from switch memory. Refer to page 12-20 for details.

Upload PRAM — Enables you to compare the configuration file in switch PRAM to the configuration file in the NMS database. Refer to page 12-22 for details.

Generate PRAM — Enables you to create a file of the SNMP set requests for offline management. Refer to page 12-26 for details.

Establishing NMS-to-Switch Communications

You can establish NMS-to-switch communications using the following methods:

Console Install — You run this procedure from the switch console using the Install command. It is the fastest and easiest way to enter the basic configuration into switch PRAM to enable NMS-to-switch communications.

PRAM Kermit — This method uses the CascadeView Generate PRAM command to create a copy of the PRAM files for the SP module and all populated IOMs. You then use the Kermit file transfer protocol to transfer these files from a host (the NMS workstation or a stand-alone PC) to the switch via the switch console port. Once you transfer these files and the Kermit protocol warmboots the SP and all affected IOMs, NMS-to-switch communications are enabled. You can use this method for both gateway and non-gateway switches, and it works for all types of NMS connections.

Initialization File Download — This method uses the CascadeView Initialize Switch command to create a file that contains all the necessary SNMP set requests to replicate the entire switch, card, physical port, logical port, and trunk configuration. You then transfer the file from a host (which can be the NMS workstation or a stand-alone PC) to the switch via the switch console port. NMS-to-switch communications are enabled once you transfer this file. You can use this method for both gateway and non-gateway switches, and it works for all types of NMS connections.

Using the Console Install Procedure

This procedure is often the quickest way to establish NMS communications with a switch. The procedure has a number of configuration options. These options and their use are summarized below:

Direct Ethernet — For use in cases where the NMS workstation and the switch share the same Ethernet segment

Indirect Ethernet — For use in cases where the NMS workstation has connectivity to the Ethernet interface on the switch through a gateway device such as a router.

Direct Trunk — For use in cases where the NMS workstation has connectivity to the switch via a Direct Trunk connection to the gateway switch (or any other switch that has NMS connectivity)

ATM Optimum Trunk — For use in cases where the NMS workstation has connectivity to the switch via an ATM Optimum Trunk connection to the gateway switch (or any other switch that has NMS connectivity)

If this switch has an existing configuration in PRAM, you must first clear PRAM using the Erase PRAM command, before you can run the Install program (refer to page 12-20). In addition, before you run the console Install program, make sure you have the following information:

- IP address and netmask of the network in which the switch will reside.
- Internal IP address of the switch you are configuring.
- IP address and community name of the NMS workstation.
- External IP address of the switch you are configuring (only required when using the direct or indirect Ethernet option).
- IP address of the port on the gateway device assigned to the NMS and switch (only required when using the indirect Ethernet option).
- Internal IP address of the adjacent switch (only required when using the direct or OPTimum trunk option).
- Interface index of the local and remote switch trunk endpoint logical ports. This is only required for the direct or OPTimum trunk option. If you use the OPTimum trunk option, you must also know the local feeder port interface index and local VPI.
- Relevant physical layer parameters used on the trunk (only required when using the direct or optimum trunk option).

To run the console Install program:

1. Establish a connection to the switch console port using either the NMS workstation or stand-alone PC.

2. At the >> prompt, enter **install**. The system responds with the following message:

```
Cascade Communications Corporation
      Switch Installation

This installation procedure is used to establish initial
connectivity between the sWitch and the NMS. Once this
connectivity is established, the remaining configuration
actions should be performed directly from the NMS.

The following NMS connectivity options are available for
this switch:
- Direct Ethernet
- Indirect Ethernet (through a gateway device)
- Direct Trunk (through an adjacent switch)
- ATM OPTimum Trunk (through an adjacent switch)
```

3. The system prompts you for the following information. Enter the appropriate response and press Return after each entry.

```
Enter the network number:
```

Enter the IP address of the switch's network.

```
Enter the network mask:
```

Use the default, Class B, or enter 255.255.255.0 for Class C.

```
Enter the address of this switch:
```

Use the default internal IP address shown if this is the first switch in the network, or modify the last octet to represent the actual switch address.

```
Enter the NMS IP address:
```

Enter the IP address of the NMS workstation used to manage this switch.

```
Enter the SNMP community name:
```

Enter the community name of the NMS used to manage this switch. The default community name is cascade.

4. The system displays the following menu.

```
Which interface will this switch use to communicate with the
NMS?

1. Direct Ethernet
2. Indirect Ethernet (through a gateway device)
3. Direct Trunk (through an adjacent switch)
4. ATM OPTimum Trunk (through an adjacent switch)
```

   - If Direct Ethernet is used, then continue with Step 5.
   - If Indirect Ethernet is used, then continue with Step 6 on page 12-6.
   - If Direct Trunk is used, then continue with Step 7 on page 12-6.
   - If ATM Optimum Trunk is used, then continue on to Step 8 on page 12-8.

5. Select 1 for Direct Ethernet and enter the external IP address assigned to the switch and press Return. The system then provides the entered values as shown in the following example.

```
Network                  201.201.250.0
Network mask       255.255.0.0
Switch Address     201.201.250.1
NMS address:       152.148.81.20
SNMP community:cascade
Interface -> NMSDirect Ethernet
Ethernet IP           152.148.81.69

Is this configuration correct? (Y/N):
```

   - If the selected configuration is correct, enter **Y** and continue with Step 9 on page 12-9.
   - If not, enter **N**. You are prompted to re-enter the correct information.

6. Select 2 for Indirect Ethernet and enter the IP address of the gateway device and Ethernet port assigned to the switch and press Return. The system then provides the entered values as shown in the following example.

```
Network                  201.201.250.0
Network mask       255.255.0.0
Switch Address     201.201.250.1
NMS address:       150.124.100.1
SNMP community:cascade
Interface -> NMSIndirect Ethernet (through a gateway device)
Gateway to NMS     150.124.100.2

Ethernet IP           152.148.81.69

Is this configuration correct? (Y/N):
```

- If the selected configuration is correct, enter **Y** and continue with Step 9 on page 12-9.
- If not, enter **N**. You are prompted to re-enter the correct information.

7. Select 3 for Direct Trunk. At the following prompts, enter the appropriate response and press Return after each entry.

```
What card type is used for the trunk?
   1       8 port DS3
   2       8 port E3
   3       4 port OC3/STM1
   4       1 port OC12/STM4
   5       8 port T1
   6       8 port E1
Enter choice: 1

Enter the slot # of the trunk card: 3

Enter the port number of the trunk: 1

Enter the local trunk interface # of the trunk: 10
```

```
Enter the remote trunk interface # of the trunk: 100

Enter the IP address of the switch at the remote end:
201.201.201.14

Enter the Cell Payload Scrambling Mode:
      1      Disabled
      2      Enabled

Enter Choice: 1

Enter Cell Mapping Mode:
      1      PLCP
      2      Direct Mapping
Enter Choice: 1

Configuration selected:
      Network:                                  201.201.201.0
      Network mask:                             255.255.0.0
      Switch address:                           201.201.201.1
      NMS address:                              152.148.21.20
      SNMP community:                           cascade
      Interface->NMS:                           Direct Trunk
(through an adjacent switch)
      IP address of SWITCH at the remote end: 201.201.201.14
      Remote trunk interface #:                     100
      Card type:                                    8 port DS3
      Slot number:                                  3
      Port number:                                  1
      Local trunk interface #:                      10
      Cell payload scrambling:                      Disabled
      Cell mapping mode:                        PLCP

Is this configuration correct? (Y/N):
```

- If the selected configuration is correct, enter **Y** and continue with Step 9 on page 12-9.
- If not, enter **N**. You are prompted to re-enter the correct information.

8. Select 4 for ATM Optimum Trunk. At the following prompts, enter the appropriate response and press Return after each entry.

```
What card type is used for the trunk?
          1         8 port DS3
          2         8 port E3
          3         4 port OC3/STM1
          4         1 port OC12/STM4
          5         8 port T1
          6         8 port E1
Enter choice: 1

Enter the slot # of the trunk card: 3

Enter the port number of the trunk: 1

Enter the local user link (feeder) interface # of the trunk: 9

Enter the local trunk interface # of the trunk: 10

Enter the remote trunk interface # of the trunk: 100

Enter the IP address of the switch at the remote end:
201.201.201.14

Enter the Cell Payload Scrambling Mode:
          1       Disabled
          2       Enabled

Enter Choice: 1

Enter Cell Mapping Mode:
          1       PLCP
          2       Direct Mapping

Enter Choice: 1

Enter VPI for local OPTimum trunk endpoint: 5
```

```
Configuration selected:
      Network:                                  201.201.201.0
      Network mask:                             255.255.0.0
      Switch address:                           201.201.201.1
      NMS address:                              152.148.21.20
      SNMP community:                           cascade
      Interface->NMS:                           ATM Optimum Trunk
(through an adjacent switch)
      IP address of SWITCH at the remote end: 201.201.201.14
      Remote trunk interface #:                 100
      Card type:                                8 port DS3
      Slot number:                              3
      Port number:                              1
      Local trunk interface #:                  10
      Local user link (feeder) interface #      9
      Cell payload scrambling:                  Disabled
      Cell mapping mode:                        PLCP
      VPI                                  5

Is this configuration correct? (Y/N):
```

- If the selected configuration is correct, enter **Y** and continue with Step 9.
- If not, enter **N**. You are prompted to re-enter the correct information.

9. After selecting **Y**, the system displays the following message:

```
Committing
Preliminary installation complete!
Use NMS to complete the full installation
```

At this point, the NMS can communicate with the switch. You now must PRAM Sync the SP module and all populated IOMs (refer to page 12-18).

If the NMS cannot communicate with the switch, verify that the NMS has the proper routing information. Use the UNIX **netstat -rn** command to verify that a route exists from the NMS workstation to the switch.

Using the PRAM Kermit Procedure

To use the Kermit procedure, first use the CascadeView Generate PRAM command to generate the exact PRAM configuration file for the SP module and IOMs. Then use the Kermit file transfer protocol to transfer this configuration file to the switch. If this is a gateway switch, you only need to transfer the SP PRAM file. If this is a non-gateway switch, you must transfer the SP PRAM file and the PRAM file for the IOM that provides the trunk connection to the gateway switch.

To use Kermit to download the PRAM files to the switch:

1. Use the Generate PRAM function (refer to page 12-26) to generate a configuration file for the SP and IOM(s).

   - *If this is a gateway switch*, you do not have to use the Generate PRAM command for any IOMs.
   - *If this is not a gateway switch*, you must generate a PRAM file for the IOM that provides the trunk connection to the gateway switch.

   The NMS stores the generated PRAM files in the */opt/CascadeView.var/cfgSyncFiles* directory. The directory that contains the PRAM files associated with CBX 500 switches, running release 02.00.00 switch code, may look like the following:

   500-02_00_00

   In this directory, there are files that include the name of the switch associated with the file followed by a .Pslot number. For example, for switch Westford1, the SP PRAM file would look like *Westford1.P01*. If the PRAM file was from the IOM in slot 14, the PRAM file would look like *Westford1.P14*. These are the files you must transfer to the switch.

2. From either the NMS or PC, make a console connection to the switch (19200 bps).
3. At the console prompt, enter **kermit**. The console port is set in kermit mode for file transfer.
4. Start a kermit session with binary-file transfer mode selected.
5. Transfer the SP PRAM file. Once complete, the kermit session automatically closes out and the SP should automatically “warmboot”.

6. (*Optional*) To transfer the IOM PRAM file(s), repeat Step 3 through Step 5.

7. Once complete, the NMS should be able to access the switch. If the Switch Back Panel dialog box displays any of the remaining IOMs in yellow, PRAM Synch them. Refer to "Using the Synchronize PRAM Command" on page 12-18 for details.

Using the Initialization File Download Procedure

The CascadeView/UX Initialize Switch command creates a file containing all the SNMP set requests necessary to replicate the entire switch, card, physical port, logical port, and trunk configuration. You can then transfer this file to the switch using either a text transfer protocol, such as Tip, or terminal emulation.

The Initialize Switch command generates an initialization-script file that contains the SNMP SET commands for each configuration. The initialization-script file is then used to load the initial switch configuration or to reload the configuration if the original configuration is removed or destroyed. The initialization-script file is stored in the */var/CascadeView/initFiles/[switchname].init* directory.

To download a new initialization script file to a switch that already contains a configuration, you must first erase the existing configuration. Refer to "Erasing Parameter RAM" on page 12-20.

Generating the Initialization Script File

To initialize switches:

1. On the network map, select the switch object and from the Misc menu, select CascadeView ⇒ Logon. Enter your operator password.

2. From the Administer menu, select Cascade Switches ⇒ Initialize Switches. The Initialize Switches dialog box appears.

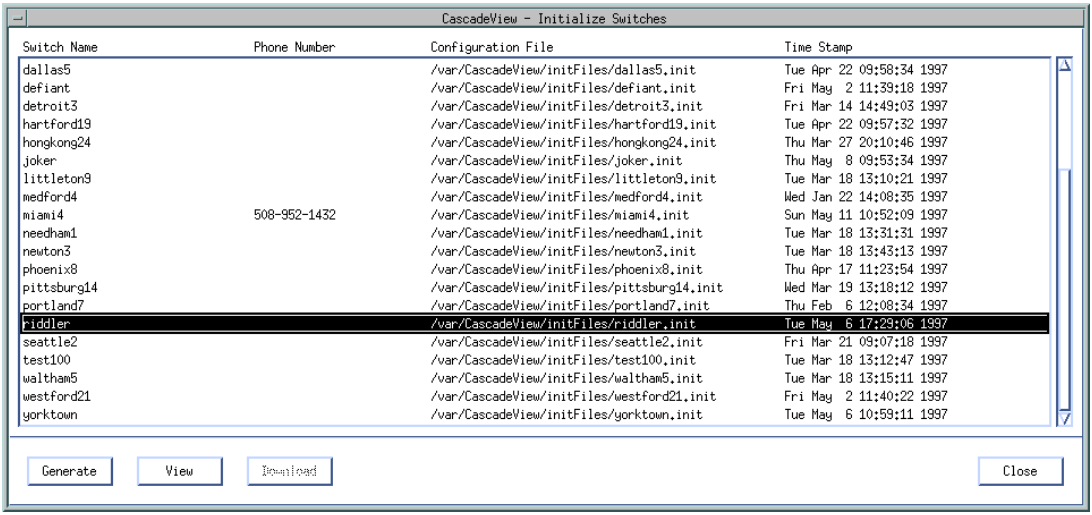


Figure 12-1. Initialize Switches Dialog Box

3. From the list provided, select the switch you want to initialize.

4. Choose Generate to create the initialization script file containing the SNMP SET commands with a date and time stamp. This is the file you need to download to the switch.

5. Repeat Step 3 and Step 4 for each switch you need to initialize. To view the file, first refer to “Downloading the File to the Switch” on page 12-14.

Viewing the Initialization Script File

To view the initialization script file before downloading it to the switch:

1. From the Initialize Switches dialog box, highlight the desired switch.
2. Choose View. The system displays the file contents. Figure 12-2 shows a sample script file.

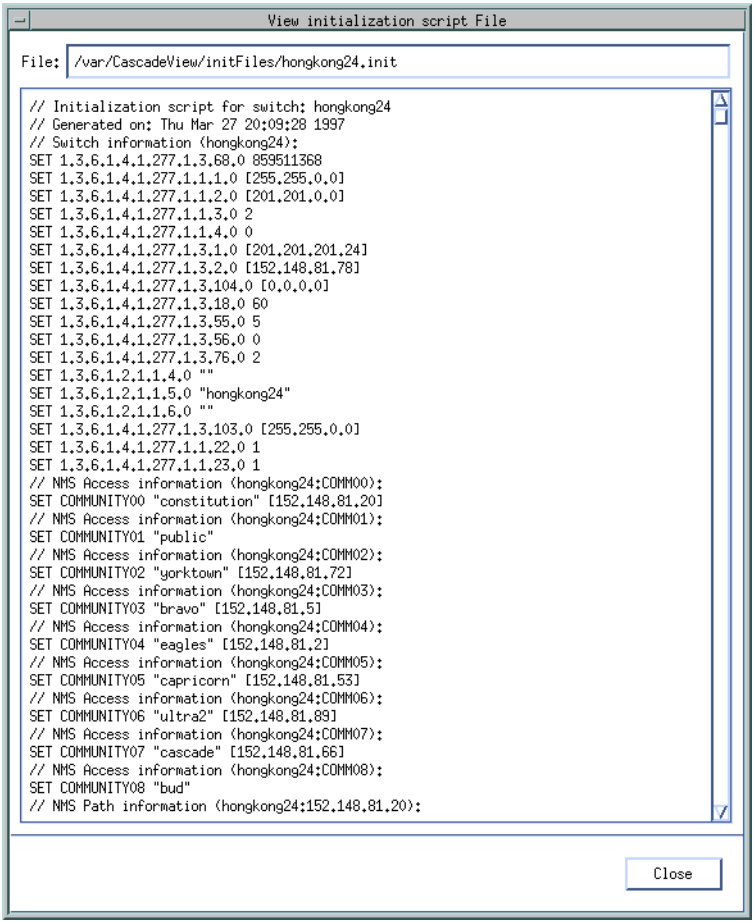


Figure 12-2. Initialization Script File Sample Output

3. When you finish viewing the file, choose Close to return to the Initialize Switches dialog box.

Downloading the File to the Switch

There are two methods you can use to download the initialization script file from the NMS to the switch over a serial line:

Tip — You can use the Solaris Tip program.

Terminal Emulation — You can use a PC that has terminal emulation software. Refer to page 12-16 for instructions.

Method 1 – Using Tip

Before you can download text files using Tip, verify the following:

- ☑ The console cable connects to serial port A on the back of your workstation. Refer to your workstation hardware guide to locate serial port A.
- ☑ The hardwire entry device (dv) is set for /dev/cua/a.
- ☑ The hardwire entry in the */etc/remote* file is set for 19200 bps. The following example displays this entry in the */etc/remote* file using port /dev/cua/a and 19200 bps (br#):

```
hardwire:\
:dv=/dev/cua/a:br#19200:el=^C^S^Q^U^D:ie=%$:oe=^D
```

In UNIX, ^D means while holding down the Ctrl key, press the letter d.

Accessing the Switch Using Tip

1. In an xterm window, enter **su - root**.
2. Enter the root login and password.
3. Enter **tip hardwire**.

   You should get a connection message.
4. Enter **~#**.

   This command sends a break character to the switch. The console prompt appears.

5. Log in to the switch.
6. At the > prompt, enter the following:

```
enable debug <Return>
password: [your debug password] <Return>
```

7. At the ## prompt, enter

```
## reset pram all <Return>
Are you sure (YES/NO)? YES <Return>
```

(YES must be uppercase.)

8. At the ## prompt, enter

```
## reset system <Return>
Are you sure (YES/NO)? YES <Return>
```

(YES must be uppercase.)

The system displays the following message:

```
resetting switch, stand by . . .
```

Once the switch comes up (1-2 minutes), the >> prompt appears, indicating that PRAM is erased. You can now download the new initialization script file.

Downloading the Initialization File

You can access the script file in */opt/CascadeView/bin*.

To download the initialization file:

1. Open a second xterm window.
2. Enter the following command:

```
./script-download -in [ifn] -out [ofn] -linedelay [delay]
```

Where:

[ifn] is the initialization file name (for example, */var/CascadeView/initFiles/shuttle38.init*)

[ofn] is the output file name (for example, */dev/cua/a*)

[delay] is the value of the line delay in 1/10 of a second (for example, use 300000 to specify a 3/10th second line delay). Do not use a value less than 100000.

3. When you finish, enter **^D** in the xterm window to exit the Tip session.

If you receive the error "Couldn't open input file" when you download the script file, use the following command to change permissions on the /dev/cua/a device:

chmod 666 /dev/cua/a <Return>

4. Observe the switch on the network map. If the switch remains yellow and does not turn green within a few minutes, PRAM Synch the switch (refer to page 12-19).

Method 2 – Using Terminal Emulation Software

You can use any commercially available terminal emulation package to download the initialization script file from a PC. Refer to the emulation software user guide for specific instructions on downloading text files.

Whichever emulation package you use, set the following variables:

Transfer protocol — To text mode transfer.

Line delay — To a minimum of 3/10 second.

Before you transfer the configuration text file to the PC, you may need to run the UNIX command, **unix2dos**, on this file.

Using PRAM Functions

The Switch Back Panel dialog box provides access to PRAM commands.

