Network Configuration Guide for B-STDX/STDX

Ascend Communications, Inc.

Product Code: 80017
Revision 01
March 1997

ASCEND COMMUNICATIONS, INC. END-USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

Contents

3 Getting Started

4 Managing Network Maps

11 Configuring Circuits

12 Downloading the Configuration

A Upgrading to a B-STDX Switch

B Configuring Poll Server

C Adjusting the CAC

List of Figures

List of Tables

About This Guide

The *Network Configuration Guide for B-STDX/STDX* 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 describes all the features supported in CascadeView/UX Release 2.3 and Cascade switch software, Release 4.2.

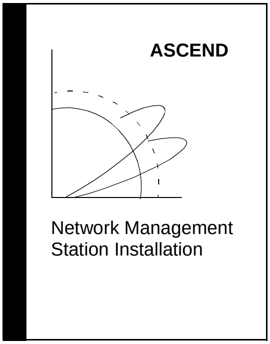
What You Need to Know

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. Refer to the appropriate hardware installation guide for information:

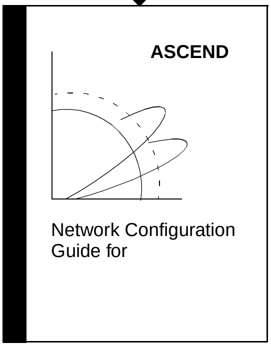
- *STDX 6000 Hardware Installation Guide*
- *B-STDX 8000/9000 Hardware Installation Guide*

Documentation Reading Path

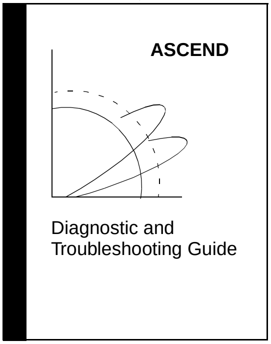
The following manuals provide the complete document set for the NMS Release 2.3:



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



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



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

Customer Comments

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

How to Use This Guide

Before you read this guide, read the Software Release Notice (SRN) that accompanies the software. This section highlights the chapters and contents 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 start up and shut down • CascadeView/UX security passwords • Audit Trail utility • Database backups
Chapter 3	Creating a sample Frame Relay direct-line 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 • Delete network maps
Chapter 5	Adding a switch object to the map. For example, • Configure a gateway switch for routing SNMP information to and from the NMS • Define additional NMS workstations • Delete a switch configuration

Read	To Learn About
Chapter 6	Configuring I/O modules and the various types of physical ports in the switch.
Chapter 7	Configuring Frame Relay logical-port services.
Chapter 8	Configuring the SMDS network by defining the logical-port services and SMDS addresses.
Chapter 9	Configuring ATM Interworking logical-port services.
Chapter 10	Configuring trunk parameters and adding trunk-line connections to your network map.
Chapter 11	Configuring circuits for Frame Relay, Frame Relay to ATM Service Interworking, and ATM logical ports. This chapter also explains how to configure point-to-multipoint circuits (multicast DLCI) and Management DLCI.
Chapter 12	Generating a configuration file and downloading this configuration to the switch. Also how to: • Synchronize the switch Parameter Random Access Memory (PRAM) • Compare the configuration files in PRAM and in the NMS database • Clear or erase PRAM
Appendix A	The SQR program updswch20.sqr, which is used to upgrade an STDX 3000/6000 switch configuration to a B-STDX 8000/9000 configuration.
Appendix B	The CascadeView Polling Server feature, which reduces CascadeView's status polling overhead when there are multiple users of CascadeView monitoring the network simultaneously.
Appendix C	Adjusting the Connection Admission Control (CAC).
Appendix D	The conversion procedure used to convert a DSX card to a channelized DS3 card.

Read	To Learn About
Appendix E	The CascadeView/UX defaults configuration file.
Appendix F	Glossary of terms, which defines many of the technical terms 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. Some of this information was previously available only in Technical Tips or Software Release Notices.

Table 1. NMS Release 2.3 Features

New Features	Enables You to...	Described in...
Single OSPF Domain	Configure and manage B-STDX switches and CBX-500 switches using one NMS.	Multiple sections
HP OpenView SNMP Management Platform, Version 4.11	Configure and manage switches using HP OpenView Version 4.11 menu options. The menu options are different than HP OpenView Version 3.3.1.	Multiple sections
Class B IP Addressing	Increase networks to include up to 400 switches and 1000 trunks.	Chapter 4
Console Authentication	Authenticate a user's login authority by verifying the user's password.	Chapter 5
CP 30, 40, and 50 I/O Modules	Configure the CP 30, 40, and 50 (which use a 170 MB internal disk) and each supports a different amount of memory.	Chapter 5
RIP Support	Run the IP Routing Information Protocol (RIP) over the B-STDX Ethernet port on the gateway switch. This enables you to use redundant gateway switches. This allows the switch software to send and receive RIP packets.	Chapter 5
Channelized DS3 I/O Module	Configure up to 28 T1s on a single physical port and configure channels. Each DS1 channel contains 24 DS0 channels.	Chapter 6

Table 1. NMS Release 2.3 Features (Continued)

New Features	Enables You to...	Described in...
AMT CS (Cell Switching) I/O Module	Perform cell switching with FR-ATM Interworking.	Chapter 6
ATM IWU (Interworking Unit) I/O Module	Perform 55 Mbps cell switching with FR-ATM Interworking.	Chapter 6
Trunk Backup	Configure a module to signal an external ISDN terminal adapter (T/A) when a circuit needs to be established. You can designate a backup trunk for any trunk in the network. If a primary trunk fails, all PVCs associated with that trunk are rerouted to the backup trunk. You can reroute the trunks automatically or manually.	Chapter 10
Set Logical Port Attributes	Set the logical port attributes, such as congestion control, trap control, and LMI for each I/O module's logical port.	Chapter 7 Chapter 8 Chapter 9
Configurable Congestion Threshold	Configure discard thresholds that determine under what network conditions packets are discarded. You configure the mild, severe, and absolute congestion thresholds and set the Be reduction percentage.	Chapter 7 Chapter 8 Chapter 9
Closed-loop Congestion Management	Prevent excess data from entering the network during congestion.	Chapter 7 Chapter 8 Chapter 9
SMDS Alien Address	Increase network scaleability by increasing the alien address capacity from 1024 to 2048 per switch.	Chapter 8

Table 1. NMS Release 2.3 Features (Continued)

New Features	Enables You to...	Described in...
SMDS Selective Group Address	Broadcast group address frames to specific addresses rather than a general broadcast.	Chapter 8
Country Code Prefix	Extend SMDS networks across international borders.	Chapter 8
SMDS Address Mask	Migrate from another vendor's SMDS network to a Cascade SMDS network.	Chapter 8
Direct-Cell Trunk	Configure a direct trunk on the ATM UNI, ATM CS, and ATM IWU module.	Chapter 9
Keep Alive Threshold / Link Trunk Protocol	Set the number of retries the trunk protocol attempts, before bringing the trunk down. The retry interval is set in seconds.	Chapter 10
Keep Alive Timer	Configure a Keep Alive (KA) timer on the trunk.	Chapter 10
Application Specific Routes / Customer Specific Routes (Virtual Private Networks)	Dedicate trunks to specific end-users and, if desired, allow customers to monitor their own networks. However, switch control and configuration stays with the network provider. Virtual Private Networks (VPNs) enable network providers to have dedicated network resources for those customers who require guaranteed performance, reliability, and privacy.	Chapter 10
Frame Relay Asymmetric CIR	Set up different QoS parameters for different directions, providing better control of traffic parameters.	Chapter 11
CLP Bit	Set the cell-loss priority on FR-ATM Service Interworking circuits.	Chapter 11

Table 1. NMS Release 2.3 Features (Continued)

New Features	Enables You to...	Described in...
Traffic Shaping	Improve performance and bandwidth utilization.	Chapter 11
Single-step Action PVC Establishment	Configure a circuit in one step between multiple nodes.	Chapter 11
Zero CIR	Assign a PVC a CIR value of zero to indicate a best effort delivery service. Customers who subscribe to zero CIR service are allowed to burst to the port speed if there is network bandwidth available to deliver frames.	Chapter 11
Priority Routing	Configure the routing priority on PVCs. A PVC with higher configured priority select the most optimal path that satisfies its Qos. You configure the bandwidth priority and bumping priority.	Chapter 11
Install Program	Establish a connection from a switch (with no PRAM) to an NMS.	Chapter 12
Poll Server	Reduce CascadeView's status polling overhead when there are multiple users of CascadeView monitoring the network simultaneously. The poll server acts like a daemon running in the background waiting for requests from an NMS session.	Appendix B
CAC	Enables you to control circuit creation on your ATM physical ports based on the specified cell-loss ratio. Appendix C describes how to tune the Cascade Call Master Connection Admission Control (CAC) to achieve a desired cell-loss ratio across all physical ports in your network.	Appendix C

Table 1. NMS Release 2.3 Features (Continued)

New Features	Enables You to...	Described in...
DSX to Channelized DS3 Conversion Procedure	Convert a DSX card to a channelized DS3 card.	Appendix D

Coventions

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

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

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

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

Related Documentation

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

Cascade

- *Networking Services Technology Overview* (80001)
- *B-STDX 8000/9000 Hardware Installation Guide* (80005)
- *STDX 6000 Hardware Installation Guide* (80006)
- *CBX 500 Hardware Installation Guide* (80011)
- *CBX Network Administrator's Guide* (80012)
- *Network Management Station Installation Guide* (80014)
- *Cascade Enterprise MIB Definitions* (80015)
- *Diagnostic and Troubleshooting Guide for B-STDX/STDX* (80018)
- *Bulk Statistics Collector for B-STDX/STDX* (80032)
- *Configuring ISDN Services for B-STDX/STDX* (80039)
- *SYBASE 11 SQL Server Upgrade Guide* (80040)
- *Upgrading to Solaris 2.5.1 and HP OpenView 4.11* (80045)

Third Party

- *Solaris 2.5 System Configuration and Installation Guide*
- *HP OpenView Windows User's Guide (for HP 9000 Series and Sun SPARCstation)*
- *SYBASE Commands Reference Manual*
- *SYBASE System Administration Guide*

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 battery-backed 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 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's Cascade Objects selection enables you to obtain status information for a switch, port, trunk, circuit, Multicast DLCI, and Management DLCI. 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 B-STDX/STDX*.

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 (refer to "Trunk Coloring" on page 10-25). For more information, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

2

Managing the NMS

This chapter describes how to start the NMS and run CascadeView/UX. This procedure includes starting the Sybase server and initiating an HP OpenView session. This chapter also describes how to shut down the NMS.

This chapter describes the following administrative tasks:

- Defining passwords and assigning access levels
- Using the Audit Trail feature to keep track of changes you make
- Backing up the Sybase and HP OpenView databases

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 sections. 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, login 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. Otherwise, follow Step 4 through Step 10 to start the Sybase server and access OpenView.
4. Log in as the sybase user by typing:

   su - sybase <Return>
5. At the prompt, type [*your Sybase password*].
6. Enter the following command 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, type the root password.
10. Access the HP OpenView Services directory by entering:

    /usr/OV/bin/ovstart <Return>
11. To start HP OpenView, enter **/usr/OV/bin/ovw &** in the console window.

The default HP OpenView window appears as shown in Figure 2-1.

> *As part of the installation procedure, you should have created a static route for the switch(es) CascadeView/UX will manage. If you did not define a static route, enter the following command to temporarily set a route:*
>
> **route add net *[sw. net. #] [gw. addr]* 1**
>
> *For example, if you have an internal network ID of 152.12.13.0, and a switch Ethernet port of 159.9.200.6, then enter:*
>
> ***route add net 152.12.13.0 152.9.200.6 1***
>
> *This temporary route exists only as long as the NMS is up. When you power off the NMS, the route is erased. For more information about creating a static route, refer to the* Network Management Station Installation Guide*.*

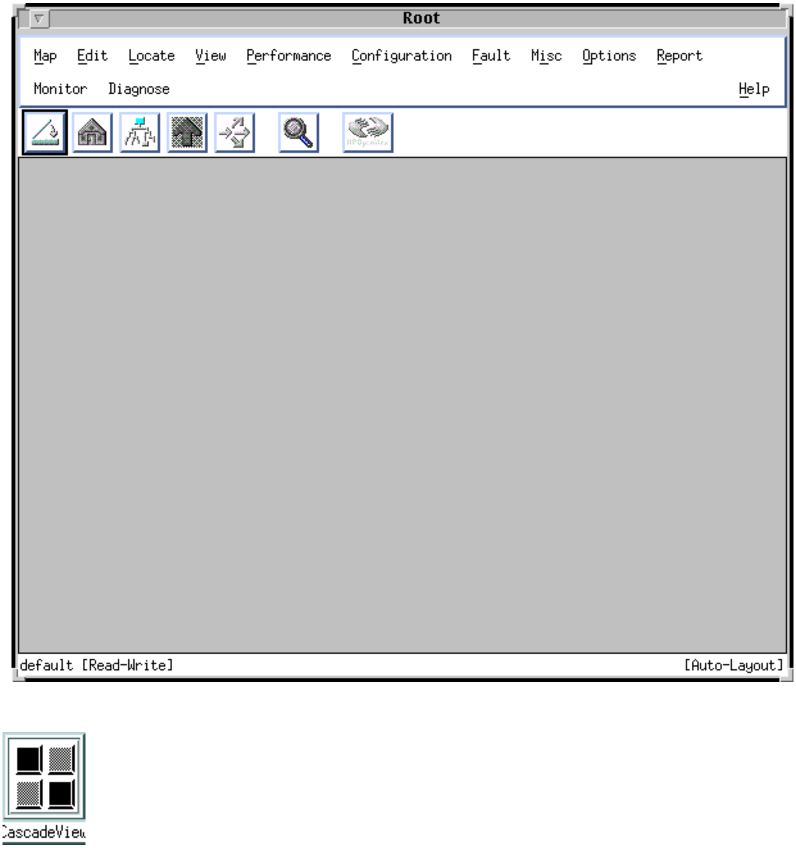


Figure 2-1. HP OpenView Window (Default) and CascadeView/UX Icon

The CascadeView icon shown in Figure 2-1 should appear on the window manager desktop. This indicates that Cascadeview/UX is running. Do not invoke any CascadeView commands until this icon appears. Do not close this icon unless one of the supporting programs (such as HP OpenView) stops processing.

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, choose File ⇒ Exit to exit CascadeView/UX.
2. To log in as the root user, enter **su - root**.
3. At the prompt, enter the root password.
4. Enter the following line to shut down HP OpenView services:

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

5. To log in as the Sybase user, enter **su - sybase**.
6. At the prompt, enter the Sybase password.
7. *If you are using Sybase 11*, type the following commands to shutdown 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, type:

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

9. To log in as the root user, enter **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.

Defining 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/UX as described in Table 2-1.

Table 2-1. CascadeView/UX Password Levels

Access Level...	Enables You to...
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. You must log on with this password to configure physical ports and download a switch configuration. The default is *cascade*.
Provisioning	Configure logical ports, trunks, and circuits and to monitor 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.

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

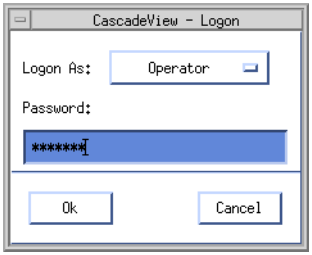


Figure 2-2. CascadeView Logon Dialog Box

Defining Access Levels

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 as shown in Figure 2-3.

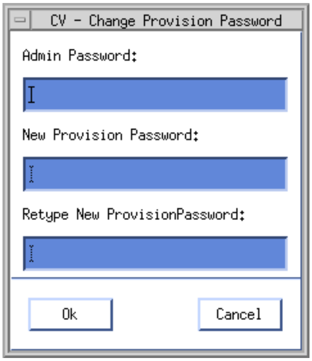


Figure 2-3. CV - Change Provision Password Dialog Box

2. Complete the required dialog box fields described in Table 2-2.

Table 2-2. CV-Change Provision Password Fields

Field	Action/Description
Admin Password	Enter the Admin Password.
New [*level*] Password	Enter a new [*level*] password.
Retype New [*level*] Password	Retype the new password.

3. Choose OK.

4. Repeat Step 1 through Step 3 to define additional passwords for each access level.

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 log in
- 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 time out

Enabling Audit Trail

To enable the audit trail, use the following steps:

1. In a command window, edit the cascadeview.cfg file by entering:

   vi /opt/CascadeView/etc/cascadeview.cfg <Return>

2. Set the *CV_AUDIT_TRAIL_ENABLED* environment variable in cascadeview.cfg by entering:

   CV_AUDIT_TRAIL_ENABLED=TRUE <Return>
   export CV_AUDIT_TRAIL_ENABLE <Return>

To disable Audit Trail, enter: CV_AUDIT_TRAIL_ENABLED=FALSE

3. Enter **:wq!** to exit the vi editor and save your changes.

4. You must now shut down and then restart CascadeView/UX. To do this:

   a. From the HP OpenView File menu, select File ⇒ Exit to exit CascadeView/UX.

   b. Enter **su - root** and press Return.

   c. At the prompt, enter the root password.

   d. Type the following commands to shut down HP OpenView services:

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

   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 file name 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**.**

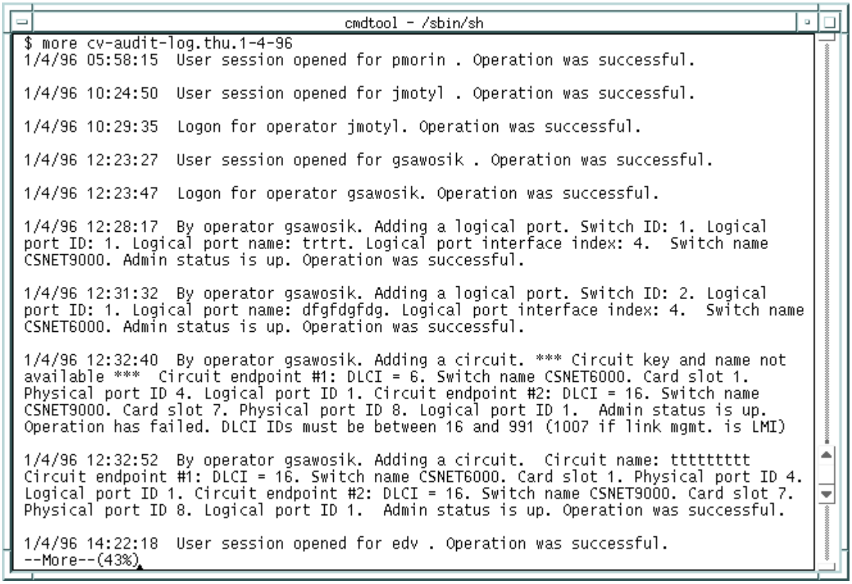
   The Audit Trail function creates a different file for each day of operation (a file for Monday, a file for Tuesday, etc.).

Use any editor to view this ASCII file. The following example uses the UNIX more command.

5. To view the ASCII log file, enter:

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

Figure 2-4 shows an example ASCII Log file.



```
cmdtool - /sbin/sh
$ more cv-audit-log.thu.1-4-96
1/4/96 05:58:15  User session opened for pmorin . Operation was successful.

1/4/96 10:24:50  User session opened for jmotyl . Operation was successful.

1/4/96 10:29:35  Logon for operator jmotyl. Operation was successful.

1/4/96 12:23:27  User session opened for gsawosik . Operation was successful.

1/4/96 12:23:47  Logon for operator gsawosik. Operation was successful.

1/4/96 12:28:17  By operator gsawosik. Adding a logical port. Switch ID: 1. Logical
port ID: 1. Logical port name: trtrt. Logical port interface index: 4.  Switch name
CSNET9000. Admin status is up. Operation was successful.

1/4/96 12:31:32  By operator gsawosik. Adding a logical port. Switch ID: 2. Logical
port ID: 1. Logical port name: dfgfdgfdg. Logical port interface index: 4.  Switch name
CSNET6000. Admin status is up. Operation was successful.

1/4/96 12:32:40  By operator gsawosik. Adding a circuit. *** Circuit key and name not
available ***  Circuit endpoint #1: DLCI = 6. Switch name CSNET6000. Card slot 1.
Physical port ID 4. Logical port ID 1. Circuit endpoint #2: DLCI = 16. Switch name
CSNET9000. Card slot 7. Physical port ID 8. Logical port ID 1.  Admin status is up.
Operation has failed. DLCI IDs must be between 16 and 991 (1007 if link mgmt. is LMI)

1/4/96 12:32:52  By operator gsawosik. Adding a circuit.  Circuit name: ttttttttt
Circuit endpoint #1: DLCI = 16. Switch name CSNET6000. Card slot 1. Physical port ID 4.
Logical port ID 1. Circuit endpoint #2: DLCI = 16. Switch name CSNET9000. Card slot 7.
Physical port ID 8. Logical port ID 1.  Admin status is up. Operation was successful.

1/4/96 14:22:18  User session opened for edv . Operation was successful.
--More--(43%)
```

Figure 2-4. ASCII Log File Example

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. Once the NMS can communicate with the gateway switch, you can configure the second switch (and subsequent switches) on the network.

Once you define the first two switches, this chapter describes the steps you need to follow to configure a Frame Relay direct-line trunk connection between the gateway switch and another switch. Use these procedures to verify your hardware and software installation. Although you may be using a service other than Frame Relay, this basic example highlights many of the steps required to configure any other service such as SMDS or ATM.

Basic Configuration Procedures

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's PRAM before you can download a new configuration. (Refer to "Erasing Parameter RAM" on page 12-27 for instructions.)

These instructions also assume a typical Frame Relay configuration in which the NMS uses a local Ethernet or SLIP 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), follow the instructions in Chapter 5 to configure the NMS connection.

For specific information about setting up SMDS or ATM networks:

- Start with the instructions in Chapter 4 to create a map.
- Proceed to Chapter 5 to configure switch parameters.
- Continue with Chapter 6 to configure the physical port parameters.
- Proceed to the appropriate service chapter to define the logical ports.
- Refer to *Configuring ISDN Services for B-STDX/STDX* for information on ISDN services.

Before You Begin

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

- ☑ Install the Cascade switch hardware and power it on as described in your hardware manual. (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 *B-STDX 8000/9000 Hardware Installation Guide*. Note whether the NMS is connected via direct Ethernet, indirect Ethernet (on a separate LAN segment), or through a SLIP connection.
- ☑ 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. (If you choose not to download the configuration file from the NMS, you can copy the configuration file to any workstation that can access the switch. You can then run any terminal emulation package to download the configuration to the switch's PRAM.)
- ☑ Install and configure the NMS software as described in the *Network Management Station Installation Guide*. (During the CascadeView/UX installation, make a 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.)

> *If RIP State and Send Host Routes are enabled (see Table 3-8 on page 3-25) you do not need to create a static route. However, you do need to define the NMS path on the gateway switch.*

Configuring the Gateway Switch and NMS

The following sections outline the procedures to get the gateway switch and NMS SPARCstation synchronized and communicating with each other.

Creating the Network Map

To create a new network map, use the following steps:

1. Access HP Openview and start CascadeView/UX as described in Chapter 2.
2. From the Map menu, select Maps⇒New. The New Map dialog box appears as shown in Figure 3-1.

> *Once set, you cannot modify these 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.*

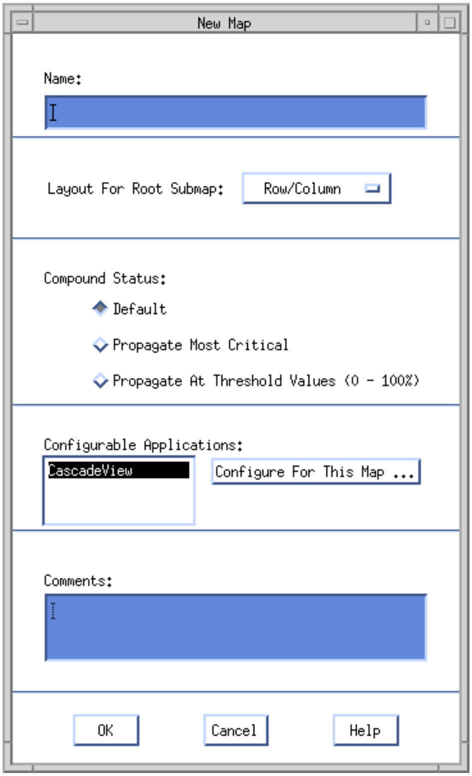


Figure 3-1. New Map Dialog Box

3. Complete the required dialog box fields described in Table 3-1.

Table 3-1. New Map Fields

Field	Action/Description
Name	Enter an alphanumeric name that identifies the map.
Layout For Root Submap	CascadeView/UX uses the default Row/Column. This option affects how the objects are arranged on the screen.
Compound Status	Compound status is how HP OpenView propagates the status 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*. Select the desired status propagation: *Default* – Causes HP OpenView to propagate status according to a predefined algorithm. *Propagate Most Critical* – Causes HP OpenView to propagate the status of the most critical symbol in the child submap, to the symbols of the parent object. *Propagate At Threshold Values (0 - 100%)* – Displays four fields that enable you to set threshold values that determine when HP OpenView propagates status. The number shown for each field is the default value. – %warning 30 – %minor 20 – %major 10 – %critical 5
Comments	Enter any additional information you want for this map.
Configurable Applications	In the Configurable Applications box, select CascadeView. Choose Configure For This Map. The Configuration dialog box appears (see Figure 3-2).

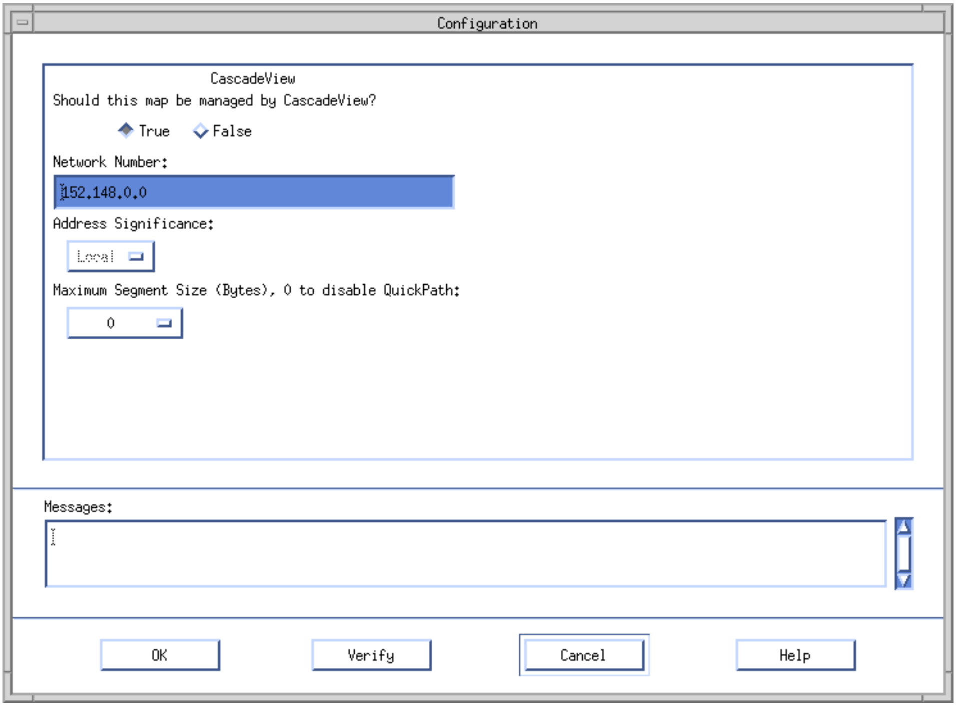


Figure 3-2. Configuration Dialog Box

4. Complete the required dialog box fields described in Table 3-2.

Table 3-2. Configuration Fields

Field	Action/Description
Should this map be managed by CascadeView?	Select True.

Table 3-2. Configuration Fields (Continued)

Field	Action/Description
Network Number	Displays the switch IP Network Number you specified when you added a static route during the CascadeView/UX install (refer to the *Network Management Station Installation Guide*). Check with the Cascade Technical Response Center if you must 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.

5. Choose Verify to confirm your settings. Choose OK. The New Map dialog box reappears.

6. Choose OK. The system displays the following message (see Figure 3-3).

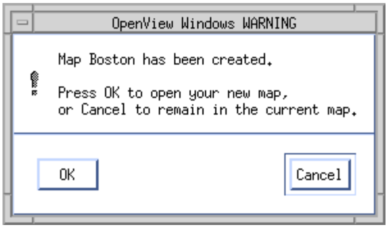


Figure 3-3. OpenView Windows WARNING Dialog Box

7. 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.

8. To log on to the network map, from the Misc menu, select CascadeView ⇒ Logon and enter the logon password (*cascade* is the default). (See Figure 3-4.)

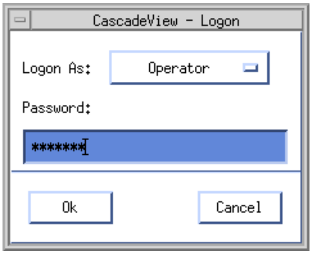


Figure 3-4. Logon Dialog Box

Creating a Subnet ID

To add a subnet ID, use the following steps:

1. From the Administer menu select Cascade Parameters ⇒ Set All Subnets.

   The Set All Subnets dialog box appears as shown in Figure 3-5.

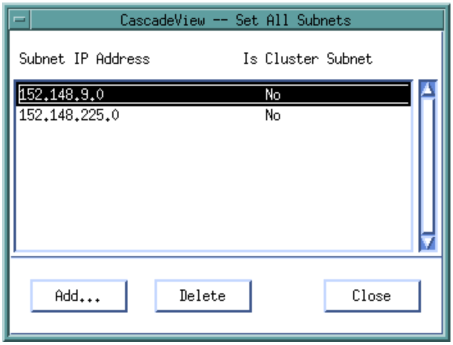


Figure 3-5. Set All Subnets Dialog Box

2. Select Add. The Add Subnet dialog box appears as shown in Figure 3-6.

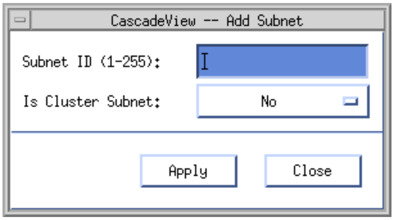


Figure 3-6. Add Subnet Dialog Box

3. Complete the required dialog box fields described in Table 3-3.

Table 3-3. Add Subnet Fields

Field	Action/Description
Subnet ID (1-255)	Enter a subnet number between 1 and 255.
Is Cluster Subnet (*optional*)	Select *Yes* in the Is Cluster Subnet field 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.

Creating Clusters

A cluster defines a group of switches that operates in a single OSPF routing domain. The switch number in the IP address increments according to the cluster ID, as described in Table 4-5 on page 4-13. Refer to Chapter 4 for more information about clusters.

To create a cluster, use the following steps:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Clusters.

   The Set All Clusters dialog box appears as shown in Figure 3-7.

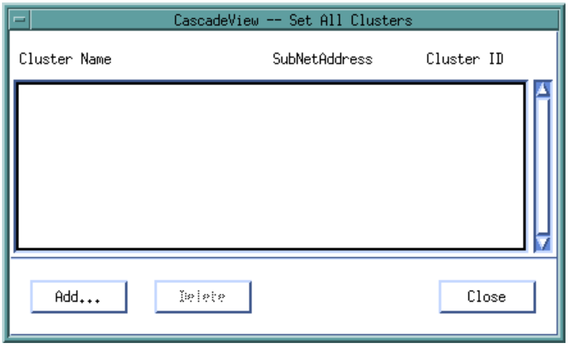


Figure 3-7. Set All Clusters Dialog Box

2. Select Add. The Add Cluster dialog box appears as shown in Figure 3-8.

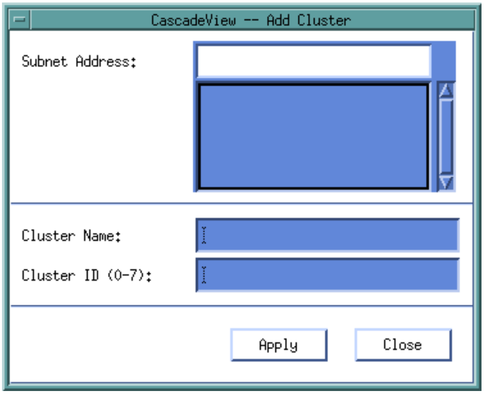


Figure 3-8. Add Cluster Dialog Box

3. Complete the required dialog box fields described in Table 3-4.

Table 3-4. Add Cluster Fields

Field	Action/Description
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.

Configuring the Gateway Switch

To add the first switch to the map, use the following steps:

1. From the Edit menu, select Add Object. The Add Object:Palette dialog box appears as shown in Figure 3-9.

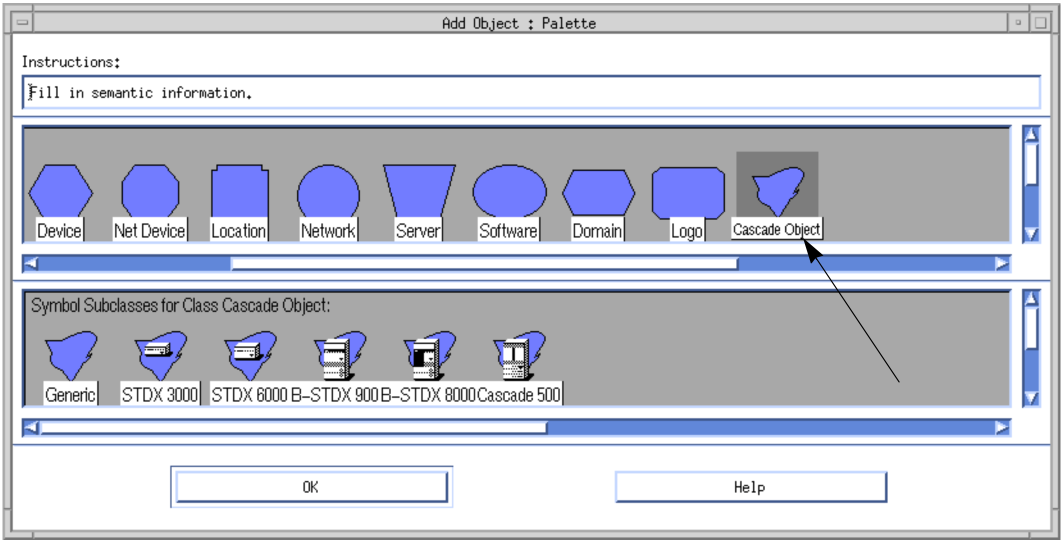


Figure 3-9. Add Object:Palette Dialog Box

2. Scroll through the Object Palette to locate the Cascade Object symbol.

3. Select Cascade Object. The Symbol Subclasses for Class Cascade Object appear.

4. Add the desired Cascade switch to the network map (STDX 3000, STDX 6000, B-STDX 8000, B-STDX 9000 or Cascade 500). To do this, position the mouse pointer on the object, hold down the *middle* mouse button, drag the object to the map, and release the mouse button. The Add Object dialog box appears as shown in Figure 3-10. For information on configuring Cascade 500 switches, refer to the *CBX 500 Network Administrator's Guide.*

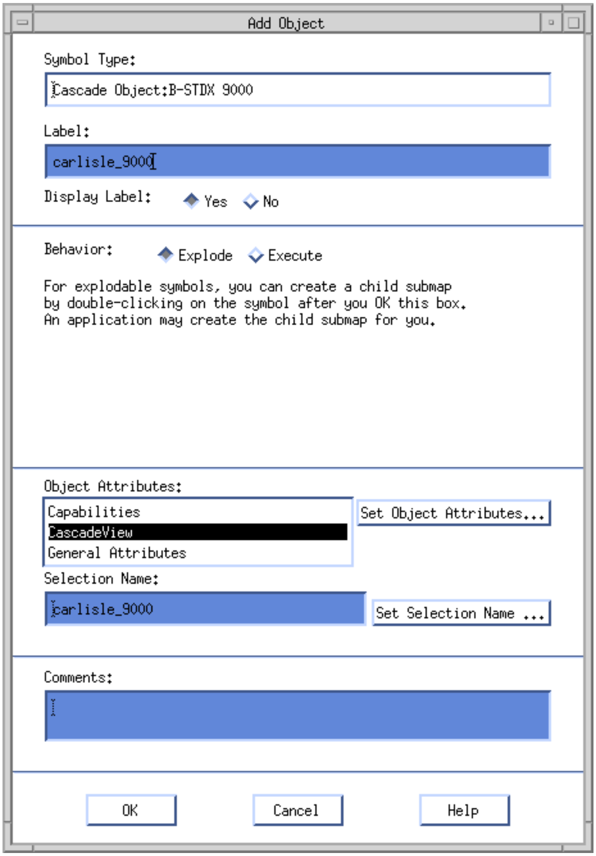


Figure 3-10. Add Object Dialog Box

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

Table 3-5. Add Object Fields

Field	Action/Description
Symbol Type	Displays the selected switch type (object) to add 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/UX 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 Add Object–Set Attributes dialog box appears as shown in Figure 3-11.

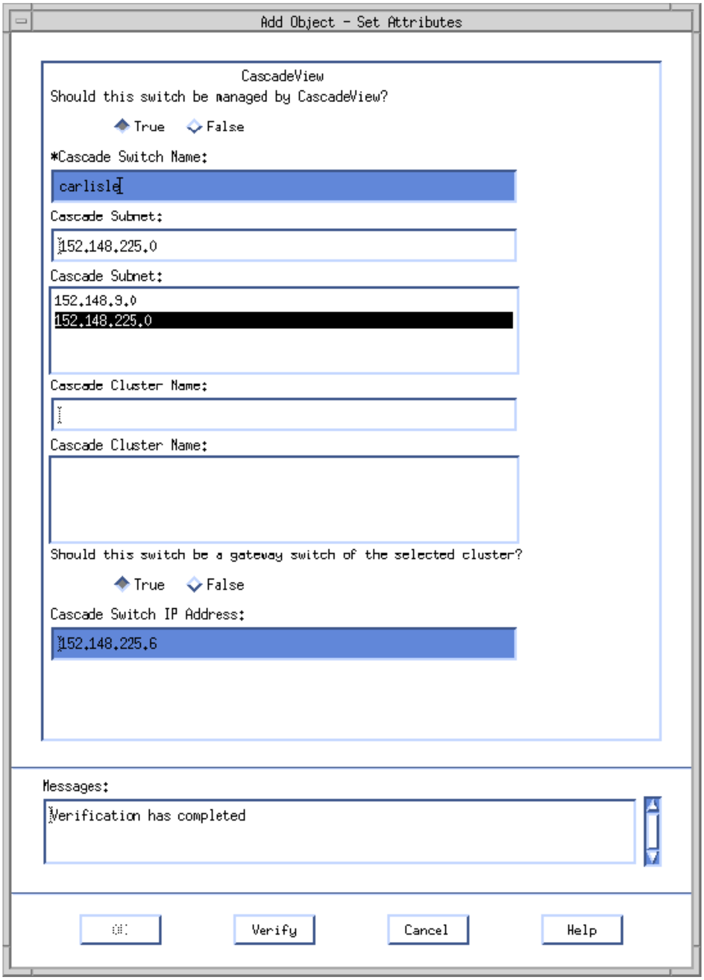


Figure 3-11. Add Object-Set Attributes Dialog Box

6. Complete the required dialog box fields described in Table 3-6.

Table 3-6. Add Object-Set Attributes Fields

Field	Action/Description
Should this switch be managed by CascadeView?	Select True.
Cascade Switch Name	Enter a unique name for the switch.
Cascade Subnet	Highlight the Cascade subnet to which this switch belongs.
Cascade Cluster Name	Displays the name of the cluster to which this subnet belongs. Refer to "Creating Clusters" on page 3-10 for more information.
Should this switch be a gateway switch of the selected cluster?	Select *True* to make this a gateway switch. Select *False* if you do not want this switch to be a gateway switch for the selected cluster.
Cascade Switch IP Address	CascadeView/UX displays the switch's IP address. Every time you add an object to the map, CascadeView/UX increments the last octet (host ID) by 1. If the next host ID number is already in use, CascadeView/UX selects the next available number. If you want a different IP address from the one displayed, you can manually change the last octet. If you created a cluster, the system displays the IP address range (shown in Table 4-5 on page 4-13).

7. Choose Verify to confirm your settings. The following message appears in the Messages field:

```
Verification has completed.
```

> *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. Choose OK to return to the Add Object dialog box.

   Note that the Selection Name field automatically defaults to the value you entered for the Label name. The Selection Name must be a unique name throughout all HP OpenView objects. Cascade recommends you leave the selection name as it appears in the comments field. (*Optional*) Enter any additional information pertaining to the objects.

9. Choose OK. The Add Object Palette dialog box reappears.

10. Choose OK. The network map displays an object icon representing the new switch. The object appears blue and quickly turns to red, indicating that 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. (*Optional*) Repeat Step 1 through Step 11 to add more Cascade switches to the network map.

> *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.*

About Virtual Private Networks

Virtual Private Networks (VPNs) enable network service providers to provide dedicated bandwidth to those customers who require guaranteed performance, reliability, and privacy. When you add a trunk (described in Chapter 10), you can dedicate trunks to specific customers and, if desired, allow customers to monitor their own networks. However, control and configuration of the switches stays with the network service provider. You assign trunks to a VPN when you configure the trunk.