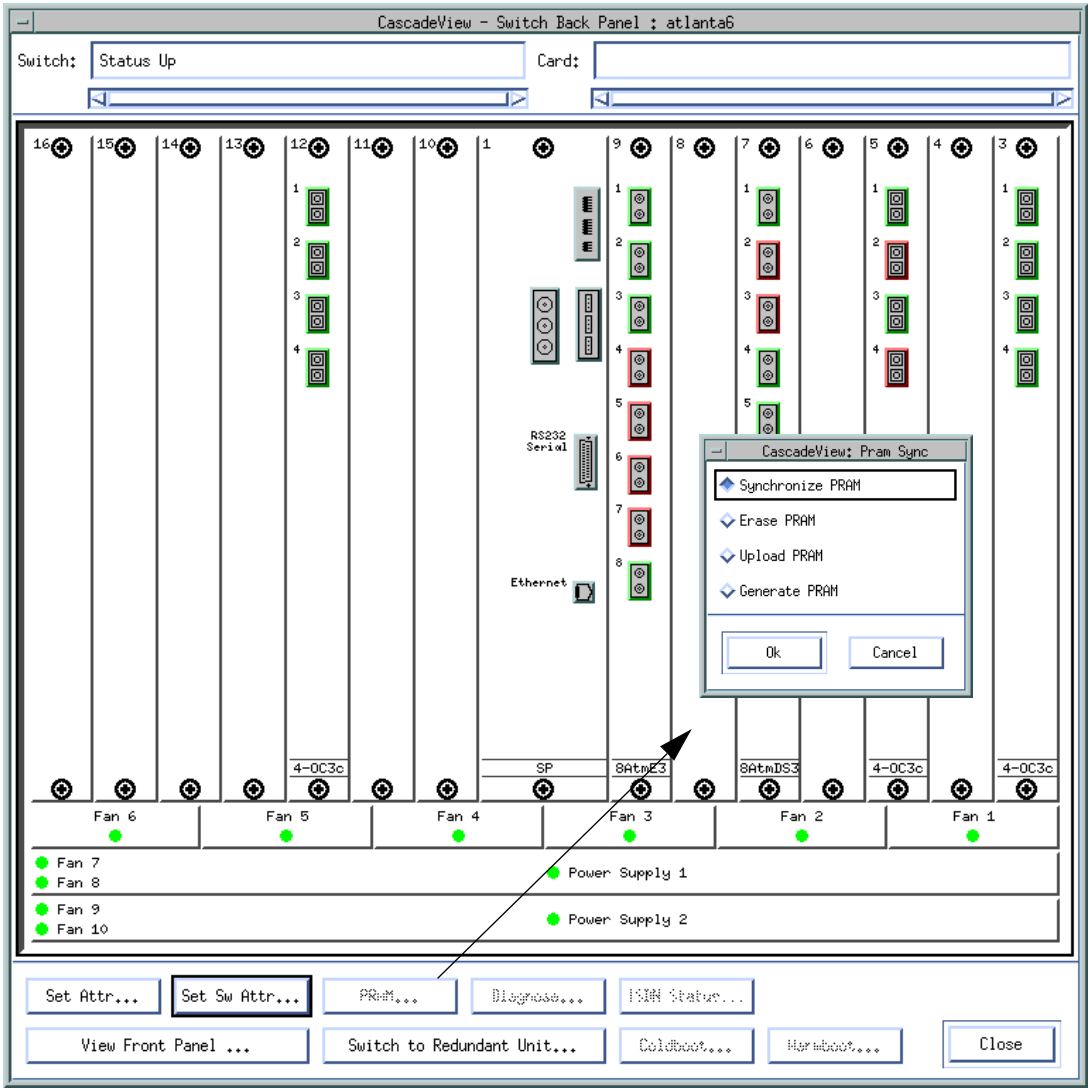


Figure 12-3. Switch Back Panel Dialog Box

The following sections describe these commands.

Using the Synchronize PRAM Command

The Synchronize PRAM command enables you to correct inconsistencies between the NMS database and switch PRAM. When you download an initialization script file from the NMS to the switch for the first time, you may need to synchronize PRAM for the switch to receive complete configuration information. Occasionally, you may also need to synchronize a switch to correct a mismatch between the NMS database and the configuration that resides in switch PRAM. This situation occurs when you use the NMS to make modifications to a switch that is unmanaged or not actively communicating with the NMS (unreachable). The NMS displays the switch object in yellow.

If you made only minimal changes to the configuration, you can synchronize PRAM at a later time to avoid interrupting network traffic.

Before you synchronize a switch, verify that you have defined or specified the following:

- ☑ NMS IP Address (page 5-21)
- ☑ Community Name (page 5-20)
- ☑ Read/Write privileges (page 5-20)

CPU-intensive operations, such as PRAM synchronization, can cause CascadeView to drop node polls. To avoid this problem, increase the amount of time between SNMP retries. Edit the /opt/CascadeView/etc/cascadeview.cfg file and increase the CV_SNMP_RETRY_INTERVAL value from 15 to a higher value. This value is in tenths of a second.

Cascade recommends a value of 1.5 seconds for a configuration with 10 to 15 simultaneous instances of CascadeView and more than 15 switches in the network. This change takes effect when you restart HP OpenView.

Synchronizing a CBX 500 Switch

To synchronize a CBX 500 switch:

1. Select the switch you want to synchronize and, from the Misc menu, select CascadeView ⇒ Logon.
2. Enter the operator password. (You can only synchronize one switch at a time.)
3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears (Figure 12-3 on page 12-17).
4. Select the I/O module you need to synchronize.

> *If you changed some switch attributes, such as the NMS path, you must synchronize the SP module first. To synchronize more than one module, always start with the SP, then work your way, right to left, toward the module that has the highest slot ID.*

5. Choose the PRAM command. The Pram Sync dialog box appears.

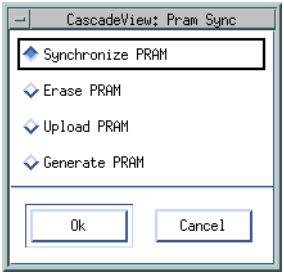


Figure 12-4. Pram Sync Dialog Box

6. Select Synchronize PRAM and choose OK. This sends the binary image of the configuration to the selected module, causing it to perform a warmboot. When the module reboots, all physical ports, logical ports, PVCs, and active sessions stall for approximately 0-30 seconds. If you have a heavily configured module, it may take several minutes or more to reboot.

Erasing Parameter RAM

Use the Erase PRAM command to clear an existing switch configuration file. You may have to erase PRAM before you download the initialization script file to the switch; for example, if you suspect the switch configuration file is corrupt. If you have problems with a new release of switch software, you might also need to download the file as part of a switch downgrade or upgrade procedure.

You can clear the existing configuration file from the CBX 500 using the following methods:

Method 1 — (Recommended) Uses the NMS software to clear PRAM.

Method 2 — Requires you to connect a console terminal to the switch and clear the configuration on each I/O module by slot number. Use this second method only as a backup.

Method 1

1. On the network map, select the switch for which you want to clear PRAM.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters.
3. Select each I/O module (one at a time) and choose the PRAM command button.
4. From the Pram Sync dialog box (Figure 12-4 on page 12-19), choose Erase PRAM.
5. Choose OK.
6. Repeat Step 3 through Step 5 until you erase the PRAM for each module.

Method 2

1. Install a console terminal to the network management port on the SP module. (Refer to the *CBX 500 Hardware Installation Guide* for details.)

2. Force a line-break condition to the switch. Enter a minimum of three characters for login name and enter a valid community name as the password ("cascade" is the default community name).

3. At the > prompt, enter:

   ```
   enable debug <Return>
   password: [your debug password] <Return> (or cascade)
   ```

   If you are erasing PRAM on all I/O modules in the switch, including the SP, clear the PRAM on the highest numbered slot first and continue to the lowest numbered slot (left to right).

4. At the ## prompt, enter:

   ```
   ## reset pram [#] <Return>
   ```

   (where [#] is the module or slot number)

   ```
   Are you sure (YES/NO)? YES <Return>
   ```

5. At the ## prompt, enter:

   ```
   ## reset system <Return>
   ```

   (This step reboots all modules.)

   ```
   Are you sure (YES/NO)? YES <Return>
   ```

Once the switch comes up (1-2 minutes), the >> prompt appears, indicating that PRAM is erased. You can now download the new initialization script file.

Using the Upload PRAM Command

Upload PRAM enables you to compare the configuration files in the switch (PRAM) and in the NMS database. Occasionally, the configuration file in the switch for a specific I/O module and the configuration in the NMS database do not match. This mismatch can occur when you upgrade your switch software, use third-party network management products to manage the switch, or use the MIB to change a switch configuration.

To resolve PRAM conflicts, use the Upload PRAM command to view the switch configuration file stored in PRAM.

- Use Upload PRAM to replace the configuration file in the NMS database with the switch configuration file.
- Use Synchronize PRAM to replace the configuration file in switch PRAM with the one in the NMS database. Refer to page 12-18 for information about Synchronizing PRAM.

Guidelines for Using Upload PRAM

The Upload PRAM function currently supports:

- Physical ports
- Logical ports (except trunk ports)

Before you use the Upload PRAM function, review the following points:

- You can use Upload PRAM to add objects from switch PRAM to the NMS database, as long as the objects being added do not conflict with existing objects in the database; for example, the NMS database already contains a switch with that name.
- Due to the interdependency of objects with other objects in the database, *be careful* when you use Upload PRAM to delete objects from the database. In general, do not create a situation where there are dangling objects (i.e., an object without a parent) in the switch before applying Upload PRAM. For example, deleting a logical port without first deleting all associated SVC addresses or PVCs creates dangling objects and causes a problem during the Upload PRAM process.

Uploading a Switch Configuration File

To upload the switch configuration file stored in PRAM:

1. On the network map, select the switch object.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (Figure 12-3 on page 12-17).
3. Select either the I/O module or the SP module and choose the PRAM command. The CascadeView PRAM Sync dialog box appears (Figure 12-4 on page 12-19).
4. Select Upload PRAM and choose OK. The Card PRAM Upload and NMS Synchronization dialog box appears.

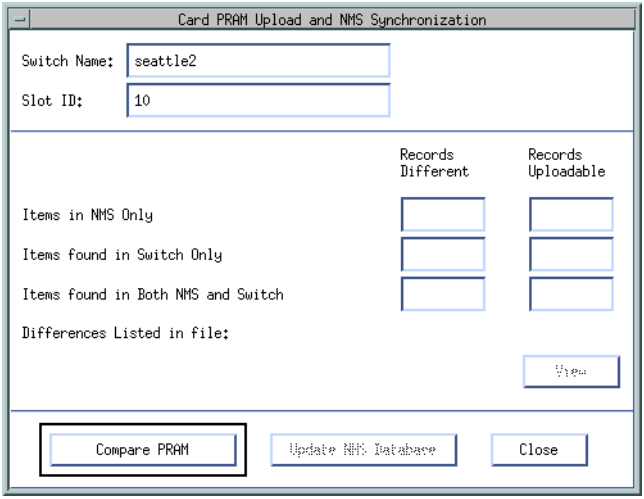


Figure 12-5. Card PRAM Upload and NMS Synchronization Dialog Box

5. Choose Compare PRAM.

6. The dialog box displays information about the number of inconsistencies between the PRAM configuration file and the NMS database. If the field displays a zero, there are no differences between the PRAM and NMS configurations.

   An *item* can be a single physical port or logical port definition. This dialog box displays the following fields:

Table 12-1. Card PRAM Upload and NMS Synchronization Fields

Field	Description
Items in NMS only	The item exists in the NMS database, but not in the switch PRAM. This situation occurs if you make configuration changes to an unmanaged switch.
Items found in Switch only	The item exists in switch PRAM, but not in the NMS database. This situation can occur if you configure a switch using a third-party network management station or use the MIB to change configuration information.
Items found in both NMS and Switch	This item exists in both places, but there are discrepancies in the configuration. This situation can occur when you modify the configuration directly from the console. For example, if you use console commands to change the admin status of a logical port, the logical port definition in switch PRAM indicates that the logical port is Down; the NMS database records indicate the logical port as Up. These discrepancies can also occur if a PRAM synchronization or SNMP set request fails. The name and location of the file that stores the inconsistencies appears on the dialog box.

7. Choose View to compare the files. The system displays the contents of the two files (Figure 12-6 on page 12-25).

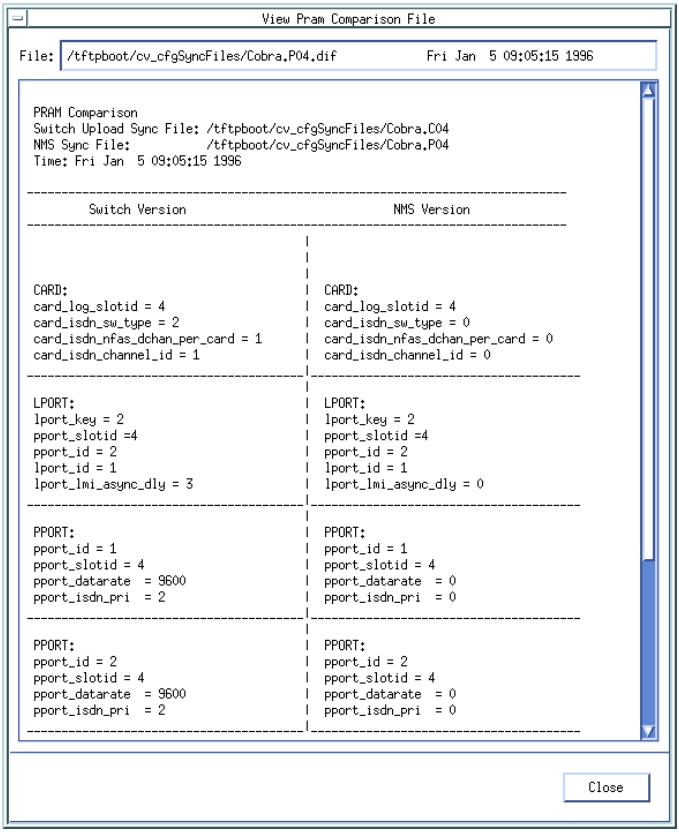


Figure 12-6. View PRAM Comparison File Dialog Box

Choose Close to return to the Card PRAM Upload and NMS Synchronization dialog box (Figure 12-5 on page 12-23).

8. To synchronize the information between switch PRAM and the NMS database, you can:
   - Choose the Update NMS Database command to use the configuration stored in switch PRAM.
   - Choose Close to use the configuration in the NMS database. Use the Synchronize PRAM command to update PRAM (refer to page 12-18 for details).
9. Repeat Step 3 through Step 8 for each I/O module to complete the configuration PRAM upload process.

If an error occurs during the upload process, a message dialog box appears. After closing this dialog box, you can choose Update NMS Database to continue the upload process for the remaining items.

If there are problems with the PRAM configuration file, refer to page 12-11 for instructions to download the configuration file stored in the NMS database.

Using the Generate PRAM Command

The Generate PRAM command generates a configuration file that can be used for off-line management. This command enables you to view the configuration file before uploading it to the switch.

To access the Generate PRAM command:

1. On the network map, select the switch object.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears (Figure 12-3 on page 12-17).
3. Choose the PRAM command. The Pram Sync dialog box appears (Figure 12-4 on page 12-19).
4. Choose Generate PRAM. The NMS stores the generated PRAM file in the */opt/CascadeView.var/cfgSyncFiles* directory.

13

Closed User Groups

A Closed User Group (CUG) is a division of all SVC network users into logically linked groups of users. Members of the same CUG have particular calling privileges that members of different CUGs may not have. CUGs form one level of security between users of a network, allowing only those users who are members of the CUG to set up calls to each other. Information about CUG membership and rules is available throughout the network.

A CUG is comprised of a set of rules called members. These rules represent SVC port addresses and prefixes for which you have enabled the CUG termination option (refer to page 10-23). You configure CUG member rules in either AESA or E.164 address format. When you configure a member rule, you can replace some digits with the * or ? UNIX wildcard characters. If a member rule does not contain a wildcard character, it maps to a specific network user. If the member rule includes a wildcard, then this member can potentially map to multiple network users.

Throughout this document, most address descriptions use the term "SVC address." Unless otherwise noted, the term SVC address is used interchangeably with term "SVC prefix".

About CUG Member Rules

CUG member rules correspond to SVC addresses. You can enter a rule as a UNIX-style expression. You can use the * as a wildcard to replace 0, one, or more digits, or the ? as a wildcard to replace a single digit. You can only use the * once in a string. Keep in mind that an AESA digit is 4 bits and an E1.64 digit is 8 bits.

The following examples show how you can use wildcards to represent multiple E.164 addresses.

Example	Description
1508952*	This CUG includes all numbers using area code 508 and exchange number 952.
1508952148?	This CUG includes all numbers using area code 508, exchange number 952, and an extension starting with 148 (i.e., 1480 – 1489).

When you define a CUG member, these addresses define the *member value* for the CUG member rule. Each CUG member rule is defined by an ASCII name, an address type (either E.164 or AESA), and the CUG member value (rule).

Defining Incoming and Outgoing Access

In addition to defining CUG member address values, you can also define the incoming and outgoing access attributes which complete the CUG member rule.

The *incoming access* (IA) attribute enables you to define how a CUG member handles calls coming from other CUGs or non-CUG users. A user mapping to a CUG member with incoming access enabled can receive calls coming from non-CUG users as well as calls coming from other CUGs. If you disable incoming access, the CUG member can only receive calls from other members of the same CUG.

The *outgoing access* attribute (OA) enables you to define how a CUG member handles calls to other CUGs and non-CUG users. A user mapping to a CUG member with outgoing access enabled can make calls to other CUGs and non-CUG users. If you disable outgoing access, the CUG member can only make calls to other members of the same CUG.

Examples

You define the following CUG member rule:

Member Rule Name	rule1
Member Value/Type	1508* (E.164)
Incoming Access	Y
Outgoing Access	N

This member rule applies to E.164 addresses beginning with digits 1508. Users that map to this rule can receive calls from members of their own CUG, members of other CUGs, and non-CUG users (incoming access is enabled), but they cannot make calls outside their own CUG.

Developing Closed User Groups

For each CUG you create, you can assign up to 128 different member rules; you can use an individual member rule in up to 16 different CUGs. In this way, a CUG is made up of all users that map to the addresses that these rules define. You can configure up to 1024 CUGs per switch.

When you create a CUG (“CUG A”), the attributes you configure for each CUG member rule (“Rule1”) that you associate with the CUG define how the CUG handles calls between members. For example, if you enable the *incoming calls barred* (ICB) attribute for Rule1, users that map to Rule1 cannot receive calls from other CUG A members. Conversely, disable ICB to allow users that map to Rule1 to receive calls from other CUG A members.

If you enable the *outgoing calls barred* (OCB) attribute for Rule1, users that map to Rule1 cannot make calls to other CUG A members. Conversely, disable OCB to allow users that map to Rule1 to make calls to other CUG A members.

Using CUGs in the Network

The following example illustrates how you can implement CUGs in your network.

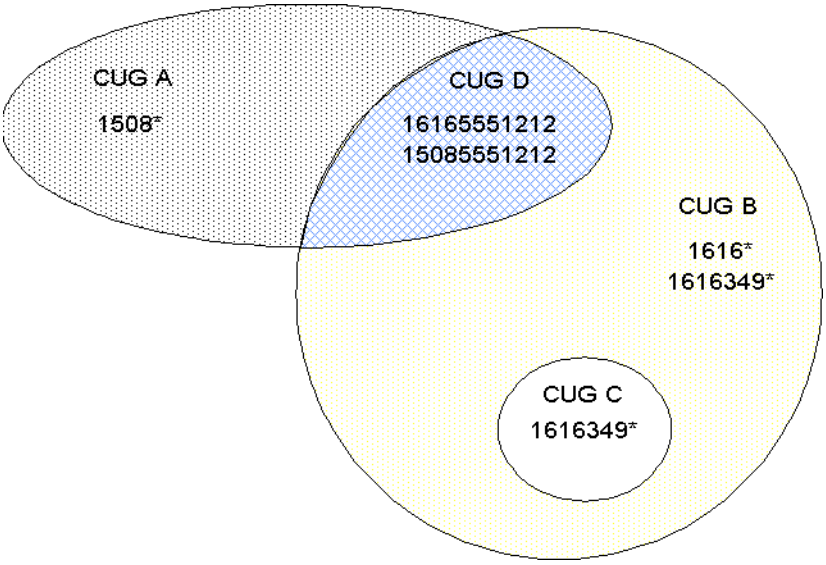


Figure 13-1. Implementing CUGs

The CUGs used in this example represent the following:

- CUG A: Business Unit A
- CUG B: Business Unit B
- CUG C: Independent entity within Unit B
- CUG D: Joint venture between Units A and B

For each of these CUGs, the following table defines the incoming calls barred (ICB) and outgoing calls barred (OCB) attributes and member rules. Each member rule is made up of an expression that represents an E.164 address and an incoming access (IA) and outgoing access (OA) attribute.

	ICB	OCB	Member Rules	IA	OA
CUG A	No	No	1508*	No	No
CUG B	No Yes	No Yes	1616* 1616349*	No No	Yes No
CUG C	No	No	1616349*	No	No
CUG D	No No	No No	16165551212 15085551212	No Yes	Yes No

Call Setup Examples

- A call is made from 15085551212 to 16165551212:
  - 15085551212 (IA enabled): Address belongs to CUG A and CUG D
  - 16165551212 (OA enabled): Address belongs to CUG B and CUG D

  Result: Call succeeds because both addresses belong to CUG D.
- A call is made from 16163498888 to 16165551212:
  - 1616349: Address belongs to CUG B (ICB, OCB enabled) and CUG C
  - 16165551212 (OA enabled): Address belongs to CUG B and CUG D

  Result: Although both addresses belong to CUG B, the call fails because the outgoing calls barred (OCB) attribute is enabled on CUG B for member 1616349*. Users mapping to matching rule 1616349* cannot make calls to other CUG B members.
- A call is made from 12035551212 to 15085551212:
  - The address 12035551212 does not belong to any CUG.
  - 15085551212 (IA enabled): Address belongs to CUG A and CUG D

  Result: Call succeeds because the incoming access (IA) attribute enabled is enabled for 15085551212. This member rule allows users mapped to 15085551212 to receive calls from non-CUG users.

Configured Addresses and CUG Membership

Using the CUG design depicted in Figure 13-1 on page 13-4, Table 13-1 illustrates how a single configured address can match multiple member rules, and can belong to more than one CUG.

Table 13-1. Configured Address and Corresponding CUG Membership

Address	OA	IA	CUG	ICB	OCB
15085551212	N	Y	A	N	N
			D	N	N
16165551212	Y	N	B	N	N
			D	N	N
15082178989	N	N	A	N	N
16161234567	Y	N	B	N	N
16163498888	Y	N	B	Y	Y
			C	N	N

Member rules that specify an address prefix only can simplify call routing since the logical port only needs to check the address prefix digits to route the call. However, CUG membership must be recalculated at call time if the port to which this address is routed contains other CUGs with member rules which begin with the digits 1616.

For example, if a CUG contains a member rule that uses a prefix format (i.e.,1616*) as well as other member rules which are more specific (1616349*), you are likely to encounter performance issues due to address ambiguity.

The more specific you make the CUG member rules, the more quickly CUG membership can be determined.

Configuring Closed User Groups

Use the following sequence to configure CUGs. Remember that each member rule should correspond to at least one SVC address.

Step 1. Create SVC addresses and enable CUG termination (refer to page 10-23).

Step 2. Define the CUG member rules that represent the member addresses and call access (page 13-8).

Step 3. Define the CUG names (page 13-11).

Step 4. Associate CUG members to specific CUGs. You can also modify call access attributes for a specific CUG (page 13-12).

Defining CUG Members

A CUG member is defined by a rule that matches one or more port addresses/prefixes and attributes which specify incoming and outgoing call access. Once you define these members, you can associate them with specific CUGs.

To define a CUG member:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUG Members. The following dialog box appears.

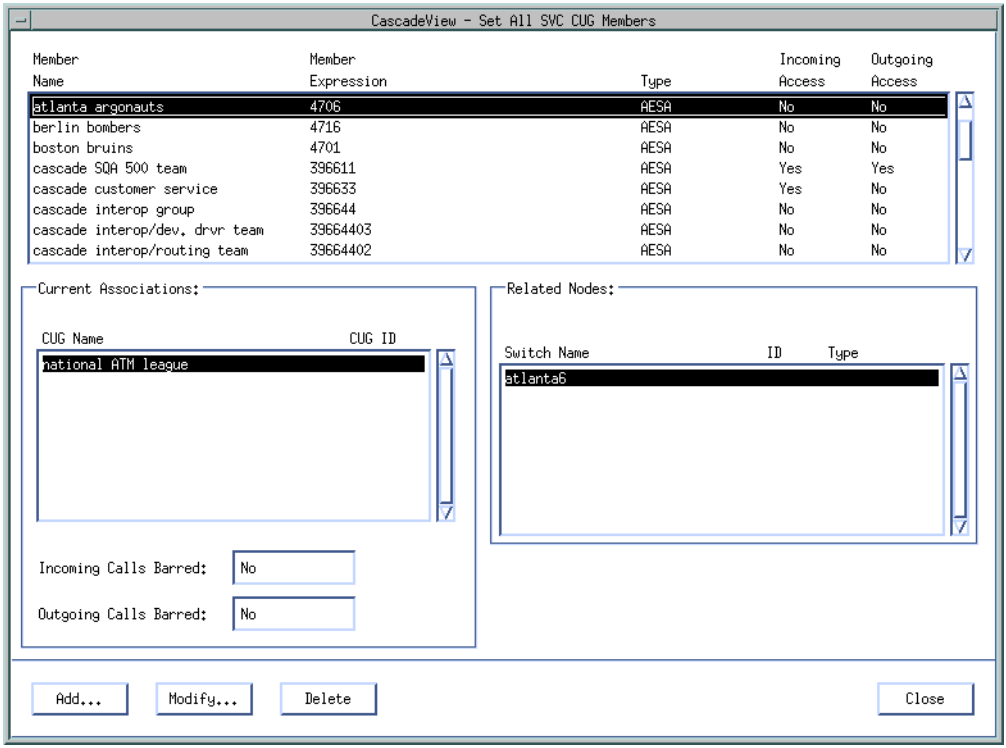


Figure 13-2. Set All SVC CUG Members Dialog Box

This dialog box provides a list of previously defined CUG members and their rules. For each member name you select, it provides the name of the CUG(s) to which it is associated.

- To Modify an existing member name, select a name from this list and choose Modify.
- To Delete an existing member name, select a name from this list and choose Delete

2. Choose Add to define a CUG member. The following dialog box appears.

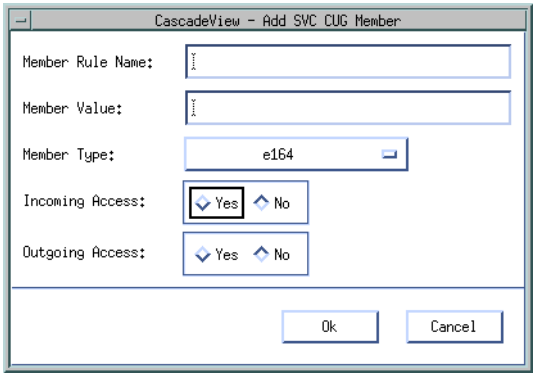


Figure 13-3. Add SVC CUG Member Dialog Box

3. Configure the member attributes as described in Table 13-2.

Table 13-2. Add SVC CUG Member Fields

Field	Description
Member Rule Name	Enter a name (up to 32 characters).
Member Value	Enter the CUG member rule using the guidelines on page 13-2. Do not enter more than 15 characters for an E.164 address or more than 40 characters for an AESA address.
Member Type	Select the either AESA or E.164.
Incoming Access	This attributes specifies how incoming calls from non-CUG users or users of a different CUG are handled. • Select Yes to accept calls from users that do not belong to the same CUG. • Select No (default) to reject calls from users that do not belong to the same CUG.
Outgoing Access	This attribute specifies how outgoing calls to non-CUG users or users of a different CUG are handled. • Select Yes to allow calls to users not belonging to the same CUG. • Select No (default) to block calls to users not belonging to the same CUG.

4. When you finish, choose OK.
5. You can use these fields to define additional members, or choose Cancel to exit this dialog box.

Defining a Closed User Group

Next, set up the CUGs for your network. This is a simple process of supplying a name for each CUG. CascadeView/UX supports up to 1024 CUGs per switch.

To create a CUG:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The following dialog box appears.

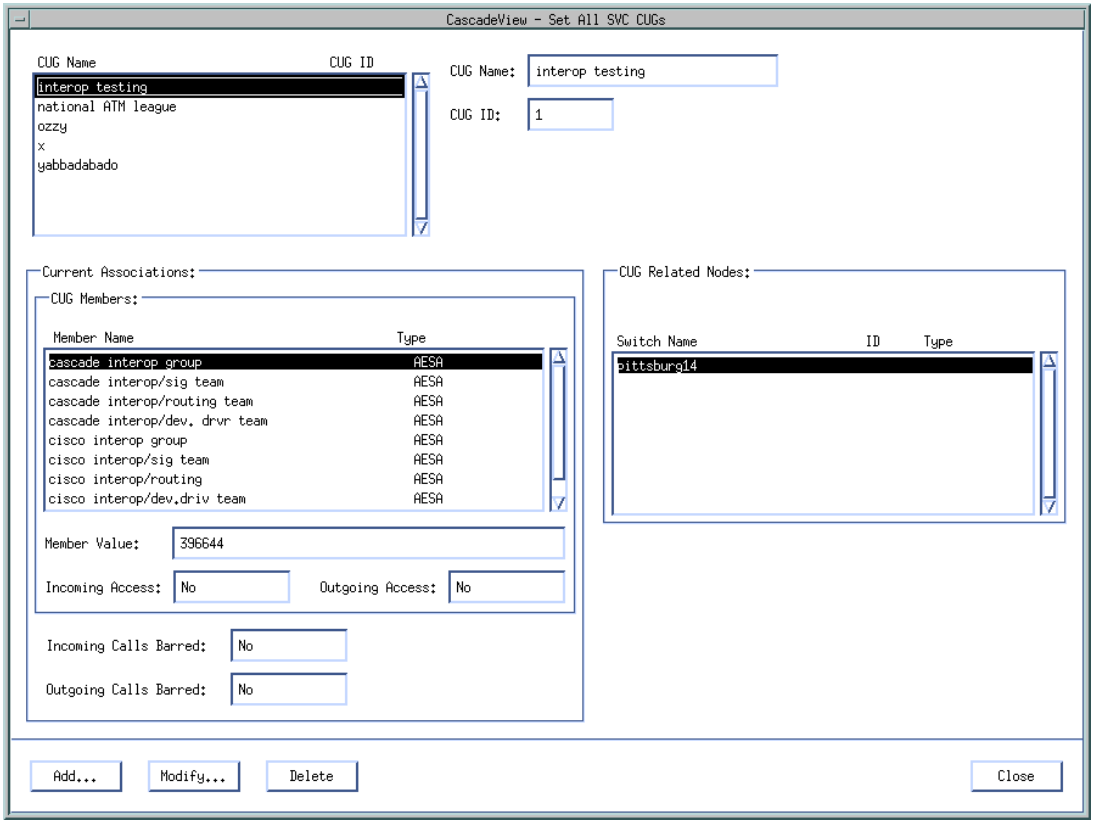


Figure 13-4. Set All SVC CUGs Dialog Box

This dialog box provides a list of previously configured CUG names as well as a listing of members for each CUG you select.

- To Modify an existing CUG, select a name from this list and choose Modify.
- To Delete an existing CUG, select a name from this list and choose Delete.

2. Choose Add to create a new CUG. The following dialog box appears.

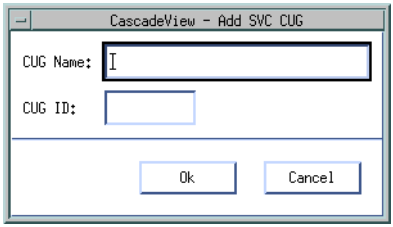


Figure 13-5. Add SVC CUG Dialog Box

3. Enter a CUG name (up to 32 characters). The NMS assigns a CUG ID.
4. Choose OK.

Assigning Member Rules to CUGs

To complete the CUG definition process, you need to assign member rules to each CUG. You can assign up to 128 members per CUG. You can assign each member to as many as 16 CUGs.

To assign members to a CUG,

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The Set All SVC CUGs dialog box appears (Figure 13-4).
2. From the CUG Name list, select the CUG to which you want to add members.
3. Choose Modify. The following dialog box appears.

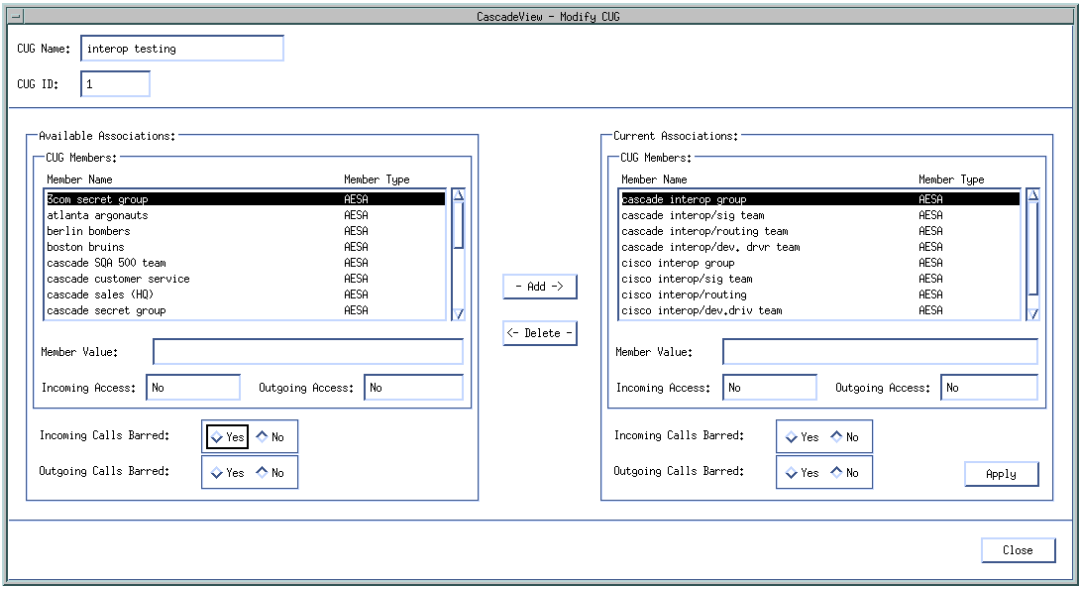


Figure 13-6. Modify CUG Dialog Box

This dialog box displays the current list of CUG member rules with Current Associations. It also provides a list of member names you can associate with this CUG.

4. From the list of Available Associations, select the member you want to associate with this CUG and specify Incoming Calls Barred and Outgoing Calls Barred:

   Incoming Calls Barred — Specifies how incoming calls from the same CUG are handled. Select Yes to reject calls from users of the same CUG. Select No (default) to allow calls from users of the same CUG.

   Outgoing Calls Barred — Specifies how outgoing calls to the same CUG are handled. Select Yes to block calls to users of the same CUG. Select No (default) to allow calls to users of the same CUG.

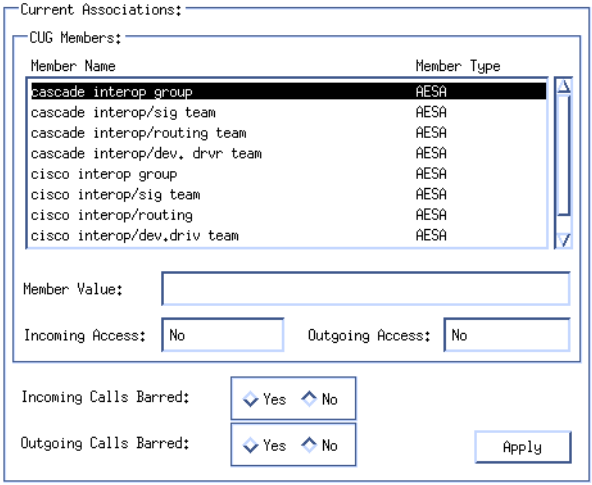
5. Choose Add. The member name appears in the Current Associations list. All SVC addresses and prefixes that match the member rule take on the attributes specified for this CUG.

6. To associate additional member names, repeat Step 4 and Step 5. When you finish, choose Close to exit this dialog box.

Modifying Call Access for CUG Members

Use the following steps to modify the incoming and outgoing call access for an existing CUG member.

1. From the Administer menu, select Cascade Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The Set All SVC CUGs dialog box appears (Figure 13-4).
2. From the CUG Name list, select the CUG that contains this member.
3. Choose Modify. The Modify CUG dialog box appears (Figure 13-6 on page 13-13).
4. Select the CUG member name from the Current Associations list.



5. Use the instructions on page 13-10 to modify incoming and outgoing call access.
6. Choose Apply.
7. Choose Close to exit this dialog box.

14

Port Security Screening

The Port Security Screening feature is a mechanism you can use to ensure that your network cannot be compromised by unauthorized SVC access. You do this by creating screens that can allow/disallow incoming and outgoing SVCs. You configure each screen with the following information:

SVC direction — Screen either ingress (incoming) or egress (outgoing) SVCs.

Screen type — Pass or block SVCs according to the configured screen.

Address type — Any address type used in a public or private UNI. This includes E.164, E.164-AESA, DCC-AESA, ICD-AESA, and custom AESA.

Matching information — Address criteria that either allows or disallows the SVC.

Once you develop a set of screens, you can apply them 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 SVC it receives for the matching criteria specified in the screen(s). If the SVC meets the matching criteria specified in at least one of these screens, the port either passes or blocks that SVC according to the security screen design.

Implementing Port Security Screening

Although you can apply multiple security screens to a single logical port, the decision as to whether an SVC is passed or blocked is made based on the combined effects of the following:

- The default ingress/egress screen mode for the logical port.
- The security screens you assign to this logical port.
- The incoming/outgoing SVC address criteria defined in the security screen.

Default Screens

For each logical port, you configure default screen criteria that specifies the behavior of any SVC on this port. You can use security screens on both ingress user ports that represent SVC originating endpoints or egress user ports, which in turn represent SVC terminating endpoints. The default screens enable you to quickly override the security screens you assign to the logical port; use the default screens to either pass or block all incoming or outgoing SVCs.

Table 14-1 describes the default ingress and egress security screen options. These defaults represent the port screen activation parameters.

Table 14-1. Default Screens

Default	Value	Description
Ingress Screen Mode	All Screens	All ingress screens you apply to this port are used to determine whether an incoming SVC is passed or blocked.
	Default Screen (*default*)	Disables the ingress security screens applied to this port. Incoming SVCs are screened according to how you set the Default Ingress Screen.

Table 14-1. Default Screens (Continued)

Default	Value	Description
Default Ingress Screen	Pass (*default*)	If you set the Ingress Screen Mode to Default Screen, all incoming SVCs to this port are passed; if it is set to All Screens, all incoming SVCs are passed, unless one of the ingress security screens assigned to this port blocks the SVC.
	Block	If you set the Ingress Screen Mode to Default Screen, all incoming SVCs to this port are blocked; if it is set to All Screens, all incoming SVCs are blocked unless one of the ingress security screens assigned to this port passes the SVC.
Egress Screen Mode	All Screens	All egress screens you apply to this port are used to determine whether an outgoing SVC is passed or blocked.
	Default Screen (*default*)	Disables the egress security screens applied to this port. Outgoing SVCs are screened according to the Default Egress Screen.
Default Egress Screen	Pass (*default*)	If you set the Egress Screen Mode to Default Screen, all outgoing SVCs from this port are passed; if it is set to All Screens, all outgoing SVCs are passed, unless one of the egress security screens assigned to this port blocks the SVC.
	Block	If you set the Egress Screen Mode to Default Screen, all outgoing SVCs from this port are blocked; if it is set to All Screens, all outgoing SVCs are blocked, unless one of the egress security screens assigned to this port passes the SVC.

Security Screens

The security screens you assign to a logical port represent exceptions to the default screens. You can assign up to 16 security screens per logical port. Once you assign security screens to a port and set the ingress/egress screen mode to All Screens, the logical port uses these security screens to screen SVCs that match the criteria they specify.

You define a security screen based on two attributes: SVC direction and screen type. SVC direction defines the SVCs to which this screen applies, either ingress (incoming) or egress (outgoing). The screen type attribute determines whether or not the port passes or blocks these SVCs.

About Security Screen Addresses

To provide a more detailed level of SVC screening, you can specify either an E.164 or AESA-style address. You can enter the entire address as a number, or enter a UNIX-style expression using wildcards. When you use a UNIX expression, a single screen can match multiple endpoint addresses. Use the ? wildcard to replace a single digit or the * wildcard to replace one or more digits. You can only use the * once in a string. Refer to “Address Formats” on page 10-2 for more information on addressing.

The following examples show how you can use a UNIX expression to represent an E.164 North American address.

Example	Description
1508952*	This screen applies to all numbers using area code 508 and exchange number 952.
1508952148?	This screen applies to all numbers using area code 508, exchange number 952, and an extension starting with 148 (i.e., 1480 – 1489).
150895?*5?	This screen applies to all numbers using area code 508, with an exchange number value of 950 – 959. The number 5 must appear as the third digit of the extension.

Table 14-2 describes some examples using the port security screens.

Table 14-2. Security Screens

SVC Direction	Screen Type	Calling Address	Calling Subaddress	Called Address	Called Subaddress	Description
Ingress	Pass	Ignore	Ignore	1800* Type: E.164	Ignore	Pass all incoming calls to 1800 numbers.
Ingress	Block	Ignore	Ignore	1800* Type: E.164	Ignore	Block all incoming calls to 1800 numbers.
Egress	Block	Ignore	Ignore	* Type: E.164	Ignore	Block all outgoing calls with E.164 called addresses.
Egress	Block	15089700705 Type: E.164	Ignore	1908870* Type: E.164	Ignore	Block all calls to called address 1908870* from calling address 15089700705.

Port Security Screening Sample Configuration

Once you assign security screens to a logical port, if you set the ingress and egress screen modes to All Screens (refer to Figure 14-3 on page 14-13), the port checks incoming/outgoing SVCs for the matching criteria specified in each assigned screen. If an SVC meets the criteria specified in at least one screen, then the SVC is screened according to the action this screen recommends. The SVC is further checked for the matching criteria of this screen's default behavior. If it meets the matching criteria specified in at least one of these screens, then the SVC exhibits the default behavior (either pass or block).

Thus, although you can apply multiple screens to a single port, the decision on whether the port should block or pass an SVC is made based on the combined effect of the default screens specified for the logical port, the security screens you assign to that port, and the matching address criteria defined in each screen (if applicable).

If you set the ingress/egress screen mode to Default Screens, the port does not check SVCs for the matching criteria specified in an assigned security screen. It takes the action (either pass or block) the Default Screen specifies.

The following example provides a logical port configuration which blocks all incoming SVCs, except incoming 1800 SVCs, with one exception. You want to block all incoming SVCs that contain the 234 exchange number.

Logical Port Configuration Examples

1. For the logical port, configure the following default screen:

Ingress Screen Mode:	All Screens
Default Ingress Screen:	Block

   Setting the default ingress screen to *block* enables you to block all incoming SVCs on this port by default; setting the ingress screen mode to *all screens* enables the port to screen SVCs based on the ingress security screens you assign.

2. Create and assign two security screens.

   – The following screen passes all incoming 1800 SVCs:

Screen Name:	pass_in_800
SVC Direction:	Ingress
Screen Type:	Pass
Calling Address:	Ignore
Calling Subaddress:	Ignore
Called Address:	Type: E.164 1800*
Called Subaddress:	Ignore

– The following screen blocks all SVCs from the 234 exchange:

Screen Name:	blk_234_exchg
SVC Direction:	Ingress
Screen Type:	Block
Calling Address:	Ignore
Calling Subaddress:	Ignore
Called Address:	Type: E.164 1???234*
Called Subaddress:	Ignore

Summary

As you begin to design port security screening features for your network, keep the following points in mind:

1. Configure the default screen for a logical port. This default mode determines whether or not to pass or block SVCs from certain addresses. The previous example blocks all incoming SVCs for the logical port. You can quickly revert back to the default mode if necessary.
2. Configure and assign the security screen exceptions. The previous example passes all incoming 1800 SVCs.
3. Configure and assign any exceptions to these screen. The previous example specifically blocks incoming SVCs from the 234 exchange; this includes incoming SVCs from 1800234*.