The following steps outline the procedure to set up a VPN.

Step 1. Create the VPN (page 3-18).

Step 2. Add customers to a specific VPN (page 3-20).

Step 3. *For PVC traffic*, dedicate each circuit endpoint to a specific VPN and customer. Specify the net overflow parameters that determine whether this PVC is restricted to trunks in its own VPN or uses public (shared) trunks during overflow conditions (page 7-12).

Step 4. Dedicate a trunk to a specific customer (refer to Chapter 10).

Creating a VPN

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. The Set All Virtual Private Networks dialog box appears as shown in Figure 3-12.

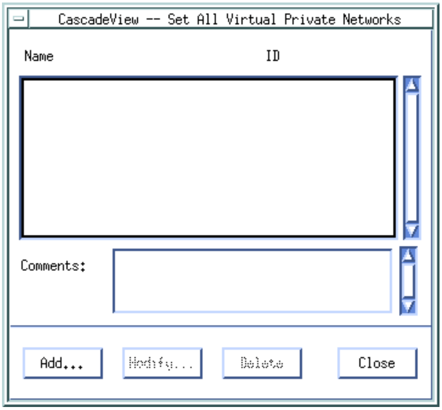


Figure 3-12. Set All Virtual Private Networks Dialog Box

2. Choose Add. The Add Virtual Private Network dialog box appears as shown in Figure 3-13.

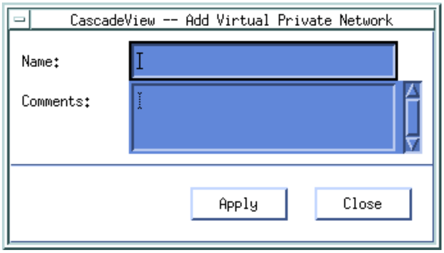


Figure 3-13. Add Virtual Private Network Dialog Box

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

Adding Customers to the VPN

To add customers to the VPN, use the following steps:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Customers.

   The Set All Customers dialog box appears as shown in Figure 3-14.

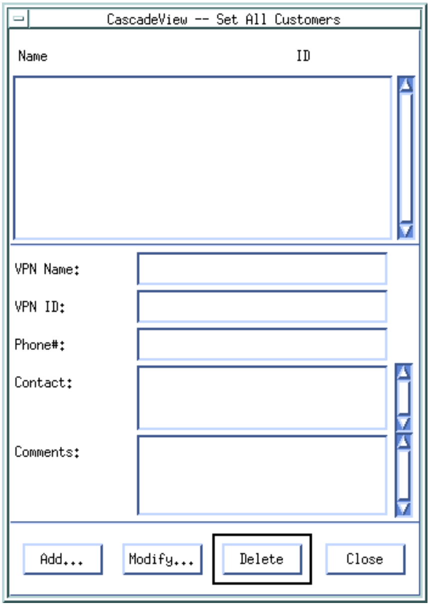


Figure 3-14. Set All Customers Dialog Box

2. Choose Add. The Add Customer dialog box appears as shown in Figure 3-15.

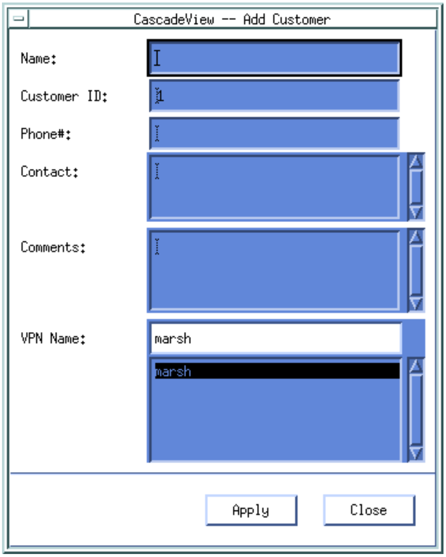


Figure 3-15. Add Customer Dialog Box

3. Complete the required dialog box fields described in Table 3-7.

Table 3-7. Add Customer Fields

Field	Action/Description
Name	Enter a customer name.
Customer ID	CascadeView/UX assigns the customer ID.
Phone#	Enter the phone number.
Contact	Enter the contact name.
Comments	Enter any additional comments
VPN Name	Select the VPN name to which this customer belongs.

4. Choose Apply. Choose Close to return to the network map.

Configuring Switch Parameters

To configure switch parameters, use the following steps:

1. Select the switch object and from the Misc menu, select CascadeView ⇒ Logon. Enter your operator password.

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

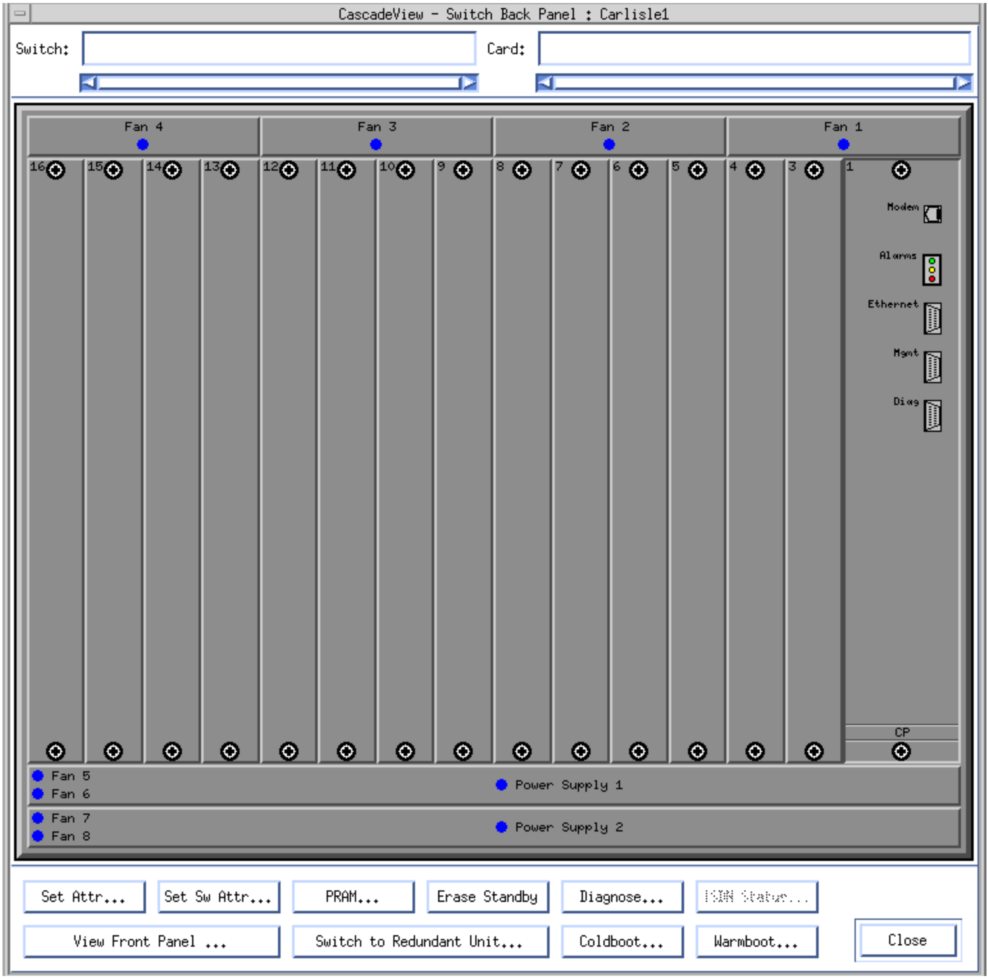


Figure 3-16. Switch Back Panel Dialog Box

The Switch Back Panel dialog box varies depending on the type of switch (this example shows a sample B-STDX 9000 configuration). The steps for defining the switch parameters for a B-STDX 8000/9000 or STDX 3000/6000 are similar.

For information about the command buttons on this dialog box, refer to *"The B-STDX Switch Back Panel Dialog Box" on page 5-9.*

3. To configure switch parameters, choose Set Sw Attr. The Set Switch Attributes dialog box appears as shown in Figure 3-17.

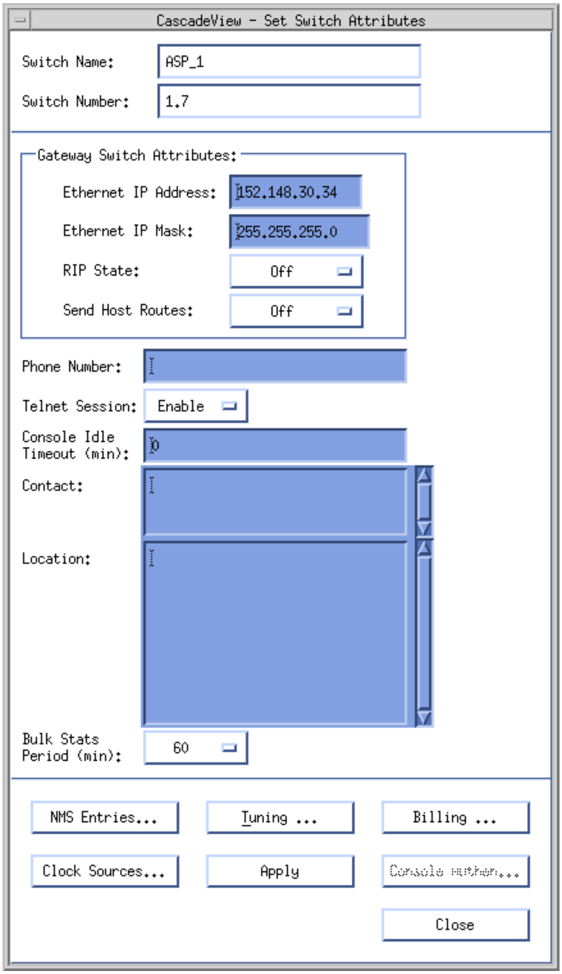


Figure 3-17. Set Switch Attributes Dialog Box

4. Do one of the following:

- If this is a gateway switch, complete the Gateway Switch Attributes fields as described in Table 3-8.
- If this is not a gateway switch, proceed to Step 5.

Table 3-8. Set (Gateway) Switch Attributes Fields

Field	Action/Description
Ethernet IP Address	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. ***Note****: You only need to enter the Ethernet IP address for the switch or switches that have an Ethernet connection and will communicate with the NMS via this connection.*
Ethernet IP Mask	Enter the In-band (Ethernet) IP mask for this switch. The default is 255.255.255.0.
RIP State	Set the RIP State parameters. The RIP feature enables the switch to send/receive RIP packets to/from all routers in the network and pass route information to each destination (switch) in the network. *Off (default)* – Disables RIP. *On* – Enables the switch to process received RIP packets and send RIP updates to routers connected to the Ethernet.
Send Host Routes	Set the Send Host Routes parameters. The Send Host Routes field determines the RIP packet contents sent by the gateway switch. *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.

5. Complete the required dialog box fields described in Table 3-9.

Table 3-9. Set Switch Attributes Fields

Field	Action/Description
Phone Number	Enter the phone number of the contact person responsible for switch operations.
Telnet Session	The default, *Enable*, allows the switch to accept a remote terminal connection for troubleshooting purposes. Cascade recommends that you do not disable this function.
Console Idle Timeout (min)	Specify the time period (in minutes) of console inactivity before the console is logged off. The default is 5 minutes.
Contact	Enter the name of the contact person responsible for operating the switch.
Location	Enter the switch's location.
Bulk Stats Period (min)	Specify the bulk statistics collection interval (in minutes). A setting of zero disables collection from the switch.

6. Choose Apply to set the parameters.

7. Choose Close to exit the dialog box.

8. To configure the Control Processor (CP) type for a B-STDX 8000/9000, point to the CP module slot on the switch back panel and double-click the left mouse button (refer to page 5-33). The Set Card Attributes dialog box appears as shown in Figure 3-18.

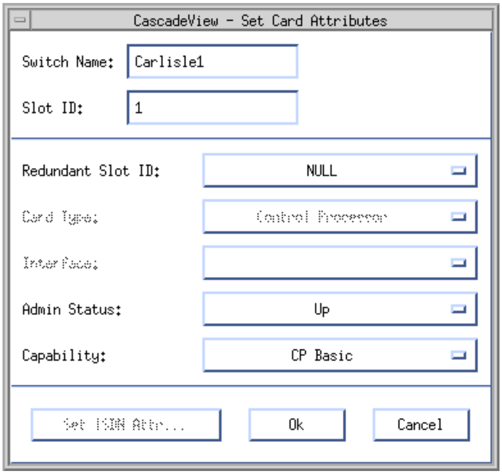


Figure 3-18. Set Card Attributes Dialog Box

9. Complete the required dialog box fields described in Table 3-10.

Table 3-10. Set Card (CP) Attributes Fields

Field	Action/Description
Redundant Slot ID (*Optional*)	To configure a redundant CP, select redundant Slot ID 2. You must always configure the main CP in Slot 1. The default, NULL, indicates there is no redundant module installed.
Card Type	This read-only field automatically defaults to Control Processor.

Table 3-10. Set Card (CP) Attributes Fields (Continued)

Field	Action/Description
Admin Status	Set this field as follows: *Up (default)* – This CP becomes fully operational when you start the switch. *Down* – This CP does not come online when you start the switch. This setting saves the configuration in the database but does not download it to the switch. Use this option when you run foreground diagnostics.
Capability	Set this field as follows: *CP Basic* – This CP module has a black dip switch located on the front panel. It is often used in both the B-STDX 8000 and 9000 models. *CP Plus* – This CP module has a red dip switch located on the front panel. It has more memory than the CP Basic and can be used in either B-STDX model. This CP type is required for SMDS Billing. ***Note**: If you do not know the CP type and cannot physically view it, you can use the show card or show system console commands to retrieve this information. Refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for a list of console commands.*

Table 3-10. Set Card (CP) Attributes Fields (Continued)

Field	Action/Description
Capability (continued)	The CP 30, 40, and 50 use a 170 MB internal disk and each supports a different amount of memory. You must be running switch code Version 4.2 or higher before you configure the CP 30, 40, or 50. For more information on installing these CP cards, refer to the *B-STDX 8000/9000 Hardware Installation Guide.* *CP 30* – This CP module replaces the CP Basic and has 16 MB IRAM. *CP 40* – This CP module replaces the CP Plus and has 64 MB memory for IP routing. *CP 50* – This CP module replaces the CP Plus and has 128 MB memory for IP routing. ***Note**: Do not select CP 30, 40, or 50 until you replace both the active and standby CP modules. Use the following selections:* *CP 30 – Select CP Basic* *CP 40 and 50 – Select CP Plus* *For example, if the active CP module is a CP Plus and the redundant CP module is a CP 40, select CP Plus for both modules.*

10. Choose OK. The Set Switch Back Panel dialog box reappears.

11. To configure the first I/O module, double-click on its slot. The Set Card Attributes dialog box appears.

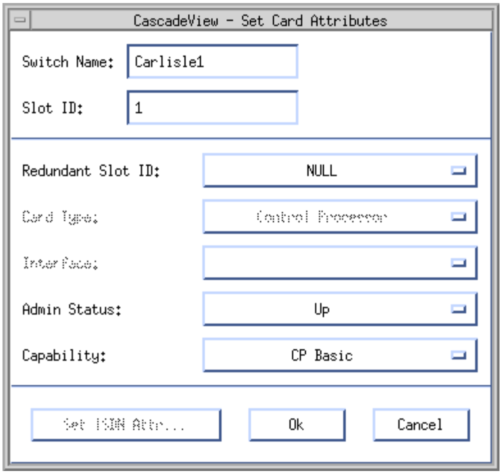


Figure 3-19. Set Card Attributes Dialog Box

12. Select the appropriate card type (refer to page 6-4).

    - If you are configuring a B-STDX 8000/9000, verify the Admin status is *Up*.
    - If there is a redundant module installed in the B-STDX 8000/9000 switch, in the Redundant slot ID field, specify the module's slot location. This standby module must be installed and configured in the higher numbered slot than its active partner.

13. Choose OK. Repeat Step 11 and Step 12 for each I/O module in this switch. When you finish, choose Close to return to the network map.

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

14. Select the switch object and from the Administer menu, select Cascade Parameters ⇒ Set NMS Paths (refer to page 5-30). The Set NMS Paths dialog box appears.

15. Choose Add. The Add NMS Path dialog box appears as shown in Figure 3-20. The following example shows an Ethernet (Direct) NMS Path.

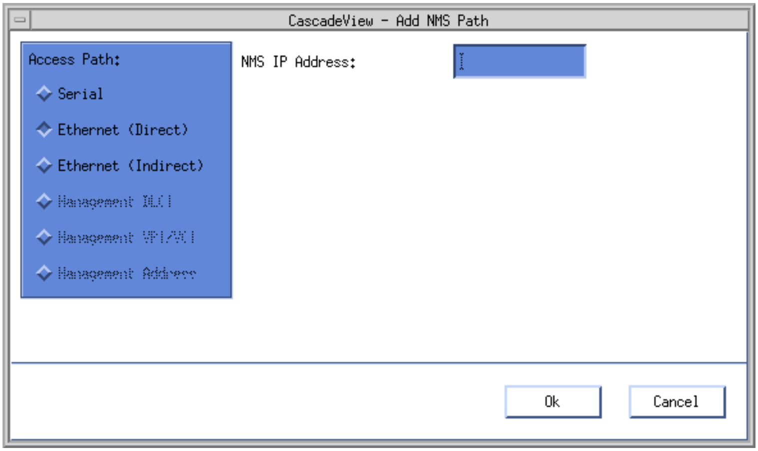


Figure 3-20. Add NMS Path Dialog Box

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.

Generating the Configuration File

You now need to initialize the switch to generate an ASCII text file. This creates a configuration file that contains the basic parameters needed to activate the switch (refer to page 12-2). This enables the gateway switch to communicate with the NMS.

1. From the Administer menu, select Cascade Switches ⇒ Initialize Switches.

2. From the Initialize Switches dialog box, select the name of the switch you just configured and choose Generate.

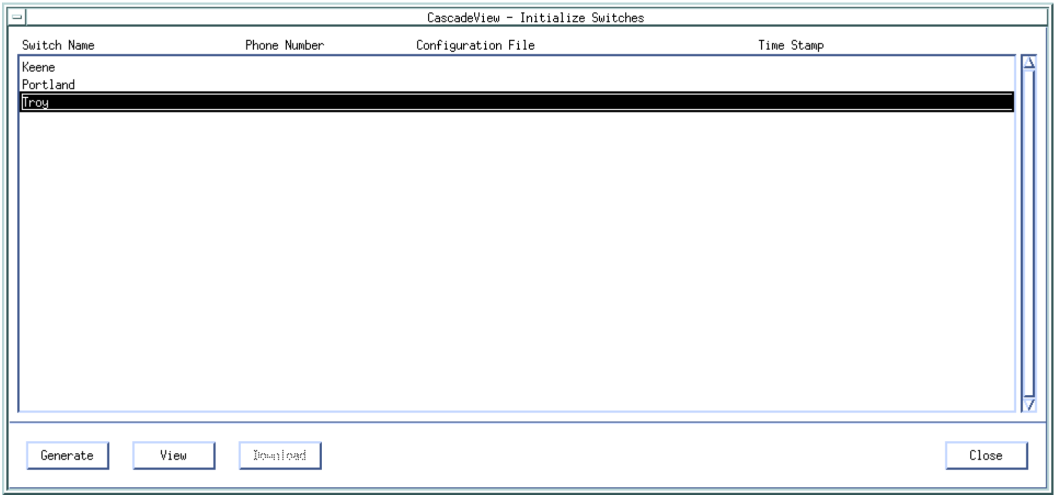


Figure 3-21. Initialize Switches Dialog Box

3. Note the configuration file name and path. This is the configuration file you download to the switch. Choose Close to return to the network map.

Downloading the Configuration File

The next step is to download the configuration file. This file is stored in the */var/CascadeView/initFiles* directory as [*switchname*].init. Solaris comes with a program called *tip* that you can use to download text files over a serial line. *Follow the procedure on* *page 12-5* *to download this configuration text file*.

> *If you use another terminal emulation program to download this file, set the program baud rate to 19200 for a B-STDX 8000/9000 and 9600 for an STDX 3000/6000.*

Verifying the Download

To verify that the download was successful, use the following steps:

1. Select the switch object on the network map and from the Map menu, select Manage Objects. The switch object on the map should change from a wheat color to yellow. If the switch does not change to yellow, review the previous steps, and check the RS-232 console connection between the NMS SPARCstation and the switch.

2. When the switch object turns yellow, synchronize the switch so it can communicate directly with the NMS (refer to page 12-16). On the network map, select the switch object.

   - If you are synchronizing an STDX 3000 or 6000 switch:
     - From the Administer menu, select Cascade Parameters ⇒ Set Parameters to display the Switch Back Panel dialog box (refer to Figure 12-8 on page 12-17).
     - Choose *PRAM*.
     - On the Pram Sync dialog box, select Synchronize PRAM and choose OK.
   - If you are synchronizing a B-STDX 8000/9000 switch:
     - From the Administer menu, select Parameters ⇒ Set Parameters to display the Switch Back Panel dialog box.
     - For each module installed in the switch (starting with the Control Processor), select the module and choose PRAM.

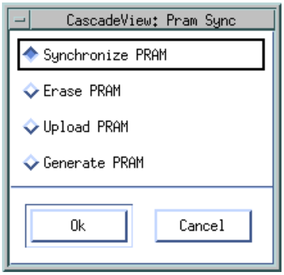


Figure 3-22. PRAM Sync Dialog Box

- On the Pram Sync dialog box, select Synchronize PRAM and choose OK (refer to page 12-16).

When you issue the synchronize command, the NMS sends the binary image to the selected switch, causing a warm reboot. This process can take up to several minutes, depending on your switch configuration.

3. Display the network map to verify that the switch and NMS are properly configured. The switch object changes from yellow to red (briefly), and then to green. If the switch object does not change to green, review the previous steps, and check the physical connections between the NMS SPARCstation and the switch.

Configuring the Second Switch on the Network Map

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

- ☑ Set up the NMS SPARCstation and gateway switch as described in the previous section. The gateway switch object should be green on the map.
- ☑ Install the physical connection for creating a trunk line between this switch and the gateway (or any active switch you can configure as a hop between this switch and the gateway). Refer to the appropriate hardware installation guide.

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. To do this, you must add a second switch to the same map, configure the physical and logical port, and define a trunk connection between the two switches.

1. If necessary, start the NMS and access CascadeView/UX.
2. From the Misc menu, select CascadeView ⇒ Logon.
3. From the Map menu, select Maps⇒ Open/List Maps and select the desired map. Choose OK.
4. To add the second switch to the map, refer to “Configuring the Gateway Switch” on page 3-12. When you finish, the network map should display the second switch; which is “unmanaged” (wheat color).

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

6. To configure the Control Processor (CP) type for a B-STDX 8000/9000, double-click the left mouse button on the CP module slot (refer to page 5-33). Verify that the Admin Status is *Up* and set the capability for CP module type as described in Table 3-10 on page 3-27.

7. Choose OK. The Switch Back Panel dialog box reappears.

8. To configure the first I/O module, double-click on its slot. Select the appropriate card type (refer to page 6-4).

   - If you are configuring a B-STDX 8000/9000, verify the Admin status is *Up*.

   - If there is a redundant module installed in the B-STDX 8000/9000 switch, in the redundant Slot ID field, specify the module's slot location. This standby module must be installed and configured in the higher numbered slot than its active partner.

9. Choose OK. Repeat Step 8 for each I/O module in this switch. When you finish setting the card attributes, choose Close to return to the network map.

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

Configuring a Trunk Connection

This section describes how to configure a Frame Relay direct-line trunk connection between the first switch (known as the *gateway switch*) and the second switch in a new Cascade network. To configure a direct-line trunk, you must first configure the physical port and logical port on the gateway switch and the second switch.

Configuring the Trunk's Physical Port

To configure the physical port, use the following steps:

1. On the network map, select the *gateway switch* and from the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

2. To configure a physical port, select the appropriate I/O module. Double-click on the port to use for the trunk connection (refer to page 6-9). The Set Physical Port Attributes dialog box appears (Figure 3-23 shows an 8-port Universal I/O module in a B-STDX switch).

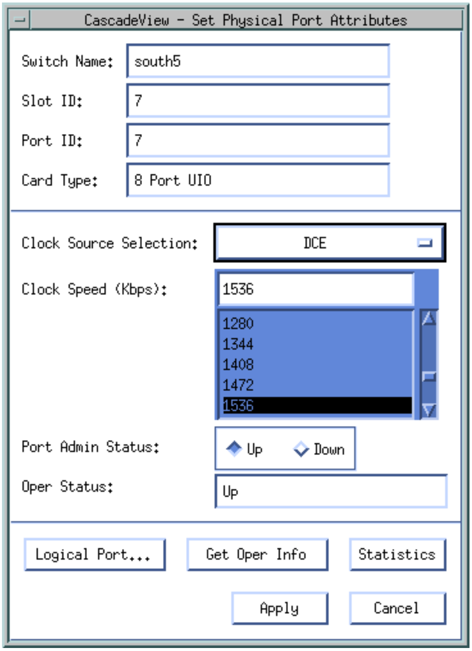


Figure 3-23. Set Physical Port Attributes

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

4. Choose Apply to enter your selections.

Configuring the Trunk's Logical Port

To configure the logical port settings for the trunk, use the following steps:

1. Choose the Logical Port command button on the Set Physical Port Attributes dialog box. The Set All Logical Ports dialog box appears (refer to Figure 7-4 on page 7-17).

2. Choose Add. The Add Logical Port dialog box appears.

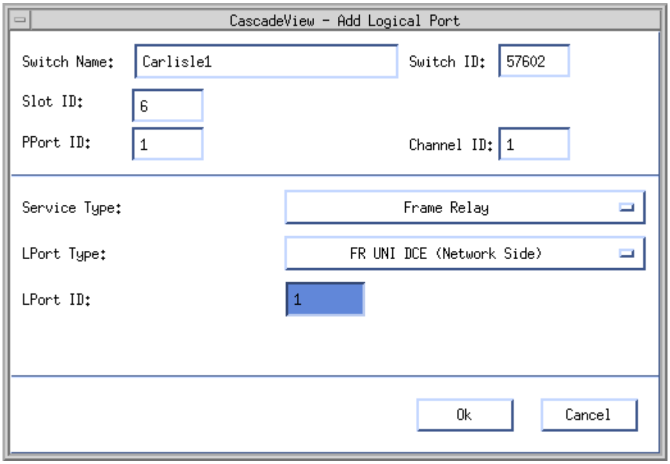


Figure 3-24. Add Logical Port Dialog Box

3. In the Service Type field, select Others.

4. In the LPort Type field, select Direct Line Trunk (refer to "Defining Other Types of Frame Relay Logical Ports" on page 7-41).

5. In the LPort ID filed, for a T1 module, enter a number between 1 and 24; for an E1 module, enter a number between 1 and 30. Otherwise, accept the default LPort ID.

6. Choose OK.

7. The Add Logical Port dialog box appears. Enter a logical port name and specify the bandwidth.

Define the same bandwidth on both ends of the trunk connection.

8. 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 for the second switch. Repeat the last two procedures to configure a physical and logical port for the switch at the other end of the trunk.

Defining the Trunk Configuration

To configure the trunk between the gateway switch and the second switch, use the following steps:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears (page 10-9).
2. Choose Add. The Select End Logical Ports dialog box appears. Choose Add. The Select Logical Ports dialog box appears as shown in Figure 3-25.

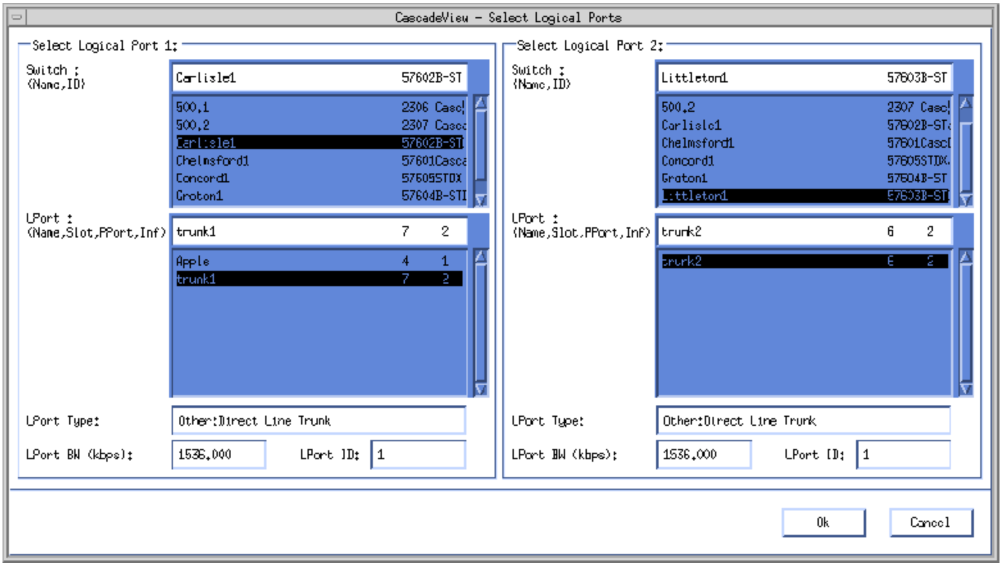


Figure 3-25. Select Logical Ports Dialog Box

3. Complete the required dialog box fields described in Table 3-11 for both Logical Port 1 and Logical Port 2.

Table 3-11. Select Logical Port Fields

Field	Action/Description
Switch (Name, ID)	Select a switch for each endpoint. The dialog box displays the parameters for the selected switch.
LPort (Name, Slot, PPort, Inf)	Select the same trunk logical port type for each endpoint. Choose from the following logical port types depending on the type of logical port service: • Frame Relay OPTimum Trunk • Other:Direct Line Trunk • SMDS OPTimum Trunk • ATM: Direct Trunk • ATM OPTimum Frame Trunk • ATM OPTimum Cell Trunk This field also displays the physical port number and I/O slot (number) in which the module resides. ***Note****: Review the LPort Bandwidth field for each endpoint to make sure the bandwidth is the same.*
LPort Type	Displays the configured logical port type.
LPort BW (kbps)	Displays the bandwidth configured for the logical port. This must be the same for both endpoints.
LPort ID	Displays the logical port number.

4. Choose OK. The Add Trunk dialog box appears, displaying the trunk's parameters for both Logical Port 1 and Logical Port 2.

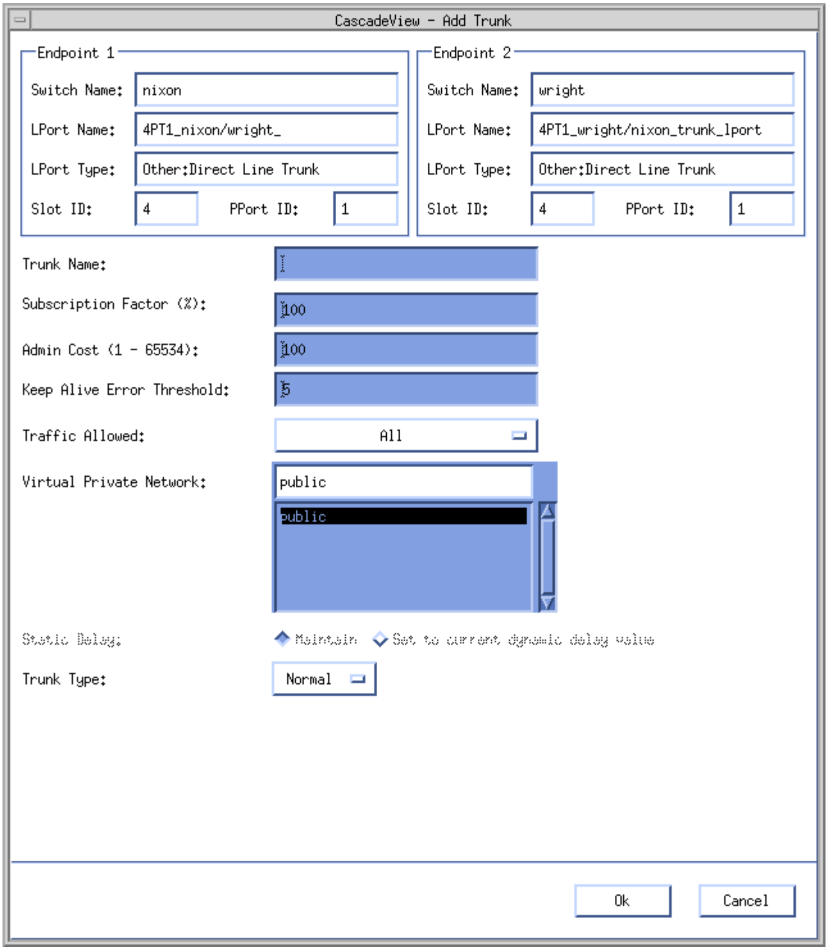


Figure 3-26. Add Trunk Dialog Box

5. Complete the required Add Trunk dialog box fields described in Table 3-12.

Table 3-12. Add Trunk Fields

Field	Action/Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk. You use this same name when you create the trunk connection (refer to page 10-21).
Subscription Factor (%)	The trunk over-subscription factor percentage enables you to optimize the aggregate CIR you can configure on the trunk, by allowing you to over-subscribe the trunk. The over-subscription factor represents the V value for this trunk. The bandwidth on a trunk is reserved at runtime, based on the configured CIR value of the PVCs that traverse that trunk. For a detailed explanation of this parameter, refer to page 10-2.
Admin Cost (1-65534)	Assign an administrative cost value of 1 to 65534. The lower the admin cost of the path, the more likely OSPF will select it for circuit traffic. The default admin cost value is 100. For a detailed explanation of this parameter, refer to page 10-3. ***Note***: *When you increase or decrease the administrative cost of a trunk, the reroute tuning parameters control the rate at which the switch adds or removes circuits from the trunk. Refer to page 5-24 for information about reroute tuning. You cannot use trunk admin cost to disable a trunk.*

Table 3-12. Add Trunk Fields (Continued)

Field	Action/Description
Keep Alive Threshold (%)	You can configure the keep alive threshold for a value between 3 and 255 seconds. The default is 5 seconds. For a detailed explanation of this parameter, refer to page 10-5. ***Note****: Service is disrupted if you change this value after the trunk is online.*
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – The trunk can carry network management traffic, user traffic, and OSPF address distribution. *Mgt Only* –The trunk can carry *only* network management traffic, such as SNMP communication between a switch and the NMS. *Mgt & User* – The trunk can carry network management traffic and user traffic. ***Note****: To calculate the most efficient route for network management traffic, OSPF uses Trunk Admin Cost. OSPF ignores trunk bandwidth when it selects a route for management traffic; management traffic can use a negative bandwidth trunk.*
Virtual Private Network	Select a Virtual Private Network (VPN). The default is Public.
Static Delay	Defaults to maintain.

Table 3-12. Add Trunk Fields (Continued)

Field	Action/Description
Trunk Type	Displays *Normal*, *Primary*, or *Backup*. Normal is a common trunk. Primary indicates that the trunk has a backup for fault tolerance. Backup indicates that it is the backup trunk (when failure occurs on the primary trunk). If you select Backup, complete Step 7.

6. (*Optional*) If you selected *Primary* as the Trunk Type, complete the additional parameters that appear on the Add Trunk dialog box or accept the default parameters.

7. (*Optional*) If you selected *Backup* as the Trunk Type, complete the additional parameters that appear on the Add Trunk dialog box:

   Primary Trunk of the backup — Select the name of the trunk to back up to this configuration.

   Switch Initializing the Call Setup — Select the name of the switch initializing the call setup.

8. Choose Close to return to the network map.

Adding a Trunk Line Connection

To add the trunk line graphic to the network map, use the following steps:

1. From the Edit menu, select Add Connection. The Add Connection dialog box appears as shown in Figure 3-27.

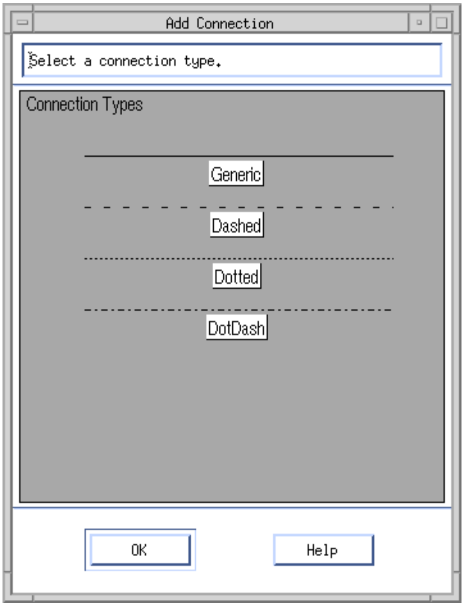


Figure 3-27. Add Connection Dialog Box

2. Select a Connection Type from the palette.

3. To create a trunk line connection between the two Cascade switches on the network map, click on the first switch object (source symbol) and then the second switch object (destination symbol).

4. The Add Object dialog box appears as shown in Figure 3-28.

Figure 3-28. Add Object Dialog Box

5. Complete the required dialog box fields described in Table 3-13.

Table 3-13. Add Object Fields

Field	Action/Description
Symbol Type	Displays the type of connection you are adding to the map.
Label	Enter the trunk name you specified on the Add Trunk dialog box (refer to page 3-41).

Table 3-13. Add Object Fields (Continued)

Field	Action/Description
Display Label	Select Yes to have the label appear below the object on the network map. Select No if you do not want the label displayed.
Behavior	Select Explode to create the basic CascadeView/UX 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 Add Object – Set Attributes dialog box appears as shown in Figure 3-29.

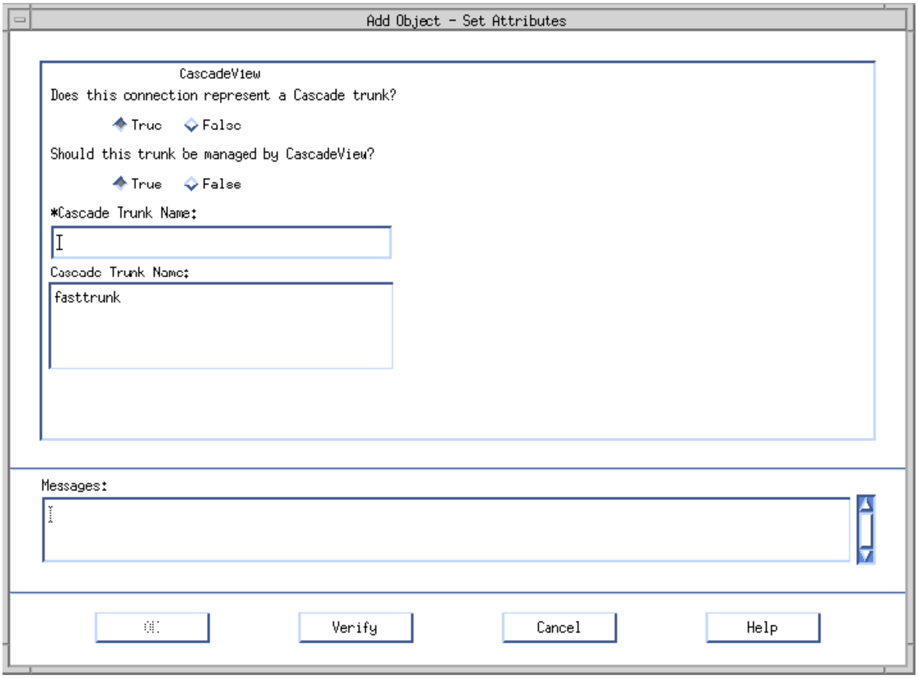


Figure 3-29. Add Object - Set Attributes Dialog Box

6. Complete the required dialog box fields described in Table 3-14.

Table 3-14. Add Object - Set Attributes Fields

Field	Action/Description
Does this connection represent a Cascade Trunk?	Select True.
Should this trunk be managed by CascadeView?	Select True.
Cascade Trunk Name	Enter the name you assigned to the trunk. This should be the same name you entered for the label in the Add Object dialog box on page 3-46.

7. Choose Verify to confirm your selections.

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

9. Choose OK to return to the network map. The trunk line appears between the two switches on the network map.

Downloading the Configuration File to the Second Switch

Last, you need download the configuration file, and synchronize the second switch. To do this, use the following steps:

1. Follow the steps in "Generating the Configuration File" on page 3-31

2. Follow the steps in "Downloading the Configuration File" on page 3-32. Make sure you use Step 2 on page 3-33 to synchronize the second switch.

3. Follow the steps in "Verifying the Download" on page 3-33.

When you finish, the trunk line graphic and switch objects should be green, indicating a successful configuration.

If the trunk graphic is black, make sure the following environment variable is specified in each NMS user's .profile

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

If necessary, log in as root and modify .profile. Then log out of CascadeView/UX and log back in 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 subnet ID, 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 network maps, you can define the topology of the network and monitor network activity.

This chapter also describes how to:

- Use IP and subnet addressing schemes
- Create a network map and subnet
- Add objects to the map in CascadeView/UX
- Create a VPN and add customers to the VPN
- Import maps from the Microsoft Windows (DOS) version of CascadeView
- Delete a network map

IP Address Overview

This section provides an overview on 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 identifie*r (*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.

Network ID 152.148	Host ID 225.10

Figure 4-1. Class B IP Address

Three Primary Classes of IP Addresses

There are three primary classes of IP addresses. 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 Classifications

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)

Table 4-1. IP Address Classifications (Continued)

Class	Network ID	Host ID	Format
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. 100	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 1000 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 could start numbering your hosts at 150.100.0.1 and go up to host number 150.100.255.254. Using this example, you would have a total of 65,534 host addresses in the Class B network. Using Class B IP addresses, you can group single addresses into subnets to create several smaller networks.

If you have a mixed network (for example, switches running Version 4.1 and Version 4.2), you must configure all switches in the 4.1 network with circuits within the same subnet. For restrictions and special considerations, refer to the Software Release Notice.

About 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).

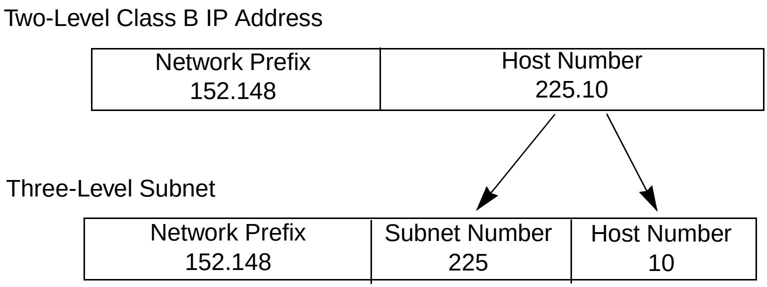


Figure 4-2. Subnet Example

A subnet can be used for the following purposes:

- Connecting different physical networks
- Distinguishing between different network LANs
- Isolating parts of the network
- Delegating network administration by assigning administrators to different subnets

Choosing a Subnet ID (Mask)

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

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

Virtual Private Network Overview

Virtual Private Networks (VPNs) enable network service providers to provide dedicated bandwidth to those customers who require guaranteed performance, reliability, and privacy. When you add a trunk (refer to Chapter 10), you can dedicate trunks to specific customers and, if desired, allow customers to monitor their own networks. However, control and configuration of the switches stays with the network service provider.You assign trunks to a VPN when you configure the trunk (see Chapter 10).

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 line:

```
OVwRegDir=/opt/CascadeView/registration
export OVwRegDir
```

This line disables the Administer menu and all its provisioning functions; the NMS user only sees the Monitor menu functions.

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 the Network Map" on page 4-6).

Step 2. Create a subnet ("Creating a Subnet ID" on page 4-11).

Step 3. Add the Cascade switch objects to the map ("Adding Cascade Switch Objects to the Map" on page 4-15).

Step 4. (*Optional*) Create virtual private networks (VPNs) and customer names ("Creating a VPN" on page 4-22 and "Adding Customers to the VPN" on page 4-23)

These procedures assume you have started CascadeView/UX.

Creating the Network Map

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

To create the network map, use the following steps:

1. From the Map menu, select Maps⇒New. The New Map dialog box appears as shown in Figure 4-3.

> *Once set, you cannot modify these 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. If you must change this setting, first check with the Cascade Technical Response Center for recommended guidelines.*

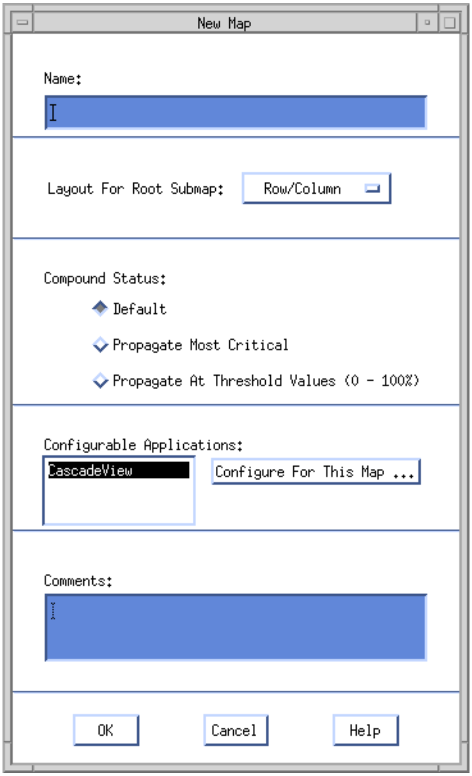


Figure 4-3. New Map Dialog Box

2. Complete the required dialog box fields described in Table 4-2.

Table 4-2. New Map Fields

Field	Action/Description
Name	Enter an alphanumeric name that identifies the map.
Layout For Root Submap	CascadeView/UX uses the default Row/Column. This option affects how the objects are arranged on the screen.

Table 4-2. New Map Fields (Continued)

Field	Action/Description
Compound Status	Compound status defines how HP OpenView propagates symbol status 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*. Select the desired status propagation: *Default* — Causes HP OpenView to propagate status according to a predefined algorithm. *Propagate Most Critical* — Causes HP OpenView to propagate the status of the most critical symbol in the child submap, to the symbols of the parent object. *Propagate At Threshold Values (0 - 100%)* — Displays four fields that enable you to set threshold values that determine when HP OpenView propagates status. The number shown for each field is the default value. – %warning 30 – %minor 20 – %major 10 – %critical 5
Comments	Enter any additional information for this map.
Configurable Applications	In the Configurable Applications box, select CascadeView. Choose Configure For This Map. The Configuration dialog box appears (see Figure 4-4).

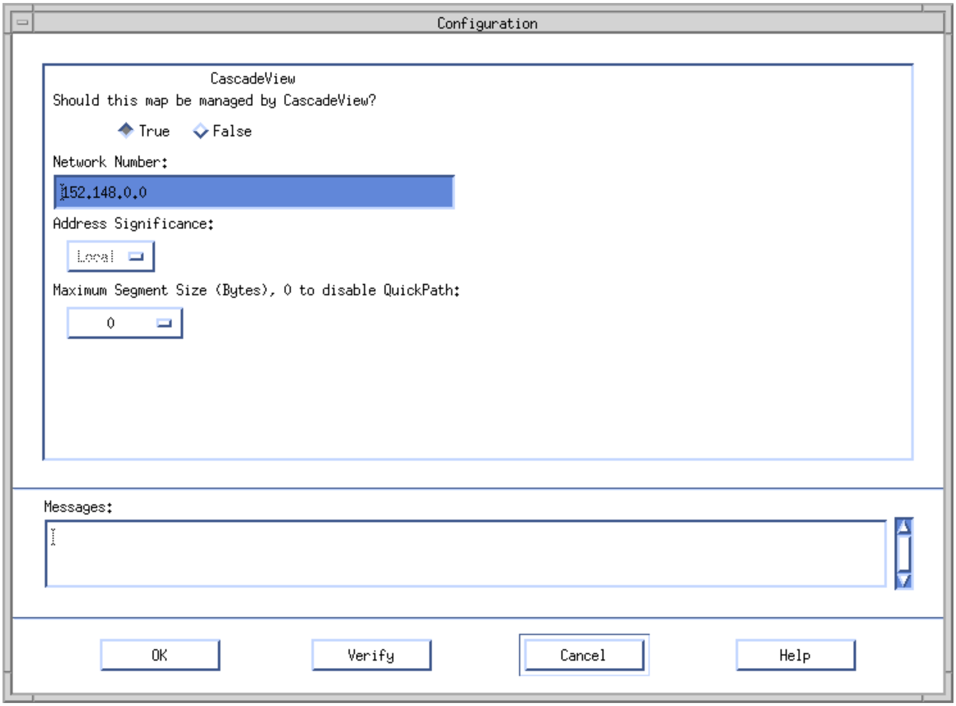


Figure 4-4. Configuration Dialog Box

3. Complete the required dialog box fields described in Table 4-3.

Table 4-3. Configuration Fields

Field	Action/Description
Should this map be managed by CascadeView?	Select True.

Table 4-3. Configuration Fields (Continued)

Field	Action/Description
Network Number	Displays the switch IP Network Number you specified when you added a static route during the CascadeView/UX install (refer to the *Network Management Station Installation Guide*). Check with the Cascade Technical Response Center if you must 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.

4. Choose Verify to confirm your settings. Choose OK. The New Map dialog box reappears.

5. Choose OK. The system displays the following message (see Figure 4-5).

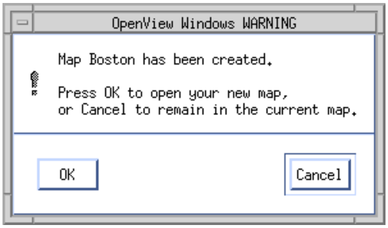


Figure 4-5. OpenView Windows WARNING Dialog Box

6. 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.*

7. To log on to the network map, from the Misc menu, select CascadeView ⇒ Logon and enter the logon password (*cascade* is the default). See Figure 4-6.

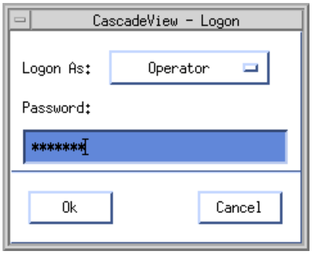


Figure 4-6. Logon Dialog Box

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, use the following steps:

1. From the Administer menu select Cascade Parameters ⇒ Set All Subnets.

   The Set All Subnets dialog box appears as shown in Figure 4-7.

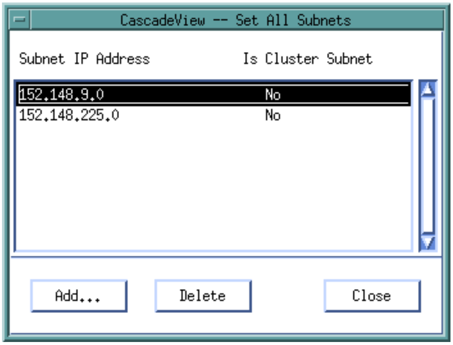


Figure 4-7. Set All Subnets Dialog Box

2. Select Add. The Add Subnet dialog box appears as shown in Figure 4-8.

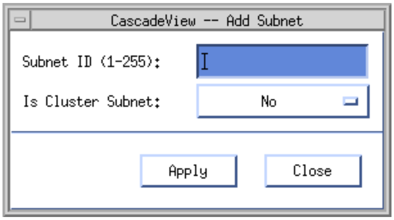


Figure 4-8. Add Subnet Dialog Box

3. Complete the required dialog box fields described in Table 4-4.

Table 4-4. Add Subnet Fields

Field	Action/Description
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*. If you select Yes, you must create a cluster as described in the next section.

4. Choose Apply to add the subnet ID.

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

Creating a Cluster

A cluster defines a group of switches that operate in a single OSPF routing domain. The switch number in the IP address increments according to the cluster ID, as shown in Table 4-5.

Table 4-5. 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 (see Table 4-4) you must create a cluster.

To create a cluster, use the following steps:

1. From the Administer menu select Cascade Parameters ⇒ Set All Clusters.

   The Set All Clusters dialog box appears as shown in Figure 4-9.

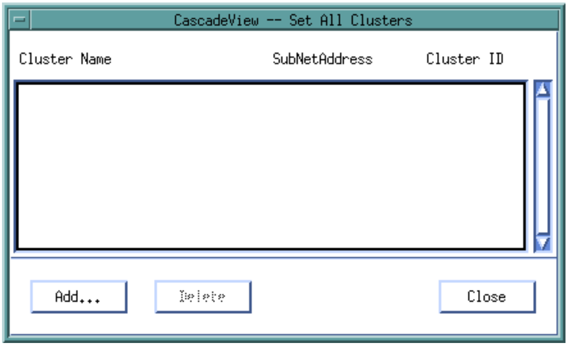


Figure 4-9. Set All Clusters Dialog Box

2. Select Add. The Add Cluster dialog box appears as shown in Figure 4-10.

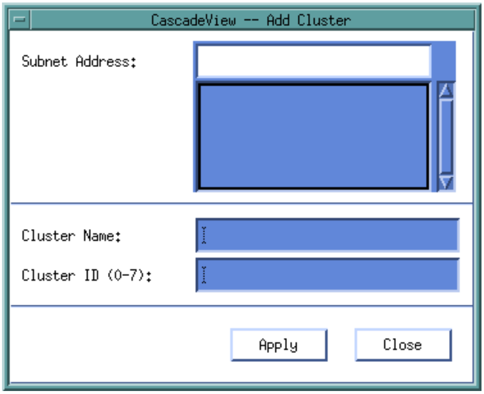


Figure 4-10. Add Cluster Dialog Box

3. Complete the required dialog box fields described in Table 4-6.

Table 4-6. Add Cluster Fields

Field	Action/Description
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.

Adding Cascade Switch Objects to the Map

When you add a CascadeView/UX switch object to the network map, you first select and drag the Cascade switch object to the network map. You then define the object attributes that enable CascadeView/UX to manage this switch through HP OpenView.

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 as shown in Figure 4-11.

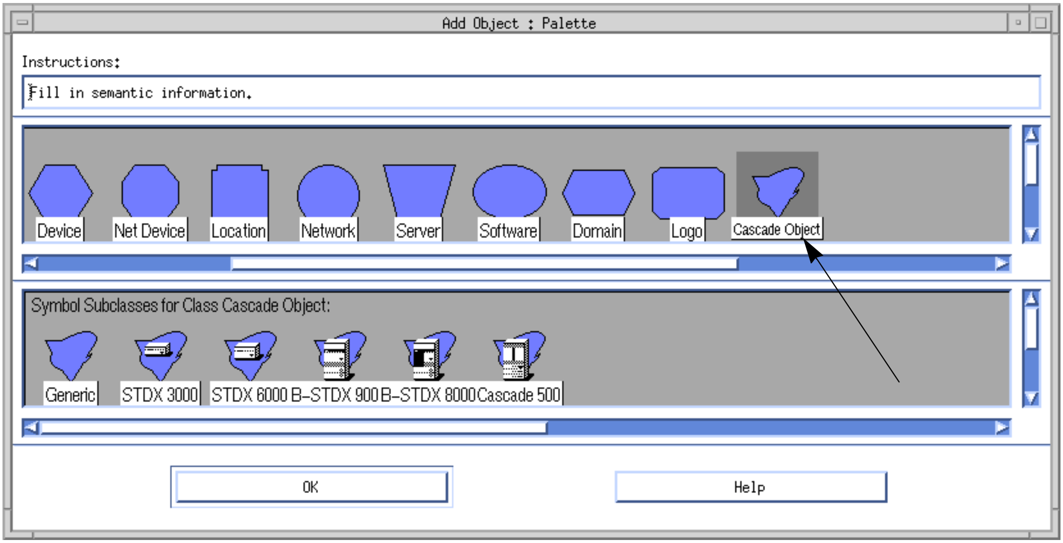


Figure 4-11. Add Object:Palette Dialog Box

2. Scroll through the Object Palette to locate the Cascade Object symbol.
3. Select Cascade Object. The Symbol Subclasses for Class Cascade Object appear.
4. Add the desired Cascade switch to the network map (STDX 3000, STDX 6000, B-STDX 8000, B-STDX 9000 or Cascade 500). To do this, position the mouse pointer on the object, hold down the *middle* mouse button, drag the object to the map, and release the mouse button. The Add Object dialog box appears as shown in Figure 4-12. For information on configuring Cascade 500 switches, refer to the *CBX 500 Network Administrator's Guide.*

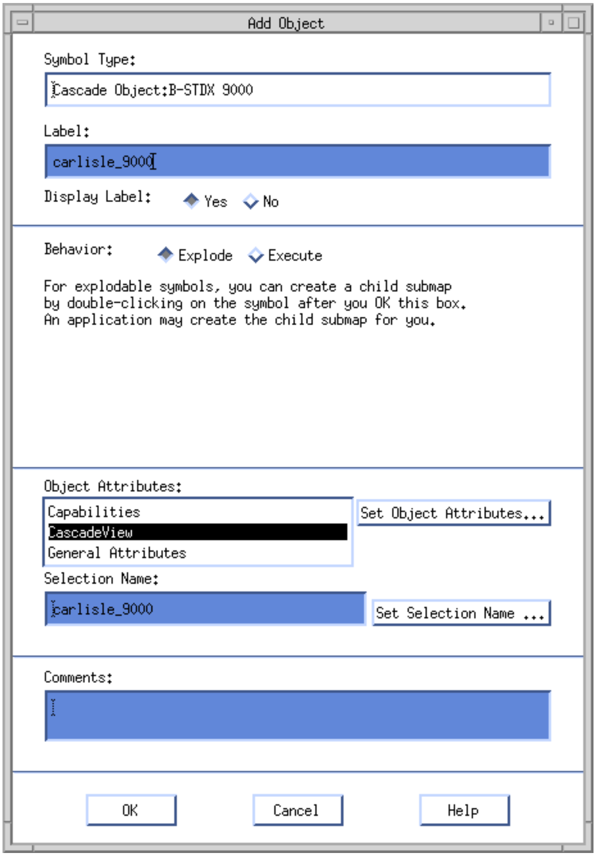


Figure 4-12. Add Object Dialog Box

5. Complete the required dialog box fields described in Table 4-7.

Table 4-7. Add Object Fields

Field	Action/Description
Symbol Type	Displays the selected switch type (object) to add 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/UX 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 Add Object–Set Attributes dialog box appears as shown in Figure 4-13.

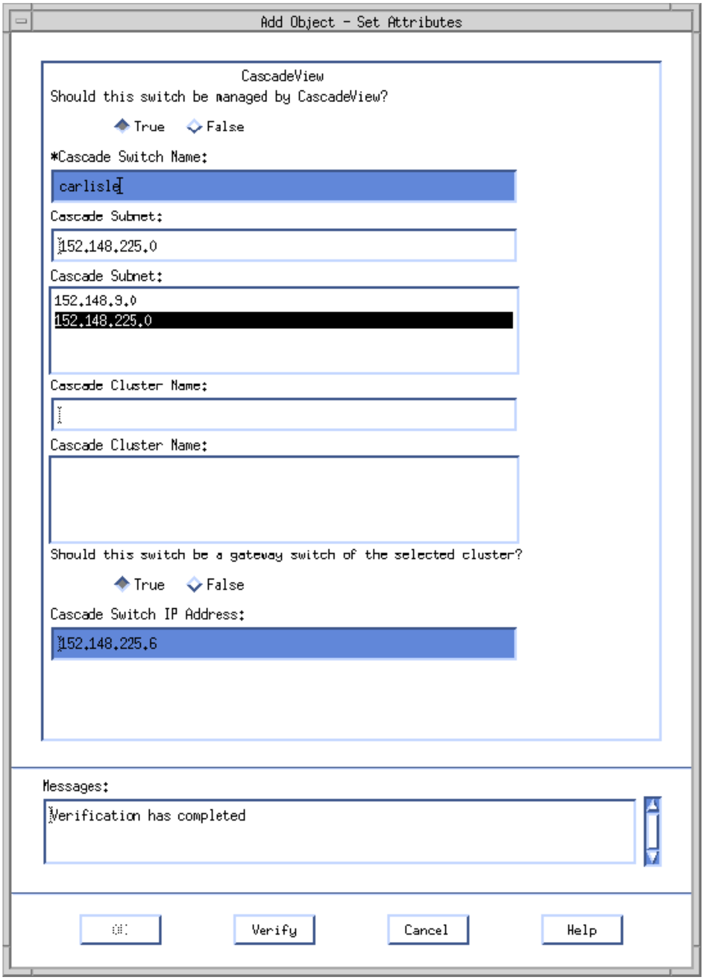


Figure 4-13. Add Object-Set Attributes Dialog Box

6. Complete the required dialog box fields described in Table 4-8.

Table 4-8. Add Object-Set Attributes Fields

Field	Action/Description
Should this switch be managed by CascadeView?	Select True.
Cascade Switch Name	Enter a unique name for the switch.
Cascade Subnet	Highlight the Cascade subnet to which this switch belongs.
Cascade Cluster Name	Displays the name of the cluster to which this subnet belongs. Refer to “Creating a Cluster” on page 4-13 for more information.
Should this switch be a gateway switch of the selected cluster?	Select *True* to make this a gateway switch. Select *False* if you do not want this switch to be a gateway switch for the selected cluster.
Cascade Switch IP Address	CascadeView/UX displays the switch’s IP address. Every time you add an object to the map, CascadeView/UX increments the last octet (host id) by 1. If the next host ID number is already in use in the network, CascadeView/UX selects the next available number. If you want a different IP address from the one displayed, you can manually change the last octet. If you created a cluster, the system displays the IP address range (shown in Table 4-5 on page 4-13).

7. Choose Verify to confirm your settings. The following message appears in the Message field:

```
Verification has completed.
```

> *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. Choose OK to return to the Add Object dialog box.

   Note that the Selection Name field automatically defaults to the value you entered for the Label name. The Selection Name must be a unique name throughout all HP OpenView objects. Cascade recommends you leave the selection name as it appears. In the comments field, enter any additional information pertaining to this object.

9. Choose OK. The Add Object Palette dialog box reappears.

10. Choose OK. The network map displays an object icon representing the new switch. The object appears blue and quickly turns to red, indicating that 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. Repeat Step 1 through Step 11 to add more Cascade switches to the network map.

When you finish adding switch objects to your network map, continue with Chapter 5 for information about configuring switch parameters and defining the path between the NMS and a Cascade switch.

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

Creating a VPN

The following steps outline the procedure you must follow to set up a VPN.

Step 1. Create the VPN (page 4-22).

Step 2. Add customers to a specific VPN (page 4-23).

Step 3. *For PVC traffic*, dedicate each circuit endpoint to a specific VPN and customer. Specify the net overflow parameters that determine whether this PVC is restricted to trunks of its own VPN or uses public (shared) trunks during overflow conditions (refer to page 7-12).

Step 4. Dedicate a trunk to a specific customer (refer to Chapter 10).

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. The Set All Virtual Private Networks dialog box appears as shown in Figure 4-14.

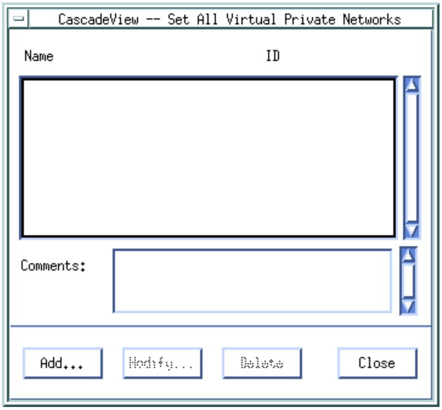


Figure 4-14. Set All Virtual Private Networks Dialog Box

2. Choose Add. The Add Virtual Private Network dialog box appears as shown in Figure 4-15.

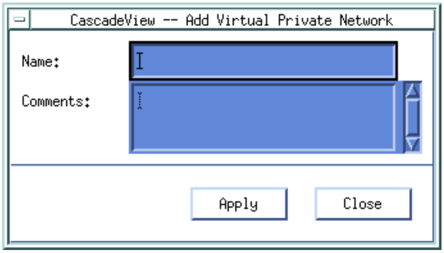


Figure 4-15. Add Virtual Private Network Dialog Box

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

Adding Customers to the VPN

To add customers to the VPN, use the following steps:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Customers.

   The Set All Customers dialog box appears as shown in Figure 4-16.

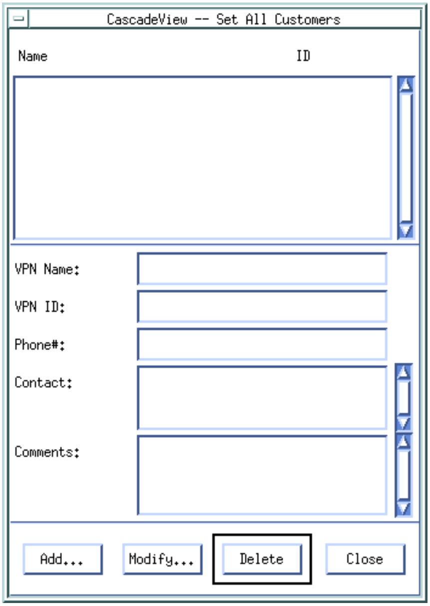


Figure 4-16. Set All Customers Dialog Box

2. Choose Add. The Add Customer dialog box appears as shown in Figure 4-17.

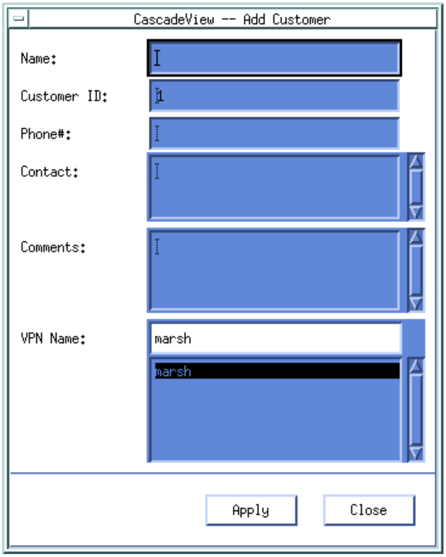


Figure 4-17. Add Customer Dialog Box

3. Complete the required dialog box fields described in Table 4-9

Table 4-9. Add Customer Fields

Field	Action/Description
Name	Enter a customer name.
Customer ID	CascadeView/UX assigns the customer ID.
Phone#	Enter the phone number.
Contact	Enter the contact name.
Comments	Enter any additional comments.
VPN Name	Select the VPN to which this customer belongs.

4. Choose Apply. 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 HP OpenView database, 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** and press Return.
6. Type the root password.
7. To shut down HP OpenView services, enter:

   /usr/OV/bin/ovstop <Return>

> *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 commands 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 y/n” prompt, press Return.

The system displays the following message:

```
Configuring CascadeView Environment.

Install CascadeView successful...
```

The system recreates the cascview environment. You now have a clean 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 its switch object. You will learn how to configure the NMS and the first switch to which it connects (*gateway switch)*. These steps are similar regardless of the type of network service (e.g., Frame Relay, ISDN, or SMDS).

> *If you are using ISDN for your network service, refer to* Configuring ISDN Services for B-STDX/STDX.

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

- ☑ Create a network map (page 4-5)
- ☑ Create a subnet ID (page 4-11)
- ☑ Add a Cascade switch to the network map (page 4-15)

About the NMS and Gateway Switch

You must configure one switch in the network as the *gateway switch* for routing management-protocol requests and responses to the NMS. The NMS accesses all other switches in the network through this gateway switch. The NMS can then control and monitor all other 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 5-26.

About RIP Routing State and Send Host Route

Routing is the task of finding a path from a sender to a desired destination and sending information. Routing Information Protocol allows hosts and gateways to exchange information for computing routes through the network.

> *The NMS server system must be running Routed software in order for RIP to function. Routed is a UNIX-network routing daemon used to maintain up-to-date kernel routing table entries.*

The RIP feature enables the switch to send/receive RIP packets to/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 a failure 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 State on the gateway switch only. You can set the RIP State parameters to *On/Off* to enable and disable the RIP state. 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 5-21 for instructions on configuring the RIP parameters.

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

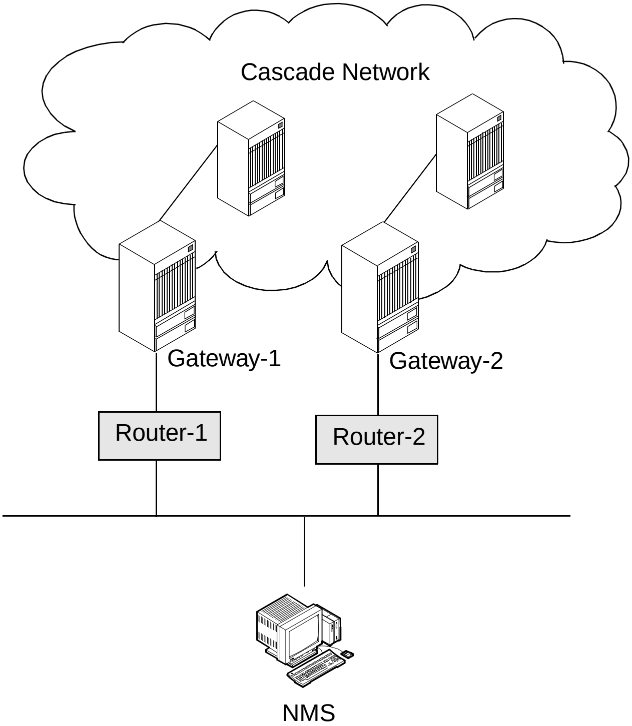


Figure 5-1. Routing Information Protocol Example

About Reroute Tuning

The *Reroute Tuning* 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 option enables you to tune the rate of reroute requests per switch. Reroute tuning defines the number of reroute requests 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. You must enable this parameter for circuits to benefit from the tuning parameters you define for a switch. For more information about reroute balance, refer to Chapter 11.

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 cards, each with 50 PVCs, and you set the reroute count to five (5) and the reroute delay to fifty (50) seconds, the switch performs a batch reroute, consisting of the first five circuits on each card (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 ten 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.

Setting Authentication Parameters

Console authentication is a domain security feature that is handled by the Remote Access Dial-in User Service (RADIUS) protocol. It is used to authenticate users connecting to a Cascade switch console port via remote dial-up and Telnet access.

RADIUS Authentication Requirements

In order for RADIUS authentication to take place, you must have an active RADIUS Server that the switch can reach via UDP/IP. If you can not 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 also use the shared secret password for 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 (password) 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 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 server parameters, use the following steps:

1. Select a switch and from the Administer menu, select Cascade Parameters ⇒ Set Authentication Domains. The Set All Authentication Domains dialog box appears as shown in Figure 5-2.

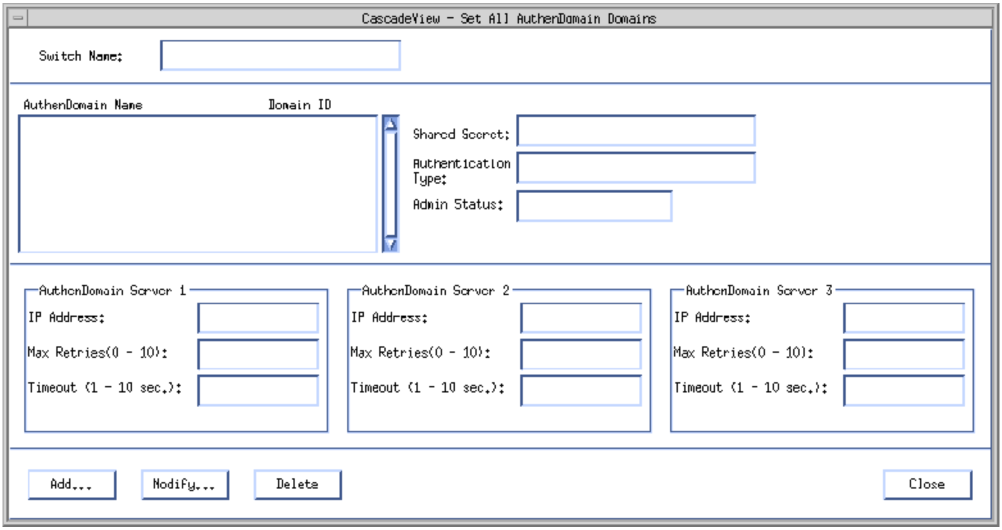


Figure 5-2. Set All Authentication Domains Dialog Box

2. Choose Add. The Add Authentication Domain dialog box appears as shown in Figure 5-3.

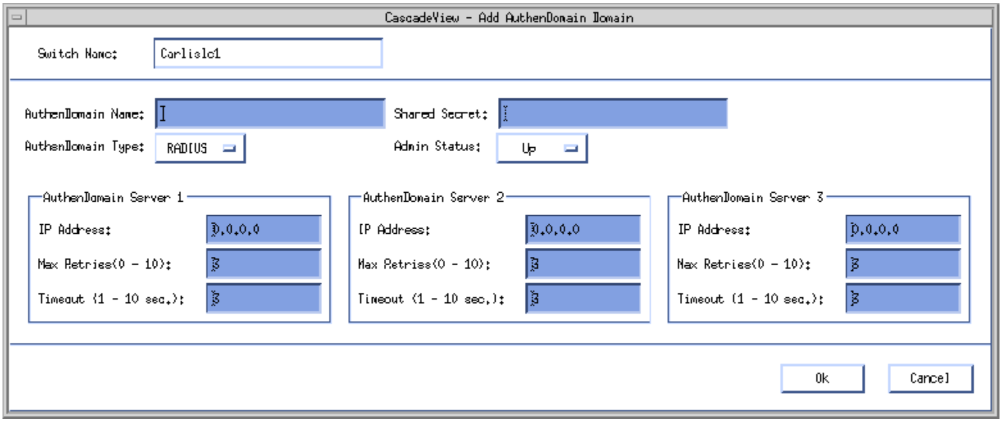


Figure 5-3. Add AuthenDomain Dialog Box

3. Complete the required dialog box fields described in Table 5-1.

Table 5-1. Add AuthenDomain Fields

Field	Action/Description
AuthenDomain Name	Enter an alphanumeric name for this domain. The name can be up to 32 characters in length.
AuthenDomain Type	Defaults to RADIUS and cannot be changed.
Shared Secret	Enter an alphanumeric shared secret (password) for this switch and all RADIUS Servers in this domain.
Admin Status	Set the Admin Status to *Up* to allow immediate access. Set the Admin Status to *Down* to disable the server. This does not disable console authentication.

4. Complete the AuthenDomain Server fields for Server 1, 2, and 3 as described in Table 5-2.

Table 5-2. AuthenDomain Server Fields

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 makes to authenticate this user. The default is three (3) retries.

Table 5-2. AuthenDomain Server Fields (Continued)

Field	Action/Description
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 retrying the request or sending the request to the next server. The default is three (3) seconds.

5. Choose OK to set the authentication parameters. The Set All AuthenDomain dialog box reappears.

6. Choose Close to return to the network map.

7. (*Optional*) Enable the authentication parameters as described in "Enabling Console Authentication" on page 5-25.

The B-STDX Switch Back Panel Dialog Box

The Switch Back Panel dialog box (Figure 5-4) displays a B-STDX switch back panel from which you can:

- Access switch attributes, PRAM functions, and physical and logical port attributes
- Configure each slot with the appropriate I/O module and configure physical ports.

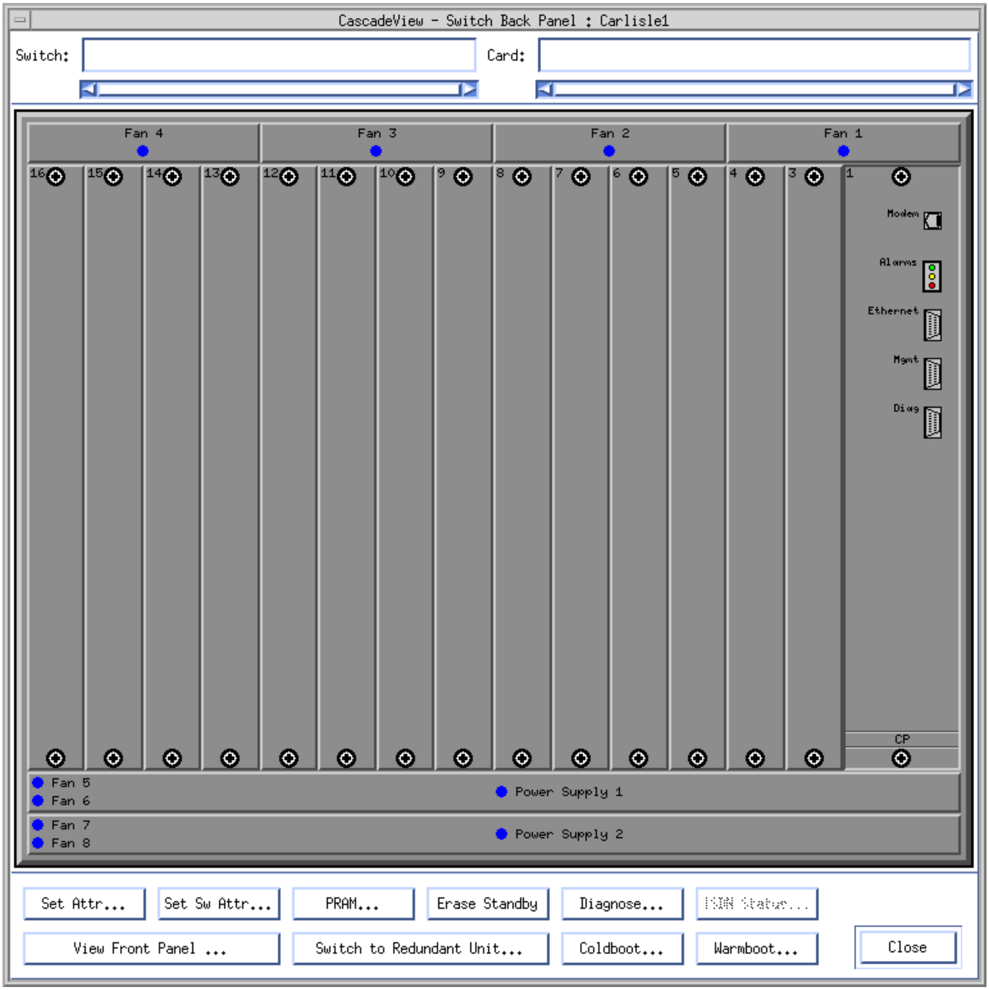


Figure 5-4. Switch Back Panel Dialog Box

The Switch Back Panel dialog box varies according to the type of switch (this example shows a sample B-STDX 9000 configuration). The Switch Back Panel dialog box displays the following command buttons described in Table 5-3 and Table 5-4.

Table 5-3. Switch Back Panel Command Buttons

Command	Function
Set Attr	Enables you to configure an I/O module for the selected slot. For more information about configuring I/O modules, refer to "Configuring B-STDX 8000/9000 I/O Modules and Redundancy" on page 6-4.
Set Sw Attr	Enables you to set the switch attributes, including the local IP address of the switch. Refer to "The B-STDX Switch Back Panel Dialog Box" on page 5-9.
View Front Panel	Displays the front panel of the switch. Refer to page 5-14 for more information.
Switch to Redundant Unit	Passes operation changes from an active I/O module to a redundant standby module. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information.

Table 5-4 describes the commands and functions you can access when the CP module (Slot 1) is selected.

Table 5-4. Switch Back Panel Commands and functions

Command	Function
PRAM	Cascade switches use battery backed-up PRAM to store switch configuration files. When you download a configuration file from the NMS to the switch, the NMS generates an initialization script. This file contains the SNMP SET commands that control the switch's configuration. Use the PRAM command to access one of the following functions: *Synchronize PRAM* – If the switch already contains a configuration file, use this command to send an updated binary image of the configuration to the selected I/O module. *Erase PRAM* – Use this command to clear a configuration file from PRAM. Use Erase PRAM before you replace an existing configuration file. *Upload PRAM* – Sometimes a switch can be "out of synch" because the switch configuration file and the database configuration in the NMS do not match. Use this command to upload the switch configuration file stored in PRAM to the NMS. This feature is currently supported only for SMDS services. *Generate PRAM* – This command generates set commands to configure PRAM but does not upload the switch configuration file to the NMS. This allows you to view the file before uploading it. (Refer to "Synchronizing a B-STDX 8000/9000 Switch" on page 12-18 for more information about PRAM functions.)

Table 5-4. Switch Back Panel Commands and functions (Continued)

Command	Function
Erase Standby	Erases the configuration and switch software on the standby card. The configuration and switch software are then copied from the active card to the standby card.
Diagnose	Enables you to access diagnostics for a selected module. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information on diagnostics.
ISDN Status	Displays the Show ISDN Status dialog box. This dialog box shows the call status and alarm status of all 4 ports on an ISDN card. This option is only available when you select a slot containing an ISDN card.
Coldboot	Restarts the switch as if it were powered off, then on.
Warmboot	Resets the selected module. As it reboots, all physical ports, logical ports, and PVCs on the module stall for approximately 20-30 seconds.

Switch Back Panel Status LEDs

Table 5-5 describes the operating status indicators on the Switch Back Panel dialog box, which indicate the operational status of fans and power supply units.

Table 5-5. Back Panel Status LEDs

LED Color	Indicates
Green	Fan or power supply unit is operational.
Red	Fan or power supply unit is not operational.
Blue	NMS cannot access a fan or power supply unit for status.

Switch Back Panel Port Colors

Table 5-6 describes the physical port colors, which indicate port operational status.

Table 5-6. Back Panel Port Colors

Port Color	Indicates
Gray	Port is unknown. This condition usually occurs if the configuration has not been downloaded or if the configurations in the NMS and PRAM do not match.
Green	Port is accurately configured and operational.
Red	Port is configured but has an admin status of Down and/or an operational status of Down.

Switch Back Panel Card Colors

Table 5-7 describes the B-STDX 8000/9000 card colors, which indicate card operational status.

Table 5-7. Back Panel Card Colors

Card Color	Indicates
Red	Card is bad or not present.
Yellow	Card may be in a marginal state or “out of sync”.
Gray	Card is operational.

Switch Front Panel Indicators

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

To display the Show Switch Front Panel dialog box, choose View Front Panel from the Switch Back Panel dialog box. The Show Switch Front Panel dialog box appears as shown in Figure 5-5.