Configuring Port Security Screening

Use the following sequence to configure port security screening.

Step 1. Configure logical ports (refer to Chapter 7).

Step 2. Configure SVCs (refer to Chapter 10).

Step 3. Create a set of security screens (refer to page 14-8).

Step 4. Define the logical port security screening defaults. If necessary, assign the security screens that provide exceptions to these defaults (refer to page 14-12).

Creating Port Security Screen Definitions

To create a security screen:

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

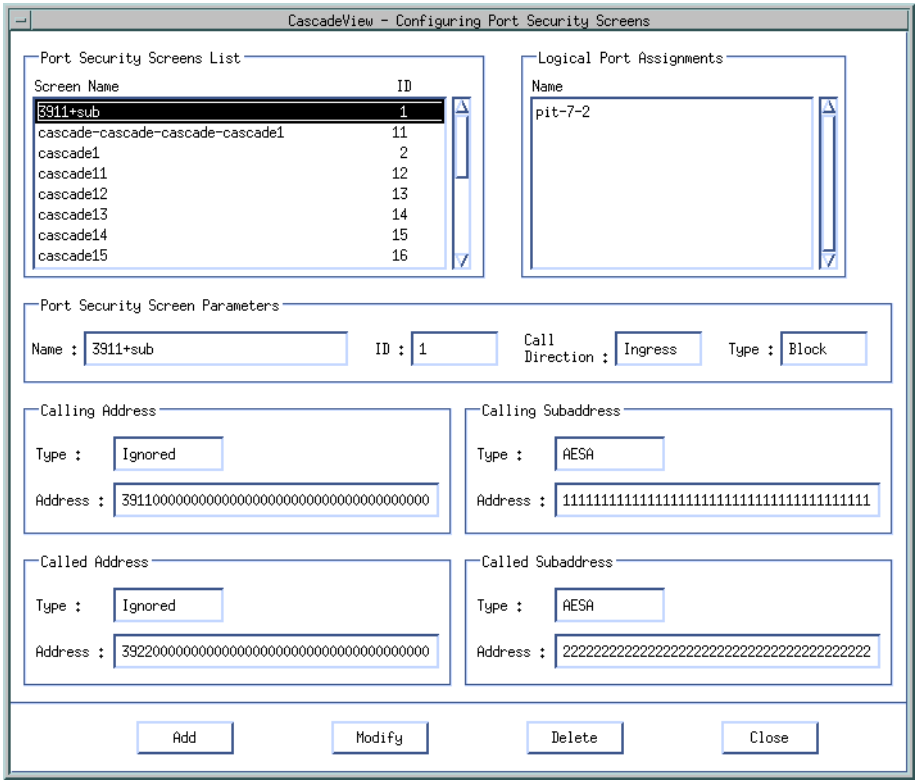


Figure 14-1. Configuring Port Security Screens Dialog Box

This dialog box displays a list of previously configured security screens. It provides the configured parameters for each screen you select from the Port Security Screens List.

- To modify an existing screen, select a screen name and choose Modify.
- To delete an existing screen, select a screen name and choose Delete.

2. Choose Add to create a new screen. The following dialog box appears.

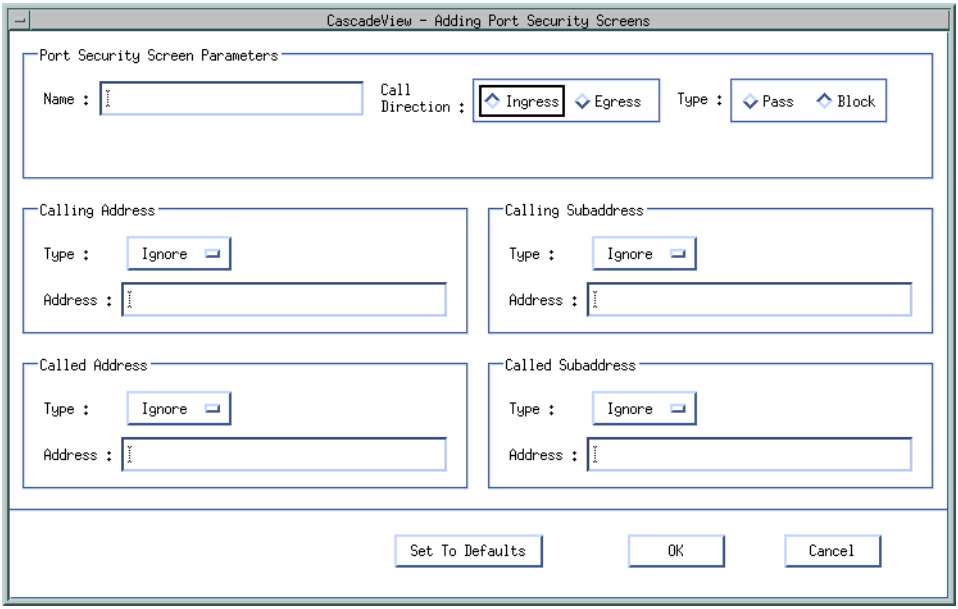


Figure 14-2. Adding Port Security Screens Dialog Box

3. Complete the dialog box fields as described in Table 14-3.

Table 14-3. Adding Port Security Screens Fields

Field	Action/Description
Name	Enter a name (up to 32 characters) for this security screen.
SVC Direction	The screen you configure is only applied to these SVCs. *Ingress* (default) – Screen incoming SVCs. *Egress* – Screen outgoing SVCs.
Type	Select the Type of screen. This determines the action this screen performs. *Block* (default) – Blocks all SVCs that match the criteria. *Pass* – Passes all SVCs that match the criteria.

Table 14-3. Adding Port Security Screens Fields (Continued)

Field	Action/Description
Calling Address	Configure the Calling Address if this screen is for incoming SVCs. *Type* – Select the address type, either AESA or E.164. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen using the guidelines on page 14-4. Enter up to 15 characters for an E.164 address; enter up to 40 characters for an AESA address.
Calling Subaddress	Configure the Calling Subaddress for incoming AESA SVCs only. This parameter provides an optional level of screening. *Type* – Select AESA. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen (up to 40 characters) using the guidelines on page 14-4.
Called Address	Configure the Called Address if this screen is for outgoing SVCs. *Type* – Select the address type, either AESA or E.164. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen using the guidelines on page 14-4. Enter up to 15 characters for an E.164 address; enter up to 40 characters for an AESA address.
Called Subaddress	Configure the Called Subaddress for outgoing AESA SVCs only. This parameter provides an optional level of screening. *Type* – Select AESA. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen (up to 40 characters) using the guidelines on page 14-4.

4. Choose OK to create the new screen.

5. The Adding Port Security Screen dialog box (Figure 14-2 on page 14-10) is designed to allow you to create several screens in a single session. To create additional screens, repeat Step 3 and Step 4 on page 14-11. Choose *Set To Defaults* to retrieve the default values if necessary.

6. When you finish creating your screens, choose Cancel to exit this dialog box.

Assigning Security Screens to Logical Ports

Once you create the security screens, you must modify existing logical ports to assign these screens to the individual logical ports. The default security screens you configure for each logical port enable you to quickly pass or block incoming or outgoing SVCs, without having to remove or modify the screen you have applied. For information about reverting back to the default security screen, refer to "Activating Default Screens" on page 14-15.

You also have the option of assigning several different security screens to this port, but configuring them as "inactive". You can then activate them as necessary, at a later time. For more information, refer to "Activating and Deactivating Security Screens" on page 14-16.

To assign security screens to a port:

1. Use the instructions on page 7-14 to access the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15).

2. Select the logical port to which you will assign a screen and choose Modify.

3. Review the logical port type and ID and choose OK. The Modify Logical Port dialog box reappears.

4. From the Select:Options: menu, select Screen Assignments and choose Set. The following dialog box appears.

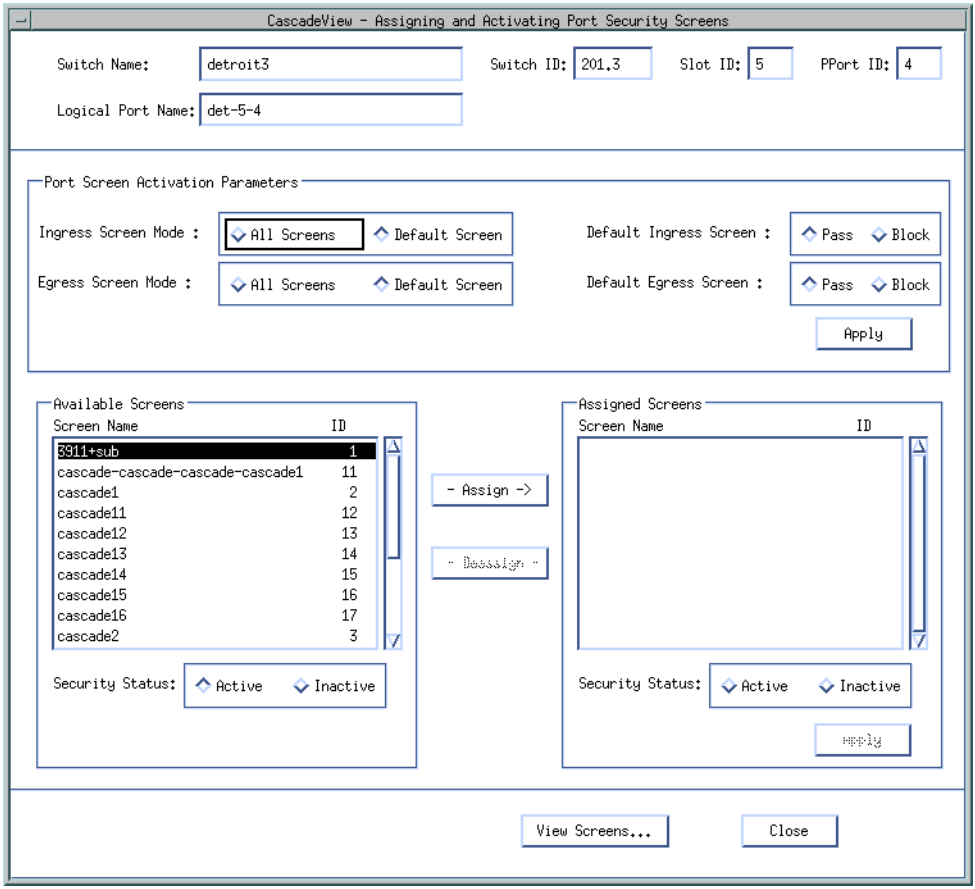


Figure 14-3. Assigning and Activating Port Security Screens

5. Refer to Table 14-1 on page 14-2 to configure the Port Screen Activation Parameters to meet your network needs.
6. Choose Apply to set the Port Screen Activation Parameters.
7. The Available Screens list provides the list of security screens you can assign to this port. Select the name of the screen you want to assign.
8. The Security Status of the screen you select defaults to active. This logical port will begin screening SVCs according to the rules of this screen as soon as you assign it.

   Select Inactive and choose Apply to assign a screen to this logical port without making it active immediately.

You can choose the View Screens command button to view the parameters configured for the screen you want to use.

9. Choose Assign to assign a screen to this logical port. The screen name appears in the Assigned Screens list.
10. The Assigning and Activating Port Security Screens dialog box (Figure 14-3 on page 14-13) is designed to allow you to assign several screens in a single session. To create additional screens, repeat Step 7 through Step 9. (You can assign up to 16 screens per logical port.)
11. When you finish creating your screens, choose Close to exit this dialog box.

Deassigning Security Screens

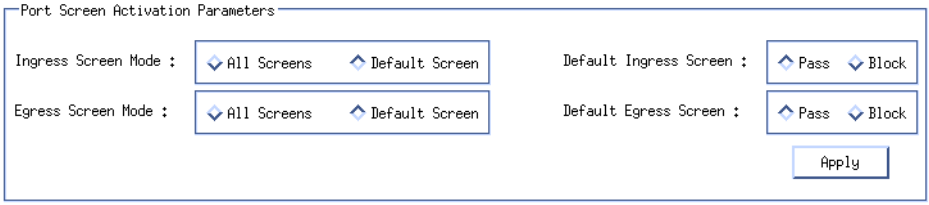
Use the following steps to remove a security screen assignment for a logical port:

1. Use Step 1 through Step 4 starting on page 14-15 to access the Assigning and Activating Port Security Screens dialog box (Figure 14-3 on page 14-13).
2. Review the list of Assigned Screens and select the screen.
3. Choose Deassign. This screen should now appear in the Available Screens list.

Activating Default Screens

Use the following steps to activate the default screening parameter(s) to temporarily override assigned security screens.

1. Use the instructions on page 7-14 to access the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15).
2. Select the logical port for which you will activate the default screen(s) and choose Modify.
3. Review the logical port type and ID and choose OK. The Modify Logical Port dialog box reappears.
4. From the Select:Options: menu, select Screen Assignments and choose Set. The Assigning and Activating Port Security Screens dialog box appears (Figure 14-3 on page 14-13).
5. Review the information configured in the Port Screen Activation Parameters group box. Refer to Table 14-1 on page 14-2 if you need information to modify these parameters.

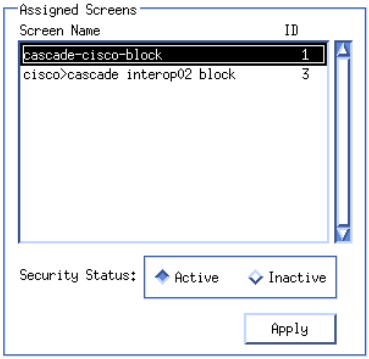


6. Choose Apply to activate the default screen.
7. Choose Close to exit this dialog box.

Activating and Deactivating Security Screens

Use the following steps to activate or deactivate a security screen according to your network needs:

1. Use the instructions on page 7-14 to access the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15).
2. Select the logical port for which you will change the security status and choose Modify.
3. Review the logical port type and ID and choose OK. The Modify Logical Port dialog box reappears.
4. From the Select:Options: menu, select Screen Assignments and choose Set. The Assigning and Activating Port Security Screens dialog box appears (Figure 14-3 on page 14-13).
5. In the Assigned Screens list, select the screen and modify the Security Status as necessary (Active or Inactive).



You can choose the View Screens command button to view the parameters configured for the screen you want to modify.

6. Choose Apply. The change takes effect immediately.
7. Repeat Step 5 and Step 6 to activate/deactivate additional screens.
8. Choose Close when you finish to exit this dialog box.

Viewing Screen Assignments

Use the following steps to view screen assignments for a specific logical port:

1. Use the instructions on page 7-14 to access the Set All Logical Ports in PPort dialog box (Figure 7-1 on page 7-15).
2. Select the logical port for which you want to view screen assignments.
3. Use the Select:Options menu to select Screen Assignments. Choose View. The following dialog box appears.

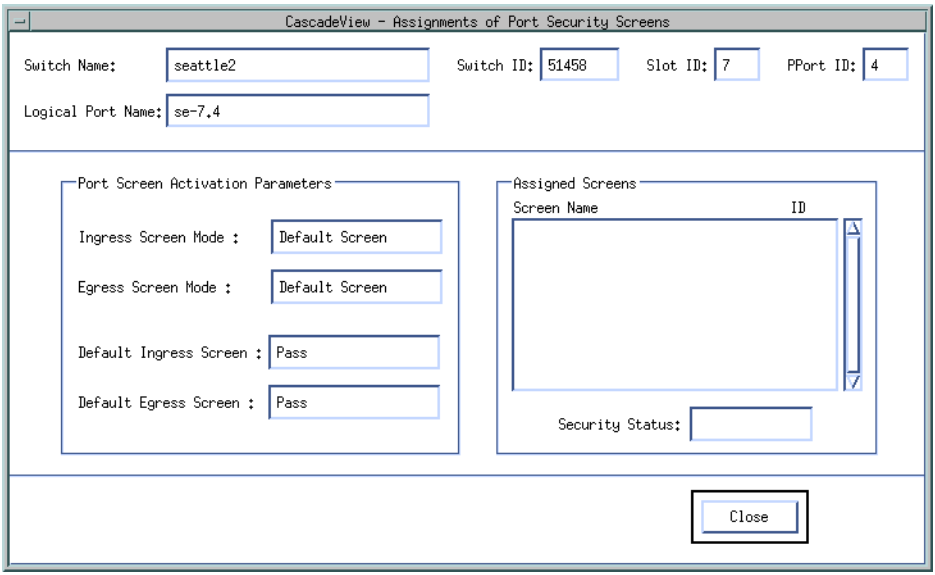


Figure 14-4. Assignments of Port Security Screens Dialog Box

- The *Port Screen Activation Parameters* fields provide the default security screen settings for this logical port. Refer to Table 14-1 on page 14-2 for field descriptions.
- The *Assigned Screens* list provides each screen name assigned to this logical port.

4. Choose Close to exit this dialog box.

A

Adjusting the CAC

This appendix describes how to tune the Cascade Call Master Connection Admission Control (CAC) to achieve a desired cell loss ratio objective across all physical ports in your network.

When creating a circuit, the CAC function computes a bandwidth allocation for that circuit and updates the bandwidth allocation for the circuit's QoS class. This bandwidth allocation depends on the specified CAC implementation, the circuit's QoS class and the circuit's specified traffic descriptor. If you try to create a circuit that causes the allocated bandwidth for a given QoS class to exceed the bandwidth available for that class, the circuit will not be created.

The CAC configuration option enables you to choose between three CAC implementations. You can choose the Cascade CAC implementation or configure one of two customized CAC implementations: "customize VBR-NRT and ABR" and "customize VBR-RT, VBR-NRT, and ABR".

The Cascade CAC implementation allows you to control the Quality of Service and bandwidth allocation by specifying cell loss ratio and cell delay variation objectives while the customized CAC implementations allow you to directly control the bandwidth allocation for circuits. The “customize VBR-NRT and ABR” CAC implementation allows you to control the amount of bandwidth that is reserved for VBR Non-Real Time and ABR circuits, while the “customize VBR-RT, VBR-NRT, and ABR” CAC implementation allows you to control the amount of bandwidth that is reserved for VBR Real Time, VBR Non-Real Time, and ABR circuits. In either implementation, you can control the amount of bandwidth reserved based on the physical port type, or based on configurable ranges of SCR values, or both. With these two customized implementations you also control the establishment of circuits based on configurable ranges of maximum MBS values.

Quality of service for the VBR-RT and VBR-NRT QoS classes is not guaranteed when using the “customize VBR-RT,VBR-NRT, and ABR” CAC implementation. Also, the Quality of Service for the VBR-NRT QoS class is not guaranteed when using the “customize VBR-NRT and ABR” CAC implementation.

When adjusting the CAC function, you can choose only one of these options. Whether you are tuning the Cascade CAC or configuring a customized CAC, the adjustments you make apply only to the VBR-RT,VBR-NRT, and ABR traffic types.

Before tuning the Cascade CAC or configuring a customized CAC, you should closely monitor your network to achieve a good understanding of the network’s traffic profile. Be conservative when you adjust the CAC to ensure quality of service. After you make adjustments, monitor the network closely to determine the effect of these adjustments, making sure you have not adversely impacted the quality of service on the network.

About the Customizable CAC Options

Both of the customizable CAC implementations enable you to directly control the amount of bandwidth that is reserved for VBR-NRT and ABR circuits. In addition, you can control the amount of bandwidth that is reserved for VBR-RT circuits if you choose the “customize VBR-RT,VBR-NRT, and ABR” CAC implementation. You can control the amount of bandwidth reserved based on the physical port type, or based on the SCR requirements of the circuit, or both. When you use the customized CAC options, the following formula determines the amount of bandwidth that is required for a given circuit:

```
Bwidthreq = SCR*F1*F2
```

where F1 is the physical port factor (entered as a percentage), and F2 is the SCR scale factor (also entered as a percentage). You can configure only an F1 factor, only an F2 factor, or both factors. If you do not configure one of these factors, then the value of that factor is, by default, 100%.

Example

A circuit request is made, and the circuit needs to reserve bandwidth based on an SCR of 10,000 cells/sec. You configure the F1 factor for DS3 ports at 150%, the F1 factor for OC3c ports at 80%, and the F2 factor for circuits with an SCR from 8,001-15,000 cells/sec at 80%.

- If the circuit request is made on a DS3 port, then the bandwidth requirements of the circuit will be based on an SCR of 12,000 cells/sec, instead of 10,000 cells/sec (10,000 x 150% x 80% = 12,000).
- If the circuit request is made on an OC3c port, then the circuit bandwidth requirements will be based on an SCR of 6,400 cells/sec (10,000 x 80% x 80%= 6,400).

Configuring the CAC

To configure a customized CAC:

1. On the network map, select the switch for which you need to adjust the CAC.
2. From the Administer menu, select Cascade Parameters ⇒ Set All CAC Parameters. The Modify CAC Parameters dialog box appears.