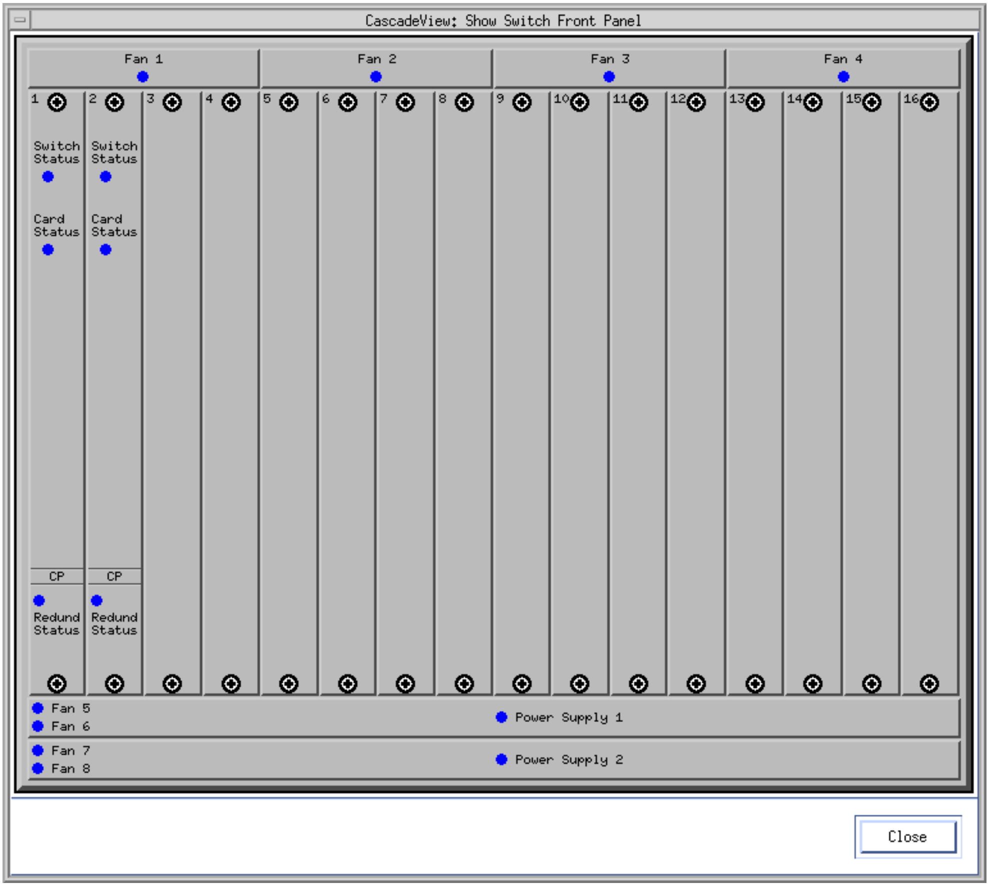


Figure 5-5. Show Switch Front Panel Dialog Box

As with the back panel, status LEDs indicate the operational status.

Show Switch Front Panel LEDs

Table 5-8 describes the front panel status LED indicators.

Table 5-8. Switch and Card Status LEDs

LED Color	Indicates
Green	Module is operational.
Red	Module is not operational.
Blue	NMS cannot access the unit for status.Used on the STDX 3000/6000 Packet Processor (PP), the B-STDX 8000/9000 Control Processor (CP), and on fan and power supply units.
Yellow	Switch is “out of sync”, or the switch reports a card type mismatch or a marginal state.

Alarm Status LEDs

The number and type of alarms differ depending on the type of module. Refer to Table 5-9 for a complete description of alarm LEDs.

Table 5-9. Alarm Status Light Indicators

LED Color	Indicates
No LED	No alarm conditions on the 4-port T1/E1, 10-port DSX, Channelized DS3, HSSI, or ATM DS3 cards.
Red	Red alarm condition.
Yellow	Yellow alarm condition.

The STDX Switch Back Panel Dialog Box

To access the Switch Back Panel dialog box for an STDX 3000/6000:

1. Select the switch object. The selected object appears highlighted.

> *If you are not logged on, select a switch and from the Misc menu, select CascadeView ⇒ Logon. Enter your operator password.*

2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for the selected switch as shown in Figure 5-6. Refer to page 5-10 for a description of the Switch Back Panel dialog box commands.

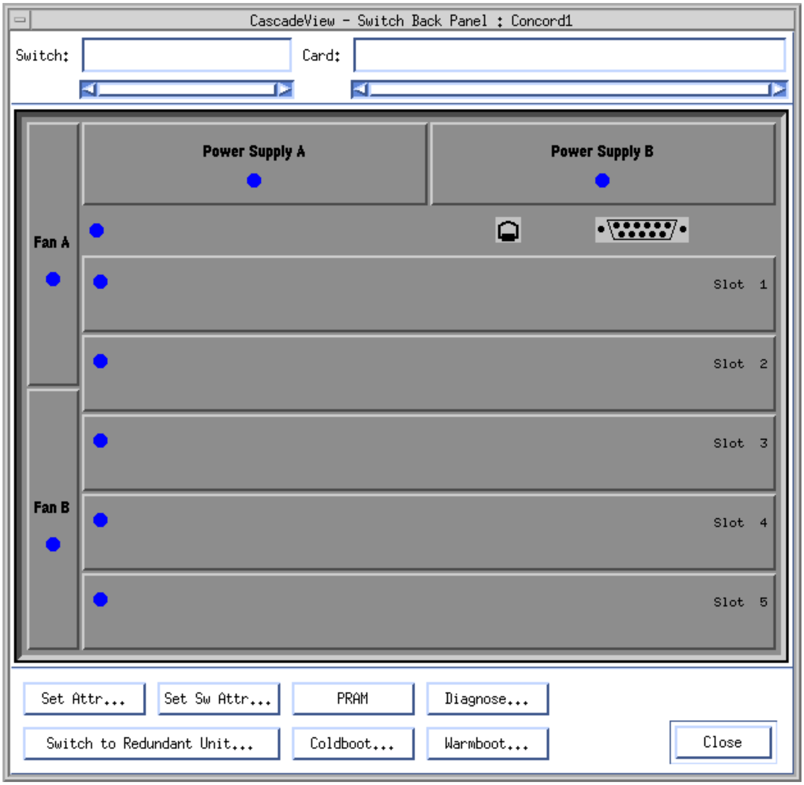


Figure 5-6. STDX Switch Back Panel Dialog Box

Before You Begin

Before you begin, you need the following information:

- The local IP address of the gateway switch
- The SNMP community name specified in the *cascadeview.cfg* file in */opt/CascadeView/etc*
- The IP address of the SPARCstation (for serial connections)
- 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. Set the switch attributes

Step 2. Define the circuit reroute tuning parameters (refer to page 5-24)

Step 3. Define the console authentication parameters (refer to page 5-5)

Step 4. Define an additional NMS, if necessary (refer to page 5-26)

Step 5. Configure the IP address and access attributes for the NMS or IP host (refer to page 5-29)

Step 6. Configure the control processor (CP) module (refer to page 5-33)

Setting Switch Attributes

You can set the following attributes for each switch as shown in Figure 5-7.

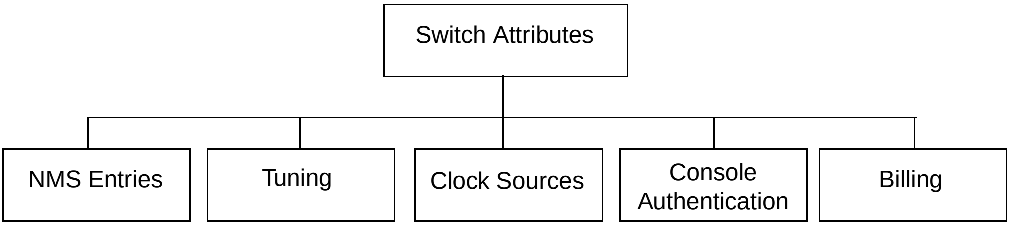


Figure 5-7. Switch Attributes

To set the switch attributes:

1. Start CascadeView/UX and access the network map.

2. Select the switch object and from the Misc menu, select CascadeView ⇒ Logon. Enter your operator password.

3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for the selected switch (see Figure 5-4 on page 5-9).

   The steps for defining the switch parameters for a B-STDX 9000 or STDX 3000/6000 switch are similar.

4. To configure switch parameters, choose Set Sw Attr. The Set Switch Attributes dialog box appears as shown in Figure 5-8.

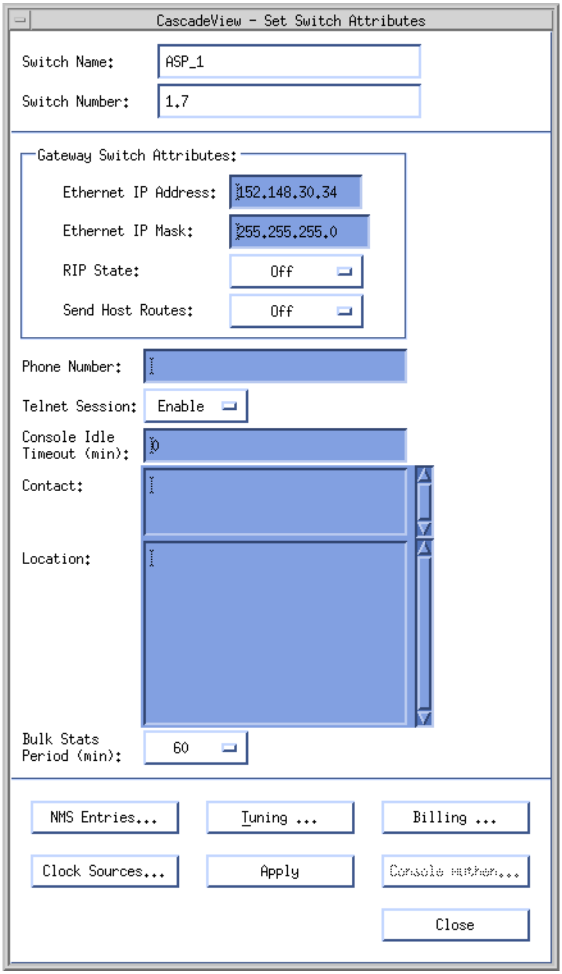


Figure 5-8. Set Switch Attributes Dialog Box

This dialog box displays the switch name (assigned to 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.

5. Do one of the following:

- If this is a gateway switch, complete the Gateway Switch Attributes fields in the Set Switch Attributes dialog box as described in Table 5-10.
- If this is not a gateway switch, proceed to Step 6.

Table 5-10. Set (Gateway) Switch Attributes Fields

Field	Action/Description
Ethernet IP Address	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. ***Note**: You only need to enter the Ethernet IP address for the switch or switches that have an Ethernet connection and will communicate with the NMS via this connection.*
Ethernet IP Mask	Enter the inband (Ethernet) IP mask for this switch. The default is 255.255.255.0.
RIP State	Set the RIP State parameters. The RIP feature enables the switch to send/receive RIP packets to/from all routers in the network and pass route information to each destination (switch) in the network. *Off (default)* – Disables RIP. *On* – Enables the switch to process received RIP packets and send RIP updates to routers connected to the Ethernet.
Send Host Routes	Set the Send Host Routes parameters. The Send Host Routes field determines the RIP packet contents sent by the gateway switch. *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.

6. Complete the required dialog box fields described in Table 5-11.

Table 5-11. Set Switch Attributes Fields

Field	Action/Description
Phone Number	Enter the phone number of the contact person responsible for switch operation.
Telnet Session	The default, *Enable*, allows the switch to accept a remote terminal connection for troubleshooting purposes. Cascade recommends that you do not disable this function.
Console Idle Timeout (min)	Specify the time period (in minutes) of console inactivity before the console is logged off. The default is 5 minutes.
Contact	Enter the name of the contact person responsible for operating the switch.
Location	Enter the switch's location.
Bulk Stats Period (min)	Specify the bulk statistics collection interval (in minutes). The base collection period length is stored in each translated statistics record. A setting of zero disables collection from the switch. Options include: 60 (*default*) 30 20 15 5 0

7. *(Optional)* To define parameters that enable the NMS to balance circuits between switches, choose the Tuning command on this dialog box. Refer to "Defining Circuit Reroute Tuning Parameters" on page 5-24 for more information.

8. *(Optional)* If you are using the Cascade Billing feature, choose Billing to define additional parameters. Refer to the *SMDS Billing System Administrator's Guide* for more information.

9. *(Optional)* To define additional NMS workstations, choose NMS Entries and continue with "Defining Additional Network Management Stations" on page 5-26.

10. (*Optional*) To define the clock source on an ATM CS or ATM IWU module, choose Clock Sources and continue with "Defining the Clock Source for ATM CS and ATM IWU Modules" on page 6-64. You must first configure an ATM CS or ATM IWU module in the switch before you set the clock source (Refer to "Configuring B-STDX 8000/9000 I/O Modules and Redundancy" on page 6-4 for more information).

11. *(Optional)* To set password protection for the switch, choose the Console Authen command and continue with "Enabling Console Authentication" on page 5-25. Console authentication allows you to assign a password (other than "cascade") to each switch.

12. When you are finished with this screen, choose Apply to set the parameters and choose Close to exit the dialog box.

13. Proceed to "Configuring the IP Address" on page 5-29.

Defining Circuit Reroute Tuning Parameters

To set the tuning parameters:

1. From the Set Switch Attributes dialog box, choose Tuning. The Set Switch Tuning Attributes dialog box appears as shown in Figure 5-9.

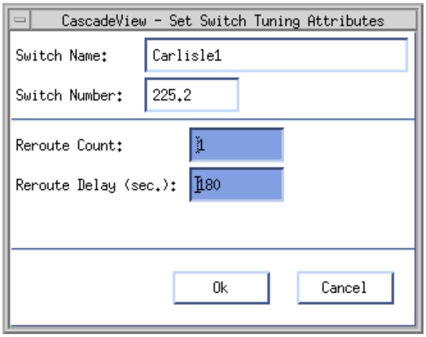


Figure 5-9. Set Switch Tuning Attributes Dialog Box

2. Complete the required dialog box fields described in Table 5-12.

Table 5-12. Set Switch Tuning Attributes Fields

Field	Action/Description
Reroute Count	Enter a value between 0 and 64. The reroute count represents the number of circuits from each card that can issue reroute requests in a single batch. The default is one (1). For more information, refer to “About Reroute Tuning” on page 5-4.
Reroute Delay	Enter a value between 1 and 32767. The reroute delay represents the time delay (in seconds) that each card in the switch waits between reroute batch requests. This parameter controls the rate at which each card polls the virtual circuits for a better route. The default value of 188 seconds is a very conservative setting for normal operation. For more information, refer to “About Reroute Tuning” on page 5-4.

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

4. *(Optional)* To define additional NMS workstations to have access to the gateway switch, continue with "Defining Additional Network Management Stations" on page 5-26.

5. When you are finished, choose Apply to set the parameters and choose Close to exit the dialog box.

6. Proceed with "Configuring the IP Address" on page 5-29.

Enabling Console Authentication

On the Set Switch Attributes dialog box, you can access the Console Authentication command to enable and disable authentication on a switch that you added in "Adding an Authentication Domain" on page 5-5.

To enable/disable the authentication parameters, use the following steps:

1. From the Set Switch Attributes dialog box (see Figure 5-8 on page 5-20), choose *Console Authen*.The Console Authen dialog box appears as shown in Figure 5-10.

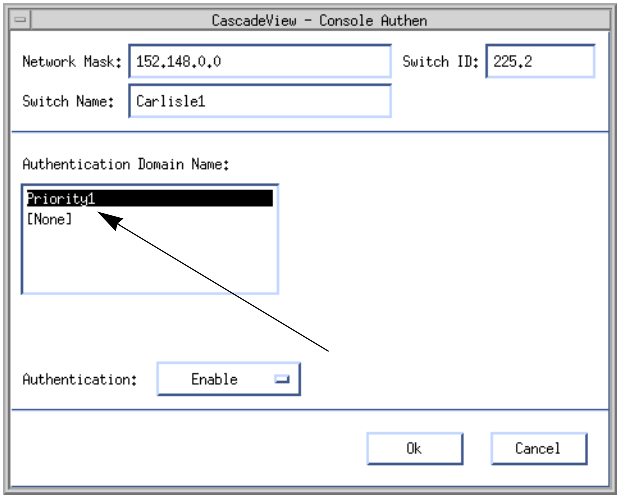


Figure 5-10. Console Authen Dialog Box

The Authentication Domain Name list box displays all configured authentication domain names.

2. Select a domain from the list.

3. Set the Authentication parameter to Enable to enable authentication or Disable (default) to diable authentication.

4. Choose OK to set the authentication parameters. The Set Switch Attributes dialog box reappears.

Defining Additional Network Management Stations

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

The Cascade switch supports a maximum of 16 NMS entries and 32 NMS paths.

As you configure additional switches on your network map, use the Set Switch Attributes command to enter an Ethernet IP address if applicable. Always leave the Telnet Session parameter enabled, so that each switch can accept remote terminal connections for troubleshooting purposes.

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, use the following steps:

1. From the Set Switch Attributes dialog box (Figure 5-8 on page 5-20), choose NMS Entries. The Set NMS Entries dialog box appears, displaying the current NMS entries as shown in Figure 5-11.

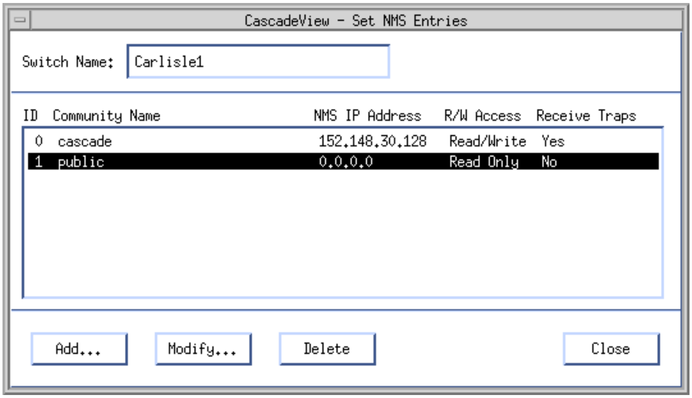


Figure 5-11. Set NMS Entries Dialog Box

2. Choose Add. The Add NMS Entry dialog box appears as shown in Figure 5-12.

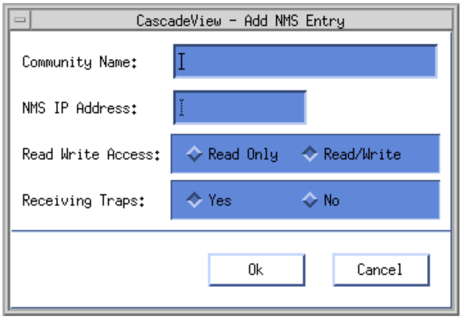


Figure 5-12. Add NMS Entry Dialog Box

3. Complete the required dialog box fields described in Table 5-13.

Table 5-13. Add NMS Entry Fields

Field	Action/Description
Community Name	Enter the community name. ***Note***: *If you need to modify the Community Name, you must first modify this dialog box and then edit the value* CV_SNMP_READ_WRITE_ COMMUNITY *in the cascadeview.cfg file.*
NMS IP Address	Enter the NMS IP address for the target NMS workstation.
Read Write Access	Select the access rights for this NMS. *Read Only* – Allows you to monitor network functions from this NMS. *Read/Write* – Allows you to monitor and configure network maps from this NMS.
Receiving Traps	Select the default, *Yes*, to enable the NMS to receive traps. Trap alarm conditions notify the operator of events taking place on the switch.

4. Choose OK. Repeat Step 1 through Step 3 for each NMS.
5. (*Optional*) Choose Modify to modify an NMS entry, or Delete to delete an NMS entry.
6. Choose OK to set the parameters.

Configuring the IP Address

The Set NMS Path function enables you to configure the IP address and access attributes for the NMS workstations. If you do not specify the NMS IP address, the NMS cannot configure a switch or receive switch status information.

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

Serial (SLIP) — The NMS workstation connects to the switch’s serial Network Management port on either the Packet Processor (PP) (STDX 3000/6000) or Control Processor (CP) (B-STDX 8000/9000) module. The NMS IP address must be the same as the workstation IP address. Serial (SLIP) is not supported on a UNIX workstation.

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

Indirect Ethernet — This connection indicates that the NMS and the switch's Ethernet IP address are on two separate LANs and communicate via a gateway router(s). For this connection method, you 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 in “Creating the Network Map” on page 4-6.

Management DLCI — This connection is used when the NMS connects to a LAN that contains a router with a Frame Relay connection to the switch. The switch does not need an Ethernet module in the PP or CP for this type of NMS connection. Network traffic is tunneled through the attached Frame Relay UNI-DCE connector as a PVC.

If you plan to use Management DLCI, refer to “Accessing Logical Port Functions” on page 7-14 to define the logical ports for a Frame Relay network. Then refer to “Configuring Point-to-Multipoint Circuits” on page 11-57.

Management Address (SMDS In-band Management) — This connection indicates that the NMS is connected remotely to the Cascade network using SMDS services to transport the SNMP/UDP/IP protocol packets.

> *If you plan to use SMDS In-band Management, refer to Chapter 8 to define the logical ports for an SMDS network. Then refer to "Configuring Management DLCIs" on page 11-76.*

Setting the NMS Path

To set the NMS path, use the following steps:

1. On the network map, select the switch to connect to the NMS.
2. From the Administer menu, select Cascade Parameters ⇒ Set NMS Paths. The Set NMS Paths dialog box appears as shown in Figure 5-13.

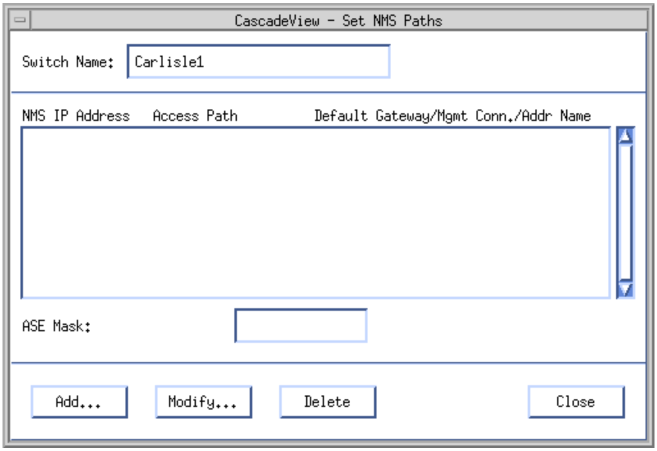


Figure 5-13. Set NMS Paths Dialog Box

3. Choose Add. The Add NMS Path dialog box appears as shown in Figure 5-14.

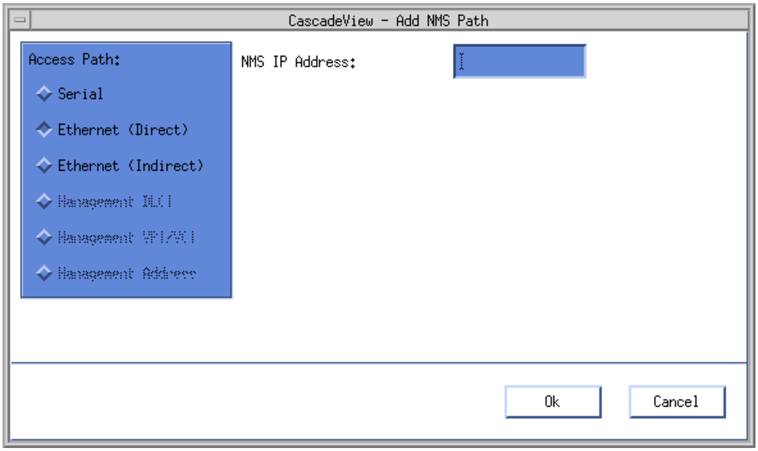


Figure 5-14. Add NMS Path Dialog Box (Direct Ethernet)

4. Complete the Add NMS Path dialog box fields, as follows:

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

   b. Enter the NMS IP address. This should be the IP address of the SPARCstation.

   c. The following fields appear depending on the type of connection you select:

      Ethernet (Indirect) — In the Default Gateway IP Address field, enter the IP address of the gateway router that connects the NMS to the switch.

      Management VPI/VCI — Refer to the *CBX 500 Network Administrator's Guide* for more information.

      Management DLCI — In the Management DLCI Name field, select the name of the Management DLCI. If you plan to use Management DLCI, refer to Chapter 7 to define the logical ports for a Frame Relay network. Then refer to "Configuring Management DLCIs" on page 11-76.

      Management Address — In the Management Port Name field, select the name of the logical port that has the In-Band Management Address defined. If you plan to use a Management Address, refer to Chapter 8 to define the logical ports for SMDS. Then refer to Table 11-24 on page 11-80.

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

5. Choose Close to return to the network map.

Deleting a Switch Configuration from the Database

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

To delete a switch configuration from the database, use the following sequence**.**

Step 1. Delete all PVCs defined for the switch.

Step 2. Delete all trunk connections for the switch.

Step 3. Delete all logical ports and physical ports on the switch.

Step 4. Delete all I/O module configurations on the switch.

Step 5. Delete the switch icon from the map.

Configuring the CP Module for the B-STDX

When you first install a B-STDX 8000/9000 switch, you must configure the CP module in Cascadeview. You can also configure a *redundant standby module* for the CP module.

To configure the CP module, use the following steps:

1. On the network map, select the switch object.

> *If you are not logged on, select a switch object and select CascadeView ⇒ Logon from the Misc menu. Enter your operator password.*

2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears as shown in Figure 5-15, showing the back panel of the selected switch.

> *Refer to "The B-STDX Switch Back Panel Dialog Box" on page 5-9 for information about functions contained on this dialog box.*

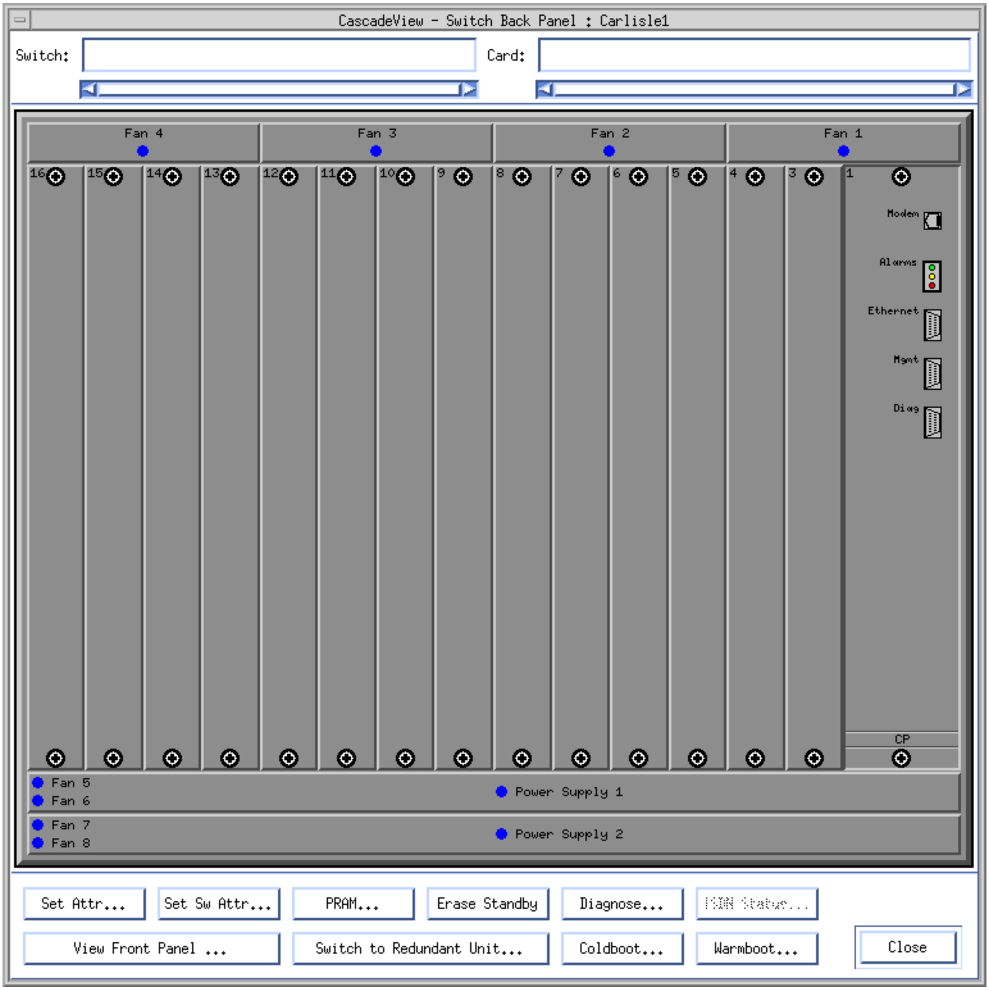


Figure 5-15. Switch Back Panel Dialog Box

Slots 1 and 2 are reserved for the main CP module and the optional redundant CP. Slot 1 is always configured with the main CP module.

3. Select the CP module (slot) you want to configure and choose Set Attr. The Set Card Attributes dialog box appears as shown in Figure 5-16.

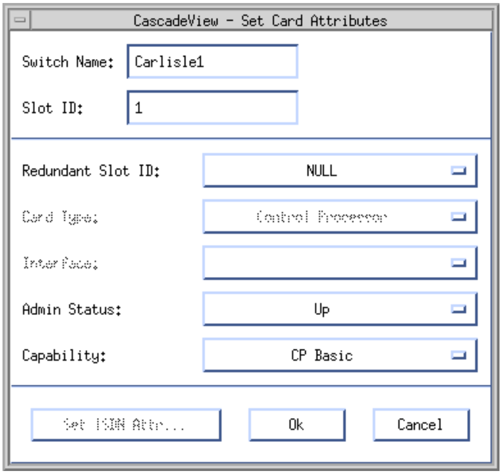


Figure 5-16. Set Card Attributes Dialog Box

4. Complete the required dialog box fields described in Table 5-14.

Table 5-14. Set Card (CP Card) Attributes Fields

Field	Action/Description
Redundant Slot ID (*Optional*)	To configure a redundant CP, select the Redundant Slot ID 2. You must always configure the main CP in Slot 1. The default, NULL, indicates there is no redundant CP module installed.
Card Type	This read-only field automatically defaults to Control Processor.

Table 5-14. Set Card (CP Card) Attributes Fields (Continued)

Field	Action/Description
Admin Status	Set this field as follows: *Up (default)* – This CP becomes fully operational when you start the switch. *Down* – This CP does not come online when you start the switch. This setting saves the configuration in the database but does not download it to the switch. Use this option when you run foreground diagnostics.
Capability	Set this field as follows: *CP Basic* – This CP module has a black dip switch located on the front panel. It is often used in both the B-STDX 8000 and 9000 models. *CP Plus* – This CP module has a red dip switch located on the front panel. It has more memory than the CP Basic and can be used in either B-STDX model. This CP type is required for the SMDS Billing application. ***Note****: If you do not know the CP type and cannot physically view it, you can use the show card or show system console commands to retrieve this information. Refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for a list of console commands.*

Table 5-14. Set Card (CP Card) Attributes Fields (Continued)

Field	Action/Description
Capability (continued)	The CP 30, 40, and 50 use a 170 MB internal disk and each supports a different amount of memory. You must be running switch code Version 4.2 or higher before you configure the CP 30, 40, or 50. For more information on installing these CP cards, refer to the *B-STDX 8000/9000 Hardware Installation Guide.* *CP 30* – This CP module replaces the CP Basic and has 16 MB IRAM. *CP 40* – This CP module replaces the CP Plus and has 64 MB memory for IP routing. *CP 50* – This CP module replaces the CP Plus and has 128 MB memory for IP routing. ***Note**: Do not select CP 30, 40, or 50 until you replace both the active and standby CP modules. Use the following selections:* *CP 30 – Select CP Basic* *CP 40 and 50 – Select CP Plus* *For example, if the active CP module is a CP Plus and the redundant CP module is a CP 40, select CP Plus for both modules.*

5. Choose OK. The Switch Back Panel dialog box reappears, displaying the configured CP module.

   If you selected a redundant configuration, the two slots appear as a single configuration that occupies the space of two slots. (To determine which is the active module, click on the slot ID; the status line at the top of the dialog box indicates the active module.)

6

Configuring I/O Modules

This chapter describes how to configure each I/O slot with the appropriate I/O module in the switch. For each I/O module, you must configure its physical port parameters, which determine how a port handles clock source and clock rate. This chapter also describes how to set up a redundant configuration.

Before you configure I/O modules, verify the following tasks are complete:

- ☑ Set switch attributes (page 5-18)
- ☑ (*Optional*) Define the circuit reroute tuning parameters (page 5-24)
- ☑ Define an additional NMS, if necessary (page 5-26)
- ☑ Configure the IP address (page 5-29)
- ☑ Set the NMS path (page 5-30)
- ☑ Configure the control processor (CP) module for a B-STDX 8000/9000 (page 5-33)

Configuring STDX 3000/6000 I/O Modules

To configure I/O modules for an STDX 3000 or 6000:

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 Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears, displaying the back panel of the selected switch. Figure 6-1 shows an STDX 6000.

   Refer to "The STDX Switch Back Panel Dialog Box" on page 5-17 for more information about the commands and functions you can access on this dialog box.

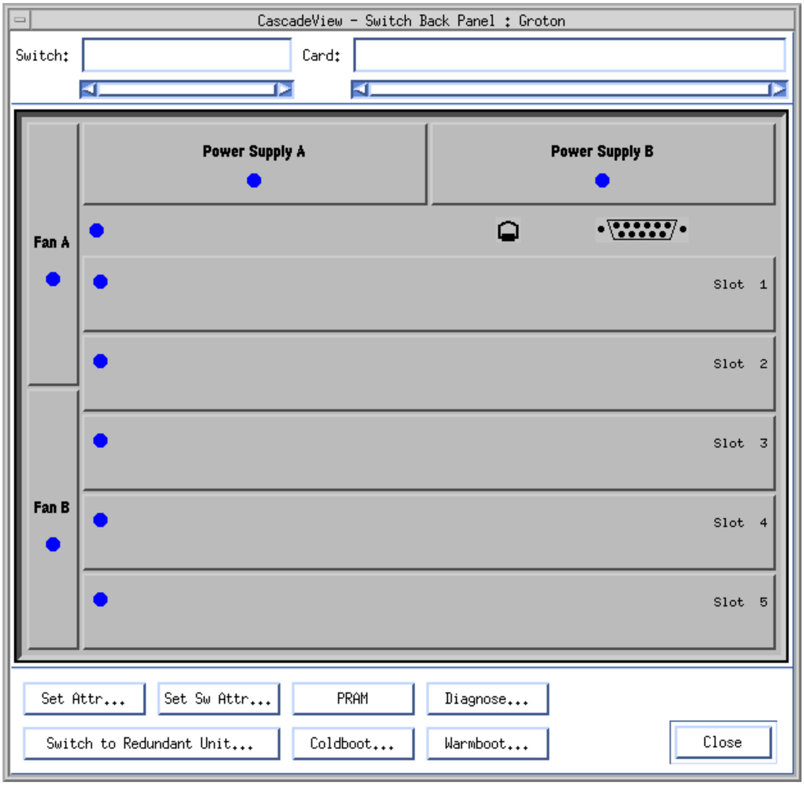


Figure 6-1. Switch Back Panel (STDX 6000)

3. Select (double-click) the I/O module (slot) you want to configure. Note that the top slot is reserved for the Packet Processor (PP) module.

   The Set Card Attributes dialog box appears, displaying the switch name and slot ID as shown in Figure 6-2.

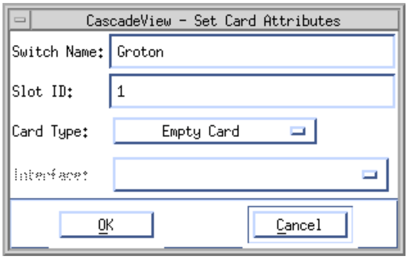


Figure 6-2. Set Card Attributes Dialog Box

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

Table 6-1. Set Card Attributes Fields (STDX 6000)

Field	Action/Description
Card Type	Select the type of I/O module installed in this slot.
Interface	Select the interface for the module. For a 1-port 30 channel E1 module, select either coaxial pair 75 ohm or DB15 120 ohm. For a 6-port Universal I/O module, select V.35, EIA 449, X.21, EIA 530, or EIA 530A. For 8/18 port Universal I/O modules, select either V.24 or X.21.

5. Choose OK. The Switch Back Panel dialog box reappears, displaying the configured I/O module.

6. Repeat Step 3 through Step 5 until you have defined all I/O modules for the selected switch.

Once you configure all the I/O modules in the switch, you can define the physical port parameters. Refer to "Configuring Physical Ports" on page 6-9.

Configuring B-STDX 8000/9000 I/O Modules and Redundancy

This section describes how to configure I/O modules for the B-STDX 8000/9000. It also describes how to configure a redundant module called *redundant standby partner.*

To configure I/O modules for a B-STDX 8000/9000:

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 Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears, displaying the back panel of the selected switch. Figure 6-3 displays a B-STDX 9000 back panel.

   Refer to "The B-STDX Switch Back Panel Dialog Box" on page 5-9 for information about commands and functions you can access on this dialog box.

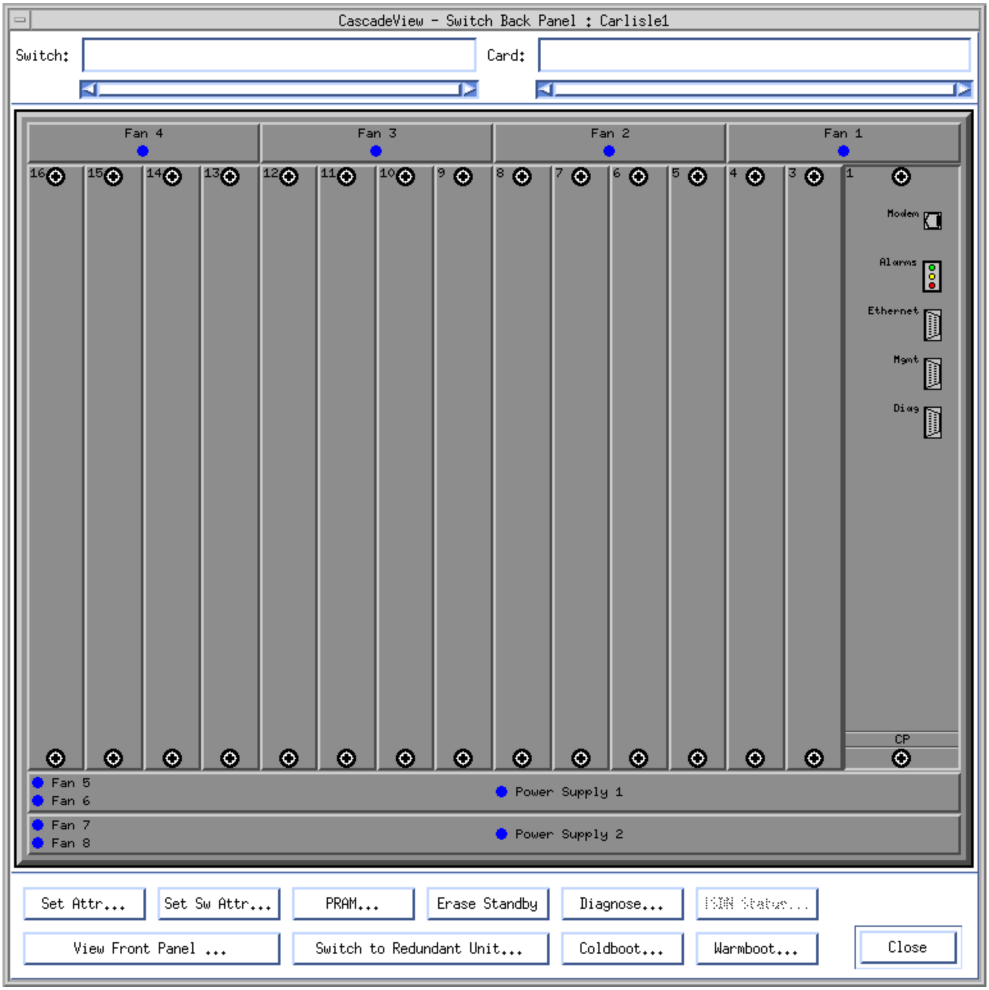


Figure 6-3. Switch Back Panel Dialog Box (B-STDX 9000)

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

3. Select (double-click) the I/O module (slot) you want to configure. The Set Card Attributes dialog box appears as shown in Figure 6-4, displaying the switch name and slot ID.

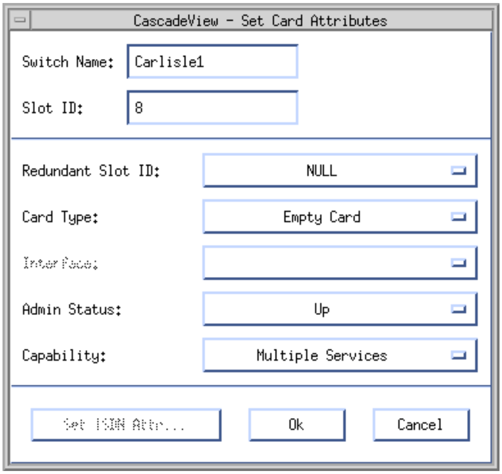


Figure 6-4. Set Card Attributes Dialog Box

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

Table 6-2. Set Card Attributes Fields (B-STDX)

Field	Action/Description
Redundant Slot ID (*Optional*)	Select the redundant slot ID if this I/O module is to have a redundant standby partner installed. You must install and configure the redundant module in the next higher slot (ID) adjacent to the primary module. For example, if the slot ID for this I/O module is 5, the redundant slot ID must be 6. A redundant slot ID of Null indicates no redundancy.

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

Field	Action/Description
Card Type	Select the type of I/O module you want to install in this slot. ***Note****: If you are installing an ATM CS or ATM IWU module, refer to "Defining the Clock Source for ATM CS and ATM IWU Modules" on page 6-64.*
Admin Status	Set this field as follows: *Up (default)* – The I/O module becomes fully operational when you start the switch. To become operational, the module gets its application code from the CP and loads its drivers. *Down* – The I/O module 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. This setting enables you to erase PRAM when a card is out of sync. *Maintenance* – The I/O module does not receive the application software when you start the switch. A module in this state only has its boot flash running; application code is not running. Use this setting to: • Reset PRAM for a module that was failing to boot due to invalid PRAM • Troubleshoot a hardware problem

5. You may have additional options to specify, depending on the Card Type you select. Complete the additional options as described in Table 6-3.

Table 6-3. Set Card Attributes Fields (B-STDX)

Field	Action/Description
Interface	Select the interface for the module. For an 8-port Universal I/O module, Options include V.35, EIA 449, and X.21 For a 10-port DSX-1 module, this field defaults to RJ48. For an ATM CS/IWU module select SONET or SDH.
Capability	Select either Frame Relay (for Frame Relay networking services only) or Multiple Service (to support Frame Relay, ATM, or SMDS networks). Refer to your hardware guide for information about which modules support multiple services. To configure ISDN services, refer to *Configuring ISDN Services for B-STDX/STDX*. Multiple Services is the default and cannot be changed for the following modules: • ISDN 4-port, 24-channel PRI T1 • 1-port, 28-channel DS3 • 2-port HSSI • 4-port Unchannelized T1/E1 • 1-port ATM UNI E3 • 1-port ATM CS/DS3 • 1-port ATM UNI DS3 • 1-port ATM IWU/OC3

6. Choose OK. The Switch Back Panel dialog box reappears, displaying the configured I/O module.

If you selected a redundant configuration, the primary and secondary slots appear as a single configuration and occupy the space of two slots. (To determine which is the active module, click on the slot ID; the status line at the top of the dialog box indicates the active module.)

7. Repeat Step 3 through Step 6 until you define all I/O modules for the selected switch.

When you finish setting the card attributes, define the physical port parameters. Refer to the next section, "Configuring Physical Ports".

Configuring Physical Ports

The physical port parameters specify how a port on an I/O module handles clock source and clock rate.

Before you begin, verify the card attributes are set as described in:

- ☑ "Configuring STDX 3000/6000 I/O Modules" on page 6-2.
- ☑ "Configuring B-STDX 8000/9000 I/O Modules and Redundancy" on page 6-4.

To configure the I/O module physical ports, use the following steps:

1. On the network map, select the switch object that contains the physical port.

> *If you are not logged on, select a switch and select CascadeView ⇒ Logon from the Misc menu. Enter your operator password.*

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

3. To select the physical port, select (double-click) the port you want to configure. The Set Physical Port Attributes dialog box appears. The attributes vary according to the type of I/O module you select. Figure 6-5 displays the dialog box for an 8-port Universal I/O module.

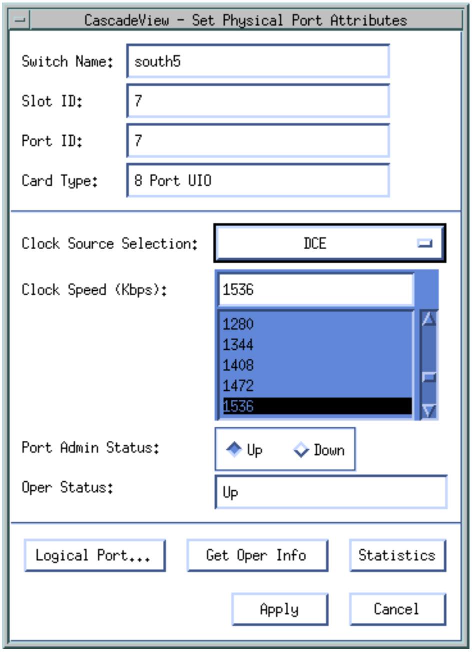


Figure 6-5. Set Physical Port Attributes Dialog Box (8 Port UIO Module)

The Set Physical Port Attributes dialog box displays the following fields described in Table 6-5.

Table 6-4. Set Physical Port Attributes Fields

Field	Description
Switch Name	The name of the switch in which the module resides.
Slot ID	The I/O slot (number) in which the module resides.
Port ID	The port (number) you are configuring.
Card Type	The type of card you are configuring.

Table 6-5 describes the commands and functions you can access on the Set Physical Port Attributes dialog box. It also describes card specific commands may appear, depending on the selected card type.

Table 6-5. Set Physical Port Attributes Dialog Box Commands

Command Button	Function
Logical Port	Enables you to configure logical ports for this physical port.
Get Oper Info	Displays a brief status for the selected physical port in the Oper Status field.
Statistics	Displays the summary statistics for the selected physical port. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Apply	Applies changes to the configuration.
Cancel	Exits the dialog box without applying changes.
Card Specific Commands	
DS3 Statistics	Displays link-performance statistics for the selected physical port. For more information about DS3 statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Chan Alarm Status	Displays the channel alarm status for all 28 channels. For more information about channel alarms, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Diagnose	Displays diagnostic test information for the selected physical port. For more information about diagnostics, refer to the *Diagnostic and*

Table 6-5. Set Physical Port Attributes Dialog Box Commands (Continued)

Command Button	Function
Set Chan Attr	Displays the Set Channel Attributes dialog box.
Verify Traffic Shaper	Determines whether or not the Shaper Priority, SCR, PCR, and/or Maximum Burst Size (MBS) values are acceptable (valid) values for the defined card. Normally, the value that you enter for SCRs and PCRs is different from the verified value since the NMS attempts to match the entered values to the closest value that is acceptable for the hardware.

4. To define specific physical port attributes, continue with the appropriate section for your type of I/O module:

– "Defining V.35 or Universal I/O Physical Ports" on page 6-13

– "Defining T1 and E1 Physical Ports" on page 6-18

– "Defining Channelized DS3 Physical Ports and Channels" on page 6-27

– "Defining 10-port DSX-1 Physical Ports" on page 6-38

– "Defining HSSI Physical Ports" on page 6-45

– "Defining ATM UNI DS3 and E3 Physical Ports" on page 6-51

– "Defining ATM Interworking Unit (IWU) Physical Ports" on page 6-56

– "Defining ATM Cell Switching (CS) Physical Ports" on page 6-61

Defining V.35 or Universal I/O Physical Ports

You can configure the physical port on the following types of Universal I/O (UIO) modules:

- 8-port
- 18-port
- 6-port UIO
- 6-port V.35

For more information, refer to Table 6-6 on page 6-14.

Before you configure a *V.35 physical port*, consider the following:

- The absolute maximum aggregate bandwidth for all V.35 ports is 16 Mbps (B-STDX 8000/9000 only).
- If the maximum port speed is 2.048 Mbps or less, you can specify any combination of port speeds. For example, 8 ports at 2.048 Mbps per port is a valid configuration. Although 8 ports configured at 2 Mbps is valid, Cascade recommends that you do not exceed 12Mbps total throughput for the UIO card.
- If the port speed is greater than 2.048 Mbps, but less than or equal to 4.096 Mbps, some configurations are based on port pairings as follows:
  - Port 1 shares hardware with port 2
  - Port 3 shares hardware with port 4
  - Port 5 shares hardware with port 6
  - Port 7 shares hardware with port 8

  As a result, if either port in any port pair is configured with more than 2 Mbps of bandwidth, its partner cannot be used or configured.
- If the port speed is greater than 4.096 Mbps, but less than or equal to 8.192 Mbps, you can only use two, nonadjacent numbered V.35 ports. For example, you can configure ports 1 and 3 at 8.192 Mbps, or port 2 at 8.192 Mbps and port 4 at 2.048 Mbps.

Table 6-6 lists the port speed, port capacity, interface, and services supported on each UIO module.

Table 6-6. Universal I/O Module Port Speed and Capacity

Module	Available on	Port Speed	Port Capacity	Frame Relay	SMDS	ATM
8-port	STDX 3000/6000	128 Kbps	V.24 X.21	Yes	No	No
18-port	STDX 3000/6000	128 Kbps	V.24 X.21	Yes	No	No
6-port V.35	STDX 3000/6000	4.096 Mbps	V.35	Yes	No	No
6-port UIO	STDX 3000/6000	4.096 Mbps	V.35 EIA 449 EIA 530 EIA530A X.21	Yes	No	No
8-port	B-STDX 8000/9000	8.192 Mbps	V.35 X.21 RS-449	Yes	Yes	Yes

You can configure an STDX 3000/6000 with up to 60 ports. As a result, you can install a maximum of three 18-port UIO modules in an STDX switch.

The STDX supports SMDS only on specific switch software releases. Contact the Cascade Technical Response Center or refer to the switch software release notes for more information.

About Clock Source

The Clock Source parameter determines how the physical port handles clocking. Table 6-7 describes the UIO clock source selections.

Table 6-7. UIO Clock Source Selections

Clock Source	Configures the port to ...
DCE	Provide clocking at the rate specified by the clock source selection. Select this option to connect to a DTE where the switch provides both the transmit and receive clock, and a straight-through cable is used. Use a crossover cable to connect to a physical DCE.
Loop-Timed DCE	Provide clocking at the configured speed. Loop-timed DCE provides the same timing as DCE except for the looped clock (transmit clock looped back to external transmit clock). Use this option for high speed applications and/or where cable length is excessive.
DTE	Receive clocking from an outside source, typically a CSU/DSU. However, you must set the clock speed, even though it is not clocking. Clock speed is required for logical port configuration.

To set up the clock signals for V.35 ports on a Cascade switch, note the following minimum requirements:

- If you configure clock source selection for DTE, verify the following clock signal inputs are received from the DCE:

W Transmit clock (-)	BB Receive clock (-)
U Transmit clock (+)	Z Receive clock (+)

- If you configure clock source selection for DCE, verify the following clock signal inputs are received from the DTE:

AA Transmit clock (-)	X Receive clock (-)
Y Transmit clock (+)	V Receive clock (+)

To define a V.35 or Universal I/O physical port, use the following steps:

1. Access the Set Physical Port Attributes dialog box as described in “Configuring Physical Ports” on page 6-9.

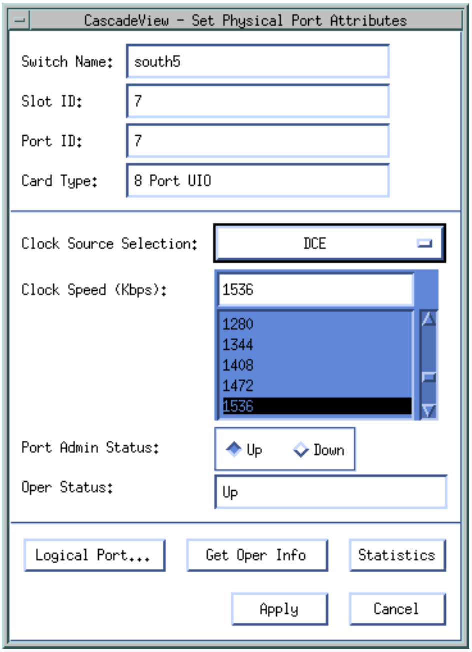


Figure 6-6. Set Physical Port Attributes Dialog Box

2. Complete the required dialog box fields described in Table 6-8.

Table 6-8. Set Physical Port Attributes Fields

Field	Action/Description
Clock Source Selection	Select the clock source for this physical port. Refer to "About Clock Source" on page 6-15 for detailed information. *DCE (default)* – Configures the port to provide clocking at the rate specified by the clock source selection. *Loop-Timed DCE* – Configures the port to provide clocking at the configured speed. *DTE* — Configures the port to receive clocking from an outside source, typically a CSU/DSU. *Direct Trunk* – Configures a switch-to-switch trunk.
Clock Speed (Kbps)	Select the clock speed to generate clock when the clock source is DCE, Loop-timed DCE, and Direct Trunk. If the clock source is DTE, the switch ignores this parameter for clocking purposes; however, you should set it for the actual clock rate since the cumulative total of all logical ports configured on the physical port cannot exceed the Clock Speed setting.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.

3. Choose Apply to save the physical port attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.

4. To define the logical port parameters that complete this configuration, refer to the appropriate chapter for your type of service.

- Chapter 7, “Configuring Frame Relay Services”.
- Chapter 8, “Configuring SMDS Services”.
- Chapter 9, “Configuring ATM Services”.

Defining T1 and E1 Physical Ports

This section describes the physical port parameters for the following Cascade T1 and E1 modules:

- 1-port channelized T1 I/O module (STDX)
- 4-port channelized T1 I/O module
- 4-port unchannelized T1 I/O module
- 4-port channelized E1 I/O module
- 4-port unchannelized E1 I/O modulee

> *For information about the 4-port channelized PRI T1 module for ISDN, refer to* Configuring ISDN Services for B-STDX/STDX*.*

When you set the physical port attributes for a T1 or E1 module, you configure the link-level parameters for a particular T1/E1 interface. The T1/E1 interface must match the parameters of the exterior equipment to which it connects, for example, a DACS or Channel Bank.

The T1/E1 physical port attributes also dictate how many DS0/TS0 channels the physical port can use. By selecting or deselecting individual DS0/TS0 channels, you can enable or disable the use of that particular DS0/TS0.

Using B8Zs zero encoding for T1 modules, you can configure up to 24 DS0 channels, each operating at a rate of 64 Kbps. Using Jammed Bit zero encoding for T1 modules (with Bit Stuffing set to On), you can configure up to 24 DS0 channels, each operating at a rate of 56 Kbps for a total of 1.344Mbps. Combined, these channels provide a DS1 signal operating at 1.544 Mbps.

About External Clock Backup for T1 and E1 Modules

You can configure physical ports to support either internal or external clocking. You use the *Transmit Clock Source* parameter to specify clocking. A channelized or unchannelized T1 module supports an external clock speed of up to 1.544 MHz. A channelized or unchannelized E1 module supports an external clock speed of up to 2.048 MHz.

If the physical port loses the external clock source, the *External Clock Backup* parameter enables the port to automatically revert to either an internal or loop-timed clock source. If the external clock reappears, the switch automatically returns to the external clock source. This feature increases the reliability of customer switched networks that include externally clocked ports.

Configuring T1 and E1 Physical Ports

The T1 and E1 module physical port configuration steps are similar. Special considerations are described in Table 6-9 on page 6-21.

To configure T1 and E1 physical ports, use the following steps:

1. Access the Set Physical Port Attributes dialog box as described in “Configuring Physical Ports” on page 6-9.

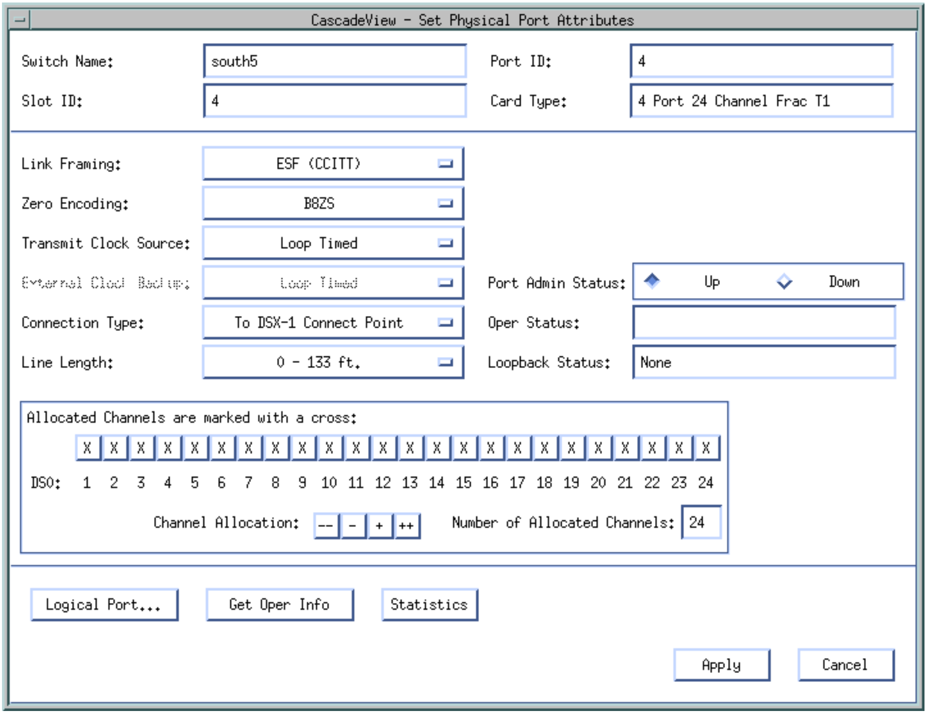


Figure 6-7. Set Physical Port Attributes Dialog Box (T1)

> *If the Loopback Status field does not display* ***None****, do not modify any physical port attributes. Choose Cancel and refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for information about loopback testing.*

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

Table 6-9. Set Physical Port Attributes Fields

Field	Action/Description
Link Framing (*T1 modules*)	Select a framing format. Framing configures the T1/E1 interface for a particular framing specification, enabling you to distinguishing between the individual channels. It is accomplished by adding one additional bit to each frame. T1 link framing options include: *ESF (CCITT) (default)* – Extended Superframe. Extends the D4 framing format from 12 frames to 24 frames, and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of ESF framing over D4 framing is that it enables the Cascade equipment to monitor and respond to a maintenance message from the network. Facility Data Link (FDL) for CCITT is the European standard. *D4 Framing* – Consists of 12 frames (also called “Superframe”). It provides end-to-end synchronization and signaling associated with a particular channel. *ESF (AT&T)* – AT&T is the US Standard for Extended Superframe. *ESF (None)* – No Facility Data Link (FDL) messaging support. ***Note****: The customer premise equipment (CPE) must use the same framing specification as the Cascade physical port.*

Table 6-9. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Link Framing (*E1 modules*)	Select an E1 link framing format. TS16 refers to time slot 16. If you enable TS16, then you can use channel 16 to send data. CRC4 performs a cyclic redundancy check when it is enabled. E1 options include: *TS16 disabled & CRC4 disabled (default)* *TS16 enabled & CRC4 enabled* ***Note****: The customer premise equipment (CPE) must use the same framing specification as the Cascade physical port.*

Table 6-9. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Zero Encoding	Select an encoding format for the T1/E1 interface. Zero encoding specifies the format of the data signal encoding. The signal has three different levels – positive, negative, and ground, which must be referenced from a master clock. ***Note**: Consult your facility service provider for more information about selecting a zero encoding method.* T1 options include: *B8ZS* (*default*) (*Bipolar with 8 zero substitution)* – Refers to the use of a specified pattern of normal bits and bipolar violation that is used to replace a sequence of eight zero bits. With B8ZS, a special code is added and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment. *Jammed Bit* – Refers to jammed bit zero encoding. Jammed Bit is also known as Alternate Mark Inversion (AMI). Using this method, at least one pulse every 8 bits is literally implemented by forcing a pulse in bit 8 of each channel. E1 selection is set at HDB3.

Table 6-9. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Transmit Clock Source	Select the transmit clock source for the T1/E1 module. Options include: *Loop-Timed (default)* – The clock source is derived from the network timing received. *Internal* – The internal T1/E1 timing generator provides the clock source. *External* – An external connection provides the clock source. If you select this option, you should also set External Clock Backup.
External Clock Backup	If the external clock source fails, this option automatically enables either a loop-timed or internal clock source. Refer to page 6-19 for more information about external clock source and backup for a T1/E1 module.
Connection Type (*T1 modules only*)	Specify the connection from the T1 module to the T1 network. *To DSX-1 Connect Point (default)* – The T1 module is connected to a T1 network, for example, a DACS. *To Network* – The T1 module is used as the T1 network interface.

Table 6-9. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Line Length (*T1 modules only*)	Select a line length for this connection. If you select To DSX-1 Connect Point as the connection type , the Line Length parameter enables you to specify the distance from the T1 module to the network equipment. The default value is 0 - 133 ft. Options include: 133 - 266 ft. 266 - 399 ft. 399 - 533 ft. 533 - 655 ft.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port, or takes the port offline to run diagnostics.

Table 6-9. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Allocated Channels are marked with a cross	Select the DS0 or TS0 channels for this configuration. If you are configuring a channelized T1/E1 module, edit the DS0 channel selection, if necessary. For unchannelized T1/E1 modules, proceed to Step 3. To deselect DS0 or TS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel
Number of Allocated Channels	Displays the number of DS0/TS0 channels allocated for use on a channelized T1/E1. This number may change according to the number of DS0 channels you add or remove from the T1/E1.

3. Choose Apply to save the attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.

4. To define the logical port parameters that complete this configuration, refer to the appropriate chapter for your type of service:

- Chapter 7, "Configuring Frame Relay Services".
- Chapter 8, "Configuring SMDS Services".

Defining Channelized DS3 Physical Ports and Channels

When you configure a 1-port, 28-channel DS3 I/O module, you need to define the physical port and channel attributes. The physical-port attributes determine the channelized DS3 clock source and clock rate.

> *If you are replacing a DSX card with a channelized DS3 card, first perform the conversion procedure as described in* *Appendix D, "DSX to DS3 Conversion"* *.*

About External Clock Backup for Channelized DS3 Modules

You can configure physical ports to support either internal or external clocking. You use the *Transmit Clock Source* parameter to specify clocking. A channelized DS3 module supports an external clock speed of up to 1.544 MHz.

If the physical port loses the external clock source, the *External Clock Backup* parameter enables the port to automatically revert to either an internal or loop-timed clock source. This feature increases the reliability of customer switched networks that include externally clocked ports.

About Channels

Channels are located between the physical port and logical port layers as shown in Figure 6-8.

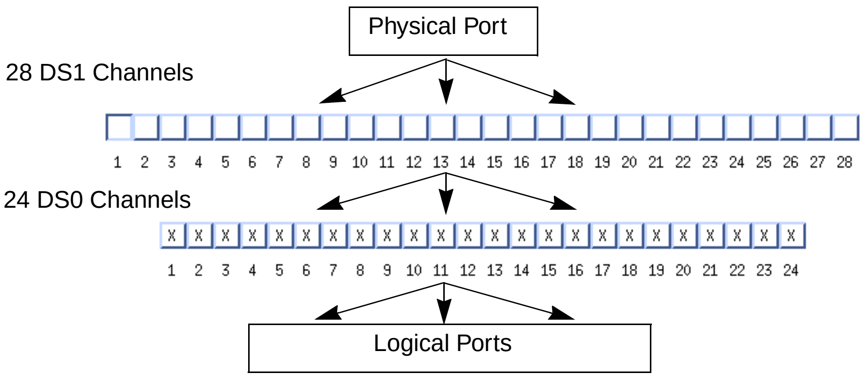


Figure 6-8. Channelized DS3 Channels

The physical port is divided into 28 fractional T1 channels. Each channel supports one user logical port (except for OPTimum trunk logical ports). Each DS1 channel contains 24 DS0 channels. The channelized DS3 channel attributes dictate how many DS0 channels the physical port can use. By selecting or deselecting individual DS0 channels, you can enable or disable the use of that particular DS0. You can configure up to 24 DS0 channels, each operating at a rate of 56 Kbps. Combined, these channels provide a DS1 signal operating at 1.544 Mbps.

About DS3 Signal Application Mode

The DS3 signal is partitioned into M-frames of 4760 bits each. The M-frames are divided into seven M-subframes of 680 bits. The first C-bit in M-subframe 1 is used as an application identification channel (AIC) to identify the specific DS3 M-frame. The AIC determines the mode of operation for a DS3 signal.

Configuring Channelized DS3 Physical Ports

To configure a channelized DS3 physical port, use the following steps:

1. Access the Set Physical Port Attributes dialog box as described in "Configuring Physical Ports" on page 6-9.

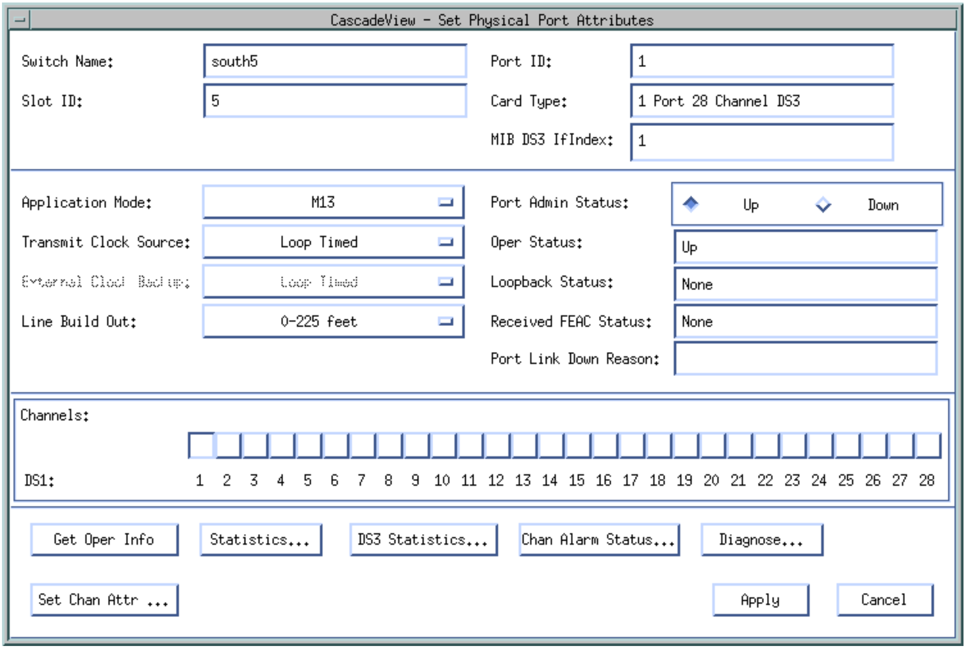


Figure 6-9. Set Physical Port Attributes Dialog Box (Channelized DS3)

2. Complete the required dialog box fields described in Table 6-10.

Table 6-10. Set Physical Port Attributes Fields (Channelized DS3)

Field	Action/Description
Application Mode	Select the DS3 application mode. Options include: *M13 (default)* – Uses C-bits in a frame to indicate the presence or absence of stuffing bits. *C-bit Parity* – Uses the first C-bit in M-subframe 1 to identify the format as C-bit parity.

Table 6-10. Set Physical Port Attributes Fields (Channelized DS3) (Continued)

Field	Action/Description
Transmit Clock Source	Select the transmit clock source. The DS3 receive clock is independent from the DS3 transmit clock. Options include: *Loop Timed (default)* – The clock source is derived from the timing received. *Internal* – The internal timing generator provides the clock source. *External* – An external connection provides a DS1 clock source. This source drives a phased locked loop circuit to provide DS3 clocking. If you select this option, you should also set an external backup clock source.
External Clock Backup	(*Optional*) If the external clock source fails, you can set this parameter to automatically enable either loop timed or internal clock source. This field is enabled only when the external clock option is selected as the transmit clock source. Refer to “About External Clock Backup for Channelized DS3 Modules” on page 6-27 for more information.
Line Build Out	Specify the distance measurement from the channelized DS3 module to the network equipment. Options include: *0 - 225 feet (default)* *225 - 450 feet*

Table 6-10. Set Physical Port Attributes Fields (Channelized DS3) (Continued)

Field	Action/Description
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Oper Status	Displays the current operational state of the card.
Loopback Status	Displays the current loopback status of the card.
Received FEAC Status	Displays the FEAC (Far-End Alarm and Control) status received by the physical port, if C-bit parity is enabled. This field indicates the status of the physical port on the other end of the connection. If you are using M13, this field displays None.
Port Link Down Reason	Displays the reason for the down link. If the link is up, this field displays None.

Configuring Channel Attributes

To configure a DS1 channel and define its attributes, use the following steps:

1. From the Set Physical Port Attributes dialog box (Figure 6-9), double-click the button of the channel you want to configure.

   The Set Channel Attributes dialog box appears as shown in Figure 6-10, displaying 24 DS0 channels.

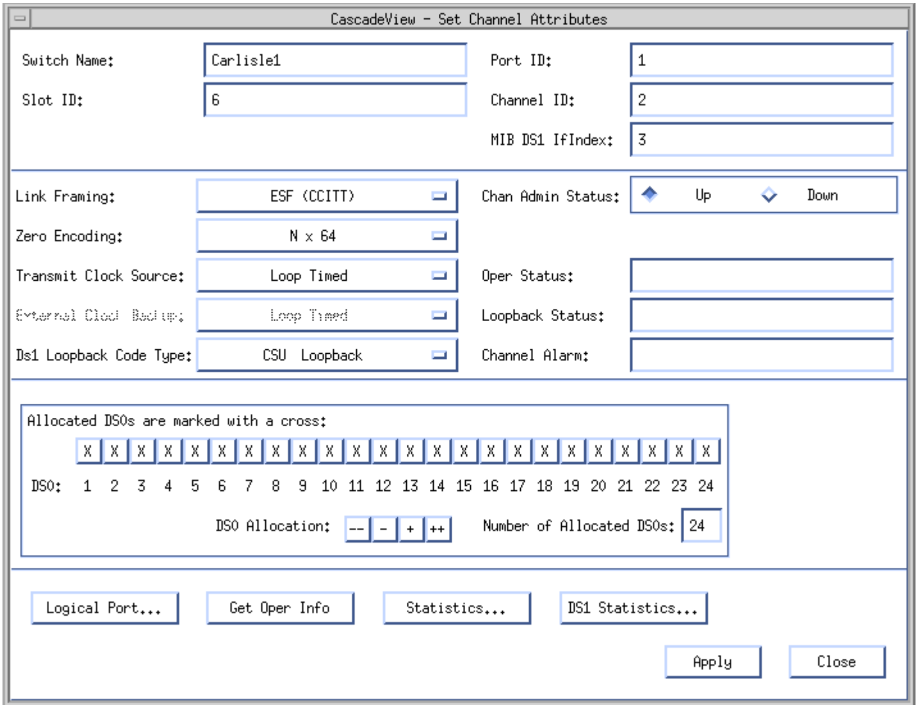


Figure 6-10. Set Channel Attributes Dialog Box

The Set Channel Attributes Dialog Box

The Set Channel Attributes dialog box displays the following fields described in Table 6-11.

Table 6-11. Set Channel Attributes Fields

Field	Function
Switch Name	Name of the switch in which the module resides.
Slot ID	Slot number where the module resides.
Port ID	Number of the port you are configuring.

Table 6-11. Set Channel Attributes Fields (Continued)

Field	Function
Channel ID	Number of the channel you are configuring.
MIB DS1 IfIndex	Interface number used for link performance. (If you use a third-party MIB Browser, the value is displayed.)
Oper Status	The card's current operational state.
Loopback Status	The card's current loopback status.
Channel Alarm	Indicates the alarm status of the channel. For information, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

The Set Channel Attributes dialog box also contains the following commands described in Table 6-12:

Table 6-12. Set Channel Attributes Dialog Box Commands

Commands	Function
Logical Port	Displays information for the selected logical port and allows you to add or modify a logical port.
Get Oper Info	Displays a brief status for the selected channel. This command updates the Oper Status field to show the current channel status.
Statistics	Displays channel summary statistics for the selected channel. For information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

Table 6-12. Set Channel Attributes Dialog Box Commands (Continued)

Commands	Function
DS1 Statistics	Displays link performance statistics for the selected channel. For information about DS1 statistics, refer to *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

2. Complete the required dialog box fields described in Table 6-13.

Table 6-13. Set Channel Attributes Fields

Field	Action/Description
Link Framing	Select a framing format. Framing configures the T1 interface for a particular framing specification, enabling you to distinguish between individual channels. It is accomplished by adding one additional bit to each frame. ***Note****: The customer premise equipment (CPE) must use the same framing specification as the Cascade physical port.* Options include: *ESF (CCITT) (default)* – Extended Superframe. Extends the D4 framing format from 12 frames to 24 frames, and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of ESF framing over D4 framing is that it enables Cascade's equipment to monitor and respond to a maintenance message from the network. Facility Data Link (FDL) for CCITT is the European standard. *D4 Framing* – Consists of 12 frames (also called "Superframe"). It provides end-to-end synchronization and signaling associated with a particular channel.

Table 6-13. Set Channel Attributes Fields (Continued)

Field	Action/Description
Zero Encoding	Select an encoding format for the T1 interface. Options include: *N x 64 (clear channel) (default)* – Refers to the speed of the channel for clear channel. Using this method, each channel uses 64 Kbps (the entire bandwidth). *N x 56 (Jammed Bit)* – Refers to jammed bit zero encoding. Jammed Bit is also known as Alternate Mark Inversion (AMI). Using this method, at least one pulse every 8 bits is implemented by forcing a pulse in bit 8 of each channel.
Transmit Clock Source	Select the transmit clock source for the DS1. Options include: *Loop Timed (default)* – The clock source is derived from the timing received. *Internal* – The internal timing generator provides the clock source. *External* – An external connection provides the clock source. If you select this option, you should also set an external clock backup.
External Clock Backup	If the external clock source fails, you can set this parameter to automatically enable either loop timed or internal clock source. Refer to page 6-27 for more information about external clock source and backup for a channelized DS3 module.

Table 6-13. Set Channel Attributes Fields (Continued)

Field	Action/Description
DS1 Loopback Code Type	Specify the loopback as one of the following: *CSU Loopback* – Specifies that the DS1 loopback loops back the CSU at the customer premise equipment (CPE). *NI Loopback* – Specifies that the DS1 loopback loopbacks the Network Interface (NI) at the customer premise equipment (CPE).
Chan Admin Status	Set the Chan Admin Status. *Up* – Enables immediate access to the channel. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Allocated DS0s are marked with a cross	Select the DS0 channels for this configuration. Configured DS0 channels are marked with an “X”. By default, all DS0 channels are configured. Click the left mouse button on the channel to deselect/select the X. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel

Table 6-13. Set Channel Attributes Fields (Continued)

Field	Action/Description
Number of Allocated Channels	Displays the number of DS0 channels allocated for use on a channelized DS3. This number may be subject to change according to the number of DS0 channels you add or remove.

3. Choose Apply to set the channel attributes. Choose Close to return to the Set Physical Port Attributes dialog box.

4. Choose Apply to save the physical port attributes and send an SNMP Set command to the switch. Choose Close to exit the dialog box.

5. To define the logical port parameters that complete this configuration, refer to the appropriate chapter for your type of service:

- Chapter 7, "Configuring Frame Relay Services"
- Chapter 8, "Configuring SMDS Services"
- Chapter 9, "Configuring ATM Services"

Defining 10-port DSX-1 Physical Ports

The 10-port DSX-1 I/O module enables fractional T1 connections at variable rates. The DSX-1 physical port attributes also dictate how many DS0 channels are used. By selecting or deselecting individual DS0 channels, you can enable or disable use of that particular DS0.

If you are converting a channelized DS3 card back to a DSX card, before proceeding verify you performed the conversion procedure as described in Appendix D, "DSX to DS3 Conversion" .

About External Clock Backup for DSX-1 Modules

You can configure physical ports to support either internal or external clocking. You use the *Transmit Clock Source* parameter to specify clocking. A DSX-1 module supports an external clock speed of up to 1.544 MHz.

If the physical port loses the external clock source, the *External Clock Backup* parameter enables the port to automatically revert to either an internal or loop-timed clock source. If the external clock reappears, the switch automatically returns to the external clock source. This feature increases the reliability of customer switched networks that include externally clocked ports.

Configuring 10-port DSX-1 Physicals Ports

To configure a 10-port DSX-1 physical port:

1. Access the Set Physical Port Attributes dialog box as described in "Configuring Physical Ports" on page 6-9.

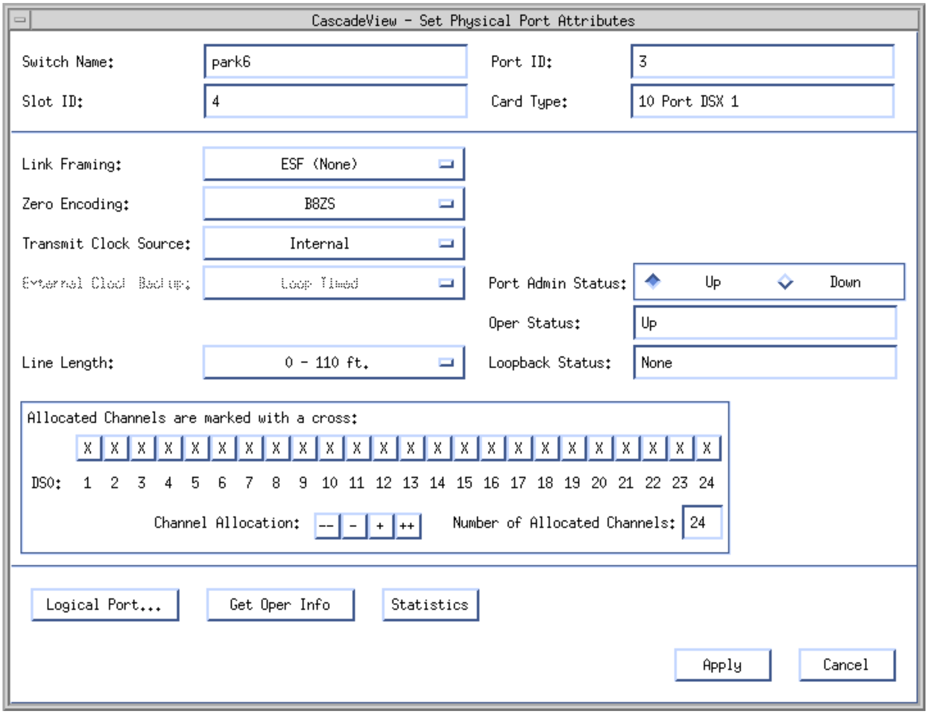


Figure 6-11. Set Physical Port Attributes Dialog Box (10-port DSX-1)

> *If the Loopback Status field does not display* ***None****, do not modify any physical port attributes. Choose Cancel and refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for information about loopback status.*

2. Complete the required dialog box fields described in Table 6-14.

Table 6-14. Set Physical Port Attributes Fields (10-port DSX)

Field	Action/Description
Link Framing	Select a framing format. Framing configures the T1 interface for a particular framing specification, enabling you to distinguish between channels. It is accomplished by adding one additional bit to each frame. ***Note**: The CPE must use the same framing specification as the Cascade physical port.Refer to your facility service provider for more information about selecting a link framing specification.* Options include: *ESF (None) (default)* – No Facility Data Link (FDL) messaging support. *D4 Framing* – Consists of 12 frames (also called "Superframe"). It provides end-to-end synchronization and signaling associated with a particular channel.

Table 6-14. Set Physical Port Attributes Fields (10-port DSX)

Field	Action/Description
Zero Encoding	Select an encoding format for the T1 interface. Zero encoding specifies the format of the data signal encoding. The signal has three different levels – positive, negative, and ground, which must be referenced from a master clock. ***Note**: Consult your facility service provider for more information about selecting a zero encoding method.* Options include: *B8ZS (Bipolar with 8 zero substitution) (default)* – Refers to the use of a specified pattern of normal bits and bipolar violation used to replace a sequence of eight zero bits. With B8ZS, a special code is added and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment. *Jammed Bit* – Refers to jammed bit zero encoding; also known as Alternate Mark Inversion (AMI). Using this method, at least one pulse every 8 bits is literally implemented by forcing a pulse in bit 8 of each channel.
Transmit Clock Source	Select the transmit clock source for the DSX-1. *Loop-Timed (default)* –The clock source is derived from the timing received. *Internal* – The internal timing generator provides the clock source. *External* – An external connection provides the clock source. If you select this option, you should also set External Clock Backup.

Table 6-14. Set Physical Port Attributes Fields (10-port DSX)

Field	Action/Description
External Clock Backup	If the external clock source fails, this option can automatically enable either a Loop-Timed or internal clock source. Refer to page 6-39 for more information about external clock source and backup for DSX-1 modules.
Line Length	Specify the distance measurement from the DSX-1 module to the network equipment. The default is 0 - 110.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Allocated Channels are marked with a cross	Select the DS0 channels for this configuration. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel

Table 6-14. Set Physical Port Attributes Fields (10-port DSX)

Field	Action/Description
Number of Allocated Channels	Displays the number of DS0 channels allocated for use on this DSX-1 port. This number changes according to the number of DS0 channels you add or remove from the DSX-1 in the Allocated Channels are marked with a cross field. 64 Kbps bandwidth is allocated for each channel you select. For example, using the B8Zs zero encoding, if you select 20 channels, a maximum of 1280 Kbps (20 x 64 = 1280) bandwidth is allocated for logical port configuration. Using the Jammed Bit zero encoding option, if you select 20 channels, a maximum of 1120 Kbps (20 x 56 = 1120) bandwidth is allocated for logical port configuration.