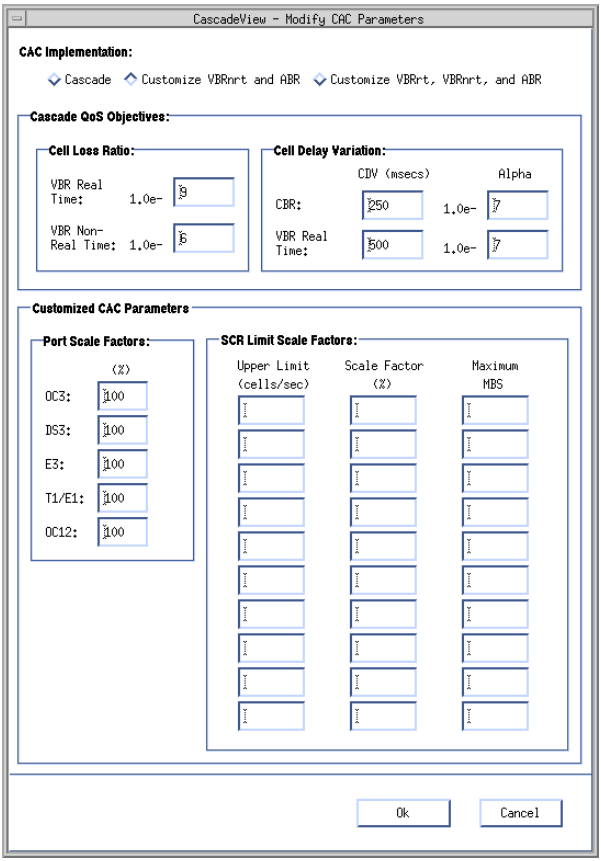


Figure A-1. Modify CAC Parameters Dialog Box

3. Select one of the following CAC Implementations:

   Cascade — Enables you to tune the Cell Loss Ratio and Cell Delay Variation only. Refer to the following section, "Tuning the Cascade CAC", for more information.

   Customize VBR-NRT and ABR — Enables you to tune the Cell Loss Ratio, Cell Delay Variation, and Customized CAC Parameters.

   Customized VBR-RT, VBR-NRT, and ABR — Enables you to tune Customized CAC Parameters only.

Tuning the Cascade CAC

To tune the Cascade CAC, specify the cell loss ratio objectives you want to meet across your network. You can specify a cell loss ratio objective in the range of 10^{-1} to 10^{-12}. For example, an entry of 10^{-5} specifies that circuits will not be created on any physical port on which:

- The cell drop ratio is currently 1 in 100,000 (because 10^{-5} is equal to 1/100,000)

OR

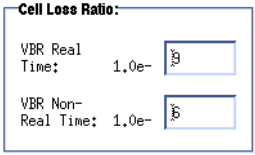
- The creation of the circuit would potentially cause the cell drop ratio to exceed 1 in 100,000

Cascade recommends that you adjust the CAC when you first configure a switch. Adjusting the CAC after several circuits have been created will not automatically change the bandwidth allocation for these circuits and may not guarantee the defined Quality of Service.

To tune the Cascade CAC:

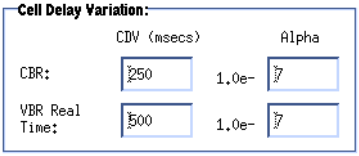
1. On the Modify CAC Parameters dialog box (Figure A-1 on page A-4), select the Cascade CAC implementation.

2. In the Cell Loss Ratio Objectives VBR Real Time and VBR Non-Real Time fields, specify the cell loss ratio objective you want to meet for each of these traffic types. This value is a negative power of ten (1.0e–). For example, if you enter 5, your cell loss ratio objective is a maximum of 1 dropped cell for every 100,000 cells. If the CAC determines that the creation of a circuit on a physical port will cause more than 1 in 100,000 cells to be dropped, then the circuit will not be created on that physical port.



   By default, VBR Real Time is set to 9 (1 in 1,000,000,000) and VBR Non-Real Time is set to 6 (1 in 1,000,000).

3. In the Cell Delay Variation CBR and VBR Real Time fields, specify the CDV (in microseconds). This value represents the CDV objective for the CBR and VBR Real Time QoS class. By default, the Cell Loss Ration (CLR) for VBR Real Time is set to 9 (1 in 1,000,000,000) and the CLR for VBR Non-Real Time is set to 6 (1 in 1,000,000).



4. In the Alpha field, specify the fraction of the CBR (or VBR Real Time) cells that can exceed this CDV objective. This value is a negative power of ten (1.0e–). By default, the Alpha field for each of the CBR and VBR Real Time classes is set to 7 (1 in 10,000,000).

5. When you finish, choose OK to send the values you entered to the selected switch.

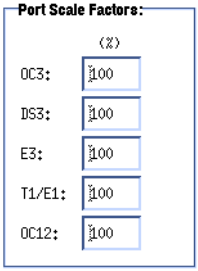
6. To send these values to another switch on the network map, select the switch and use Step 2 on page A-4 to access the Modify CAC Parameters dialog box. Choose OK.

Customizing the CAC for the VBR-RT, VBR-NRT, and ABR Classes

To customize the CAC for VBR-RT, VBR-NRT, and ABR:

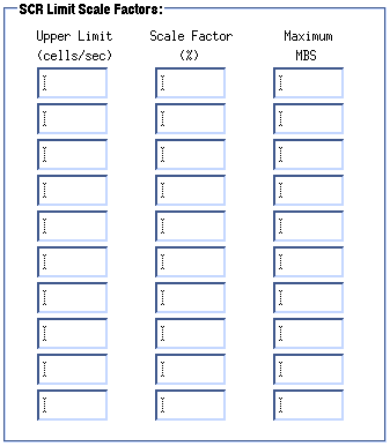
1. On the Modify CAC Parameters dialog box (Figure A-1 on page A-4), select the customize VBR-RT, VBR-NRT, and ABR CAC implementation.

2. In the Port Scale Factors box, enter a scale factor percentage to use for computing bandwidth requirements on the physical port.



For example, if you enter a value of 125% in the DS3 field, a circuit that would normally reserve bandwidth based on an SCR of 10,000 cells/sec would be allocated bandwidth of 12,500 cells/sec.

3. To customize the CAC based on the SCR and MBS values:



a. In the Upper Limit column, enter the upper limit of the SCR range for which you want to customize the amount of bandwidth reserved. You can specify up to ten upper limits. The following list shows several examples.

Example 1	Example 2	Example 3
10,000	10,000	8,000
20,000	16,000	12,000
35,000	20,000	15,000
—	24,000	20,000
—	28,000	25,000
—	35,000	30,000
—	—	35,000

This would give you the following ranges of SCR values:

Range	Example 1	Example 2	Example 3
1	0-10,000	0-10,000	0-8,000
2	10,001-20,000	10,001-16,000	8,001-12,000
3	20,001-35,000	16,001-20,000	12,001-15,000
4	—	20,001-24,000	15,001-20,000
5	—	24,001-28,000	20,001-25,000
6	—	28,001-35,000	25,001-30,000
7	—	—	30,001-35,000

To determine the ranges you should configure, monitor the VBR traffic on your network, then group your VBR circuits into appropriate SCR ranges.

b. In the Scale Factor column, enter a scale factor percentage to use when computing bandwidth requirements for circuits in each of the SCR ranges you defined.

   For example, if you enter a value of 125%, a circuit with an SCR of 12,000 cells/sec would be allocated a bandwidth of 15,000 cells/sec (assuming you did not define physical port scale factors).

c. In the Maximum MBS column, enter an MBS value which defines the maximum MBS value allowed for each range of SCR values.

   For example, if you enter a maximum MBS value of 256 for the range of SCR values (0-10000), a circuit with an SCR of 7,000 cells/sec and MBS of 300 cells will be rejected by the CAC function because its MBS exceeds the specified maximum MBS.

4. When you finish, choose OK to send the values you entered to the selected switch.

5. To send these values to another switch on the network map, select the switch and use Step 2 on page A-4 to access the Modify CAC Parameters dialog box. Choose OK.

Customizing the CAC for the VBR-NRT and ABR Classes

To customize the CAC for VBR-NRT and ABR:

1. On the Modify CAC Parameters dialog box (Figure A-1 on page A-4), select the customize VBR-NRT and ABR CAC implementation.
2. Refer to "Tuning the Cascade CAC" on page A-5 to enter the desired values for the Cell Loss Ration and Cell Delay Variation objectives.
3. Refer to "Customizing the CAC for the VBR-RT, VBR-NRT, and ABR Classes" on page A-7 to enter the desired values in the Port Scale Factors, SCR ranges, and SCR scale factors and maximum MBS fields.
4. When you finish, choose OK to send these values to the selected switch.

How the CBX 500 Handles UBR VCs

This section explains how the CBX 500 handles UBR virtual circuits (VCs) from a UPC (Usage Parameter Control or "policer") and CAC standpoint. A UBR VC is a VC that is assigned to the CBX 500 UBR Service Category either through provisioning at the NMS (PVC) or through UNI signaling from a user device (SVC).

Depending on the Traffic Descriptors used when provisioning or signaling in the VC, a VC in the CBX 500 UBR Service Category may either be policed (at PCR) or not policed (best effort). In addition, depending on the switch software version used, the UBR VC may or may not have an "equivalent bandwidth" value associated with it for CAC purposes. The following sections describe these dependencies.

UBR and Policing

When you configure PVCs, CascadeView/UX prompts you to enter the QoS Class in the forward and reverse directions. Once you select the UBR QoS Class, you choose the Traffic Descriptor associated with the QoS Class. This is where the first switch software dependency enters in. The following sections explain the options you have for provisioning UBR PVCs according to the switch software and CascadeView/UX version you are using.

CascadeView 2.3 & CBX 500 Release 1.3 (and Later Versions)

If you are using version 2.3 of CascadeView/UX and version 1.3 of CBX 500 switch software (or greater), you have the following options for configuring UBR PVCs:

PCR 0+1 Best Effort (*default*) — If you select this Traffic Descriptor option with the UBR QoS Class, the PVC will not be policed. Since the UPC does not police the PVC, the NMS does not require you to enter a PCR value. The logical port bandwidth is used to calculate the circuit utilization percentages that are available using Circuit Summary Statistics (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).

This traffic descriptor option is most useful for providing "best effort" ATM service in cases where the service provider does not wish to restrict (i.e., police) the level of user traffic.

PCR 0+1 — If you select this Traffic Descriptor option with the UBR QoS Class, the PVC will be policed at the PCR you enter. The NMS not only passes the PCR to the UPC (policer) component, but it also examines the PCR to ensure it is not greater than assigned logical port bandwidth. The NMS uses the PCR value to calculate the Circuit Utilization percentages that are available under Circuit Summary Statistics (refer to the *Diagnostic and Troubleshooting Guide for CBX 500*).

This traffic descriptor option is most useful for providing "best effort" ATM service, but with some policing controls in place to ensure the user traffic does not exceed the entered PCR value.

CascadeView 2.2 & CBX 500 Release 1.2.x (and Prior Versions)

If you are using version 2.2 of CascadeView/UX and version 1.2.x of CBX 500 switch software (or earlier), the only option available for provisioning UBR PVCs is the PCR 0+1 Best Effort option described above. Version 2.2 of CascadeView prompts you to enter a PCR value for a UBR PVC. The number you enter is only used to calculate the circuit utilization percentages under circuit summary statistics.

With SVCs, if the SETUP message from the calling party includes the Best Effort Indicator, the VC will not be policed. If the SETUP message does not include the Best Effort Indicator, the VC will be policed at the PCR rate that is signalled in. This behavior is the same regardless of switch software or CascadeView/UX version used.

UBR and CAC

The CBX 500 CAC assigns an equivalent bandwidth (EBW) number to each VC (PVC or SVC) as explained earlier in this appendix. For UBR VCs, the EBW assigned to each VC depends on the CBX 500 switch software version used. If you use CBX 500 Release 1.2.x (or previous releases), the EBW assigned to UBR VCs is always zero. This zero value effectively allows a logical port to support an unlimited number of UBR VCs, as the zero value caused the CAC function to “admit” as many UBR VCs as you choose to configure or signal in. This is why CascadeView/UX prevents you from oversubscribing the UBR Service Category (it is not necessary since you are already allowed unlimited UBR VCs).

While this approach is consistent with the “best effort” nature of UBR, it presents problems when routing over parallel trunks between switches. Because the UBR VCs have no EBW associated with them, situations could occur where if the admin cost were equal on the parallel trunks, all or a majority of the UBR VCs could be established over one of the trunks. This condition would prevent the desired load balancing over the two trunks.

To solve this problem, UBR VCs no longer have a EBW of zero. This change was introduced in Release 1.3 and is included in future releases. The EBW of UBR VCs is now 100 cps. The software uses this value regardless of PCR (configured or signalled) or regardless of whether the Best Effort indicator is used. EBW for UBR VCs is always 100 cps.

As part of this change, CascadeView/UX version 2.3 (and greater) now permits the oversubscription of the UBR service category up to 1000% (same limit provided by the other service categories).

B

The cascadeview.cfg File

This appendix describes the CascadeView/UX defaults configuration file, *cascadeview.cfg*. This file is located in */opt/CascadeView/etc/* and contains the default variables for many features used on the STDX 3000/6000, B-STDX 8000/9000, and CBX 500 switches.

To view the contents of this file, enter the following:

```
cat /opt/CascadeView/etc/cascadeview.cfg
```

Whenever you modify this file, you must stop and then restart CascadeView for the changes to take effect. Refer to Chapter 2 for instructions on stopping and starting CascadeView/UX.

cascadeview.cfg File

```
#!/bin/sh
#  @(#)cascadeview.cfg  (version: $Revision:   1.22  $Date$)
#  CascadeView configuration file.
#  Copyright 1994 Cascade Communications Corp.
#  All rights reserved.
#
#  Config for tracing:
CV_TRACE_ENABLED=0
CV_TRACEFILE=
export CV_TRACE_ENABLED CV_TRACEFILE
#
#  Config for message catalogs:
CV_ERROR_MSG_CAT_PATH=/opt/CascadeView/nls/C/cascadeview-errors.cat
export CV_ERROR_MSG_CAT_PATH
#
#  Config for database:
CVDB_TRACE_FILE_NAME=
export CVDB_TRACE_FILE_NAME
#
#  Config for map application:
CV_DEF_ADDRESS_SIGNIFICANCE=2       #local
CV_DEF_NETWORK_NUMBER=152.148.0.0
export CV_DEF_ADDRESS_SIGNIFICANCE CV_DEF_NETWORK_NUMBER
#
#  Config for switch initialization:
CV_SWITCH_INIT_FILE_DIR=/var/CascadeView/initFiles
export CV_SWITCH_INIT_FILE_DIR
#
```

```
#  Config for configuration sync.:
CV_SYNC_FILE_DIR=/tftpboot/cv_cfgSyncFiles
CV_SYNC_CHECK_DELAY=8
CV_SYNC_CHECK_INTERVAL=3
CV_SYNC_CHECK_COUNT=10
export CV_SYNC_FILE_DIR
export CV_SYNC_CHECK_DELAY CV_SYNC_CHECK_INTERVAL CV_SYNC_CHECK_COUNT
#
# Config for offline pram sync file name
CV_SYNC_FILE_OFFLINE_LIST=/tftpboot/cv_cfgSyncFiles/offline.lst
export CV_SYNC_FILE_OFFLINE_LIST
#
#  Config for SNMP management
CV_SNMP_IS_ENABLED=1
CV_SNMP_REQUEST_TIMEOUT=256
CV_SNMP_MAX_RETRIES=4
CV_SNMP_RETRY_INTERVAL=30
CV_SNMP_PUBLIC_COMMUNITY=public
CV_SNMP_READ_WRITE_COMMUNITY=constitution
export CV_SNMP_IS_ENABLED CV_SNMP_REQUEST_TIMEOUT CV_SNMP_MAX_RETRIES
export CV_SNMP_RETRY_INTERVAL CV_SNMP_PUBLIC_COMMUNITY
export CV_SNMP_READ_WRITE_COMMUNITY
#
#  Config for diagnostics (all time periods are in seconds):
CV_BG_DIAG_POLL_INTERVAL=3
CV_FG_DIAG_CHECK_DELAY=5
CV_FG_DIAG_CHECK_INTERVAL=1
CV_FG_DIAG_CHECK_COUNT=3
CV_DIAG_REASON_CATALOG=/opt/CascadeView/nls/C/cvDiagReasons.cat
export CV_BG_DIAG_POLL_INTERVAL CV_FG_DIAG_CHECK_DELAY
export CV_FG_DIAG_CHECK_INTERVAL CV_FG_DIAG_CHECK_COUNT
export CV_DIAG_REASON_CATALOG
#
```

```
#  Config for switch configuration:
CV_NODE_QOS_POLL_TIMER=60
export CV_NODE_QOS_POLL_TIMER
#
#  Config for status monitoring (time periods are in seconds):
CV_STATUS_POLL_INTERVAL=30
export CV_STATUS_POLL_INTERVAL
#
#  Config for physical port performance tuning:
CV_PPORT_DEF_DISCARD_HIGH=32
CV_PPORT_DEF_DISCARD_LOW=10
CV_PPORT_DEF_AQL_THRESHOLD=16
export CV_ENV_PPORT_DEF_DISCARD_HIGH
export CV_ENV_PPORT_DEF_DISCARD_LOW
export CV_ENV_PPORT_DEF_AQL_THRESHOLD
#
#  Config for SMDS Prefix Length: (temporary)
CV_SMDS_MASK_SIZE=6
export CV_SMDS_MASK_SIZE
#
#  Disable Smds Switching System
#  0 to enable and 1 to disable
CV_DISABLE_SMDS_SS=0
export CV_DISABLE_SMDS_SS
#
#  Enable audit trail
CV_AUDIT_TRAIL_ENABLE=TRUE
export CV_AUDIT_TRAIL_ENABLE
#
```

```
#  Determine how frequent to refresh the out-of-sync flag from the database.
#  0 will be used to disable this feature and
#  N implies out-of-sync flag will be refreshed for every N node poll intervals
#
CV_OUT_OF_SYNC_REFRESH_CNT=5
export CV_OUT_OF_SYNC_REFRESH_CNT
#
#  Enable HSSI PPort over clocking
#  Warning: User is not recommended to enable this feature because overclocking
#  the HSSI pport may cause instability to the HSSI card.
#
CV_ENABLE_HSSI_PPORT_OVERCLOCKING=FALSE
export CV_ENABLE_HSSI_PPORT_OVERCLOCKING
#
#  Enable ATM OPTimum Trunk Bandwidth over subscribing.
#
CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE=FALSE
export CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE
#
#  Override default max LPorts per STDX 3000/6000.
#  <= 0 or missing - use default (currently 150). > 0 - use this value.
CV_MAX_INTERFACES_PER_STDX=150
export CV_MAX_INTERFACES_PER_STDX
CV_POLL_SERVER_PORT=10888
CV_POLL_SERVER_ADDRESS=localhost
export CV_POLL_SERVER_PORT CV_POLL_SERVER_ADDRESS
#
```

```
#  ATM UNI logical port defaults.
#
#    o  "UNI Type" defaults can be "PUBLIC" or "PRIVATE"
#    o  "Connection Type" defaults can be "NET_ENDSYS" or "NET_NET"
#
CV_ATMUNI_UNI_TYPE_DEFAULT=PUBLIC
CV_ATMUNIDCE_CONN_TYPE_DEFAULT=NET_ENDSYS
export CV_ATMUNI_UNI_TYPE_DEFAULT
export CV_ATMUNIDCE_CONN_TYPE_DEFAULT
#
#  Enable Move All Circuit
CV_ENABLE_MOVE_ALL_CIRCUIT=TRUE
export CV_ENABLE_MOVE_ALL_CIRCUIT
#
#  Checking the card type for Move All Circuit
CV_MV_CKT_CARD_TYPE_CHECKING=TRUE
export CV_MV_CKT_CARD_TYPE_CHECKING
#
# VPN/Customer configuration
# CV_CUR_VPNCUST =[VPN | CUSTOMER ]
CV_CUR_VPNCUST=
CV_CUR_VPN_NAME=
CV_CUR_CUST_NAME=
export CV_CUR_VPNCUST
export CV_CUR_VPN_NAME
export CV_CUR_CUST_NAME
#
#  Default Login settings
# CV_LOGON_TYPE =[OPERATOR | PROVISIONING]
#
#CV_LOGON_TYPE=OPERATOR
#export CV_LOGON_TYPE
#
```

```
#  Network distribution evaluation interval.
#
#    o  CV_NET_DIST_EVAL_INTERVAL is the number of seconds to pause
#       between evaluations when determining the network distribution
#       of a distributed Cascade object.  To be used when defining an
#       evaluation threshold for a Cascade distributed object.  Allowable
#       values are "1" to "60".
#
CV_NET_DIST_EVAL_INTERVAL=2
export CV_NET_DIST_EVAL_INTERVAL
#
#  SVC Closed User Groups network distribution evaluation threshold.
#
#    o  CV_SVC_CUG_NODE_EVAL_THRESH is the number of nodes (out of all of
#       the nodes in the network to be evaluated) on which to match configured
#       SVC addresses against a member rule regular expression at one time
#       before pausing for CV_NET_DIST_EVAL_INTERVAL seconds.  A value of
#       zero ("0") results in all nodes in the network being evaluated at
#       once with no pause.
#    o  CV_SVC_CUG_LOGFILE is the path and filename to log the results of
#       matching configured SVC addresses against a member rule regular
#       expression when determining whether or not a node belongs in a member
#       rule's network distribution.  A valid value enables logging.  A null
#       or invalid value disables logging.  The CascadeView PID will be
#       appended to the filename.
#
CV_SVC_CUG_NODE_EVAL_THRESH=0
CV_SVC_CUG_LOGFILE=
export CV_SVC_CUG_NODE_EVAL_THRESH
export CV_SVC_CUG_LOGFILE
#
```

```
#  CBX 500 shared switching fabric thread bandwidth limit enforcement
#
#    When this variable is set to "TRUE" CascadeView will restrict the sum
#    of the logical port bandwidth on two IOMs sharing a common switching
#    fabric thread to the thread's maximum supported bandwidth.  Setting this
#    variable to "FALSE" will disable this restriction and permit logical
#    ports to oversubscribe the thread.
#
CV_ENFORCE_CBX500_THREAD_BW_LIMIT=TRUE
export CV_ENFORCE_CBX500_THREAD_BW_LIMIT
#
#  Config for Loading Profile Rate Tables
#
CV_PROFILE_DISCARD_FILE=/opt/CascadeView/etc/cvDiscard.dat
CV_PROFILE_CONGESTION_FILE=/opt/CascadeView/etc/cvCongestion.dat
CV_PROFILE_RIF_FILE=/opt/CascadeView/etc/cvRif.dat
CV_PROFILE_RDF_FILE=/opt/CascadeView/etc/cvRdf.dat

export CV_PROFILE_DISCARD_FILE
export CV_PROFILE_CONGESTION_FILE
export CV_PROFILE_RIF_FILE
export CV_PROFILE_RDF_FILE
#
#
#  end cascadeview.cfg
#
```

cascadeview.cfg Variables

The following list describes each variable defined in *cascadeview.cfg*:

CV_TRACE_ENABLED=0 — This trace tool variable is for Cascade Customer Support diagnostic purposes only. Set to 1 to enable tracing.

CV_TRACEFILE — Specifies the location of the trace file.

CV_ERROR_MSG_CAT_PATH=/opt/CascadeView/nls/C/cascadeview-errors.cat — Sets the location of the error file that CascadeView uses. **Do not modify** this path and filename.

CVDB_TRACE_FILE_NAME — Displays the trace file name for database trace. This file is used in conjunction with the previous trace variable. This file is used by Cascade Customer Support.

CV_DEF_ADDRESS_SIGNIFICANCE=2 # local — Indicates that the addressing scheme used for DLCIs is of local significance only. A DLCI must only be unique to a logical port. **Do not modify** this value.

CV_DEF_NETWORK_NUMBER — Displays the internal IP address for the Cascade network. The NMS uses this number to contact and communicate with the gateway switch. This number must be a unique number within the LAN environment and must not be the same as any external Ethernet address. Refer to page 4-9 for more information about configuring the network number with the NMS.

CV_SWITCH_INIT_FILEDIR=/var/CascadeView/initFiles — Sets the location of the switch initialization files. **Do not modify** this path and filename.

CV_SYNC — These variables provide specific PRAM Sync information:

CV_SYNC_FILE_DIR=/tftpboot/cv_cfgSyncFiles — Sets the location of the following PRAM Synchronization files. **Do not modify** this path and filename.

CV_SYNC_CHECK_DELAY=8

CV_SYNC_CHECK_INTERVAL=3

CV_SYNC_CHECK_COUNT=10

CV_SYNC_FILE_OFFLINE_LIST=/tftpboot/cv_cfgSyncFiles/offline.lst (*B-STDX only*) — Sets the location of the offline PRAM synchronization files. **Do not modify** this path and filename.

CV_SNMP_IS_ENABLED=1 — This setting enables SNMP. **Do not modify**.

CV_SNMP_REQUEST_TIMEOUT =256 — This variable is not used.

CV_SNMP_MAX_RETRIES=4 — Specifies the number of retries the SNMP Client attempts before it declares the request to be timed out. The default is 4. In larger networks where the NMS is on a very busy LAN segment or is multiple hops away from the switch containing the Ethernet module, you may need to increase this value to 5.

CV_SNMP_RETRY_INTERVAL=30 — Specifies the amount of time (in tenths of a second) between SNMP retries. CPU-intensive operations such as PRAM synchronization, can cause CascadeView to drop node polls. Increase the amount of time between SNMP retries to avoid this problem. Restart OpenWindows if you modify this value.

Cascade recommends a value of 30 seconds for a configuration with 10 to 15 simultaneous instances of Cascadeview/UX and more than 15 switches in the network.

CV_PUBLIC_COMMUNITY=public — Specifies the SNMP public community name.

CV_SNMP_READ_WRITE_COMMUNITY=cascade — Specifies the default master Community Name of the NMS. Each NMS you define must use this name. Refer to page 5-11 for more information about configuring the NMS.

CV_BG_DIAG_POLL_INTERVAL — This field has no effect since background diagnostics does not poll the background diagnostic result.

CV_FG_DIAG_CHECK_DELAY=3 — Sets the time delay (in seconds) that the NMS waits before it sends the first PDU to check that foreground diagnostics are complete.

CV_FG_DIAG_CHECK_INTERVAL=1 — The NMS sends a check PDU multiple times until the diagnostics are complete. The CHECK_INTERVAL is the interval (in seconds) between the check PDUs.

CV_FG_DIAG_CHECK_COUNT=3 — The CHECK_COUNT is the maximum number of check PDUs that the NMS will send.

The value of CHECK_COUNT is used as the interval and the value of CHECK_INTERVAL is used as the count. ***Do not modify*** *these values.*

CV_DIAG_REASON_CATALOG=/opt/CascadeView/nls/C/cvDiagReasons.cat — This variable points to the catalog file that contains the diagnostics result strings. **Do not modify** this path and filename.

CV_NODE_QOS_POLL_TIMER=60 — Sets the default value for the Quality of Service (QoS) Statistics for retrieving circuit data from the switches.

CV_STATUS_POLL_INTERVAL=300 — The NMS node poll status interval variable sets the time interval that CascadeView uses to poll the nodes in the network. The default value is in seconds and the default is 5 minutes (300 seconds).

You can change the interval based on the number of users running CascadeView. A system with 30 users polls approximately once every 10 seconds. This change takes effect when you restart HP OpenView. In a configuration with 10-15 simultaneous instances of CascadeView, 60 seconds is an acceptable value for this variable.

The following values of "CV_PPORT_DEF" are used for physical port performance tuning. ***Do not modify*** *these values.*

CV_PPORT_DEF_DISCARD_HIGH=32

CV_PPORT_DEF_DISCARD_LOW=10

CV_PPORT_DEF_AQL_THRESHOLD=16

CV_SMDS_MASK_SIZE=6 (*B-STDX only*) — Use this variable to modify the size of the SMDS address mask for the entire network map. The mask size indicates the number of address digits a switch uses to make a switching decision. Valid values are 1 through 15. If you set the mask size of 0, it will disable the switching system. For more information, refer to the *Network Configuration Guide for B-STDX*.

CV_DISABLE_SMDS_SS=0 (*B-STDX only*) — Use this variable to enable (0) or disable (1) the SMDS switching system for the entire CascadeView network. If you modify this value, you must PRAM Sync each CP card in the network.

CV_AUDIT_TRAIL_ENABLE=TRUE — Use this variable to enable (TRUE) or disable (FALSE) the Audit Trail utility. If you modify this variable, you must shut down and then restart CascadeView. For more information about the Audit Trail utility, refer to page 2-6.

CV_OUT_OF_SYNC_REFRESH_CNT=0 — The map you display in each session of CascadeView refreshes every N node polls, where N is the number of specified node polls. To refresh, CascadeView checks the database for any out-of-sync conditions. Edit this variable to modify the refresh rate. To disable this feature, set this variable to 0.

CV_ENABLE_HSSI_PPORT_OVERCLOCKING=FALSE (*B-STDX only*) — Use this variable if you must exceed the maximum HSSI module capacity. The total bandwidth of all physical ports on the HSSI module can exceed the maximum module capacity of 44.212 Mbps. However, this setting can cause frame errors if all physical ports are running at full speed. To resolve this problem, set this variable to TRUE.

CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE=FALSE — If you set this value to True, the sum of the bandwidth of all ATM OPTimum trunk logical ports on a single physical port can exceed maximum physical port bandwidth.

CV_MAX_INTERFACES_PER_STDX=0 — This value specifies the maximum number of logical ports that can be defined on an STDX. This value can be set to a value between 0 and 254.

CV_ATMUNI_UNI_TYPE_DEFAULT=PUBLIC — This value is set to Public if at least one end of this connection attaches to a public network. It is set to Private if this connection resides completely within a private network. Refer to page 7-28 for more information about ATM UNI type.

CV_ATMUNIDCE_CONN_TYPE_DEFAULT=NET_ENDSYS — This value is set to Net_Endsys if this port connects to a router or host. It is set to Net_Net if this port connects to another ATM switch. Refer to page 7-29 for more information about connection type.

CV_POLL_SERVER_PORT=10888 — This variable represents the port CascadeView polls when using the Poll Server optional feature. The default value is 10888. The value must match the POLL_SRV_SRV_PORT.

CV_POLL_SERVER_ADDRESS=localhost — This variable provides the IP address (in dot notation) of the node used to run the Poll Server. If the Poll Server runs on the same node as CascadeView, it is set to a value of "localhost." This variable is required. Setting this variable and CV_POLL_SERVER_PORT enables Poll Server.

Refer to Appendix C for more information about Poll Server.

CV_ENABLE_MOVE_ALL_CIRCUIT=TRUE — If this variable is set to True, the Move Circuit function is enabled for this network. If it is set to False, it is disabled. Refer to page 9-28 for information about the Move Circuit function.

CV_MV_CKT_CARD_TYPE_CHECKING=TRUE — The Move Circuit function fails if the number of circuits moved exceeds the maximum allowed for the IOM. If this variable is set to True, the NMS notifies you that this problem exists before you move the circuit. If you set this variable to False, no notification is sent.

CV_CUR_VPNCUST — Indicates the current view (binding) for this map, either VPN or Customer.

CV_CUR_VPN_NAME — If CV_CUR_VPNCUST indicates a VPN binding, this variable displays the VPN name the map is using.

CV_CUR_CUST_NAME — If CV_CUR_VPNCUST indicates a customer binding, this variable displays the customer name the map is using.

CV_LOGON_TYPE — This variable displays the logon privilege you enabled for this map, either *Operator* or *Provisioning*.

CV_NET_DIST_EVAL_INTERVAL=2 — This variable represents the number of seconds to pause between evaluations when determining the network distribution of a distributed Cascade object. It is used when defining an evaluation threshold for a Cascade distributed object. Valid values range from 1 to 60.

CV_SVC_CUG_NODE_EVAL_THRESH=0 — This variable represents the number of nodes (out of all of the nodes in the network to be evaluated) on which to match configured SVC addresses against a member rule regular expression at one time before pausing for the number of seconds identified by the variable: CV_NET_DIST_EVAL_INTERVAL. A value of zero (0) results in all nodes in the network being evaluated at once with no pause.

CV_SVC_CUG_LOGFILE — This variable represents the path and filename used to log the results of matching configured SVC addresses against a member rule regular expression when determining whether or not a node belongs in a member rule's network distribution. A valid value enables logging. A null or invalid value disables logging. The CascadeView PID will be appended to the filename.

CV_PROFILE — These variables specify the location of the default buffer threshold and rate profile files used for the ATM FCP card. The ATM FCP uses these tables to determine the available bandwidth, the Rate Increase Factor (RIF), and the Rate Decrease Factor (RDF) for each VC on a port. Refer to the *ATM Flow Control Processor User's Guide* for more information.

CV_PROFILE_DISCARD_FILE=/opt/CascadeView/etc/cvDiscard.dat – Sets the location of the default discard file for CascadeView.

CV_PROFILE_CONGESTION_FILE=/opt/CascadeView/etc/cvCongestion.dat – Sets the location of the default congestion file for CascadeView.

CV_PROFILE_RIF_FILE=/opt/CascadeView/etc/cvRif.dat – Sets the location of the default RIF file for CascadeView.

CV_PROFILE_RDF_FILE=/opt/CascadeView/etc/cvRdf.dat – Sets the location of the default RDF file for CascadeView.

C

Configuring Poll Server

This release provides the optional Poll Server function, which does not run automatically until you configure and start it. By using Poll Server, you can reduce CascadeView's status-polling overhead when there are multiple CascadeView users monitoring the network simultaneously. (If there are more than five CascadeView sessions running, using the Poll Server is the most efficient way to poll the switches without causing switch congestion. The Poll Server acts like a daemon running in the background waiting for requests from an NMS session. When the Poll Server receives a request for status information, it polls the switch. Any additional NMS sessions requesting data receive status information from the Poll Server directly.

As a general guideline, with 40 consecutive users and 50 switches in the network, the Poll Server uses approximately 2 MB of RAM.

To use the Poll Server, you must set corresponding parameters in both CascadeView and Poll Server's environment variables. CascadeView uses these environment variables to locate the Poll Server. If the environment variables are not set, CascadeView assumes that Poll Server is not present and therefore communicates directly with the switch(es).

CascadeView Environment Variables

The environment variables that configure Poll Server for CascadeView are set in the *cascadeview.cfg* file (default directory */opt/CascadeView/etc*). The *cascadeview.cfg* file sets these variables such that the Poll Server is disabled. If you make changes to these variables in *cascadeview.cfg*, you must start the Poll Server node and restart all CascadeView sessions for the changes to take effect. For information about modifying the *cascadeview.cfg* file, refer to Appendix B.

Table C-1 describes the main parameters used to configure CascadeView to use the Poll Server function.

Table C-1. Poll Server Parameters (in cascadeview.cfg)

Parameter	Description
CV_POLL_SERVER_PORT	The port CascadeView polls when using the Poll Server. The default is 10888. This parameter is required and must match the POLL_SRV_SRV_PORT parameter (described in Table C-2 on page C-3). ***Note:*** *As a minimum configuration, set this parameter to 10888, and set* CV_POLL_SERVER_ADDRESS *to the node where the Poll Server is running.*
CV_POLL_SERVER_ADDRESS	IP address (in dot notation) of the node used to run the Poll Server. If the Poll Server runs on the same node as CascadeView, you can specify “localhost.” To use Poll Server, you must set this variable. ***Note:*** *As a minimum configuration, set this parameter to the node where the Poll Server is running, and set* CV_POLL_SERVER_PORT *to 10888.*
CV_STATUS_POLL_INTERVAL	*(Optional)* Status polling interval used by CascadeView. The default is 300 seconds. This setting should be greater than the POLL_TIME_INTERVAL setting.

Poll Server Environment Variables

You configure the “pollsrv” environment variables in the *run-pollsrv.sh* file, which is located in the */opt/CascadeView/bin* directory.

Table C-2 describes the main parameters used to configure the Poll Server function.

Table C-2. Poll Server Parameters (in run-pollsrv.sh)

Parameter	Description
POLL_SRV_SRV_PORT	*(Optional)* The port used to receive polls from CascadeView. This setting must match the CV_POLL_SERVER_PORT setting (described in Table C-1 on page C-2). The default is 10888.
POLL_SRV_COMMUNITY	*(Optional)* The default value for community name used to poll switches. The default is “public.”
POLL_TIME_INTERVAL	*(Optional)* The polling interval used to poll switches. This setting should be less than the CV_STATUS_POLL_INTERVAL setting. The default is 20 seconds.
POLL_SRV_DEV_PORT	*(Optional)* The port used when polling switches. This value is normally not changed. The default is 161.
POLL_SRV_DEV_TIMEOUT	*(Optional)* The timeout value used when polling switches. The default is 1500 milliseconds.
POLL_SRV_DEV_RETRIES	*(Optional)* The number of retry attempts for polling. This value is normally not changed. The default is 4.

Minimum Configuration

The minimal configuration that enables CascadeView to use the Poll Server is to set CV_POLL_SERVER_PORT to 10888 and CV_POLL_SERVER_ADDRESS to the node where the Poll Server is running. If the Poll Server runs on the same node, a value of “localhost” can be used. If these environment variables are not set, CascadeView will poll the switches directly.

The Poll Server expects that the community string to be sent to the switch will be embedded in the string that is sent from the client. If this is not found, it will use the environment variable POLL_SRV_COMMUNITY as the community name for the switches. The same value is used for all switches.

The Poll Server periodically refreshes its cached values. The expiration time for a value is given by POLL_TIME_INTERVAL. This value should be lower than CV_STATUS_POLL_INTERVAL, because values fetched more frequently than POLL_TIME_INTERVAL will not reflect changed status.

Starting and Stopping Poll Server

This section describes how to start and stop the Poll Server function. The following steps assume the default CascadeView directory is */opt/CascadeView*. If your default directory is in a different location, substitute accordingly.

When starting and stopping Poll Server (pollsrv), be sure to exit and restart all CascadeView sessions to take advantage of the configured polling service.

Starting Poll Server

To start the Poll Server:

1. As the root user, enter the following command to start the Poll Server (pollsrv):

   `/opt/CascadeView/bin/start-pollsrv.sh`

   This command adds the “run-pollsrv.sh” entry in the */etc/inittab* file and starts the pollsrv process.

2. Edit */opt/CascadeView/etc/cascadeview.cfg* as follows:

   Locate and uncomment the following CV_POLL_SERVER environment variables:

   ```
   CV_POLL_SERVER_PORT

   CV_POLL_SERVER_ADDRESS

   export CV_POLL_SERVER_PORT CV_POLL_SERVER_ADDRESS
   ```

3. Verify there is no # sign before the three environment variables.

4. (*Optional*) You may customize the Poll Server-related variables at this point.

5. Press the Escape key.

6. Enter **:wq!**

Any CascadeView sessions started after you complete these steps will use the Poll Server.

Stopping Poll Server

To stop the Poll Server:

1. As the root user, enter the following command:

   `/opt/CascadeView/bin/stop-pollsrv.sh`

   This command removes the “run-pollsrv.sh” entry in the */etc/inittab* file and stops the pollsrv process.

2. Edit */opt/CascadeView/etc/cascadeview.cfg* as follows:

   Locate and comment out the following CV_POLL_SERVER environment variables:

   - CV_POLL_SERVER_PORT
   - CV_POLL_SERVER_ADDRESS

   Any CascadeView sessions started after you complete these steps no longer use the Poll Server.

D

ATM Traffic Descriptors

This appendix describes how each traffic descriptor combination affects the cell streams under different traffic conditions. When you create either a PVC or a point-to-multipoint circuit, you select one of several traffic descriptor combinations. The traffic descriptor combination specifies which traffic parameters are used for traffic control. It also determines the number and type of cells that are admitted into a congested queue, and whether or not high-priority cells are tagged as low priority cells when traffic exceeds the traffic parameter thresholds.

The following sections describe how each traffic descriptor combination affects the cell streams under different traffic conditions.

PCR CLP=0, PCR CLP=0+1

You can select this option for CBR traffic. Traffic conformance is based on the Peak Cell Rate (PCR) of both the CLP=0 and CLP=0+1 cell streams with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0 stream; if the cell rate exceeds the PCR of CLP=0, the switch drops the CLP=0 cells arriving above that rate.
- The switch checks the cell rate of the CLP=0+1 stream; if the cell rate exceeds the PCR of CLP=0+1, the switch drops cells arriving above that rate. Cells are dropped according to a ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

Table D-1 illustrates what would happen to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the PCR for CLP=0 to 50,000 cells/sec and the PCR for CLP=0+1 to 70,000 cells/sec.

All values in the table represent the measured traffic rate at a given point in time.

Table D-1. Traffic Descriptor Combination - PCR CLP=0, PCR CLP=0+1

CLP=0 Cells/sec	CLP=1 Cells/sec	Result
45,000	22,000	The switch does not drop any cells because the CLP=0 and CLP=0+1 streams did not exceed the PCR.
50,000	22,000	The switch drops 2,000 cells/sec because the cell transmission rate exceeded the PCR of the CLP=0+1 cell stream. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	17,000	Since CLP=0 exceeds the PCR, the switch drops 5,000 CLP=0 cells/sec. This leaves 67,000 cells/sec in the CLP=0+1 stream, which is below the PCR of CLP=0+1. Therefore, no additional cells are dropped.

Table D-1. Traffic Descriptor Combination - PCR CLP=0, PCR CLP=0+1 (Continued)

CLP=0 Cells/sec	CLP=1 Cells/sec	Result
55,000	22,000	Since CLP=0 exceeds the PCR, the switch drops 5,000 CLP=0 cells/sec. This leaves 72,000 cells/sec in the CLP=0+1 stream, which also exceeds the traffic contract. Therefore, 2,000 additional cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells will be dropped for every 22 CLP=1 cells that are dropped.

PCR CLP=0, PCR CLP=0+1, Tagging

You can select this option for CBR traffic. Traffic conformance is based on the Peak Cell Rate of both the CLP=0 and CLP=0+1 cell streams with Tagging enabled. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0 stream; CLP=0 cells arriving above the PCR of CLP=0 are tagged as CLP=1 cells.
- The switch checks the cell rate of the CLP=0+1 stream; if the cell rate exceeds the PCR of CLP=0+1, the switch drops additional cells, based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

Table D-2 illustrates what would happen to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the PCR for CLP=0 to 50,000 cells/sec and the PCR for CLP=0+1 to 70,000 cells/sec.

All values in the table represent the measured traffic rate at a given point in time.

Table D-2. Traffic Descriptor Combination - PCR CLP=0, PCR CLP=0+1, Tagging

CLP=0 Cells/sec	CLP=1 Cells/sec	Result
45,000	22,000	The switch does not tag or drop any cells because the CLP=0 and CLP=0+1 streams did not exceed the PCR.
50,000	22,000	The switch drops 2,000 cells/sec because the cell transmission rate exceeded the PCR of the CLP=0+1 cell stream. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	17,000	Since CLP=0 exceeds the PCR, 5,000 CLP=0 cells/sec are tagged as CLP=1. This still leaves 72,000 cells/sec in the CLP=0+1 stream, which exceeds the PCR of CLP=0+1. Therefore, 2,000 cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	22,000	Since CLP=0 exceeds the PCR, 5,000 CLP=0 cells/sec are tagged as CLP=1 cells. This still leaves 77,000 cells/sec in the CLP=0+1 stream, which exceeds the PCR of CLP=0+1. Therefore, 7,000 cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 27, approximately 50 CLP=0 cells are dropped for every 27 CLP=1 cells that are dropped.

PCR CLP=0+1

You can select this option for CBR and UBR traffic. Traffic conformance is based only on Peak Cell Rate of the CLP=0+1 aggregate cell stream with no Best Effort. If you select this option, when the cell rate of the aggregate cell stream exceeds the specified PCR of CLP=0+1, the switch drops all non-conforming cells, whether they are CLP=0 or CLP=1 cells.

PCR CLP=0+1, Best Effort

You can select this option only for UBR traffic. A "best effort" attempt is made to deliver all traffic, but there is no guarantee the switch will not drop cells due to congestion. For more information about UBR circuits, refer to "How the CBX 500 Handles UBR VCs" on page A-10.