3. Choose Apply to save the physical port attributes and send an SNMP Set command to the switch. Choose Close to exit the dialog box.

4. To define the logical port parameters that complete this configuration, refer to the appropriate chapter for your type of service:

- Chapter 7, “Configuring Frame Relay Services”
- Chapter 8, “Configuring SMDS Services”
- Chapter 9, “Configuring ATM Services”

Defining HSSI Physical Ports

The 2-port HSSI I/O module enables connections at data rates up to 44.212 Mbps. You can configure each of the module's two physical ports at speeds that increment from 1.579 Mbps to 44.212 Mbps to support DTE connections that exceed 8 Mbps.

To configure the physical port parameters for a 2-port HSSI module:

1. Access the Set Physical Port Attributes dialog box as described in "Configuring Physical Ports" on page 6-9.

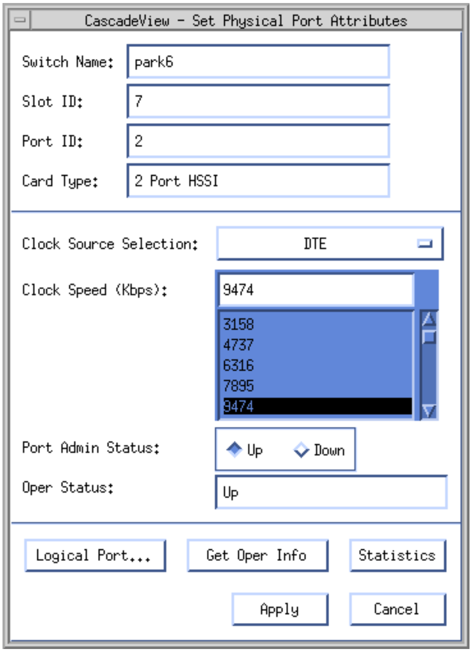


Figure 6-12. Set Physical Port Attributes Dialog Box (2-port HSSI)

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

Table 6-15. Set Physical Port Attributes Fields (2-port HSSI)

Filed	Action/Description
Clock Source Selection	Select a clock source. The switch can either supply or receive clock at a rate of up to 44.212 Mbps. Options include: *DCE* – Configures the port to provide clock at the rate specified by the clock speed selection. Use this option when connecting to a DTE, where the switch provides both the transmit and receive clocks and uses a straight-through cable. Use a crossover cable to connect to a physical DCE. *DTE* – Configures the port to receive clock from an outside source, typically a CSU/DSU. However, you should set the clock speed even though it is not clocking. You need clock speed for logical port configuration. ***Note**: B-STDX 8000/9000 ports are always electrically DCE and require a crossover cable when interfacing with a modem or other DCE. Refer to the* B-STDX 8000/9000 Hardware Installation Guide *for cable diagram pinouts.*

Table 6-15. Set Physical Port Attributes Fields (2-port HSSI) (Continued)

Filed	Action/Description
Clock Speed (Kbps)	If the clock source is set to DTE, the switch ignores the clock speed parameter for clocking purposes. However, you should set clock speed for the actual clock rate, since the cumulative total of all logical ports configured on the physical port cannot exceed the clock source setting. ***Note****: The total bandwidth of all physical ports on the HSSI module cannot exceed the maximum module capacity of 44.212 Mbps. If you exceed the maximum capacity, CascadeView displays an error message.*
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.

3. Choose Apply to save the attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.

4. To define the logical port parameters that complete this configuration, refer to the appropriate chapter for your type of service:

- Chapter 7, “Configuring Frame Relay Services”
- Chapter 8, “Configuring SMDS Services”
- Chapter 9, “Configuring ATM Services”

ATM-based I/O Modules

This section describes how to set the physical port attributes for the following ATM based I/O modules:

1-port ATM UNI DS3/E3

The Asynchronous Transfer Mode (ATM) DS3 User Network Interface (UNI) module provides the following features:

- One physical port, capable of operating full duplex at the DS3/E3 rate.
- Provides a high-performance trunk to an ATM backbone network using the standard T3 interfaces.
- Supports up to 938 Frame Relay/ATM Service Interworking PVCs.
- Supports up to 4300 PVCs, when configured to provide either an ATM Network-to-Network interface (ATM NNI) or Cascade OPTimum trunk (open packet trunking) .
- Provides up to 3568 virtual path identifier/virtual channel identifier (VPI/VCI) address combinations.

The configure the 1-port ATM UNI DS3/E3 module physical port, refer to "Defining ATM UNI DS3 and E3 Physical Ports" on page 6-51.

1-port ATM IWU/OC3

The Asynchronous Transfer Mode (ATM) Interworking Unit (IWU) module provides the following features:

- One physical port, capable of operating full duplex at the OC3c/STM1 rate.
- Supports up to 938 Frame Relay/ATM Service Interworking PVCs.
- Supports up to 2000 PVCs, when configured to provide either an ATM Network-to-Network interface (ATM NNI) or Cascade OPTimum trunk (open packet trunking).
- Supports frame-to-cell conversion with dynamic DE/CLP bit mapping.

- Provides up to 3568 virtual path identifier/virtual channel identifier (VPI/VCI) address combinations.
- Reliable and predictable network Quality of Service (QoS) parameters.

To configure the ATM IWU module physical port, refer to "Defining ATM Interworking Unit (IWU) Physical Ports" on page 6-56.

1-port ATM CS/DS3

The Asynchronous Transfer Mode (ATM) Cell Switching (CS) module provides the following features:

- One physical port, capable of operating full duplex at the DS3/E3 rate.
- Provides a high-performance trunk to an ATM backbone network using the standard T3 interfaces.
- Supports up to 938 Frame Relay/ATM Service Interworking PVCs.
- Supports up to 2000 PVCs, when configured to provide either an ATM Network-to-Network interface (ATM NNI) or Cascade OPTimum trunk (open packet trunking).
- Supports frame-to-cell conversion with dynamic DE/CLP bit mapping.
- Supports cell switching at wire speed, independent of packet size.
- Provides up to 3568 virtual path identifier/virtual channel identifier (VPI/VCI) address combinations.
- Reliable and predictable network Quality of Service (QoS) parameters.

To configure the ATM CS module physical port, refer to "Defining ATM Cell Switching (CS) Physical Ports" on page 6-61.

About Peak Cell Rates

Peak cell rate (PCR) is the maximum transmission rate at which cells are transmitted. It defines the shortest time period between cells. The circuit maps to the closest PCR queue whose PCR value is greater than the PCR value you configure. Traffic shaping uses the PCR value from the PCR queue. It defines the shortest time period between cells. You can configure up to eight (8) PCR queues with the first four queues being the high priority queues and the remaining queues being the lower priority queues. The high priority queues are served first, and any remaining bandwidth services the lower priority queues.

When you configure circuit priority (described in “Defining Frame Relay Circuits” on page 11-19), the circuit has a specific PCR queue. The PCR values provide the traffic shaping function. The default value of 96,000 cells-per-second provides adequate traffic shaping with little or no congestion, in most cases.

About Sustainable Cell Rate (SCR)

Sustainable 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 the peak cell rate) for guaranteeing that network performance objectives are met. This parameter applies only to variable bit rate traffic; it does not apply to constant bit rate (CBR) or unspecified bit rate (UBR) traffic.

About Traffic Shaping

There are 15 user configurable traffic shapers (IDs) available for cell transmission. Values from 1 through 15 specify the traffic shaper to be used for the physical port. Each shaper has associated default values for priority, SCR, PCR, and Maximum Burst Size (MBS). You can modify these defaults, however when you enter a shaper configuration and then press Verify Traffic Shaper, the NMS verifies the values for the shaper ID and will change settings as necessary depending on the hardware. The reason for this is that the hardware cannot shape at all possible settings.

Shapers are numbered from 0 to 15. Shaper 0 has the highest priority. Shaper 15 has the lowest priority. According to the configured priority, the shaper transmits data only when a shaper that has a higher priority is not waiting for transmission.

Defining ATM UNI DS3 and E3 Physical Ports

The ATM UNI DS3 and ATM UNI E3 module physical port configuration steps are similar. Special considerations are described in Table 6-16 on page 6-52.

To configure the physical port parameters for the ATM UNI DS3 or ATM UNI E3:

1. Access the Set ATM Physical Port Attributes dialog box as described in "Configuring Physical Ports" on page 6-9.

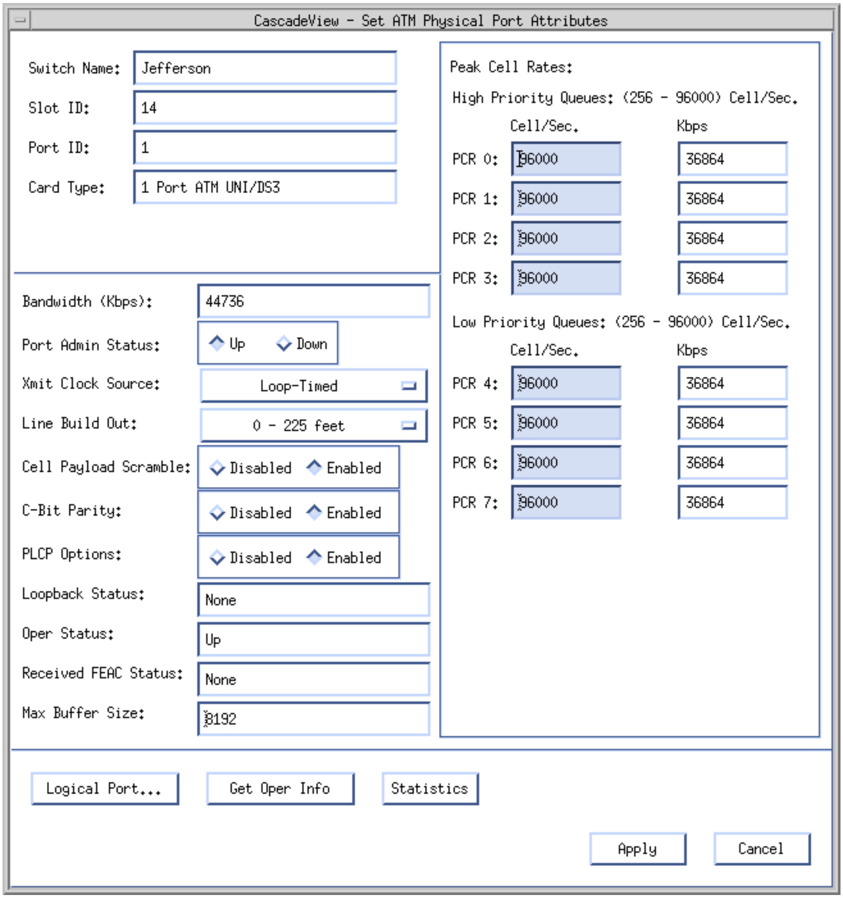


Figure 6-13. Set ATM Physical Port Attributes Dialog Box (ATM UNI DS3)

If the Loopback Status field does not display None, do not modify any physical port attributes. Choose Cancel and refer to the Diagnostic and Troubleshooting Guide for B-STDX/STDX*.*

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

Table 6-16. Set Physical Port Attributes Fields (ATM UNI DS3/E3)

Field	Action/Description
Bandwidth (Kbps)	Displays the amount of bandwidth available for this physical port.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Xmit Clock Source	Specify the transmit clock source. *Loop-Timed (default)* – The clock source is derived from the timing received. *Internal* – The internal timing generator provides the clock source.
Line Build Out (*ATM UNI DS3 only*)	Select the Line Build Out. This value represents the length of the cable from the switch to the network equipment to which it is attached. Options include: 0– 225 feet (*default*) for a short cable 226 – 450 feet for a long cable

Table 6-16. Set Physical Port Attributes Fields (ATM UNI DS3/E3)

Field	Action/Description
Cell Payload Scramble	Disable this function only if the equipment connected to this port does not support Cell Payload Scramble. The Cell Payload Scramble function prevents user data from being misinterpreted (ATM cell header delineation).
C-Bit Parity (*ATM UNI DS3 only*)	Enable or disable C-Bit Parity. The C-Bit Parity function enables you to monitor the end-to-end performance of T3 circuits. This function works in conjunction with Cell Payload Scramble.
PLCP Option (*ATM UNI DS3 only*)	Enable or disable the Physical Layer Convergence Protocol (PLCP). *Enable* – ATM UNI DS3 module uses a PLCP frame, which transmits 12 ATM cells every 125 µs. The ATM cell payload bandwidth is 36.9 Mbps (96000 x 48 x 8bps). Use this option if the customer premise equipment can handle PLCP frames. *Disable* – DS3 module uses ATM direct mapping to pack ATM cells into the DS3 bit stream. The ATM cell payload bandwidth is 40 Mbps (104268 x 48 x 8bps). This option provides the most bandwidth. Use this option only if you can disable PLCP for the CPE connected to this port.
Loopback Status	Defaults to None. If you enable loopback tests, this field displays the card's actual loopback status. For more information about loopbacks, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

Table 6-16. Set Physical Port Attributes Fields (ATM UNI DS3/E3)

Field	Action/Description
Oper Status	Displays a brief status to indicate the operational status of the selected port.
Received FEAC Status	Displays the FEAC (Far-End Alarm and Control) status received by the physical port, if C-bit parity is enabled. This field indicates the status of the physical port on the other end of the connection. If you are using M13, this field displays None.
Max Buffer Size	Specify the maximum number of bytes in the reassembly buffer. The default is 8152. By configuring a smaller size, you provide more buffers to reassemble packets and reception is improved. However, the maximum buffer size must be large enough to hold the largest packet of information. Packet are discarded if the reassembly buffer if full.

Table 6-16. Set Physical Port Attributes Fields (ATM UNI DS3/E3)

Field	Action/Description
Peak Cell Rates	Specify the Peak cell rate (PCR), which is the maximum transmission rate at which cells are transmitted. When you configure a queue, enter the PCR values in terms of cells-per-second. The corresponding value, expressed in terms of Kbps, is derived automatically according to your input. Options include: • For the ATM UNI DS3 module with PLCP enabled, specify a range from 256 cells/sec to 96000 cells/sec. • For the ATM UNI DS3 module with PLCP disabled, specify a range from 256 cells/sec to 104268 cells/sec. • For the ATM UNI E3 module, specify a range from 256 cells/sec to 80000 cells/sec.

3. Choose Apply to save the physical port attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.
4. To define the logical port parameters that complete this configuration, refer to Chapter 9, "Configuring ATM Services" to set up the ATM service.

Defining ATM Interworking Unit (IWU) Physical Ports

To configure the physical port parameters for the ATM IWU module:

1. Access the Set ATM Physical Port Attributes dialog box as described in "Configuring Physical Ports" on page 6-9.

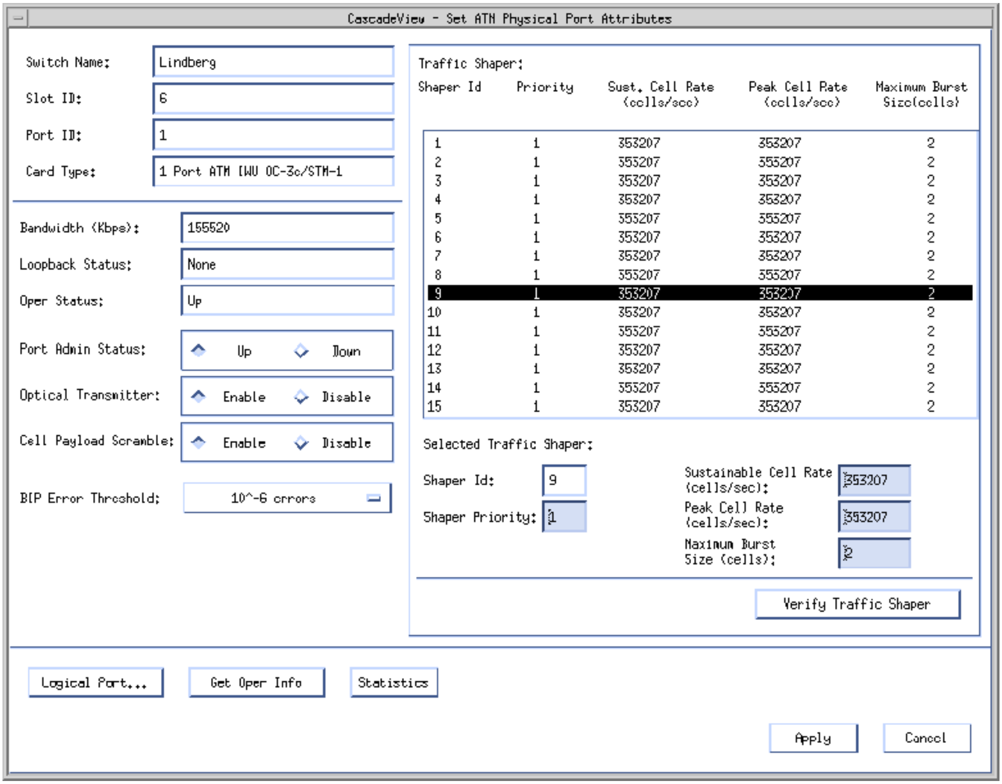


Figure 6-14. Set ATM Physical Port Attributes Dialog Box (IWU)

If the Loopback Status field does not display ***None****, do not modify any physical port attributes. Choose Cancel and refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for more information about loopback testing*.

2. Complete the required dialog box fields described in Table 6-17.

Table 6-17. Set ATM Physical Port Attributes (ATM IWU)

Field	Action/Description
Bandwidth (Kbps)	Displays the amount of bandwidth available for this physical port.
Loopback Status	Defaults to None. If you enable loopback tests, this field displays the ATM IWU card's loopback status. For more information about DS3 Loopback, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Oper Status	Displays a brief status to indicate the operational status of the selected port.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. Options include: *Up* – Enables immediate access to the port. *Down* – Saves the configuration in the database without activating the port or to take the port offline to run diagnostics.

Table 6-17. Set ATM Physical Port Attributes (ATM IWU) (Continued)

Field	Action/Description
Optical Transmitter	Set this field to On or Off. This field is a safety feature intended to prevent personal injury when you repair or replace the module, or connect cables to the module. By default, this option is set to Off. The Off setting disables the transmit for this port, and prevents the port from transmitting incoming traffic.You must set this field to *On* to transmit incoming traffic out of this port. **CAUTION:** BEFORE YOU REMOVE THE OPTICAL CABLE, SET THIS FIELD TO **OFF**. IF THE OPTICAL CONNECTORS ARE EXPOSED, THE TRANSMITTER BEAM CAN CAUSE PERSONAL INJURY. ***Note:*** *When you disable the transmitter, the CPE or switch at the other end of the connection reports a red port alarm to indicate signal loss.*
Cell Payload Scramble	Disable this function only if the equipment connected to this port does not support Cell Payload Scramble. The Cell Payload Scramble function prevents user data from being misinterpreted (ATM cell header delineation).
BIP Error Threshold	Select the Bit Interleaving Parity error threshold to indicate the physical port's sensitivity to network errors. Options include: • $10^{\wedge -6}$ errors • $10^{\wedge -5}$ errors • $10^{\wedge -4}$ errors • ignore

3. Complete the Traffic Shaper parameters as described in Table 6-18.

Table 6-18. Traffic Shaper Fields (ATM IWU)

Field	Action/Description
Shaper Id	Select a value from 1 through 15 to specify the traffic shaper to be used for this physical port. For more information, refer to "About Traffic Shaping" on page 6-50.
Shaper Priority	Select a Shaper Priority from 0 to 15. Shaper 0 has the highest priority. Shaper 15 has the lowest priority. For more information, refer to "About Traffic Shaping" on page 6-50.
Sustainable Cell Rate	Specify an SCR that is less than or equal to the peak cell rate (PCR). SCR is usually some fraction of the PCR and its value must be greater than or equal to 1/64 of the PCR. For more information, refer to "About Sustainable Cell Rate (SCR)" on page 6-50.
Peak Cell Rate	Select the peak cell rate which determines the maximum transmission rate at which cells are transmitted. For more information, refer to "About Peak Cell Rates" on page 6-50. ***Note****: The SCR is scaled up by the same amount that the configured PCR value is scaled up when it is mapped into a PCR queue. The following formula determines the actual SCR value used for traffic shaping:* *SCR (actual) = SCR (configured) * [PCR (actual)/PCR (configured)]*

Table 6-18. Traffic Shaper Fields (ATM IWU) (Continued)

Field	Action/Description
Maximum Burst Size (cells)	Select the maximum burst size which determines the maximum number of cells that can be transmitted at the Peak Cell Rate. This allows a burst of cells to arrive at a rate higher than the sustainable cell rate. This parameter applies only to variable bit rate (VBR) traffic; it does not apply to the CBR or UBR traffic.

4. Choose Verify Traffic Shaper to enable the NMS to verify the shaper settings.
5. Choose Apply to save the attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.
6. Define the clock source as described in “Defining the Clock Source for ATM CS and ATM IWU Modules” on page 6-64.

Defining ATM Cell Switching (CS) Physical Ports

To configure the physical port parameters for the ATM CS module:

1. Access the Set ATM Physical Port Attributes dialog box as described in “Configuring Physical Ports” on page 6-9.

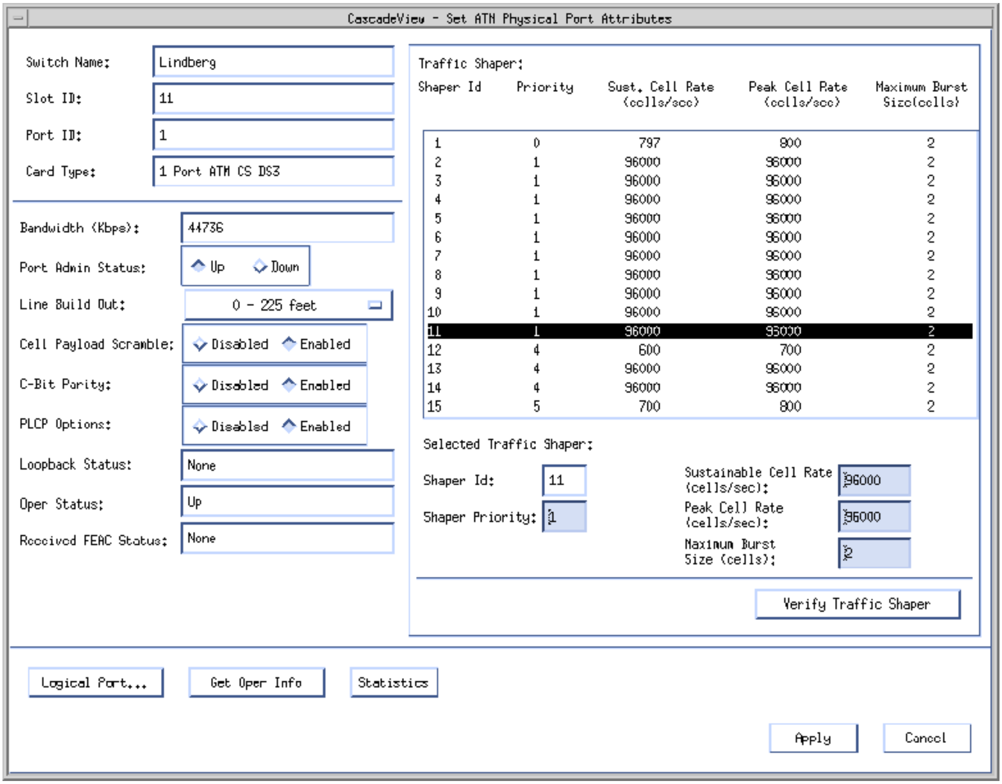


Figure 6-15. Set ATM Physical Port Attributes Dialog Box (ATM CS)

> *If the Loopback Status field does not display* ***None****, do not modify any physical port attributes. Choose Cancel and refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for more information about* *loopback testing*.

2. Complete the required dialog box fields described in Table 6-19.

Table 6-19. Set ATM Physical Port Attributes Fields (ATM CS)

Field	Action/Description
Bandwidth (Kbps)	Displays the amount of bandwidth available for this physical port.
Port Admin Status	Set the Port Admin Status. Each time you modify the Port Admin Status, choose Apply to send the change to the switch. *Up* – Enables immediate access to the port. *Down* – Save the configuration in the database without activating the port, or to take the port offline to run diagnostics.
Line Build Out (DS3 only)	Select either 0–225 feet (*default*) for a short cable, or 226–450 feet for a long cable. This value represents the length of the cable from the switch to the network equipment to which it is attached.
Cell Payload Scramble	Disable this function only if the equipment connected to this port does not support Cell Payload Scramble. The Cell Payload Scramble function prevents user data from being misinterpreted (ATM cell header delineation).
C-Bit Parity (DS3 only)	Select Disabled or Enabled. The C-Bit Parity function provides a way to monitor the end-to-end performance of T3 circuits. This function works in conjunction with Cell Payload Scramble.

Table 6-19. Set ATM Physical Port Attributes Fields (ATM CS) (Continued)

Field	Action/Description
PLCP Option (DS3 only)	Select Enabled or Disabled to enable or disable the Physical Layer Convergence Protocol (PLCP). *Enabled* – The ATM DS3 module uses a PLCP frame which transmits 12 ATM cells every 125 μs. The ATM cell payload bandwidth is 36.9 Mbps. Use this option if the customer premise equipment can handle PLCP frames. *Disabled* – The DS3 module uses ATM direct mapping to pack ATM cells into the DS3 bit stream. The ATM cell payload bandwidth is 40 Mbps. This option provides the most bandwidth. Use this option only if you can disable PLCP for the CPE connected to this port.
Loopback Status	Defaults to None. If you enable loopback tests, this field displays the ATM DS3 card's loopback status. For more information about DS3 Loopback, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Oper Status	Displays a brief status to indicate the operational status of the selected port.
Rec FEAC Status (*DS3 only*)	Displays the Far-End Alarm Control (FEAC) status received by this physical port, if C-Bit Parity is Enabled. This field indicates the physical port status on the other end of the connection.

3. Complete the Traffic Shaper parameters as described in Table 6-18 on page 6-59.

4. Choose Verify Traffic Shaper to enable the NMS to verify the shaper settings.

5. Choose Apply to save the physical port attributes and send an SNMP Set command to the switch. Choose Cancel to exit the dialog box.

6. Define the clock source as described in the next section.

Defining the Clock Source for ATM CS and ATM IWU Modules

The Clock Source command on the Set Switch Attributes dialog box enables you to define the clock source for the ATM CS or ATM IWU module. The system automatically selects *one* ATM CS or ATM IWU module as the clock master for the entire switch. The clock master provides the central clocking signal to all other ATM CS and ATM IWU modules in the switch. The clock master synchronizes to the highest configured clock source to provide the clocking signal. If no clock source is configured, the ATM CS and ATM IWU modules default to internal clocking.

To set the clock source, use the following steps:

1. From the Set Switch Attributes dialog box (see Figure 5-8 on page 5-20), choose Clock Sources.

   The Set Clock Sources dialog box appears as shown in Figure 6-16.

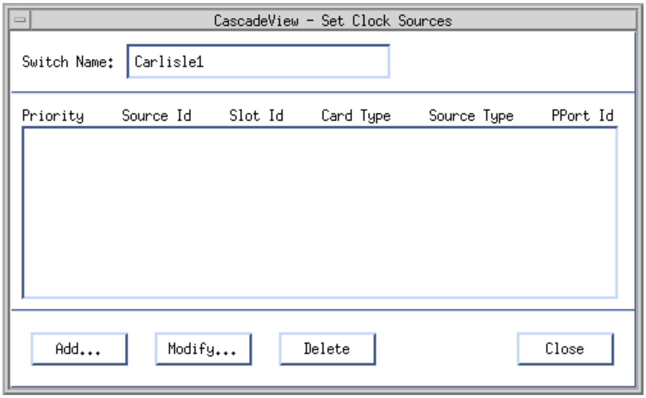


Figure 6-16. Set Clock Sources Dialog Box

2. Choose Add. The Add Clock Source dialog box appears as shown in Figure 6-17.

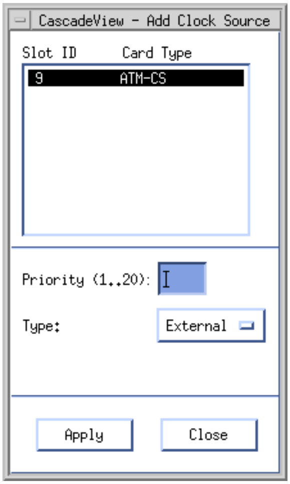


Figure 6-17. Add Clock Source Dialog Box

The Slot ID and Card Type fields display the configured ATM CS and ATM IWU modules for the selected switch.

3. Complete the dialog box fields for each module as described in Table 6-20.

Table 6-20. Add Clock Source Fields

Field	Action/Description
Priority (1..20)	Select a priority level between 1(*highest*) and 20 (*lowest*). This number determines which module is used first.
Type	Select the clock type for this module. Options include: *External (default)* – An external connection provides the clock source. *Line* – Physical port provides the clock source.
Clock Source	If you selected Line for the clock type, the Clock Source defaults to PPort 1.

4. Choose Apply to save the settings. Choose Close to exit the dialog box.

7

Configuring Frame Relay Services

This chapter describes the different Cascade Frame Relay networking services as defined by their logical port types. Frame Relay is the first packet-mode interface to ISDN networks. Frame Relay offers the following advantages:

- Accommodates bursty LAN traffic
- Provides reliability without error-correction overhead
- Relies on upper-layer protocols at the workstation level
- Runs at very high speeds

For more information about Cascade's implementation of Frame Relay, refer to the *Networking Services Technology Overview*.

About Frame Relay Logical Ports

A single physical port may contain multiple logical port configurations. The logical port differs from the physical port configuration, in that the physical port parameters specify only *clocking* and *clock speeds*. A logical port definition specifies how each channel is to communicate with the attached equipment. For example, a logical port configured as a Frame Relay *User Network Interface-Data Communication Equipment* (UNI-DCE) indicates that the port acts as the network for link management purposes. This UNI port may be physically set to provide clocking (defined as *Data Communications Equipment* or DCE) or no clocking (defined as *Data Terminal Equipment* or DTE).

The Set All Logical Ports in PPort dialog box, described later in this chapter, enables you to add, modify, or delete logical port configurations for a specified physical port. The logical port configuration defines which link management protocol is used, the amount of bandwidth allocated, and the individual link timer parameters. When you need to reroute a circuit due to a port failure, refer to "Activating a Backup Port" on page 7-48 for information.

Logical Port Types

Table 7-1 lists and describes the different types of Frame Relay logical ports.

Table 7-1. Frame Relay Logical Port Types

LPort Type...	Configures the PPort as	Performs the Frame Relay functions...
Frame Relay Switch (UNI-DCE)	Frame Relay UNI-DCE	For link management purposes and expects a Frame Relay DTE device to be attached. Frame Relay DTE devices refer to those user devices that perform the LMI/DTE and F or B protocols such as routers, bridges, cluster controllers, and front-end processors, or packetized voice and video.

Table 7-1. Frame Relay Logical Port Types (Continued)

LPort Type...	Configures the PPort as	Performs the Frame Relay functions...
Frame Relay Feeder (UNI-DTE)	Frame Relay UNI-DTE	Specified for link management. Select this option to connect to a Frame Relay DCE (network switch) where the Cascade switch acts as the DTE. You can also use this type as the link between two Cascade switches when configuring a Frame Relay OPTimum trunk on the same physical port.
Frame Relay NNI	Network-to-Network Interface	According to the Frame Relay Forum NNI Specification. NNI enables two different switches or networks to connect together using a standard protocol. The NNI port performs both the DTE and DCE *Link Management Interface* (LMI) function. You can also use this port as the link between two Cascade switches when configuring a Frame Relay OPTimum trunk on the same physical port.
Frame Relay OPTimum PVC Trunk	Switch-to-switch Cascade trunk through a Frame Relay *Public Data Network* (PDN)	Known as Open Packet Trunking (OPTimum trunk). You must first configure either a UNI-DTE feeder or a Frame Relay NNI logical port on the same physical port to enable link management between the two connections.

Table 7-1. Frame Relay Logical Port Types (Continued)

LPort Type...	Configures the PPort as	Performs the Frame Relay functions...
Encapsulated FRAD (Frame Relay Assembler Disassember)	Frame Relay encapsulation/ de-encapsulation for HDLC/SDLC-based protocols	That encapsulate traffic entering the network and de-encapsulate it upon exiting the network. This configuration enables you to establish a single circuit between any FRAD port and another non-trunk port. The incoming HDLC/SDLC frames must have a start and end flag (hexadecimal '7E') and a 16-bit cyclic redundancy check (CRC 16). The remainder of the frame is transparent to the Cascade switch.
Direct Line Trunk	Trunk connection to another Cascade switch	In which the trunk connection carries traffic destined for other switches in the network using Cascade’s trunk protocol.
PPP-to-1490 Translation	Point-to-Point Protocol	That enable a PPP DTE device to communicate with another DTE device configured for Frame Relay and encapsulating multi-protocols, according to the RFC1490 Specification. This configuration enables you to establish a single circuit between the two devices. The switch performs the PPP Link Control Protocol (LCP) and Network Control Protocol (NCP) and translates PPP encapsulation into the RFC 1490 encapsulation.

Using Fault-Tolerant PVCs

You can configure Frame Relay UNI-DCE, UNI-DTE, and Network-to-Network Interface (NNI) logical ports for backup service by implementing a fault tolerant PVC configuration. A fault tolerant PVC configuration enables a logical port to serve as a backup for any number of active NNI and/or UNI ports. If the primary port fails, you can activate the backup port through CascadeView. Refer to "Configuring Fault-Tolerant PVCs" on page 7-44 for configuration information.

Using Frame Relay OPTimum Trunks

A Frame Relay OPTimum trunk creates a switch-to-switch Cascade trunk through a PDN into another Cascade Frame Relay network. This configuration maintains the Cascade header. The Cascade OPTimum trunk feature allows private enterprise networks to purchase lower-cost, public-carrier services as the trunk between two Cascade switches instead of using a more expensive leased line. Refer to "Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 7-39 for configuration information.

About Congestion Control

Congestion control is a feature that enables you to configure threshold values for each I/O module. The congestion-control parameters determine how the switch responds to frames and enables you to configure discard thresholds for red and amber frames.

Data travels through the network and is queued for transmit. The switch checks each transmit queue's state for congestion and monitors the behavior of each PVC. The switch marks each PVC as "good-behaved" or "bad-behaved" based on the configured congestion commitment.

Congestion States and the Switch

There are three congestion states:

- Mild (light mild and heavy mild)
- Severe (light severe and heavy severe)
- Absolute (light absolute and heavy absolute)

When congestion occurs on a link, the switch sets the FECN bit on packets traveling in the direction of the congestion and the BECN bit on packets traveling in the opposite direction of the congestion. Through OSPF, the switch communicates the congestion state of all trunks in the network to each node, and reduces the flow of excess data on PVCs routed through congested trunks.

All PVCs in a switch are examined as part of the one-second rate enforcement processing. If a PVC is routed through one or more congested trunks, excess burst data is reduced beginning with the most congested trunk.

When a PVC is no longer routed through a congested trunk, the switch allows red and amber packets into the network based on the initial configuration. When congestion occurs, only new incoming frames are discarded. When there is no congestion, all green, amber, and red (if applicable) frames are transmitted. If the number of transmitted red bits is greater than the configured threshold, the PVC is marked "*bad*." For more information about red, amber, and green frames, refer to the *Networking Services Technology Overview Guide*.

Table 7-2 shows how the congested and ingress switch reacts to congestion at each threshold state.

Table 7-2. Congested and Ingress Switch Behavior

Congestion State	Ingress Switch Be Reduction	Congested Switch Discards...	FECN/BECN Marking
Light-mild	Pm% of Be of "bad" PVCs	"bad" red frames	"bad" PVCs
Heavy-mild	Pm% of Be of all PVCs	all red frames	"bad" PVCs
Light-severe	Ps% of Be of "bad" PVCs Pm% of Be of other PVCs	all red and "bad" amber frames	all PVCs
Heavy-severe	Ps% of Be of all PVCs	all red and amber frames	all PVCs

Table 7-2. Congested and Ingress Switch Behavior (Continued)

Congestion State	Ingress Switch Be Reduction	Congested Switch Discards...	FECN/BECN Marking
Light-absolute	100% of Be of “bad” PVCs Ps% of Be of other PVCs	all red, amber, and “bad” frames	all PVCs
Heavy-absolute	100% of Be of all PVCs	all red, amber and green frames	all PVCs

Closed-Loop Congestion Control

Closed-loop congestion control reduces the rate of excess data into the network during congested periods. The reduction in excess data is in relation to ill-behaved connections and is proportional to the PVC’s configured *Be* value. Using OSPF, the trunk’s congestion state is communicated to all switches in the network. The ingress switch uses this information to reduce the flow of excess data into the network. You can enable or disable the closes-loop congestion control feature for each logical port. The default is “Off” (congestion disabled).

Link State Updates

In switches containing trunks, the OSPF agent in the switch monitors the trunk’s congestion state every *N* seconds. If one or more trunks become congested, OSPF sends a Link State Update (LSU) to all other switches in the network. When the switches receive the LSU, OSPF updates its routing table with the new congestion state. Similarly, if a trunk moves out of a congested state and remains non-congested for *Nc* seconds, OSPF sends a LSU to all switches in the network.

You can configure *N* and *Nc* time intervals (refer to Table 7-12 on page 7-27). The default is 1 second and 3 seconds, respectively. Table 7-12 shows the congestion parameters you can configure for each logical port.

Congestion Parameters

Table 7-3 lists the congestion parameters you can configure for each logical port.

Table 7-3. Congestion Parameters

Parameter	Description	Default
Check Interval (N)	Congestion state check interval	1 second
Clear Delay (Nc)	Congestion state clear delay	3 seconds
Fb	“Bad” PVC factor	30
Amber Pm (%)	Be deduction percentage level 1	50%
Amber Ps (%)	Be deduction percentage level 2	75%

Threshold Parameters

You can configure the mild, severe, and absolute congestion threshold parameters for each I/O module. You change the existing (default) values for the threshold parameters by modifying the logical port congestion-control attributes. When you configure the congestion thresholds, you set the threshold values incrementally as shown in Figure 7-1.

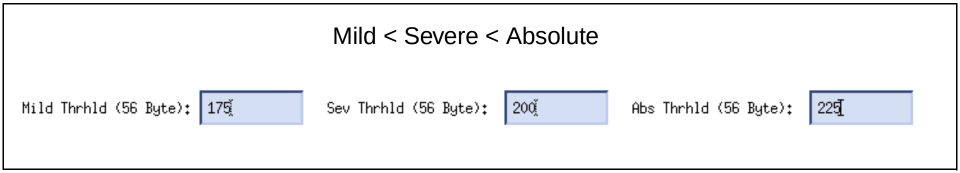


Figure 7-1. Congestion Threshold Example

In the example, if the congestion level is set at 175 for a mild threshold, the severe threshold must be greater than the mild threshold (200), and the absolute threshold must be greater than the severe threshold (225).

I/O Module Congestion Thresholds

Table 7-4 shows the maximum threshold values you can configure for each card type.

Table 7-4. Maximum Threshold Values per Logical Port

Card Type	56-Byte Buffers	Bytes
8-Port UIO	5450	305200
10-Port DSX	4668	261408
4-Port Channelized T1/T1 PRI	225	12600
4-Port Channelized E1/E1 PRI	174	9744
4-Port Unchannelized T1	5408	302848
4-Port Unchannelized E1	5408	302848
2-Port HSSI	23632	1323392
1-Port ATM UNI	60799	3404744
1-Port Channelized DS3	1922	107632

Do not exceed the maximum threshold value for each card type. The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.

*For channelized T1/T1 PRI and channelized E1/E1 PRI cards, if **n** DS0s are assigned per channel, the maximum value allowed on the number of buffers is n x 225 (T1 card) and n x 174 (E1 card).*

Table 7-5 lists the default values for a 4-port channelized T1/T1 PRI card. The threshold default values vary depending on the number of DS0s you assign to each channel. For example, if you assign each DS0 to one channel on a 4-port channelized T1 card, you can assign a maximum of 225 (56-byte) buffers to each logical port.

Table 7-5. 4-Port Channelized T1/T1 PRI Default Values

Congestion Level	1 DS0/Channel		2 DS0s/Channels		>2 DS0s/Channels	
	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
Mild	175	9800	225	12600	225	12600
Severe	200	11200	294	16464	294	16464
Absolute	225	12600	450	25200	588	32928

Table 7-6 lists the default values for a 4-port channelized E1/E1 PRI card. The threshold default values vary depending on the number of DS0s you assign to each channel. For example, if you assign each DS0 to one channel on a 4-port channelized T1 card, you can assign a maximum of 174 (56-byte) buffers to each logical port.

Table 7-6. 4-Port Channelized E1/E1 PRI Default Values

Congestion Level	1 DS0/Channel		2 DS0s/Channels		3 DS0s/Channels		>3 DS0s/ Channels	
	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
Mild	150	8400	225	12600	225	12600	225	12600
Severe	165	9240	294	16464	294	16464	294	16464
Absolute	174	9744	340	19040	520	29120	588	32928

Table 7-7 lists the default values for the ATM, HSSI, UIO, 10-port DSX, channelized DS3, and unchannelized T1/E1 cards.