PCR CLP=0+1, SCR CLP=0, MBS CLP=0

You can select this option only for VBR traffic. Traffic conformance is based on Peak Cell Rate of the CLP=0+1 aggregate cell stream, as well as the Sustained Cell Rate and Maximum Burst Size of the CLP=0 cell stream with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR. The number of CLP=0 and CLP=1 cells dropped is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0 stream. If the cell rate exceeds the SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and CDVT. The switch drops cells that arrive above the SCR after the stream exceeds this tolerance level.

For more information about these traffic conformance parameters, refer to the ATM UNI Specification, Version 3.1 *or* Bellcore's GR-1110-CORE Specification.

Table D-3 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0 is 40,000
- MBS of CLP=0 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table D-3. Traffic Descriptor Combinations - PCR CLP=0+1, SCR CLP=0, MBS CLP=0

CLP=0+1 Cells/sec	SCR of CLP=0 Stream	MBS of CLP=0 Stream	Result
68,000	40,000	30	The switch does not drop any cells because the stream does not exceed traffic parameters.
70,000	40,000	60	The switch drops CLP=0 cells from the aggregate cell stream if the burst tolerance is exceeded. The number of cells that are dropped depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are dropped.
70,000	50,000	30	The switch drops 10,000 CLP=0 cells/sec because CLP=0 exceeds the SCR. It may drop additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The switch drops 7,000 cells/sec from the CLP=0+1 stream because the stream exceeds the PCR. The number of CLP=0 and CLP=1 cells dropped depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. Additionally, the switch will drop some CLP=0 cells if they exceed the burst tolerance.

PCR CLP=0+1, SCR CLP=0, MBS CLP=0, Tagging

You can select this option only for VBR traffic. Traffic conformance is based on Peak Cell Rate of the CLP=0+1 aggregate cell stream, as well as the Sustained Cell Rate and Maximum Burst Size of the CLP=0 cell stream with Tagging enabled. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR of CLP=0+1. The number of CLP=0 and CLP=1 cells dropped is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0 stream. If the stream exceeds SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and CDVT. The switch tags cells that arrive above the SCR after the stream exceeds this tolerance level.

For more information about these traffic conformance parameters, refer to the ATM UNI Specification, Version 3.1 *or* Bellcore's GR-1110-CORE Specification.

Table D-4 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0 is 40,000
- MBS of CLP=0 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table D-4. Traffic Descriptor Combinations - PCR CLP=0+1, SCR CLP=0, MBS CLP=0, Tagging

CLP=0+1 Cells/sec	SCR of CLP=0 Stream	MBS of CLP=0 Stream	Result
68,000	40,000	30	The switch does not drop or tag any cells because the stream does not exceed traffic parameters.
70,000	40,000	60	CLP=0 cells from the aggregate cell stream are tagged if the burst tolerance is exceeded. The number of cells that are tagged depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are tagged.
70,000	50,000	30	The switch tags as many as 10,000 CLP=0 cells/sec because CLP=0 exceeds the SCR. It may tag additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The switch drops 7,000 cells/sec from the CLP=0+1 stream because CLP=0+1 exceeds the PCR. The number of CLP=0 and CLP=1 cells that are dropped depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. Additionally, the switch will tag some CLP=0 cells if they exceed the burst tolerance.

PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1

You can select this option only for VBR traffic. Traffic conformance is based on Peak Cell Rate, Sustained Cell Rate, and Maximum Burst Size of the CLP=0+1 cell stream with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR of CLP=0+1. The number of CLP=0 and CLP=1 cells that it drops is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0+1 stream. If the stream exceeds SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and CDVT. The switch drops cells that arrive above the SCR after the stream exceeds this tolerance level.

For more information about these traffic conformance parameters, refer to the ATM UNI Specification, Version 3.1 *or* Bellcore's GR-1110-CORE Specification.

Table D-5 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0+1 is 40,000
- MBS of CLP=0+1 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table D-5. Traffic Descriptor Combinations - PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1

CLP=0+1 Cells/sec	SCR of CLP=0+1 Stream	MBS of CLP=0+1 Stream	Result
68,000	40,000	30	The switch does not drop any cells because the streams do not exceed traffic parameters.
70,000	40,000	60	CLP=0+1 cells are dropped from the aggregate cell stream if the burst tolerance is exceeded. The number of cells that are dropped depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are dropped.
70,000	50,000	30	The switch drops 10,000 CLP=0+1 cells/sec because CLP=0+1 exceeds the SCR. It may drop additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The CLP=0+1 stream drops 7,000 cells per sec. because CLP=0+1 exceeds the PCR. The number of CLP=0 and CLP=1 cells that the switch drops depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. Additionally, the switch may drop some CLP=0+1 cells if they exceed the burst tolerance.

E

Glossary

access rate

The data rate of the user access channel. The speed of the access channel determines how quickly (maximum rate) the end user may inject data into the network. See also *bandwidth.*

active hub

A device that amplifies LAN transmission signals in a network, enabling signals to be sent over a much greater distance than is possible with a passive hub. Compare with *passive hub.*

address

The logical location or identifier of a network node, terminal, pc, peripheral device, or location in memory where information is stored. See also *network address.*

administration tool

A system administration utility, such as Solaris, that allows system administrators to maintain and monitor system database files, printers, user accounts, and hosts through a graphical user interface (GUI).

AIS

See *Alarm Indication Signal*.

alarm

Message notifying an operator or administrator of a network problem.

Alarm Indication Signal

An error or alarm signal transmitted in lieu of the normal signal to maintain transmission continuity to the receiving node indicating that there is a transmission fault located either at the sending node or upstream of the sending node.

Alterable Mark Inversion

A signaling format used in T1 lines that provides for the “one” pulses to have an alternating priority. Thus, if the nth-one bit is represented by a positive pulse, the nth T1 line would be a negative pulse.

alternate path

An optional automatic feature of OSPF (Open Shortest Path First) that reroutes the PVC should a trunk fail within a manually defined path.

American National Standards Institute

A private, non-governmental, non-profit organization, which develops US standards required for commerce.

American Standard Code for Information Interchange

A code representing characters in binary form.

AMI

See *Alterable Mark Inversion.*

analog

A method that transmits electrical signals at varying amplitudes. Analog often refers to transmission methods developed to transmit voice signals rather than high speed digital signals. Compare with *digital.*

ANSI

See *American National Standards Institute.*

area id

See *area number.*

ASCII

See *American Standard Code for Information Interchange.*

ASCII text file

A file that contains only text characters from the ASCII character set. An ASCII file can include letters, numbers, and punctuation symbols, but does not contain any hidden text-formatting codes.

asynchronous communications server

A LAN server that enables a network user to dial out of the network into the public-switched telephone system, or to accessed leased lines for asynchronous communications. This device also is called a dial-in/dial-out server or modem server.

Asynchronous Transfer Mode

A method used for transmitting voice, video, and data over high-speed LAN and WAN networks. See also *cell relay.*

AT command set

A set of standard instructions used to activate features on a modem. Originally developed by Hayes Microcomputer Products, most modem manufacturers now use the AT command set.

ATM

See *Asynchronous Transfer Mode.*

ATM Service Interworking Feeder

A service that enables Frame Relay network traffic to be fed into an ATM network, enabling a Frame Relay end user to communicate with an ATM end user.

ATM/DXI trunk

See *OPTimum PVC Trunk.*

ATM/DXI trunk interface

An ATM circuit used as a trunk between two Frame Relay networks that are built with Cascade switches.

attenuation

The decrease in power of a signal over distance, measured in decibels (dB).

auto-ranging

The ability for a power supply to detect the correct voltage that is being received from the power source.

B8ZS

See *Bipolar with 8 Zero Substitution.*

backbone

The part of a network that carries the bulk of the network traffic, e.g. over Ethernet cabling, fiber-optic cabling.

background diagnostics

Programs that run continuously in the background of the NMS to provide current operating status for all active switches. These programs do not interfere with switch operations.

balun

A small device used to connect a balanced line (such as a twisted-pair cable) to an unbalanced line (such as a coaxial cable).

bandwidth

The transmission capacity of a computer or a communications channel.

bandwidth-on-demand

A WAN feature that enables a user to dial up additional bandwidth as their application demands.

baud rate

The number of bits per second (bps) on a serial link.

best-effort packets

Packets delivered to the best of the network's ability, after the requirements for delivering the guaranteed packets are met. See also *guaranteed packets*.

Bipolar with 8 Zero Substitution

A T1 encoding scheme where eight consecutive zeros are replaced with the sequence 000-+0+-if the preceding pulse was+, and with the sequence 000-+0+-if the preceding value was-, where+ represents a positive pulse, -represents a negative pulse, and 0 represents no pulse.

bit

A binary unit of measurement, which may be either a one or a zero.

bits per second

The number of bits transmitted every second during a data transfer.

blue alarm

An alarm signal, both on the NMS and switch, indicating that all one pulses are being received.

BNC connector

A small connector with a half-turn locking shell for coaxial cable. Normally used with thin Ethernet cabling.

Boot Programmable Read-Only Memory

A chip mounted on a printed circuit board used to provide executable boot instructions to a computer device.

Boot PROM

See *Boot Programmable Read-Only Memory.*

bps

See *bits per second.*

broadband network

A type of network that allows for the transmitting of large amounts of information, including voice, data, and video over long distances using the same cable.

broadcast

A message that is sent to all users currently logged into the network.

burst mode

A method of data transmission in which information is collected and then sent in a single high-speed transmission, rather than one character at a time.

byte

A series of consecutive binary digits that are operated upon as a unit (for example, an eight-bit byte).

Carrier Sense Multiple Access Collision Detect

Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all transmitting devices. This collision subsequently delays retransmissions from those devices for some random length of time. CMSA/CD access is used by Ethernet and IEEE 802.3.

CascadeView/DOS

The Windows-based graphical user interface used to configure and monitor a Cascade network.

CascadeView/UX

The UNIX-based graphical user interface used to configure and monitor a Cascade network.

CBR

See *Constant Bit Rate.*

cell

Any fixed-length packet, for example, ATM uses fixed length 53-byte cells. See also *cell relay.*

Cell Loss Priority

A field in the ATM cell header that indicates the eligibility of the cell for discard by the network under congested conditions.

cell relay

A form of packet transmission that uses a fixed-length, 53-byte cell over a packet-switched network; also known as Asynchronous Transfer Mode (ATM).

cell switching

An operational feature of cellular networks that enable callers to move from one location to another without losing the call connection. The cellular system is designed to switch calls to a new cell with no noticeable drop in the conversation. Cell switching is sometimes called “handing off.” While not noticeable in voice communications, the approximate 300 milliseconds this switching takes can prove to be a problem in data transmission.

channel

Any connecting path that carries information from a sending device to a receiving device. May refer to a physical medium (e.g., coaxial cable) or a specific frequency within a larger channel.

channel bank

Equipment that converts multiple voice signals to time division multiplexed (TDM) signals for transmission over a T1 or E1 line.

Channel Service Unit

A device that functions as a certified safe electrical circuit, acting as a buffer between the customer's equipment and a public carrier's WAN.

circuit

A communications channel or path between two devices.

circuit switching

A temporary communications connection that is established as needed between a sending node and a receiving node.

Clear To Send

A hardware signal defined by the RS-232-C standard, indicating that the transmission can proceed.

client

A device that makes use of the services provided by a server.

CLP

See *Cell Loss Priority.*

coldboot

A reboot enabling the user to restart the switch as if it were powered off, then on. Compare with *warmboot.*

collision detection

See *Carrier Sense Multiple Access Collision Detect.*

Committed Burst Size

The maximum amount of data, in bits, that the network agrees to transfer under normal conditions, during a time interval Tc. Committed Burst Size is defined for each PVC.

communications protocol

A standard way of communicating between computers, or computers and terminals; also a hardware interface standard, such as RS-232C for communication between DTE and DCE devices.

community names

The name given to an SNMP community for purposes of identification. A member has associated access rights: read-only or read/write. The Cascade switch has the following default community names: public (read-only) and cascade (read/write).

concentrator

A repeater or hub that joins communications channels from several different network nodes. Concentrator devices provide bridging, routing, and other management functions.

congestion

The point at which devices in the network are operating at their highest utilization. Congestion is handled by employing a congestion avoidance mechanism. See *mild, severe,* and *absolute congestion*.

connectivity

The degree to which any given computer or application can cooperate with other network components in a shared-resource network environment.

console commands

SNMP protocol supports three important commands: Get, Set, and Next. Get enables an NMS to query one or more objects or variables in an agent MIB. Set enables an NMS to modify a value of a MIB object or variable and may be used to boot or reboot devices. Next enables an NMS to query agent MIB tables and lists.

Constant Bit Rate

A Quality of Service class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery of bits.

Control Processor

A module that makes up the hardware architecture of a B-STDX 9000 switch. A CP provides network and system management and routing functions in support of the real- time switching functions provided by the multiple, IO Processor modules (IOPs). There are two types of Control Processors: CP Basic and CP Plus. CP Basic contains more flash memory, and CP Plus is distinguished by its red DIP switches. CP Plus has increased memory for use with high speed IOPs.

CP

See *Control Processor.*

CRC

See *Cyclic Redundancy Check.*

CRC error

A condition that occurs when the CRC in a frame does not agree with the CRC frame received from the network.

CSMA/CD

See *Carrier Sense Multiple Access Collision Detect.*

CSU

See *Channel Service Unit.*

CTS

See *Clear To Send.*

Cyclic Redundancy Check

A calculation method used to check the accuracy of digital transmission over a communications link.

D4-format

In T1 transmission, 24 channels per T1 line, where channels are assigned sequentially.

daemon

A special type of program that, once activated, starts itself and carries out a specific task without user intervention. Daemons typically handle tasks that run repeatedly, such as printing, mail, and communications.

data bits

In asynchronous transmission, the bits that actually contain the data being sent. Also called “payload” in some transmission methods.

Data Bus (DB) connector

A cable connector used to connect devices to parallel or serial ports. The number following DB indicates the number of pins in the connector (e.g., DB-25 connectors have 25 pins).

Data Carrier Detect

A hardware signal defined by the RS-232-C standard, which indicates that the device is on-line and ready for transmission.

Data Communications Equipment

Any device that connects a computer or terminal to a communications channel or public network.

Data Exchange Interface

A specification, described in RFC 1483, that defines how a network device can be used to convert data for interworking between different network services (i.e. Frame Relay to ATM).

data-link layer

The second of seven layers of the ISO/OSI model for computer-to-computer communications. This layer ensures data flow and timing from one node to another by synchronizing blocks of data and controlling the flow of data.

data packet

One unit of information transmitted as a discrete entity from one network node to another. In packet-switched networks, a data packet is a transmission unit of a fixed maximum length that contains a header, a set of data, and error control information.

Data Service Unit

A device that connects DTE to digital communications lines. A DSU formats the data for transmission on the public carrier WAN, and ensures that the carrier's requirements for data formats are met.

Data Set Ready

A hardware signal defined by the RS-232-C standard, which indicates that the device is ready to operate.

Data Terminal Equipment

Any device, such as a terminal or computer, that is connected to a communications device, channel, or public network.

Data Terminal Ready

A hardware signal, defined by the RS-232 standard, exchanged between devices. For example, an RS-232-C circuit that alerts a DCE device that the DTE device is ready to send and receive data.

data transfer rate

The speed at which data is transferred, usually measured in megabits per second (Mbps) or megabytes (MB) per second.

datagram

A message unit that contains source- and destination-address information, as well as the data itself, which is routed through a packet-switched network.

DCD

See *Data Carrier Detect.*

DCE

See *Data Communications Equipment.*

D-Channel

The data channel in ISDN used for control signals and customer data. In Primary Rate ISDN (PRI), the D-Channel operates at 64 Kbps.

DE

See *Discard Eligible.*

dedicated line

A communications circuit used for one specific purpose, and not used by or shared between other users.

dedicated server

A computer on the network that functions only as a server performing specific network tasks.

define path

A function that allows a manual path to be defined for the PVC, thereby bypassing the OSPF (Open Shortest Path First) algorithm to make PVC routing decisions.

delay

In communications, a pause in activity, representing the time that a message must wait for transmission-related resources to become available.

destination address

The address portion of a packet or datagram that identifies the destination node.

digital

A method of storing, processing, and transmitting information through use of distinct electronic or optical pulses that represent the binary digits (bits) 0 and 1. Digital transmission/switching technologies employ a sequence of discrete, individually distinct pulses to represent information, as opposed to the continuously variable signal of analog technologies. Compare with *analog*.

Digital Signal (Digital Service)

A classification of digital circuits. The DS defines the level of common carrier digital transmission service. DS-0 = 64 Kbps (Fractional T1), DS-1 = 1.544 Mbps (T1), DS-2 = 6.312 Mbps (T2), DS-3 = 44.736 Mbps (T3), and DS-4 =274-176 Mbps (T4).

DIP switch

See *Dual In-line Position switch.*

direct Ethernet

A connection method used by the NMS to the network. The NMS communicates directly to the gateway switch through the Ethernet port on the NMS to the Ethernet port on the switch.

Discard Eligible

A bit in the Frame Relay header used to indicate that a frame is eligible for discard by a congested node.

disk partitions

A portion of a disk that is configured during software installations on a system or workstation.

domain

A network community of users sharing the same database information.

DS

See *Digital Signal.*

DS0

A 64-Kbps channel used in T1 transmission. There are 24 DS0 channels in a T1 line.

DS1

A standard digital transmission facility, operating at 1.544 Mbps.

DSR

See *Data Set Ready.*

DSU

See *Data Service Unit.*

DSX-1

A T1 specification that indicates the physical and electrical characteristics of the standard T1 cross-connection.

DTE

See *Data Terminal Equipment.*

DTR

See *Data Terminal Ready.*

Dual In-line Position switch

A small switch used to select the operating mode of a device.

duplex channel

The ability to transmit and receive on the same channel at the same time. Also known as full duplex.

DXI

See *Data Exchange Interface.*

dynamic routing

A routing technique that allows a message's route to change "en route" through the network.

E1

The European counterpart to the North American T1 transmission speed. Adopted by the Conference of European Posts and Telecommunications Administrations, the E1 standard carries data at the rate of 2.048 Mbps.

EDAC

See *Error Detection and Correction.*

encapsulation

The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before being transmitted. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

environment variable

A system- or user-defined variable that provides information to the UNIX shell about the operating environment.

error detection and correction

A feature used to determine whether transmission errors have occurred, and if so, to correct those errors. See also *Carrier Sense Multiple Access Collision Detect.*

error rate

In communications, the ratio between the number of bits received incorrectly and the total number of bits in the transmission.

ESF

See *Extended Superframe Format.*

Ethernet

A popular LAN protocol and cabling scheme with a transfer rate of 10 Mbps.

Ethernet address

A 48-bit number physical address. Each Ethernet address is unique to a specific network card or pc on a LAN which forms the basis of a network-addressing scheme. Compare with *IP address.*

Ethernet packet

A variable-length unit of data transmitted on an Ethernet LAN.

Excess Burst

The maximum allowed amount of uncommitted data (in bits) in excess of Bc that the network attempts to deliver during time interval Tc. In general, this data (Be) is delivered with a lower probability than Bc. See *Be.*

Extended Superframe Format

In Frame Relay, a frame structure that extends the DS1 superframe structure from 12 to 24 frames, for a total of 4632 bits. This format redefines the 8-Kbps channel consisting of framing bits previously used only for terminal and robbed-bit signaling synchronization.

external testing

A loopback test that tests the ability of the port to send and receive data. This test requires an external loopback connector installed on the physical port.

fail count

A statistic that displays the number of tests that produced an error condition.

failed LED

A red status indicator that indicates a fatal system fault (such as a system crash).

fault-tolerant PVCs

A set of backup ports (Permanent Virtual Circuits) on the switch used to restore connections from a failed data center to the backup data center. When enabled, a fault-tolerant PVC automatically reroutes all affected circuits to the set of backup ports.

FCS

See *Frame Check Sequence.*

FDDI

See *Fiber Distributed Data Interface.*

FDM

See *Frequency-Division Multiplexing.*

FECN

See *Forward Explicit Congestion Notification.*

Fiber Distributed Data Interface

An ANSI standard for fiber-optic links with a data transmission rate up to 100 Mbps.

File Transfer Protocol

A method of transferring information from one computer to another, either over a modem and telephone line, or over a network. FTP is a TCP/IP application utility.

foreground diagnostics

A set of tests used to check for non-fatal errors indicated by background diagnostics or statistics. Foreground tests may also run at start up to test new equipment functions.

Forward Explicit Congestion Notification bit

A bit in the Frame Relay header that indicates the frame has passed through a node that is experiencing congestion in the same direction in which the frame is traveling.

fractional T1

One channel of a T1 circuit. T1 circuits consist of 24, 64-Kbps channels. Customers can lease as many of these channels as needed; they are not required to lease all 24 channels in one circuit.

Frame Check Sequence

A field in a frame, which contains the standard 16-bit cyclic redundancy check used to detect errors in HDLC and LAPD frames. See also *Cyclic Redundancy Check.*

Frame Relay

A type of data transmission based on a packet-switching protocol, with transmission rates up to 2 Mbps. Frame Relay provides for bandwidth on demand. For more information about Cascade's Frame Relay services, refer to the *B-STDX Network Configuration Guide.*

Frequency-Division Multiplexing

A method of sharing a transmission channel by dividing the total bandwidth of the circuit into several smaller channels. This is accomplished by allocating specific frequency ranges to each channel. All signals are carried simultaneously. Compare with *Time Division Multiplexing.*

FTP

See *File Transfer Protocol.*

full-duplex (FDX)

See *duplex.*

full status reporting

In Frame Relay, a link-management message function that provides the user device with a complete status of all PVCs configured on that link.

gateway

A shared connection between a LAN and a larger system (such as a mainframe computer), or a large packet-switched network whose communication protocols differ.