Table 7-7. ATM, HSSI, UIO, DSX, Chan DS3, Unchan T1/R1 Defaults

Card Type	Congestion Level	56-Byte Buffers	Bytes
ATM and HSSI	Mild	4268	239008
	Severe	8535	477960
	Absolute	17070	955920
UIO, 10-port DSX, unchannelized T1/E1	Mild	225	12600
	Severe	294	16464
Channelized DS3	Mild	480	26880
	Severe	961	53816
	Absolute	1922	107632

Configuring a Logical Port for a VPN

You create a VPN and add customers to a specific VPN when you first configure a switch (see Chapter 4).

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

Step 1. Create the UNI logical port and specify the net overflow parameter (page 7-21).

Step 2. Dedicate the PVC logical port endpoints to a specific VPN and customer (page 7-43).

Step 3. Dedicate a trunk to a specific customer (refer to Chapter 10).

Net Overflow Parameters

You configure the net overflow parameters when you add a logical port. You can set the net overflow parameters to one of two modes:

Public (default) — Trunks are dedicated to the customer, however, if the trunk goes down the customer’s traffic is allowed to run over common trunks (shared by different customers).

Restrict —Trunks are dedicated to the customer, and traffic is restricted to these trunks only. A customer using restricted trunk service must purchase redundancy trunks as backup.

Configuring Frame Relay Logical Ports

This section describes how to configure logical ports for the Cascade Frame Relay network service. Figure 7-2 shows the steps in this process.

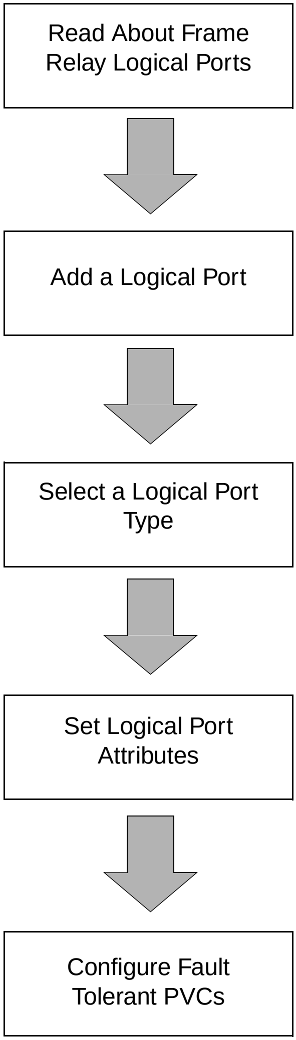


Figure 7-2. Defining a Logical Port

Before You Begin

Before you begin, verify the following tasks are complete:

- ☑ Create a network map and add a Cascade switch, add the subnet mask and VPN (Chapter 4)
- ☑ Configure the IP address and set the NMS path (Chapter 5)
- ☑ Configure the I/O module(s) and physical port parameter(s) (Chapter 6)

Accessing Logical Port Functions

To access the Logical Port functions in CascadeView/UX, use the following steps:

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

   Or, for *channelized DS3 I/O modules*, double-click the channel (button) that you want to configure. The Set Channel Attributes dialog box appears.
5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears as shown in Figure 7-3.

The Set All Logical Ports in PPort 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 many logical port functions, such as add, modify, and delete logical ports.

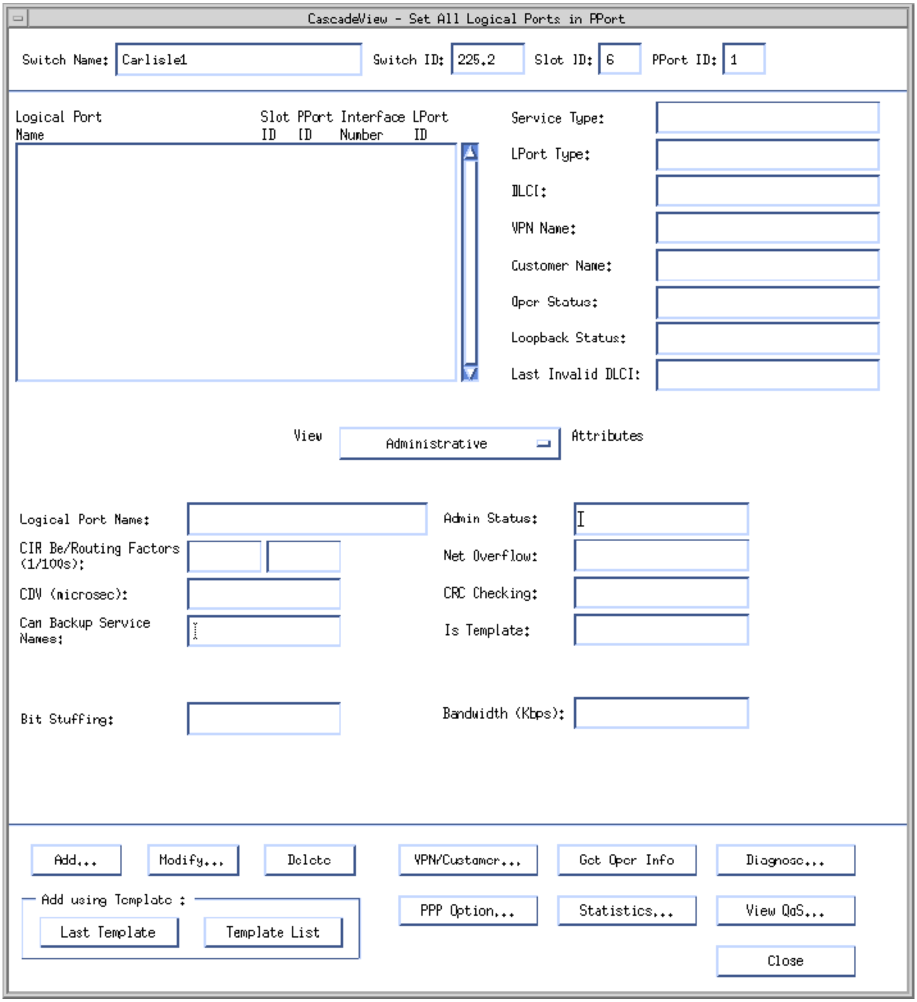


Figure 7-3. Set All Logical Ports in PPort Dialog Box

Table 7-8 describes the Set All Logical Ports in PPort command buttons.

Table 7-8. Set All Logical Ports in PPort Command Buttons

Command Button	Function
Add Modify Delete	Enables you to add a new logical port or Modify or Delete an existing logical port configuration. For information about deleting logical ports refer to "Deleting the Logical Port" on page 7-56.
Get Oper Info	Displays a status message in the *Oper Status* field for the selected logical port.
Diagnose	Accesses diagnostic tests for the selected logical port. For more information about diagnostics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Statistics	Displays the summary statistics for and existing logical port. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Last Template/ Template List	If you have already defined a logical port configuration and saved it as a template, you can use this option to define a new logical port using the same parameters. Refer to the "Administrative Tasks" on page 7-53 for more information.
VPN/Customer	Displays the Virtual Private Network customer's name.
View Qos Parameters	Displays the Quality of Service parameters.

Adding a Frame Relay Logical Port

To add a Frame Relay logical port:

1. Perform the steps in “Accessing Logical Port Functions” on page 7-14.
2. On the Set All Logical Ports in PPort dialog box, choose Add.

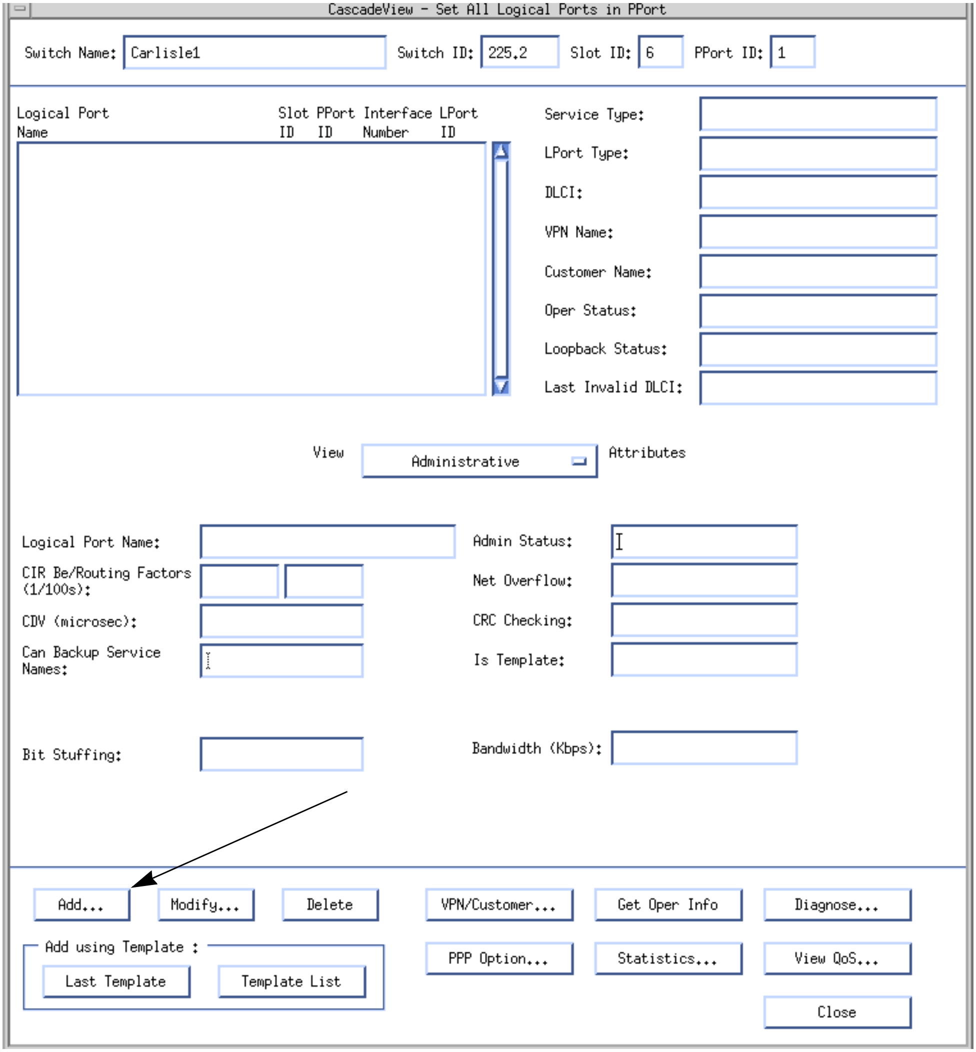


Figure 7-4. Set All Logical Ports in PPort Dialog Box

The Add Logical Port dialog box appears as shown in Figure 7-5.

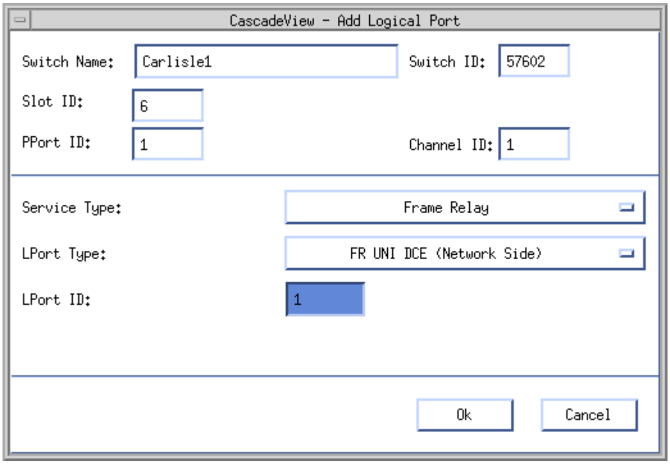


Figure 7-5. Add Logical Port Dialog Box

3. Define the specific logical port configuration. Refer to Table 7-9 on page 7-19 for more information on the different types of logical ports.

Table 7-9 describes where to find configuration instructions for the different types of logical ports.

Table 7-9. Frame Relay Logical Port Configurations

Service Type	Logical Port Type	Refer to...
Frame Relay	FR UNI-DCE	"Defining Frame Relay UNI-DCE Logical Ports" on page 7-21.
	FR UNI-DTE	"Defining Frame Relay UNI-DTE Logical Ports" on page 7-35.
	FR UNI-NNI	"Defining Frame Relay NNI Logical Ports" on page 7-37.
	Frame Relay OPTimum Trunk	"Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 7-39.
Others	Encapsulated FRAD Direct Line Trunk PPP-to-1490 Translation	"Defining Other Types of Frame Relay Logical Ports" on page 7-41.

The Set Attributes Options Menu

When you define a new logical port, the Add Logical Port dialog box displays a Set Attributes option menu (Figure 7-6) that enables you to set different attributes for each type of logical port. Attributes include:

Administrative — Sets the admin status, net overflow, and bandwidth parameters.

Congestion Control — Sets the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network.

Link Management — Sets the link management protocol used in the network and the LMI update delay and error thresholds.

Trap Control — Sets the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port.The supported logical port types are different for each I/O module.

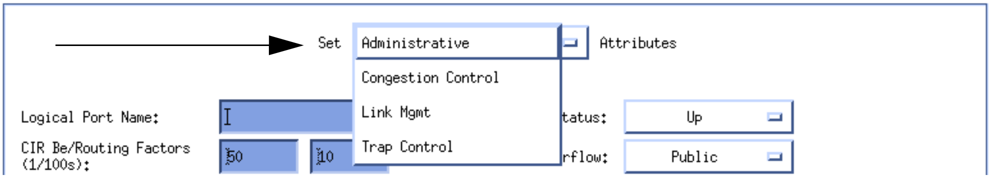


Figure 7-6. Set Attributes Option Menu

Defining Frame Relay UNI-DCE Logical Ports

A Frame Relay UNI DCE logical port performs the Frame Relay DCE functions for link management and usually connects to a Frame Relay DTE device. These devices include routers, bridges, cluster controllers, and front-end processors, or packetized voice and video.

To define a Frame Relay UNI-DCE logical port:

1. Complete the Add Logical Port dialog box (Figure 7-5 on page 7-18) fields described in Table 7-10.

Table 7-10. Add Logical Port (UNI-DCE) Fields

Field	Action/Description
Service Type	Select Frame Relay.
LPort Type	Select FR UNI DCE (Network Side).
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the LPort ID is a read-only field that automatically defaults to 1.

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields shown in Figure 7-7.

> *The following example shows the parameters you define if you select Frame Relay UNI-DCE as the logical port type for a channelized DS3 module. Parameters vary depending on the type of module.*

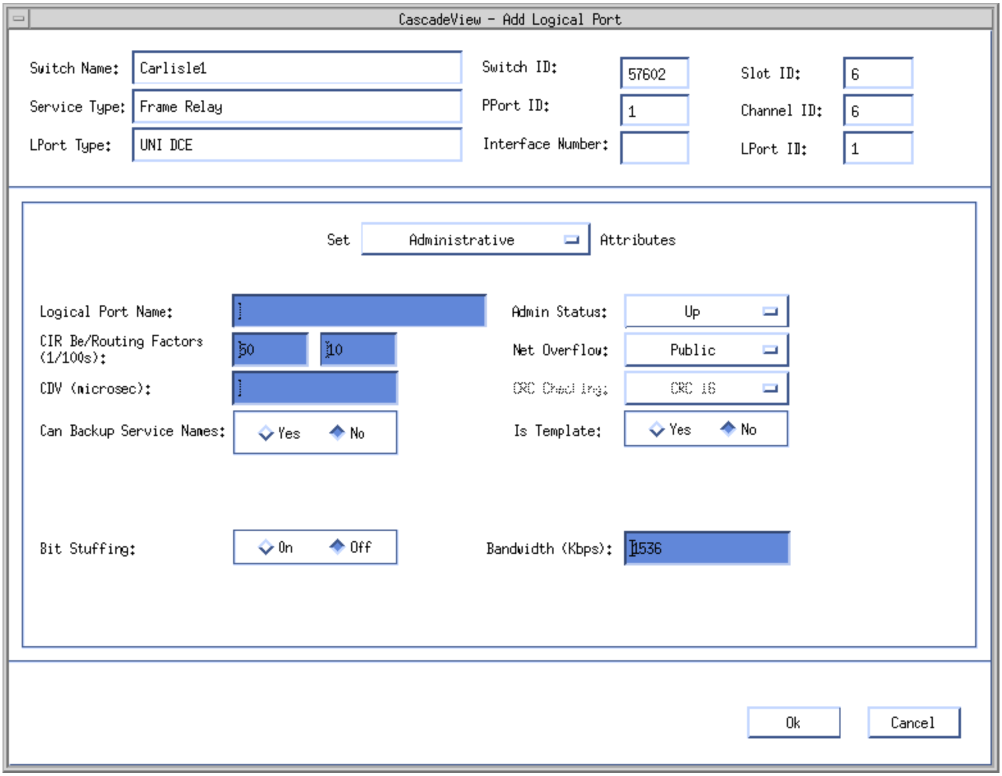


Figure 7-7. Set Administrative Attributes Dialog Box (UNI-DCE)

Administrative Attributes

Complete the required administrative attributes fields described in Table 7-11.

Table 7-11. Set Administrative Attributes Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.

Table 7-11. Set Administrative Attributes Fields (Continued)

Field	Action/Description
CIR Be/Routing	Enter a value between 0-100 percent. This value represents the UNI bandwidth percentage on all configured zero CIR circuits. The default is 100 percent.
Factors (1/100s)	Enter a value between 0-100 percent. This value represents the routing factor percentage on all rate enforcement circuits. The default is 10 percent.
CDV (microsec)	Configure the Cell Delay Variation (CDV). The UPC uses this value to police the requested traffic descriptor. Valid values are between 1 - 65535 µs. The default is 200 µs.
Can Backup Service Names	*(Fault-tolerant PVC only)* Select Yes to configure a logical port for backup service. For more information, refer to "Configuring Fault-Tolerant PVCs" on page 7-44.
Admin Status	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. *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
CRC Checking (HSSI modules only)	Set this value to match the number of error checking bits used by the CPE connected to this port. Performs a cyclic redundancy check (CRC) on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.

Table 7-11. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Is Template	(*Optional*) Save these settings as a template to use again to quickly configure a logical port with the same options. To create a template, choose Yes in the *Is Template* field. Refer to "Using Templates" on page 7-53 for more information.
Channels allocated for a Logical Port are marked by their IDs	If you are configuring a channelized T1 or E1 module, specify the DS0 (for T1) or TS0 (for E1) channel(s) assigned to the logical port. The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel ***Note***: *The logical port bandwidth either increments or decrements depending on the number of channels you select or deselect. You can configure other logical ports with different attributes, to other DS0/TS0 channels on this same physical port.*
Bit Stuffing	Select the bandwidth that matches the bandwidth capability of the customer premise equipment (CPE) connected to this logical port. Enables bit stuffing on T1/E1/DSX-1 ports. Bit stuffing effects the available bandwidth of each DS0/TS0 channel on this port. *On* – Provides 56 Kbps of bandwidth. *Off* – Provides 64 Kbps of bandwidth.

Table 7-11. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth remaining from the physical clock rate, less any logical ports already configured. To define a trunk logical port on this same physical port, decrease the amount of bandwidth on this logical port to ensure sufficient remaining bandwidth. For example: *Physical port clock speed*: 1536 Kbps *Logical port UNI-DTE/NNI Feeder Bandwidth*: 56 Kbps *Logical port Frame Relay Trunk Bandwidth*: 1480 Kbps The example configuration allocates a PDN trunk with 1480 Kbps bandwidth between two Cascade switches, each attached to a PDN network.

Congestion Control Attributes

1. Set the congestion control attributes by selecting *Congestion Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 7-8.

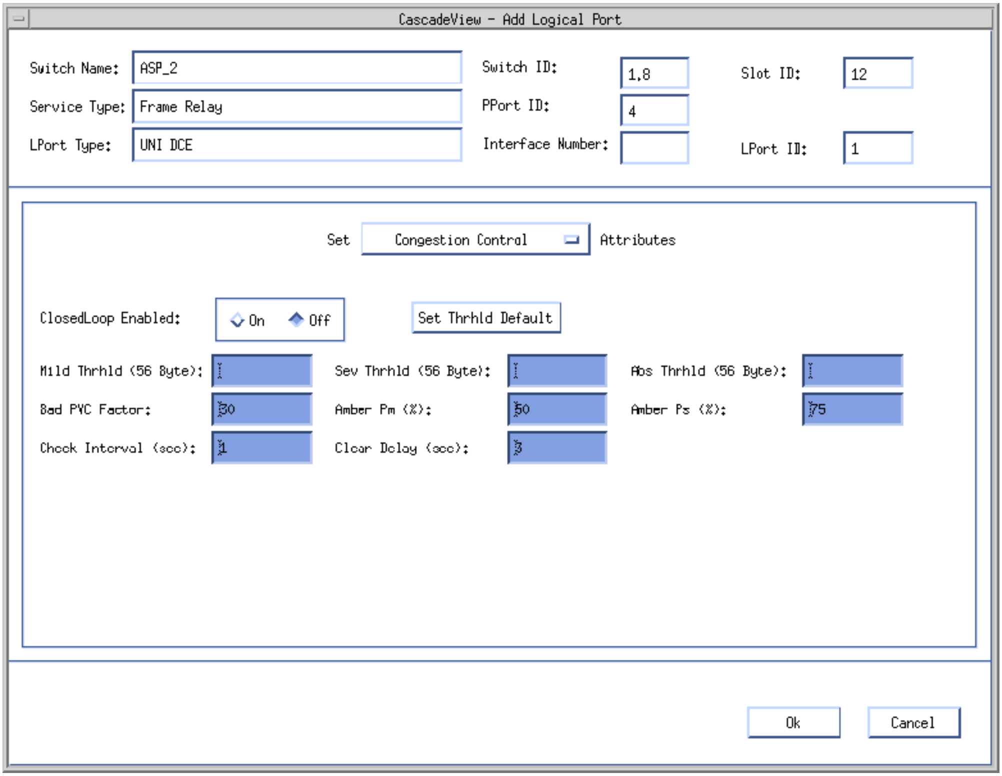


Figure 7-8. Set Congestion Control Attributes Dialog Box

> *Do not exceed the maximum threshold value for each card type (see Table 7-4 for more information). The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.*

> *For channelized T1/T1 PRI and Channelized E1/E1 PRI cards, if **n** DS0s are assigned per channel, the maximum value allowed on the number of buffers is n x 225 (T1) and n x 174 (E1).*

2. Complete the required dialog box fields described in Table 7-12.

Table 7-12. Set Congestion Control Attributes Fields

Field	Action/Description
ClosedLoop Enabled	Set the congestion control parameters. This field enables/disables OSPF closed-loop congestion control for each logical port. For more information refer to “Closed-Loop Congestion Control” on page 7-7. Options include: *Off (default)* – Disables closed-loop congestion. *On* – Enables closed-loop congestion.
Set Thrhld Default	Sets the Mild, Severe, and Absolute threshold settings to the default settings described in Table 7-5 on page 7-10 through Table 7-5 on page 7-10.
Mild Thrshld (56 Byte) Severe Thrshld (56 Byte) Absolute Thrshld (56 Byte)	Accept the defaults or enter values for the mild, severe, and absolute threshold fields as defined in Table 7-5 through Table 7-7. ***Note**: Do not exceed the maximum threshold value for each card type (see Table 7-4 for more information). The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.* ***Note**: If you are setting threshold parameters on a T1/E1 card, the default values will not appear until you set the bit stuffing and bandwidth allocation. Refer to Table 7-11 on page 7-22 for more information.* ***Note**: For channelized T1/T1 PRI and Channelized E1/E1 PRI cards, if n DS0s are assigned per channel, the maximum value allowed on the number of buffers is n x 225 (T1) and n x 174 (E1).*

Table 7-12. Set Congestion Control Attributes Fields (Continued)

Field	Action/Description
Bad PVC Factor	Enter a value between 0-32. Determines the threshold for "bad" PVC detection. The following example shows the relationship between the "bad" PVC factor and threshold. $$\text{Threshold} = \frac{Bc+(Be/2)}{2^{(32-F_b)}}$$ The default is 30. ***Note**: If you select simple as the rate enforcement scheme (see Table 11-8 on page 11-23) this feature is disabled.*
Amber Pm (%)	Controls the reduction percentage of Be when mild congestion occurs. Enter a Pm% value. The default is 50%.
Amber Ps (%)	Enter a Ps% value. This value controls the reduction percentage of Be when severe congestion occurs. The default is 75%.
Check Interval (sec)	Enter and interval. This determines the number of seconds in which the switch monitors the trunk's congestion on the port. The default is one (1) second.
Clear Delay (sec)	Enter a value. This determines the number of seconds in which the switch monitors the trunk's non-congestion state. Enter a value. The default is three (3) seconds.

Link Management Attributes

1. Set the link management attributes by selecting *Link Mgmt* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 7-9.

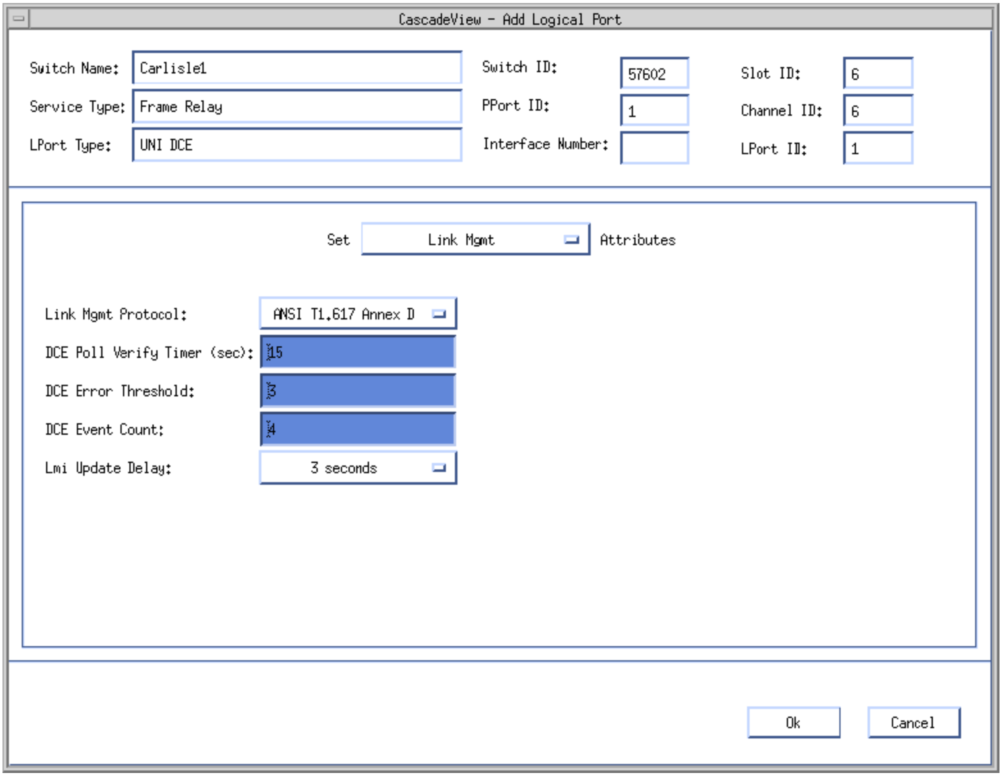


Figure 7-9. Set Link Mgmt Attributes Dialog Box

2. Complete the required fields described in Table 7-13.

Table 7-13. Set Link Mgmt Attributes Fields

Field	Action/Description
Link Mgmt Protocol	Select the link management protocol that represents the type of Frame Relay implementation used in your network. Options include: *ANSI T1.617 Annex D (default)* – The network uses DLCI 0 for link management. *LMI Rev1* – The network uses DLCI 1023 for link management. *CCITT Q.933 Annex A* – For international standard (European) use only. The network uses DLCI 0 for link management. *Auto Detect* – Use this option only if the attached CPE provides the link management protocol. This logical port can then automatically detect which protocol is in use. *Disabled* – Use this option only if the attached CPE does not support link management or to disable link management for troubleshooting purposes.
DCE Poll Verify Timer (sec) or DTE Poll Verify Timer (sec)	Set the poll verify timer (in seconds). This field specifies the value of the T392 timer, which sets the length of time the network waits between status inquiry messages. If the network does not receive a status inquiry message within the specified number of seconds, the network receives an error. The default value is 15 seconds. ***Note****: The attached CPE must be set to a value that is less than the DCE (DTE) Poll Verify Timer.* Increase this value if the DTE (DCE) device has a poll frequency that is greater than or equal to the DCE (DTE) Poll Verify Timer. Decrease this value if the DTE's (DCE's) poll frequency is less than or equal to one-half that of the DCE (DTE) poll verify timer.

Table 7-13. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
DCE Error Threshold or DTE Error Threshold	Specify an error threshold.This parameter is used with the DCE (DTE) Events Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DCE (DTE) Event Count. If the number of events found in error exceeds the specified DCE (DTE) Error Threshold, the link is declared inactive. The default value is three (3).
DCE Event Count or DTE Event Count	Specify the number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or invalid status inquiry message or expiration of the T392 timer. For example, use the default DCE (DTE) Error Threshold value of 3 and the default DCE (DTE) Event Count value of 4. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events. ***Note****: The DCE (DTE) Error Threshold and the DCE (DTE) Event Count work together. The lower you set these values, the more sensitive the logical port is to LMI poll errors. To make the logical port less sensitive to errors, increase these values.*

Table 7-13. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
LMI Update Delay	Set a timer from 1 to 9 seconds to enable asynchronous LMI updates. The default is three (3) seconds. When you set this timer, the switch sends a signal (known as an *event*) to notify other network equipment (CPE) when a circuit on this logical port goes up or down. The specified time interval creates a buffer. If the circuit recovers within this period of time, no event is issued. If you choose *No Updates*, the switch does not send a signal to the CPE. If you choose *No Delay*, the switch sends an update immediately to the CPE. For example, if the network takes a significant amount of time to recover from trunk outages, increase the LMI update delay. This delay minimizes network downtime visibility to end-users.

Trap Control Attributes

1. Set the trap control attributes by selecting *Trap Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 7-10.

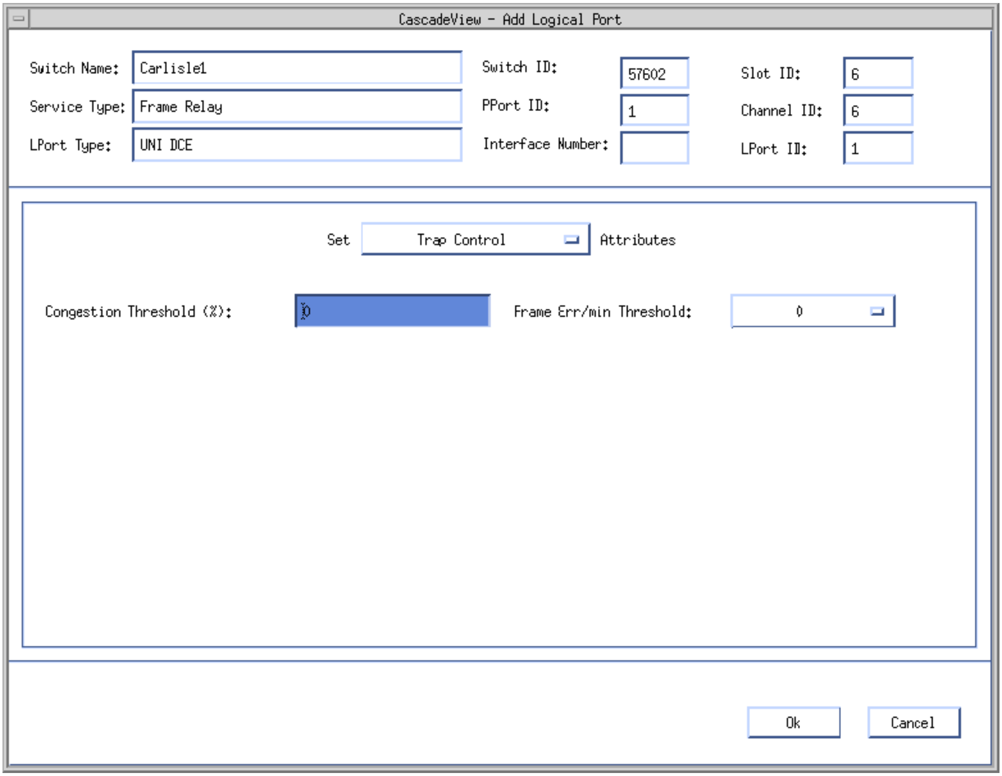


Figure 7-10. Set Trap Control Attributes Dialog Box

2. Complete the required fields described in Table 7-14.

Table 7-14. Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold (%)	Enter a value between 0 and 100 to indicate the threshold percentage for generating and sending traps to the NMS for this logical port. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the percentage value you enter. Adjust the entered value according to how sensitive this port needs to be to network congestion. Options include: *Low* – Generates a trap at the first sign of congestion. *High* – Generates traps for serious network congestion. *Zero (default)* – Disables congestion threshold. If you enter zero, no traps are generated for this logical port.
Frame Err/Min Threshold	Enter a value from 0 to 16384 to configure the threshold of frame errors on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS. Adjust this value according to how sensitive this port needs to be to frame errors. Options include: *Low* – Port is sensitive to frame errors. *High* – Generates traps when a significant number of frame errors occurs within a one-minute period. *Zero (default)* – Disables this feature, which prevents traps from being generated for this logical port.

3. Choose OK. The Set All Logical Ports in PPort dialog box appears.
4. Choose Close. The Set Physical Port Attributes dialog box appears.
5. *(Optional*) To configure this logical port for a specific VPN and customer, refer to “Selecting the VPN and Customer Name” on page 7-43.
6. Configure the remaining logical ports for this physical port.

Defining Frame Relay UNI-DTE Logical Ports

A Frame Relay UNI DTE logical port performs the Frame Relay DTE functions specified for link management. Select this option to connect to a Frame Relay DCE (network switch) where the Cascade switch acts as the DTE. You can also use this type of logical port as the link between two Cascade switches when configuring a Frame Relay OPTimum trunk on the same physical port. (Refer to page 7-39 for more information on Frame Relay OPTimum trunks.)

To define a Frame Relay UNI-DTE logical port:

1. Complete the Add Logical Port dialog box (see Figure 7-5 on page 7-18) fields described in Table 7-15.

Table 7-15. Add Logical Port (UNI-DTE) Fields

Field	Action/Description
Service Type	Select Frame Relay.
LPort Type	Select FR UNI DTE (User Side).
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the LPort ID is a read-only field that automatically defaults to one (1).

2. Choose OK. The Add Logical Port dialog box appears displaying the Set Attributes option menu and fields shown Figure 7-11.

The following example shows the parameters you define if you select Frame Relay UNI DTE (User Side) as the logical port type for a channelized T1 module. Parameters vary depending on the type of module.

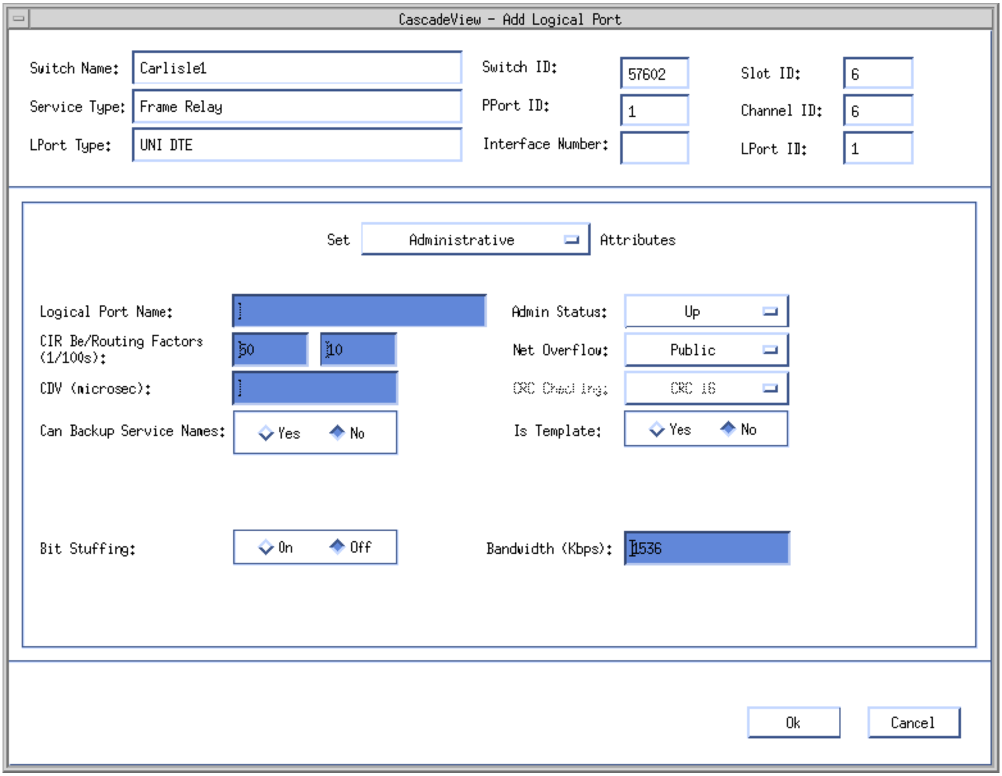


Figure 7-11. Set Administrative Attributes Dialog Box (FR UNI-DTE)

3. Complete the administrative attributes described in Table 7-11 on page 7-22.

4. Complete the congestion control attributes described in Table 7-12 on page 7-27.

5. Complete the link management attributes described in Table 7-13 on page 7-30.

6. Complete the trap control attributes described in Table 7-14 on page 7-34.

7. *(Optional)* To configure this logical port for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 7-43.

8. When you finish configuring the DTE logical port, you can add a trunk logical port. Refer to "Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 7-39 for information.

Defining Frame Relay NNI Logical Ports

A Frame Relay NNI logical port enables you to connect a Cascade switch to non-Cascade switches or networks using a standard protocol. You can also use an NNI logical port as the link between two Cascade switches when configuring a Frame Relay OPTimum trunk on the same physical port.

To define a Frame Relay NNI logical port:

1. Complete the Add Logical Port dialog box (see Figure 7-5 on page 7-18) fields described in Table 7-16.

Table 7-16. Add Logical Port (FR-NNI) Fields

Field	Action/Description
Service Type	Select Frame Relay.
LPort Type	Select FR NNI.
Logical Port ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to 1.

2. Choose OK. The Add Logical Port dialog box appears displaying the Set Attributes option menu and fields shown in Figure 7-12.

The following example shows the parameters you define if you select Frame Relay NNI as the logical port type for a channelized T1 module. Parameters vary depending on the type module.

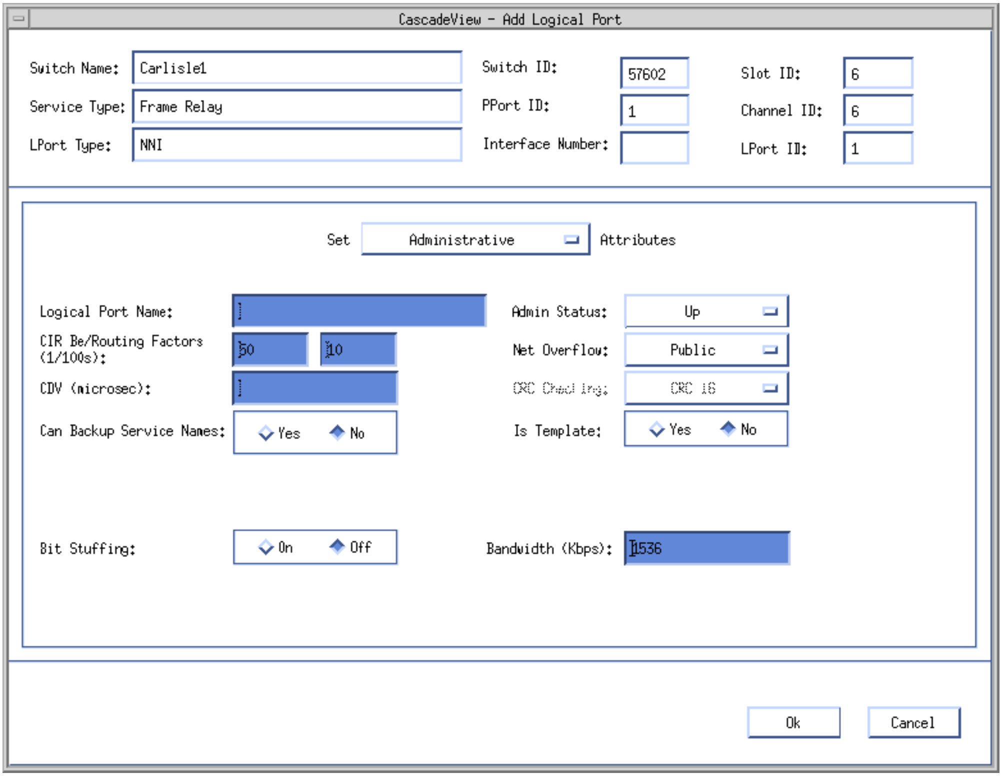


Figure 7-12. Set Administrative Attributes Dialog Box (FR NNI)

3. Complete the administrative attributes described in Table 7-11 on page 7-22.

4. Complete the congestion control attributes described in Table 7-12 on page 7-27.

5. Complete the link management attributes described in Table 7-13 on page 7-30.

6. Complete the trap control attributes described in Table 7-14 on page 7-34.

7. *(Optional*) To configure this logical port for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 7-43.