Generic Flow Control

The field in the ATM cell that controls the flow of traffic across the user-network interface (UNI), and into the network. The mechanisms for using this field are still under development.

GFC

See *Generic Flow Control.*

good LED

A green status indicator on a Cascade Switch, used during the system boot process to indicate normal system status or operation.

graceful discard

When enabled, this function turns red frames into best-effort frames. When disabled, this function discards frames.

green frames

Cascade's own class of packet frames used to identify packets as they travel through the network. Green frames are never discarded by the network except under extreme circumstances, such as node or link failure.

group addressing

The ability to send a single datagram/packet to multiple locations.

guaranteed packets

Data delivered according to some time constraint and with high reliability.

Hayes-compatible modem

Any modem that recognizes commands in the industry-standard AT command set.

HDLC

See *High-level Data Link Control*

header

The initial part of a data block, packet, or frame, which provides basic information about the handling of the rest of the block, packet or frame.

Header Error Control

In ATM, a feature that provides protection against misdelivery of cells due to addressing errors.

HEC

See *Header Error Control.*

heartbeat polling process

An exchange of sequence numbers between the network and a user device to ensure that both are operational and communicating.

HELLO

A routing protocol used principally by NSFnet nodes (nodes in the National Science Foundation Network). Hello allows trusting packet switches to discover minimal delay routes.

Hello protocol

Protocol used by OSPF systems for establishing and maintaining neighbor relationships.

heterogeneous network

A network that consists of workstations, servers, network interface cards, operating systems, and applications from many different vendors, all operating together as a single unit. Compare with *homogeneous network.*

High-level Data Link Control

An international protocol defined by ISO. In HDLC, messages are transmitted in variable-length units known as frames.

High-Speed Serial Interface

A high-speed interface (up to 52 Mbps full duplex) between a DTE and a DCE. The DCE provides the timing for the interface. HSSI can drive a 50 ft. (15m) shielded twisted-pair cable.

homogeneous network

A network that consists of one type of workstation, server, network interface card, and operating system, with a limited number of applications, all purchased from a single vendor. All nodes use the same protocol and the same control procedures. Compare with *heterogeneous network.*

hop (count)

The number of links that must be “jumped” to get from a source node to a destination node.

host name

A unique name identifying a host system.

hot swappable

A feature that allows the user to add, replace, or remove interface processors in a Cascade switch without interrupting switch operations.

HP OpenView

The UNIX-based network management application used with CascadeView/UX on an NMS to manage a Cascade Network

HSSI

See *High-Speed Serial Interface.*

hub

A wiring device that contains multiple connections of network and internetworking modules. Active hubs amplify or repeat signals to extend a LAN (in terms of distance). Passive hubs do not repeat, but split the transmission signal, allowing the administrator to add users to a LAN.

ICMP

See *Internet Control Message Protocol.*

IEEE

See *Institute of Electrical and Electronic Engineers.*

IEEE standards

Various specifications defined by the Institute of Electrical and Electronic Engineers (such as Token Ring, Ethernet) to establish common networking standards among vendors.

ILMI

See *Interim Local Management Interface.*

Indirect Ethernet

A LAN topology or an extended LAN where the NMS and the switch reside on different LANs and must use a router for access.

Input/Output Adapter

A module that connects the various IOMs in a switch. IOA configurations vary according to the specific IOM they support.

Input/Output Module

A module in a switch that manages the lowest level of a node's trunk or user interfaces. An IOM performs physical data link and multiplexing operations on external trunks and user links.

Institute of Electrical and Electronic Engineers

Professional organization that defines network standards.

Interim Local Management Interface

A management information base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep alive protocol. ILMI provides status information and statistics about virtual paths, connections, and address registration. It also determines the operational status of the logical port.

Integrated Services Digital Network

A CCITT standard for a worldwide digital communications network, intended to replace all current systems with a completely digital transmission system.

internal clocking

A hardware function of the Cascade switch, which provides the transmit and receive clocks to the user equipment.

internal testing

A hardware diagnostic that performs an internal loopback test on the I/O card and other cards.

International Standards Organization

An international standards group based in Geneva, Switzerland, that establishes global standards for communications and information exchange.

International Telecommunication Union Telecommunication Standard Sector

An advisory committee established under the United Nations to recommend worldwide standards for voice and data. One of the four main organizations of the International Telecommunications Union.

Internet Control Message Protocol

The IP portion of the TCP that provides the functions used for network layer management and control.

Internet Protocol

The TCP/IP session-layer protocol that regulates packet forwarding. See also *ICMP.*

Internet Protocol address

A 32-bit address assigned to hosts using TCP/IP. The address is written as four octets separated with periods (dotted decimal format) that are made up of a network section, an optional subnet section, and a host section.

IOA

See *Input/Output Adapter.*

IOM

See *Input/Output Module.*

IP

See *Internet Protocol.*

IP address

See *Internet Protocol Address.*

ISDN

See *Integrated Services Digital Network.*

ISDN call setup

A procedure that establishes an ISDN backup trunk.

ISO

See *International Standards Organization.*

ITU-T

See *International Telecommunication Union Telecommunication Standardization Sector.*

jitter

A type of distortion found on analog communications lines, resulting in data transmission errors.

Kbps

Kilobits per second.

keep-alives

A series of polling messages used in the Link Management Interface (LMI) of a Frame Relay port to verify link integrity between devices.

LAN

See *Local Area Network.*

LAP

See *Link Access Protocol.*

LAP-B

A bit-oriented data-link protocol used to link terminals and computers to packet-switched networks.

LED

See *Light Emitting Diode.*

Light Emitting Diode

A semiconductor light source that emits light in the optical frequency band (visible light) or the infrared frequency band. A major light source for optical fiber transmission, LEDs are used with multimode optical fiber in applications that require a low-cost light source. See also *good LED, marginal LED,* and *failed LED.*

Link Access Protocol

The link-level protocol used for communications between DCE and DTE devices.

Link Management Interface

A set of enhancements to the basic Frame Relay specification. LMI dynamically notifies the user when a PVC is added or deleted. The LMI also monitors each connection to the network through a periodic heartbeat “keep alive” polling process.

Link Management Interface Rev 1

A synchronous polling scheme used for the link management of a Frame Relay channel where the user polls the network to obtain status information of the PVCs configured on the channel. LMI exchanges this information using DLCI 1023.

link-state routing protocol

A sophisticated method of determining the shortest paths through the network. See also *OSPF.*

LMI

See *Link Management Interface.*

LMI Rev 1

See *Link Management Interface Rev 1.*

load balancing

A technique that distributes network traffic along parallel paths to maximize the available bandwidth while providing redundancy at the same time.

Local Area Network

Any physical network technology that connects a number of devices and operates at high speeds (10 Mbps through several gigabits per second) over short distances. Compare with *Wide Area Networks.*

logical port

A configured circuit that defines protocol interaction.

loopback test

A diagnostic that directs signals back toward the transmitting source to test a communications path.

loss of frame

A T1 error condition when an out-of-frame condition exists for a normal period of 2 1/2 seconds.

loss of signal

A T1 error condition when j175+_75 consecutive zeros are received.

low level debugger

A state whereby the CP switch is powered on. If both positions on the CP switch are in the OFF position (pointing left), power up diagnostics are bypassed and the system debugger is enabled.

Management Information Base

The set of variables forming a database contained in a CMIP or SNMP-managed node on a network. Network management stations can fetch/store information from/to this database.

marginal LED

An amber status indicator on a switch module that indicates a non-fatal system fault (such as low memory).

Mbps

Megabits per second.

MIB

See *Management Information Base.*

mild congestion

In Frame Relay, the state of a link when the threshold (more than 16 buffers by default) is exceeded.

mount point

A directory in a file hierarchy at which a mounted file system is added to the machine making the mount.

multicast

A type of broadcast transmission that sends copies of the message to multiple stations, but not to all possible stations.

multiplexer (mux)

A device that merges several lower-speed transmission channels into one high-speed channel at one end of the link. Another mux reverses this process at the opposite end.

multiplexing

A technique that transmits several signals over a single communications channel.

name server

A server connected to a network that converts network names into network addresses.

name service

A distributed database service that allows a single set of system configuration files to be maintained for multiple systems on a network.

network address

A network layer address refers to a logical, rather than a physical network device; also called protocol address.

Network Interface Card

A card, usually installed in a pc, that enables you to communicate with other users on a LAN; also called adapter.

Network to Network Interface

The standard that defines the interface between ATM switches and between Frame Relay switches. In an SMDS network, an NNI is referred to as Inter-Switching System Interface (ISSI).

NIC

See *Network Interface Card*.

NNI

See *Network-to-Network Interface.*

node

Any device such as a pc, terminal, workstation, etc., connected to a network and capable of communicating with other devices.

node number

A unique number that identifies a device on the network.

noise

Extraneous signals on a transmission channel that degrade the quality or performance of the channel.

Open Shortest Path First

A routing protocol that takes into account network loading and bandwidth when routing information over the network. Incorporates least-cost routing, equal-cost routing, and load balancing.

Open Systems Interconnection

An international standard program created by ISO and ITU-T to develop standards for data networking, such as the OSI model, to facilitate multi-vendor operating environments.

OPTimum PVC trunk

A logical port configuration that optimizes interoperability in performance and throughput in networks where both ends are connected by Cascade switches.

OPTimum trunking

A software function that allows public data networks based on Frame Relay, SMDS, or ATM to be used as trunk connections between Cascade switches.

OSI

See *Open Systems Interconnection.*

OSPF

See *Open Shortest Path First.*

out of frame

A T1 error condition where two or three framing bits of any five consecutive frames are in error.

packet

Any block of data sent over a network. Each packet contains sender, receiver, and error-control information, in addition to the actual message, sometimes called payload or data bits.

Packet Assembler/Disassembler

A device connected to a packet-switched network that converts a serial data stream from a character-oriented device (e.g., a bridge or router) into packets suitable for transmission. It also disassembles packets into character format for transmission to a character device.

packet processor

The Cascade switch module that performs the frame format validation, routing, queuing and protocol conversion for the switch. This module is not hot swappable.

packet-switched network

A network that consists of a series of interconnected circuits that route individual packets of data over one of several routes and services.

packet switching

Type of networking in which nodes share bandwidth with each other by intermittently sending logical information units (packets). In contrast, a circuit-switching network dedicates one circuit at a time to data transmission.

PAD

See *Packet Assembler/Disassembler.*

Parameter Random Access Memory

The PRAM on a switch that contains the module's downloaded configuration file, and which is stored in battery backup.

pass count

A statistic that displays the number of background diagnostic tests that have passed without error.

passive hub

A wiring device used in some networks to split a transmission signal, allowing additional workstations to be added to the network. Compare with *active hub.*

path

The complete location of a directory or file in the file system. See *define path* and *alternate path.*

payload

The portion of a frame that contains the actual data.

PCR

See *Peak Cell Rate.*

Peak Cell Rate

In ATM transmission, the maximum transmission rate that cells are transmitted. Equivalent to Be for Frame Relay, PCR is measured in cells per second and converted internally to bits per second. PCR defines the shortest time period between two cells.

PDN

See *Public Data Network.*

Permanent Virtual Circuit

A logical connection across a packet-switched network that is always in place and always available along a predetermined network path. See also *Virtual Circuit.*

Point-to-Point Protocol

A protocol that provides router-to-router and host-to-network connections.

polling

An access control method in which one master device, such as the NMS, polls or queries other network devices, requesting them to transmit one at a time.

PPP

See *Point-to-Point Protocol.*

PRAM

See *Parameter Random Access Memory.*

PRI

See *Primary Rate Interface.*

primary group

The main group to which associated users belong. The system identifies the primary group by the group field in the user account (stored in the /etc/password file) and by the group ID associated with a new file.

Primary Rate Interface

An ISDN interface to primary rate access. Primary rate access consists of a single 64-Kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.

protocol

A set of rules governing communication between two entities or systems to provide interoperability between services and vendors. Protocols operate at different layers of the network, e.g., Data link, network, and session.

proxy service

A management service provided for one or more devices by another. For example, the Cascade SMDS Access Servers/Switches are proxy managed through the SMDS network.

Public Data Network

Any government-owned or controlled commercial packet-switched network, offering WAN services to data processing users.

PVC

See *Permanent Virtual Circuit.*

QOS

See *Quality Of Service.*

Quality Of Service

A statistical report that specifies certain characteristics of network services, sessions, connections, or links. For example, the CascadeView/UX Statistics report describes the lost packets and round-trip delay measurements.

Random Access Memory

The main system memory in a computer used for the operating system, applications, and data.

RAM

See *Random Access Memory.*

rate enforcement

A process used to measure the actual traffic flow across a given connection and compare it to the total admissible traffic flow for that connection. Traffic outside of the acceptable level can be tagged and discarded en route if congestion develops. ATM, Frame Relay, and other types of networks use rate enforcement.

reboot

To restart the computer and reload the operating system, usually after a crash.

Receive Data

A hardware signal (defined by the RS-232-C standard) which carries data from one device to another. See also *Transmit Data.*

red alarm

A T1 alarm condition indicating a loss of signal or loss of frame at the device's local termination point.

redundancy

The duplication of hardware or software within a network to ensure fault-tolerant or back-up operation.

remote connection

A workstation-to-network connection made using a modem and telephone line or other WAN services equipment. Remote connections enable you to send and receive data over greater distances than you can with conventional cabling methods.

repeater

A device that receives data on one communication link and transmits it, bit by bit, on another link as fast as it is received without buffering.

Request For Comment

A series of notes and documents available on-line that describe surveys, measurements, ideas, techniques, and observations, as well as proposed and accepted Internet protocol standards, such as Telnet and FTP.

Request To Send

A hardware signal defined by the RS-232-C standard, which a device sends to request permission to transmit.

RFC

See *Request For Comment.*

RFC1294

A specification documenting multi-protocol access over Frame Relay.

RIP

See *Routing Information Protocol.*

route recovery

In Frame Relay, an OSPF routing function in the Cascade switch. When a tandem node or trunk is down, new shortest-path routes for those affected PVCs are recalculated immediately at the ingress nodes, due to fast convergence of the link-state updates. The PVCs are then rerouted to the new route. Recovery time is typically under four seconds. The network reports PVC rerouting as an event/alarm.

router

An intelligent LAN-connection device that routes packets to the correct LAN segments' destination address(es). The extended LAN segments may or may not use the same protocols. Routers link LAN segments at the ISO/OSI network layer.

routing

The process of directing data from a source node to a destination node.

Routing Information Protocol

A routing protocol that maintains a list of accessible networks and calculates the lowest hop count from a particular location to a specific network.

routing protocol

A protocol that implements routing using a specific routing algorithm. Routing protocols include IGRP, OSPF, and RIP.

RTS

See *Receive To Send.*

RXD

See *Receive Data.*

SCR

See *Sustainable Cell Rate.*

SEAL

See *Simple and Efficient Adaption Layer.*

Serial Line over Internet Protocol

A protocol that enables point-to-point serial communication over IP using serial lines or telephone connections and modems.

serial management port

A management port on the Packet Processor card on a Cascade switch.

shielded cable

Cable protected against electromagnetic and radio frequency interference.

shortest path routing

A routing algorithm that calculates the path distances to all network destinations. The shortest path is then determined by a cost assigned to each link. See also *OSPF.*

Simple and Efficient Adaption Layer

In ATM, an extension of the Type 3 AAL. It simplifies the SAR portion of the Adaption layer to pack all 48 bytes of the cell information field with data. This AAL makes ATM look like high-speed Frame Relay. It also assumes that only one message is crossing the UNI at a time. That is, multiple end users at one location cannot interleave messages on the same virtual circuit, but must queue them for sequential transmission.

Simple Network Management Protocol

A standard network management protocol used to manage and monitor nodes and devices on a network.

SLIP

See *Serial Line over Internet Protocol.*

smart hub

A concentrator with certain network management features built into the firmware. This capability enables the user to manage LAN configurations.

SMDS

See *Switched Multimegabit Data Services.*

SNMP

See *Simple Network Management Protocol.*

static route

A route or path that is manually entered into the routing table. Static routes take precedence over routes or paths specified by dynamic routing protocols.

subnet address

An extension of the Internet addressing scheme that allows a site to use a single Internet address for multiple physical networks.

subnet mask

A 32-bit address mask used in IP to specify a particular subnet. See also *address mask.*

superuser (root)

In UNIX, a user (also known as root) with special privileges. Only the superuser, for example, can change the password file and edit major system administration files in the /etc directory.

Sustainable Cell Rate

The average cell transmission rate in ATM transmission. Equivalent to CIR for Frame Relay, SCR is measured in cells per second and converted internally to bits per second Usually, SCR is a fraction of the peak cell rate. Cells are sent at this rate if there is no credit.

SVC

See *Switched Virtual Circuit.*

Switched Multimegabit Data Service

A high-speed WAN service based on the 802.6 standard for use over T1 or T3 circuits.

Switched Virtual Circuit

A logical connection across a packet-switched network providing as-needed connections to any other node in the network. See also *Virtual Circuit.*

synchronization

The timing of separate elements or events to occur simultaneously. In communications, hardware and software must be synchronized so that file transfers can occur.

synchronous transmission

A data transmission method that uses a clock signal to regulate data flow.

T1

A long-distance, point-to-point circuit that provides 24 channels at 64 Kbps each (for a total of 1.544 Mbps). See also *E1*.

T3

A long-distance, point-to-point circuit that provides up to 28 T1 channels. T3 can carry 672 channels of 64 Kbps (for a total of 44.736 Mbps).

Tc

See *Committed Rate Measurement Interval.*

TCP

See *Transmission Control Protocol.*

TDM

See *Time Division Multiplexing.*

telnet

The Internet standard protocol for remote terminal-connection services.

throughput

The actual speed of the network.

Time Division Multiplexing

Technique that allocates bandwidth for multiple channels onto one channel based on pre-assigned time slots.

time interval "T"

The time interval over which the number of bits used to average the number of bits transmitted, is averaged. To calculate **T,** use the following formula: Bc/CIR=T.

topology

The map or configuration design of a network. Physical topology refers to the location of hardware. Logical topology refers to the paths that messages take to get from one node to another.

traffic shaping

In Frame Relay, a set of rules that describes traffic flow. The sender has a mechanism to ensure that the transmission of its guaranteed packets behaves in a certain way. The network knows what kind of traffic to expect, and can monitor the behavior of the traffic.

transceiver

A device that connects a host interface to a LAN. A transceiver transmits and receives data.

Transmission Control Protocol

The Internet standard, transport-level protocol that provides the reliable, full duplex, stream service on which many application protocols depend.

Transmit Data

A hardware signal (defined by the RS-232-C standard) used by the DTE to transmit data to the DCE. See also *Receive Data.*

trap

An unsolicited message generated by an SNMP agent on a network device (e.g. switch) due to a pre-defined event occurring or alarm threshold being exceeded, which triggers an alarm at the NMS.

trunk

The communications circuit between two switches.

trunk backup

A configuration setting specified by a network operator via the NMS. The network operator can initiate or terminate primary trunk backups at any time via the NMS. Trunk backups take over a connection should the primary trunk fail.

trunk failure

A condition (alarm) that occurs when the Cascade switch status indicates that a trunk is no longer available.

trunk restoration

A process that reroutes the PVCs carried on the backup trunk, and frees up the circuit the backup trunk.

TXD

See *Transmit Data.*

twisted-pair cable

Cable that consists of two or more pairs of insulated wires twisted together. One wire carries the signal, and the other is grounded.

UIO module

See *Universal Input Output module.*

UDP

See *User Datagram Protocol.*

unshielded cable

Any cable not protected from electromagnetic or radio frequency interference.

UNI

See *User-to-Network Interface.*

UNI DCE

See *User Network Interface Data Communications Equipment.*

UNI DTE

See *User Network Interface Data Terminal Equipment.*

Universal Input Output Module.

A module for the Cascade switch. It has three 80-pin connectors and is used for redundancy. It is also used as an I/O module for the following interfaces: X.21, RS449, V.35, EIA530, and EIA530A.

User Datagram Protocol

An unreliable transport-layer protocol from the TCP/IP protocol suite. It simply acts as an interface to various applications through the use of different ports.

User-to-Network Interface

A standard defined by the ATM Forum for public and private ATM network access. UNI connects an ATM end system (such as a router) and an ATM switch, and is also used in Frame Relay. UNI is called SNI (Subscriber Network Interface) in SMDS.

V.35

A standard module used for communication between a network access device and a packet network. It provides clocking from 19.2 Kbps to 4.0966 Mbps.

VC

See *Virtual Channel.*

VCI

See *Virtual Circuit Identifier.*

virtual bandwidth

Channel capacity calculated to allow for oversubscription of channel usage.

Virtual Channel

A connection between two communicating ATM networks.

Virtual Circuit

A logical circuit set up to ensure reliable communication between two network devices. See also *PVCs* and *SVCs.*

Virtual Circuit Identifier

A 16-bit field in the header of an ATM cell. VCI is an addressing identifier used to route cell traffic.

Virtual Path

A group of VCs carried between two points. VP provides a way to bundle traffic headed in the same direction.

Virtual Path Identifier

A 8-bit field in the header of an ATM cell. VPI is an addressing identifier used to route cell traffic.

VPI

See *Virtual Path Identifier.*

VP

See *Virtual Path.*

WAN

See *Wide Area Network.*

warmboot

A reboot performed after the operating system has been running for a period of time. Compare with *coldboot.*

Wide Area Network

A network that usually consists of packet-switching nodes over a large geographical area.

yellow alarm

A T1 alarm that is generated when the interface receives a red-alarm signal from the remote end.

Index

C

D

E

O

Q

T

U

V

W

X