8. When you finish configuring the logical ports, you can add a trunk logical port (if necessary). Refer to "Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 7-39 for information.

Defining Frame Relay OPTimum PVC Trunk Logical Ports

To configure a Frame Relay OPTimum trunk, you must first configure either a UNI-DTE feeder or a Frame Relay NNI logical port on the same physical port.

You cannot define a trunk logical port on a channelized T1/E1 module.

Use the following sequence to configure an OPTimum trunk:

Step 1. Configure the physical port you want to use for the OPTimum trunk (refer to "Configuring Physical Ports" on page 6-9).

Step 2. Configure one of the following logical ports on this physical port:

- Frame Relay DTE (page 7-21) or
- NNI (page 7-37)

Assign this logical port a minimum amount of bandwidth.

Step 3. Follow the instructions in this section to configure a Frame Relay OPTimum trunk logical port. You can assign the remaining bandwidth to this logical port.

About DLCI Numbers

A data link connection identifier (DLCI) number is a 10-bit address that identifies PVCs. This DLCI number corresponds to the DLCI number the Frame Relay trunk uses to access the PDN. The PDN recognizes this as a normal PVC carrying user traffic.

Depending on your link management type, use the guidelines in Table 7-17 to define DLCI numbers.

Table 7-17. DLCI Number Guidelines

DLCI Number Range	Description
0-15	Reserved
16-991	Available for all link management types
992-1007	Available for LMI Rev 1 only
1008-1023	Reserved

To define a logical port as a Frame Relay OPTimum PVC trunk:

1. Complete the Add Logical Port dialog box (see Figure 7-5 on page 7-18) fields described in Table 7-18.

Table 7-18. Add Logical Port (OPTimum PVC Trunk) Fields

Field	Action/Description
Service Type	Select Frame Relay.
LPort Type	Select OPTimum PVC Trunk.
DLCI Number	Enter a data link connection identifier (DLCI) number that corresponds to the DLCI number the Frame Relay trunk uses to access the PDN. The PDN recognizes this as a normal PVC carrying user traffic.

2. Choose OK. The Add Logical Port dialog box appears and displays the Set Attributes option menu and fields shown in Figure 7-7 on page 7-22.
3. Complete the administrative attributes fields described in Table 7-11 on page 7-22.
4. Complete the congestion control attributes fields described in Table 7-12 on page 7-27.

> *Set the congestion threshold attributes on the feeder logical port only. You cannot define the threshold attributes on the optimum trunk logical port.*

5. Complete the link management attributes fields described in Table 7-13 on page 7-30.
6. Complete the trap control attributes fields described in Table 7-14 on page 7-34.
7. (*Optional*) To configure this logical port for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 7-43.
8. When you finish configuring the logical ports, you can add the trunk line connections. Refer to Chapter 10, "Configuring Trunks" for more information.

Defining Other Types of Frame Relay Logical Ports

On the Add Logical Port dialog box, you can define the following types of Frame Relay logical ports by selecting *Others* as the service type.

Encapsulated FRAD — Configures the port to perform Frame Relay encapsulation/de-encapsulation for the HDLC/SDLC-based protocol.

Direct Line Trunk — Configures the port for a trunk connection to another Cascade switch.

PPP-to-1490 Translation — Configures the port to enable a configured Point-to-Point Protocol (PPP) DTE device to communicate with another DTE device configured for Frame Relay and encapsulating multiprotocols (according to RFC1490).

To define one of these services:

1. Complete the Add Logical Port dialog box fields described in Table 7-19.

Table 7-19. Add Logical Port (Other) Fields

Field	Action/Description
Service Type	Select Others.
LPort Type	Select a logical port type from the list.
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one (1).

2. Choose OK. The Add Logical Port dialog box appears and displays the Set Attributes option menu and fields shown in Figure 7-7 on page 7-22.
3. Complete the administrative attributes described in Table 7-11 on page 7-22.
4. Complete the congestion control attributes described in Table 7-12 on page 7-27.
5. Complete the link management attributes described in Table 7-13 on page 7-30.
6. Complete the trap control attributes described in Table 7-14 on page 7-34.
7. When you finish configuring the logical ports, you can add the trunk-line connections. Refer to Chapter 10 for more information.

Selecting the VPN and Customer Name

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

1. From the Set All Logical Ports in PPort dialog box (Figure 7-4 on page 7-17), select the logical port and choose VPN/Customer. The Select Customer and VPN dialog box appears as shown in Figure 7-13. For more information about VPNs, refer to page 7-12.

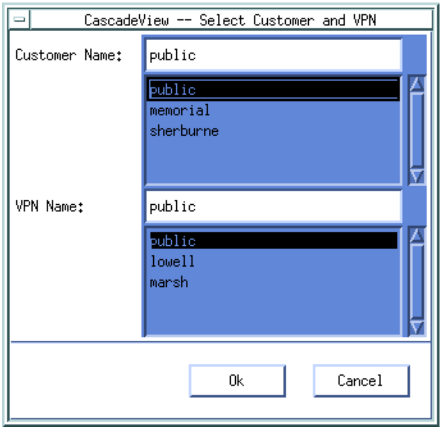


Figure 7-13. Select Customer and VPN Dialog Box

2. Select the customer and VPN name from the list.
3. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 7-4 on page 7-17).
4. Choose Close to return to the Set Physical Port attributes dialog box.
5. Choose Close to return to the Switch Back Panel dialog box.

Configuring Fault-Tolerant PVCs

A fault tolerant PVC configuration enables Frame Relay UNI DCE, DTE, or NNI logical ports to serve as a backup for any number of active NNI and/or UNI ports. If a primary port fails or if you need to take a primary port offline, you activate the backup port. When a backup port is not in use, the port is idle (no DLCIs) and does not use network resources.

To create a network configuration with fault-tolerant PVCs:

Step 1. Define a UNI-DCE (page 7-21), UNI-DTE (page 7-35), or UNI-NNI (page 7-37) logical port for backup service.

Step 2. Create a primary port and specify a service name for the primary port (refer to page 7-44).

Step 3. Configure circuits to use a service name as the endpoint (refer to "For a fault tolerant PVC Configuration" on page 11-16).

Step 4. Activate the backup port (refer to "Activating a Backup Port" on page 7-48).

Creating a Primary Port

To create a primary port, you assign a *service name* to a UNI/NNI logical port. When you configure the circuit, choose this service name as the endpoint, rather than a switch and logical port. When you activate the backup port, all PVCs on the failed primary port are rerouted automatically, preserving DLCIs in the process.

Cascade's fault tolerant PVC feature is transparent to the end user and CPE equipment. Therefore, end users can benefit from this feature through the public Cascade-based Frame Relay network, or by combining their private Cascade switch's network with their public-carrier services.

Creating Service Names

The *service name binding* is a name you assign the primary port. A circuit recognizes its service endpoint by the service name binding 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 Set Service Name Bindings dialog box appears as shown in Figure 7-14, displaying any configured service names.

   You can 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*.

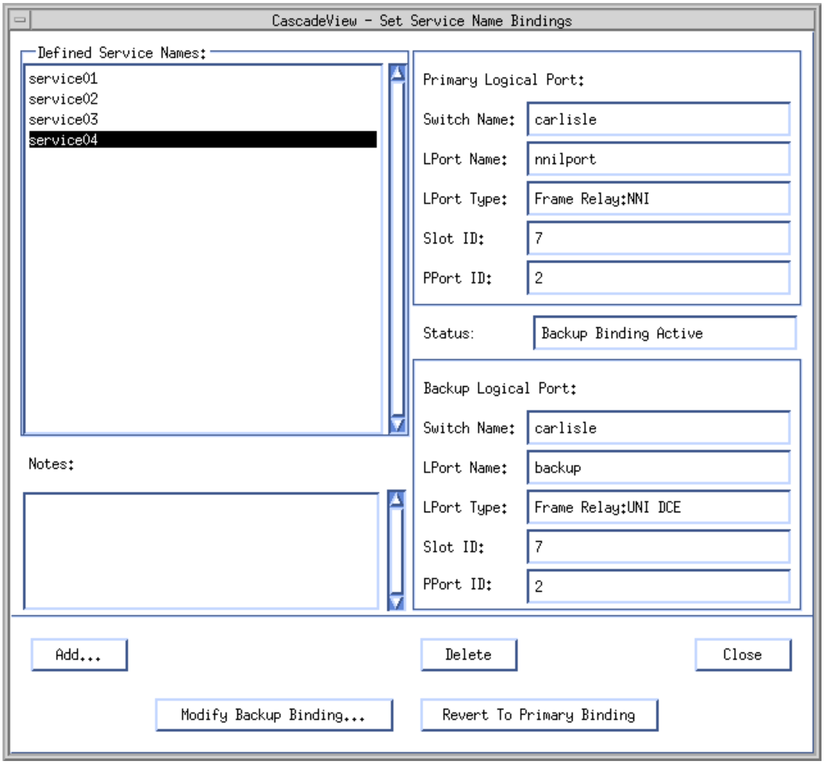


Figure 7-14. Set Service Name Bindings Dialog Box

2. Choose Add. The Select End Logical Port dialog box appears as shown in Figure 7-15.

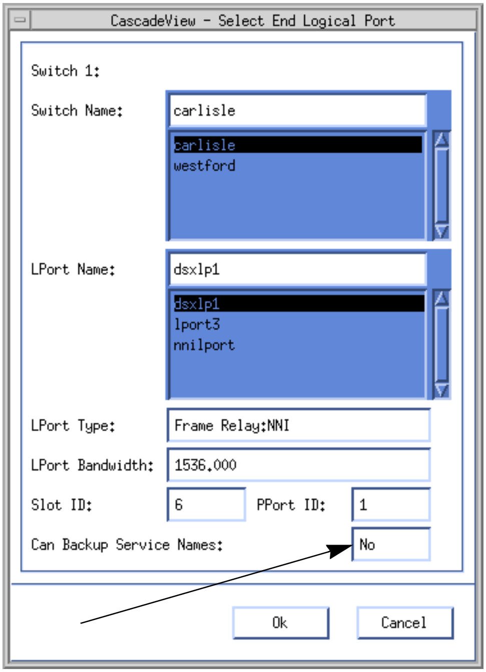


Figure 7-15. Select End Logical Port Dialog Box

3. Select the switch name and the primary logical port name.

> *Make sure that the "Can Backup Service Names" field displays No. Do not choose a port that is already configured as a backup port.*

4. Choose OK. The Add Service Name Binding dialog box appears as shown in Figure 7-16.

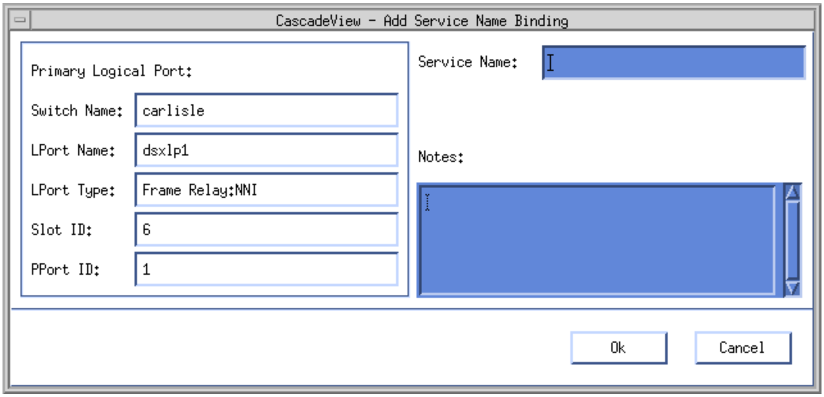


Figure 7-16. Add Service Name Binding Dialog Box

5. Enter a service name up to 32 alphanumeric characters. Optionally, you can enter a brief comment or description in the Notes box.

6. Choose OK.

7. Follow the instructions in "Accessing Circuit Functions" on page 11-12 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 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.

Before you activate a backup binding port, verify you configured a backup logical port. For more information, refer to *Table 7-11 on page 7-22**.*

To activate the backup port:

1. From the Administer menu, select Cascade Parameters ⇒ Service Name Binding. The Set Service Name Bindings dialog box appears as shown in Figure 7-17.

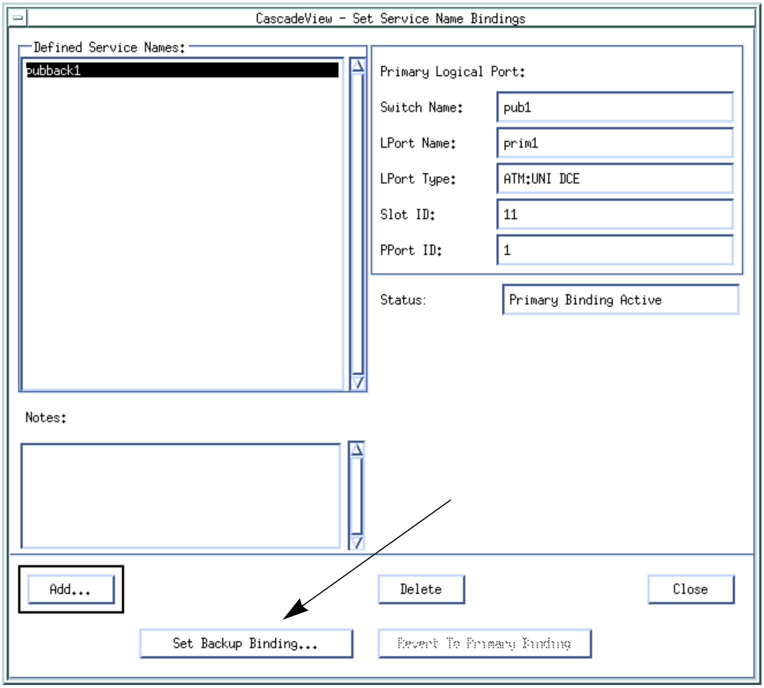


Figure 7-17. Set Service Name Binding Dialog Box

2. Choose Set Backup Binding. The Select End Logical Port dialog box appears as shown in Figure 7-18.

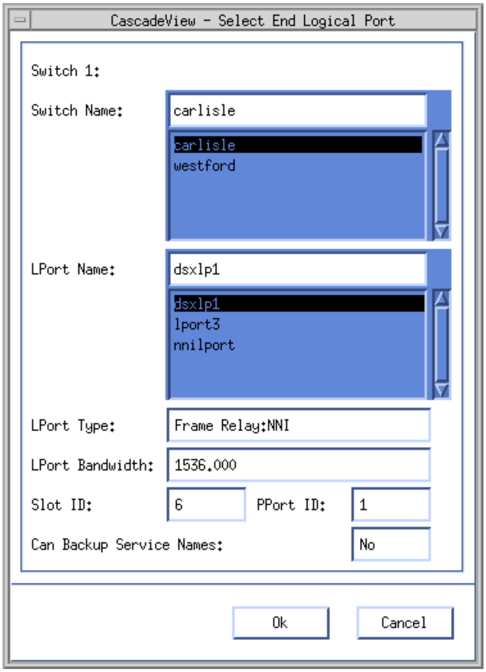


Figure 7-18. Select End Logical Port Dialog Box

3. Select the switch on which to use this backup-service name.

4. The LPort Name field displays a list of logical ports configured for this service. Select the *same* logical port type as the port you need to back up.

Make sure that the "Can Backup Service Names" field displays Yes. This field indicates you can use this logical port as a backup.

5. Choose OK. The Set/Modify Backup Service Name Binding dialog box appears as shown in Figure 7-19. This dialog displays the service name that corresponds to the switch and logical port name.

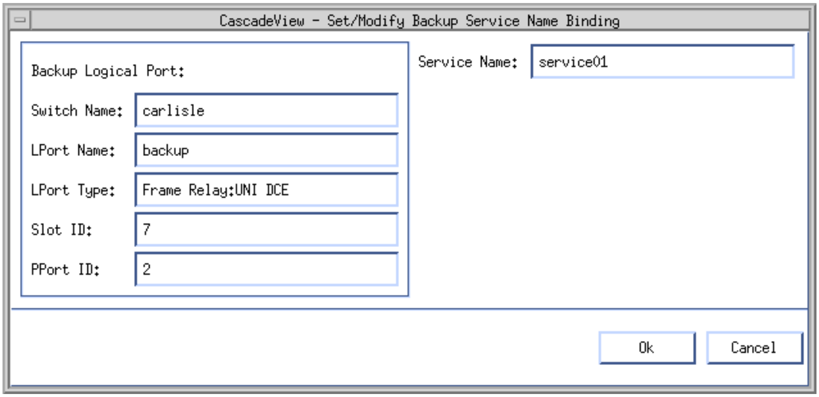


Figure 7-19. Set/Modify Backup Service Name Binding Dialog Box

6. Choose OK. The Set Service Name Bindings dialog box reappears (Figure 7-14 on page 7-46). The status field should now display the message, Backup Binding Active.

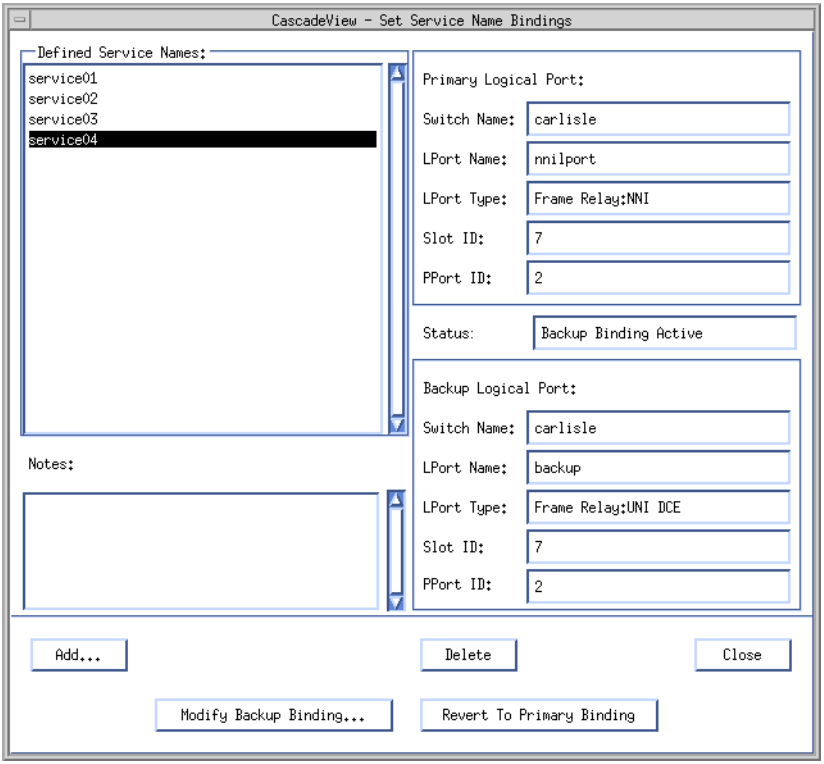


Figure 7-20. Set Service Name Bindings Dialog Box

You can perform 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.

Administrative Tasks

This section describes how to:

- Use templates to define a new logical port
- Delete circuits
- Delete trunks
- Delete management or multicast DLCIs
- Delete Frame Relay logical ports

Using Templates

If you defined a logical port configuration and saved it as a template (see *Is Template* field in Table 7-11 on page 7-22), you can define a new logical port using the same parameters.

To define a logical port from a template:

1. Choose the Add Using Template command on the Set All Logical Ports in PPort dialog box (see Figure 7-4 on page 7-17).
2. Do one of the following:
   - Choose Last Template to use the last template you defined for this switch.
   - Choose Template List to display a list of templates defined for this map. Select a template and choose OK.

Deleting Frame Relay Logical Ports

> *If the loopback status field on the Set All Logical Ports dialog box does not display "**None**", do not attempt to delete this logical port. Refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for information about loopback testing.*

Before you can delete a Frame Relay logical port, verify the following:

Step 1. No circuit uses this logical port as an endpoint.

Step 2. No trunk is defined that uses this logical port as an endpoint.

Step 3. No Management DLCI or Multicast DLCI exists on this port.

Step 4. This logical port is not defined as the feeder (FR UNI DTE/NNI) for an existing OPTimum PVC trunk logical port.

If any of these components exist and use the logical port you want to delete, you must first delete them in the following order:

- Circuits
- Trunks
- Management or multicast DLCIs
- Logical port

Deleting Circuits

To delete a circuit:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits. The Set All Circuits On Map dialog box appears.
2. To view the list of circuits, select the Search by Name field and press Return. If necessary, select each circuit and review each logical-port endpoint.
3. Select the circuit to delete.
4. Choose Delete.

5. Choose Close to return to the network map.

Deleting Trunks

To delete a trunk:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears. If necessary, select each trunk and review each logical-port endpoint.
2. Select the trunk to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting Management or Multicast DLCIs

To delete management or multicast DLCIs:

1. From the Administer menu, select one of the following:
   - Cascade Parameters ⇒ Set All Multicast DLCIs. The Set All Multicast DLCIs dialog box appears, listing the defined Multicast groups in the network configuration.
   - Cascade Parameters ⇒ Set All Management DLCIs. The Set All Management DLCIs dialog box appears, listing the Management DLCIs already configured.
2. Select the DLCI to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting the Logical Port

To delete the logical port:

1. Select the switch on which to delete a logical port.
2. Log in using either a provisioning or operator password.
3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
4. Select the physical port. The Set Physical Port Attributes dialog box appears.
5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.
6. Select the logical port to delete from the logical port list.

> *Make sure this logical port is not the UNI DTE or NNI logical port used as the feeder for a Frame Relay OPTimum trunk. You first need to take the OPTimum trunk out of service or first define another feeder, before you can delete this logical port.*

7. Choose Delete. Make sure the Loopback field displays “NONE”.
8. Choose Delete.
9. Choose Close.

8

Configuring SMDS Services

Switched Multimegabit Data Services (SMDS) is a public packet-switched service that provides local area network features and performance across wide geographical areas. Unlike Frame Relay and ATM, which require established connections to transfer data packets or cells, SMDS is a connectionless service that does not require dedicated lines to transmit data. For a complete description of Cascade's implementation of SMDS services, refer to the *Cascade Networking Services Technology Overview.*

> *CascadeView/UX does not support SMDS on STDX 3000/6000 and Cascade 500 switches. You can only configure SMDS services on B-STDX 8000 and 9000 switches.*

Before you configure SMDS services, verify the following tasks are complete:

- ☑ Create a network map and add a Cascade switch *(Chapter 4)*
- ☑ Configure the IP address and set the NMS path *(Chapter 5)*

☑ Configure the I/O module(s) and physical port parameter(s) (*Chapter 6*)

About SMDS Services

Through CascadeView, you can dynamically configure and monitor an SMDS network by defining the SMDS logical ports and SMDS addresses. The following sections describe the Cascade SMDS logical port types and addressing functions. To disable the SMDS switching system feature for the entire network, refer to "Using Templates" on page 8-69.

SMDS Logical Port Types

Table 8-1 lists the logical port types supported by SMDS.

Table 8-1. SMDS Logical Port Types

LPort Type	Description
SSI-DTE	SMDS-to-Access Server Interface Data Terminal Equipment. Provides the interface between the network supporting SMDS services and the subscriber-owned equipment.
DXI/SNI DCE	Data Exchange Interface Protocol/Subscriber-Network Interface DCE. Provides the interface to enable the CPE to exchange Level 3 protocol data units (PDUs) with the SMDS Access Server without an SMDS DSU/CSU.
DXI/SNI DTE	Data Exchange Interface Protocol/Subscriber-Network Interface DTE. The same as DXI/SNI DCE except that the CPE is connected to the Cascade switch through an SMDS DSU/CSU. ***Note:*** *The DXI/SNI DTE connection is not a typical configuration. Consult the Cascade Technical Response Center* ***before*** *you set up this type of configuration.*
SMDS OPTimum Trunk	Enables a single physical port to be shared among several interswitch trunks.

SMDS Addressing

After you configure an SMDS logical port, CascadeView/UX requires you to specify the individual and group addresses that the SMDS network uses to send and receive data.

You must specify the following address parameters you define in CascadeView/UX:

Individual address — The SMDS individual address uses the E.164 address format. Table 8-5 on page 8-12 describes the maximum number of individual addresses supported on the B-STDX.

Group address — The SMDS group address also uses the E.164 address format. Each group address may contain individual (member) addresses. Refer to Table 8-5 on page 8-12 for the maximum number of group addresses and individual (member) addresses your configuration supports.

You define each group address on a per-map basis. You define each individual address on a per-DXI basis. Each SSI has an individual "feeder" address.

SMDS Country Code and Address Prefix

You can define multiple country codes (for example, North America and International) on one map. The country code may be up to 3 digits in length and is used with the SMDS address prefix as shown in Figure 8-1 on page 8-4.

The SMDS address prefix is a numeric string consisting of at least three (3) digits. To define a unique individual address, you must first select an address prefix (from the address prefix list) and then enter the remaining digits (address suffix).

You cannot change an address prefix once you use it to define an individual address. However, you can combine the same address prefix with different address suffixes to create a unique address. For example:

prefix 1: 508692	address suffix: 2600	result: (508692)2600
prefix 2: 508692	address suffix: 2400	result: (508692)2400

To create the E.164 address, review the following example:

C15086922600

Where **C** indicates an individual address and **1** represents the country code for North America. An **E** would indicate a group address. For example, **E**15086922600.

Figure 8-1 shows the address prefix and country code with the E.164 address C440175662424.

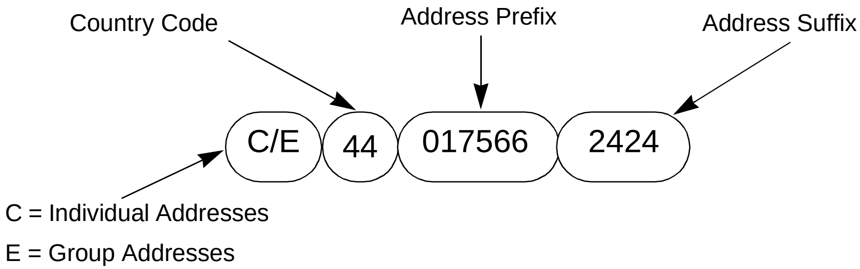


Figure 8-1. Address Prefix Example

SMDS Network-wide Address Masking

Address masking is a feature used to identify "area numbers" for SMDS. The area number is associated with the internal IP address and is identified by applying an area mask to the E.164 SMDS address. Inter-switch traffic switching uses area numbers for routing purposes.

You can modify the mask size and mask starting position for group addresses and individual addresses in the entire network. A maximum of 16 digits is allowed for the individual group address mask. Each switch in the network must have the same masking parameters.

The mask start position indicates the beginning of the mask. The mask size indicates the number of digits the switch uses to make a switching decision. The area definition is based on the mask position and mask size. OSPF uses the area definition for routing. Using the example in Figure 8-2, a mask start position of 2 and a mask size of 9 indicates the mask starts at 5 and is 9 digits in length. To modify the mask size refer to "Setting Networkwide Parameters" on page 8-16.

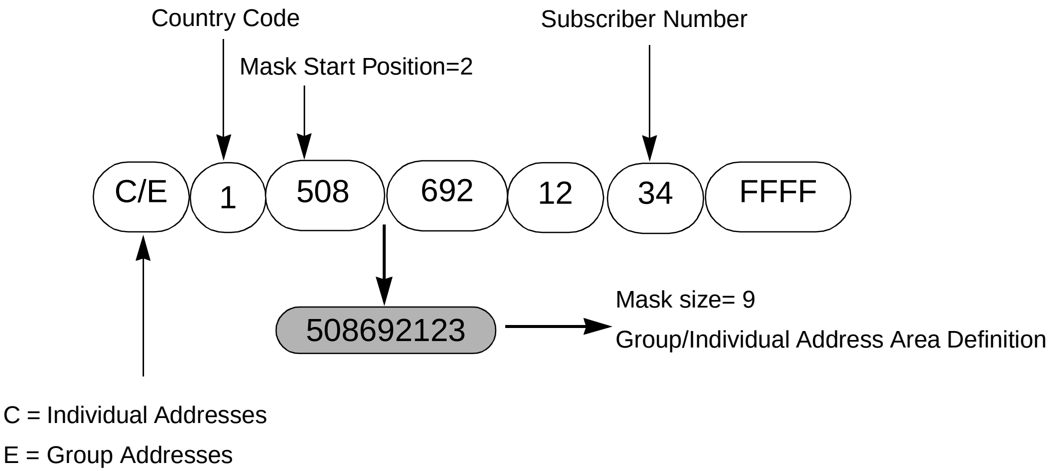


Figure 8-2. Mask Size and Start Position

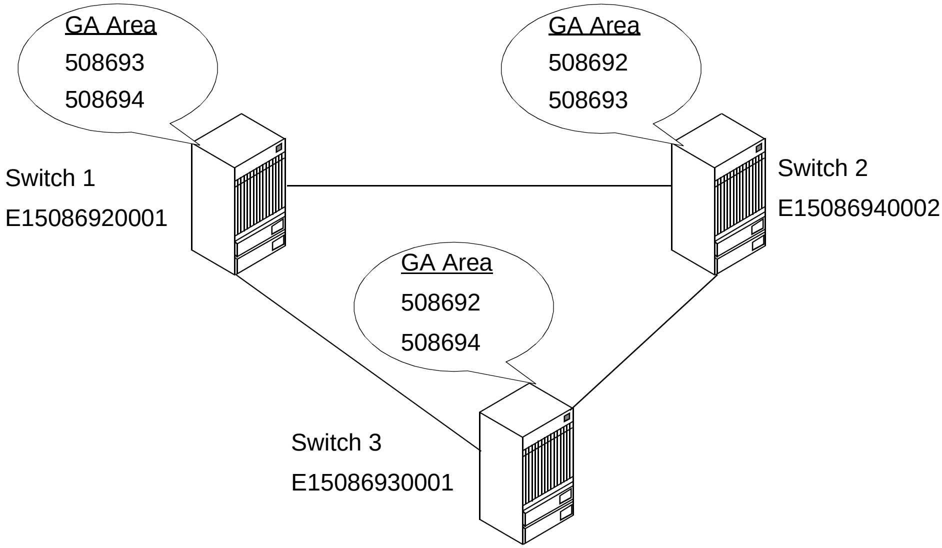
About Networkwide Group Addresses

Group addressing (GA) provides the ability for a CPE to broadcast the same data unit(s) to several recipients. When the SMDS switch receives a group-addressed packet from a DXI/SNI port, it sends a copy of the data unit to each DXI/SNI port whose address is in the same group. The SSI associated with multiplexed DXI/SNI receives a copy of the packet. However, DXI/SNIs that are multiplexed to other SSIs do not receive a copy of the group address data unit. If more than one individual address within a single DXI/SNI logical port belongs to the same group, only a single copy is sent to the DXI/SNI.

> *If an SSI link goes down, non-Cascade users must wait until the link is restored before the switching systems can transmit individual and group address traffic.*

About Selective Group Address Broadcast

Group address frames are processed based on the GA masking parameters and the defined GA area. SMDS services do not blindly broadcast frames to every member of the group; instead, frames are broadcast *only* to those members with the same defined group address area. This method relies less on the SMDS cloud and more on SMDS trunks. Figure 8-3 shows how the switch processes SMDS group address frames.



For example, using address E15086920001, only Switch 2 and Switch 3 receive the group address broadcast. Only Switch 2 and Switch 3 have a defined group address area of 508692.

Figure 8-3. Selective Group-Address Processing

Group Address Frame Processing

Table 8-2 describes how SMDS switching systems process group address frames.

Table 8-2. Group Address Processing

If/When the...	Then...
GA frame enters DXI_A(1) port	Cascade_1 switch distributes the frame to DXI_B(1), DXI_C(2), DXI_D(2) and DXI_E(none). Cascade_1 sends one frame to SSI (since originating DXI (DXI_A) is multiplexed to SSI_1, and one frame to Cascade_2 and Cascade_3 (since these switches have DXIs that are members of this GA). ***Note****: SSI multiplexing is not involved when the GA is going to the same switch.*
GA frame arrives at the trunk port on Cascade_2	The switch checks if the originating port is DXI and distributes the GA frame to DXI_F(3), DXI_G(3), DXI_H(4), DXI_I(4) and DXI_J(none). ***Note****: SSI multiplexing is not involved when the GA is going to the same switch.*
GA frame arrives at the trunk port on Cascade_3	The switch checks if the originating port is DXI and distributes the GA frame to DXI_F(3), DXI_G(3), DXI_H(4), DXI_I(4) and DXI_J(none). ***Note****: SSI multiplexing is not involved when the GA is going to the same switch.*

Table 8-2. Group Address Processing (Continued)

If/When the...	Then...
GA frame enters SSI_3 at Cascade_2	The switch checks if the Source Address and NPA/NXX (individual area definition) numbers exist in the routing table. In this example, the source address of DXI_A(1) should exist in the routing tables, so frames are discarded. The same process access frames arriving at SSI_2 and SSI_4. This eliminates duplication of GA frames to DXI ports.
Non-Cascade switch sends a GA frame to the SSIs	The Cascade switch checks the source address and the NPA/NXX numbers in the received frames. In this example, the source address and the NPA/NXX do not exist, so the GA frame is distributed according to SSI multiplexing.

Figure 8-4 shows how the switch processes group address frames. In this example, all DXIs logical ports are members of the same group address.

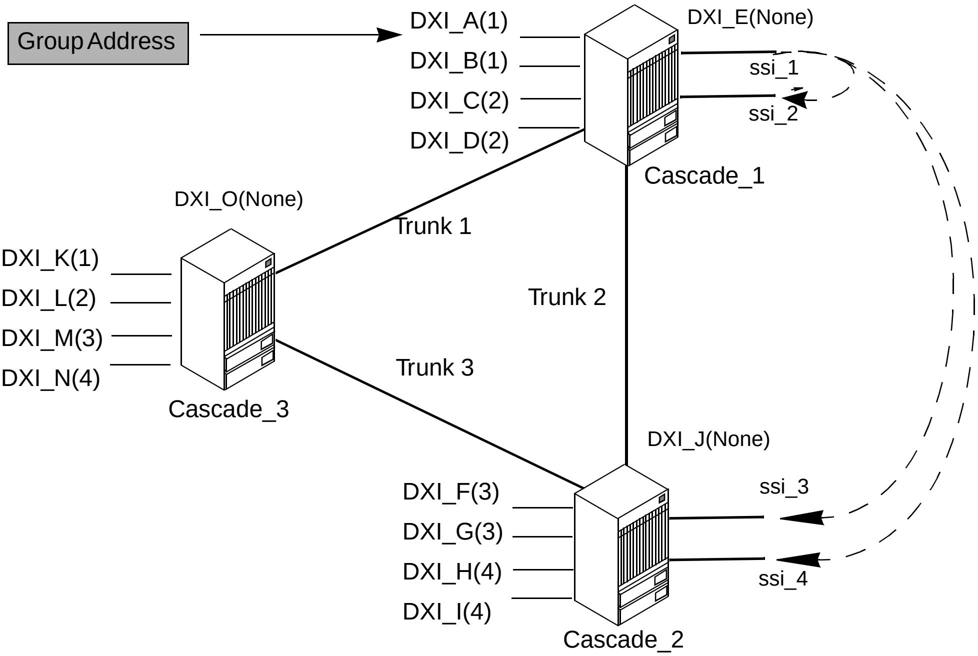


Figure 8-4. Group Address Processing

You can set the SMDS group address processing mode to either Bellcore or Cascade as described in Table 8-6 on page 8-17.

Table 8-3 describes the group address processing mode using Bellcore GA switching.

Table 8-3. Group Address Processing Using Bellcore GA Switching

Source	Destination				
	Local DXI/None	**Local DXI/SSI**	**Remote DXI/SSI**	**Remote DXI/None**	**SSI**
DXI/Local SSI	Y	Y (if same SSI)	Y (if same SSI)	Y	Y
DXI/Remote SSI	Y	Y (if same SSI)	Y (if same SSI)	Y	Y
DXI/None	Y	Y	Y	Y	N
SSI	N	Y	Y	N	N

Table 8-4 describes the group address processing modes using Cascade GA switching.

Table 8-4. Group Address Processing Using Cascade GA Switching

Source	Destination				
	Local DXI/None	**Local DXI/SSI**	**Remote DXI/SSI**	**Remote DXI/None**	**SSI**
DXI/Local SSI	Y	Y	Y	Y	Y
DXI/Remote SSI	Y	Y	Y	Y	Y
DXI/None	Y	Y	Y	Y	N
SSI (SA = Cascade)	N	Y (if same SSI)	Y (if same SSI)	N	N
SSI (SA = Cascade)	N	N	N	N	N

SMDS Address Screening

SMDS address screens enable you to set restrictions on the exchange of SMDS data units with other CPEs. Source address screening checks the data units received from a particular source, while destination address screening checks the data units sent to a particular destination.

Individual address screens — Contain a list of individual addresses and an *allowed/disallowed* option. You can apply the allowed/disallowed option globally to all individual addresses in the list. The B-STDX switch supports only one individual address screen per DXI/SNI.

Group address screens — Contain a list of group addresses and an *allowed/disallowed* option. You can apply the allowed/disallowed option globally to all group addresses in the list. The B-STDX switch supports only one group address screen per DXI/SNI logical port.

Table 8-5 lists the SMDS addressing capacities for the B-STDX switch.

Table 8-5. SMDS Capacity on the B-STDX

Maximum Capacity	Maximum for B-STDX with IOP+ and Release 4.0/4.1	Maximum for B-STDX with IOP+ and Release 4.2
DXI/SNI logical ports per switch	1680	1680
Individual address screens per DXI/SNI	1	1
Group address screens per DXI/SNI	1	1
Individual addresses that can be assigned to a DXI/SNI	240	240
Individual addresses per IOP	240	240
Individual addresses per switch	3360	3360
Group addresses per switch	1024	400
Alien addresses per switch	1024	2048
Members per group	3360	3360
Members per individual address screen	4384	5408
Members per group address screen	2048	2448
Groups in which an individual address can be a member	1024	400
Individual addresses that can be associated with an SSI	no limit	N/A

SMDS Configuration Sequence

Use the following configuration sequence to define SMDS services in CascadeView.

1. Define the country codes.
2. Define address prefixes for each switch.
3. (*Optional*) Modify the SMDS Networkwide Parameters.
4. (*Optional*) Define the SSI-DTE logical port parameters.
5. (*Optional*) Define the SMDS OPTimum trunk logical port on the same physical port as the SSI-DTE. Configure the trunk connection.
6. Define DXI/SNI logical port parameters. Configure this port to either multiplex to a specified SSI-DTE logical port, or to perform local switching only.
7. Depending on your configuration in Step 6, do the following:

   For DXI/SNI logical ports configured for local switching – Define an individual address to which the DXI/SNI logical port will subscribe.

   For DXI/SNI logical ports multiplexed to an SSI-DTE – Define an individual address to DXI/SNI logical port.
8. Define individual addresses.
9. Define group addresses.
10. Select members (individual addresses) for the group addresses.
11. Define the individual and group address screen members for the DXI/SNI(s).

Defining the Country Code and Address Prefix

To define the SMDS country code and address prefix:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SMDS Parameters ⇒ Set All Country Codes. The Define Country Code dialog box appears as shown in Figure 8-5.

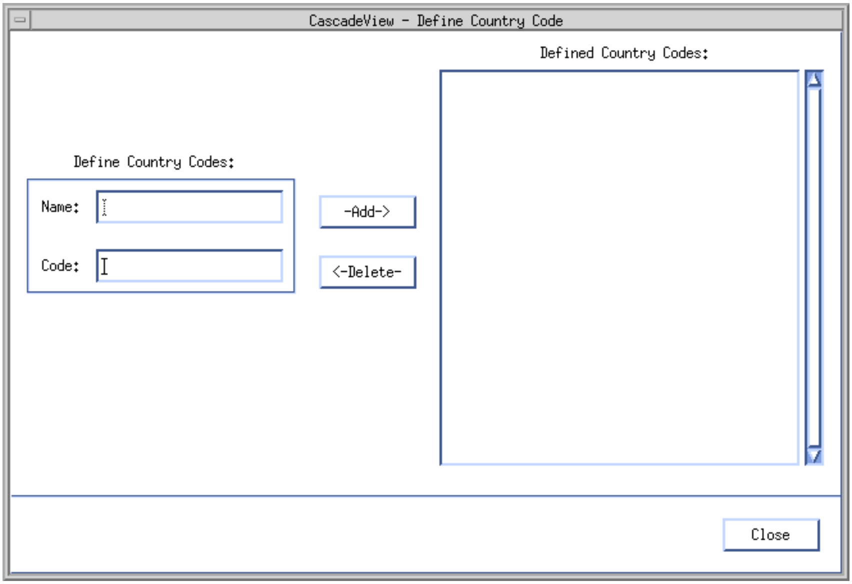


Figure 8-5. Define Country Code Dialog Box

2. Complete the fields as follows:

   Name — Enter a country code name. For example, North America.

   Code — Enter a numeric country code. For example, 1.

3. Choose Add. The defined country code is added to the Defined Country Codes field.

4. Choose Close to exit the Define Country Code dialog box and return to the map.

To configure the SMDS address prefix for a switch:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SMDS Parameters ⇒ Set All Address Prefixes. The Define Address Prefix dialog box appears as shown in Figure 8-6.

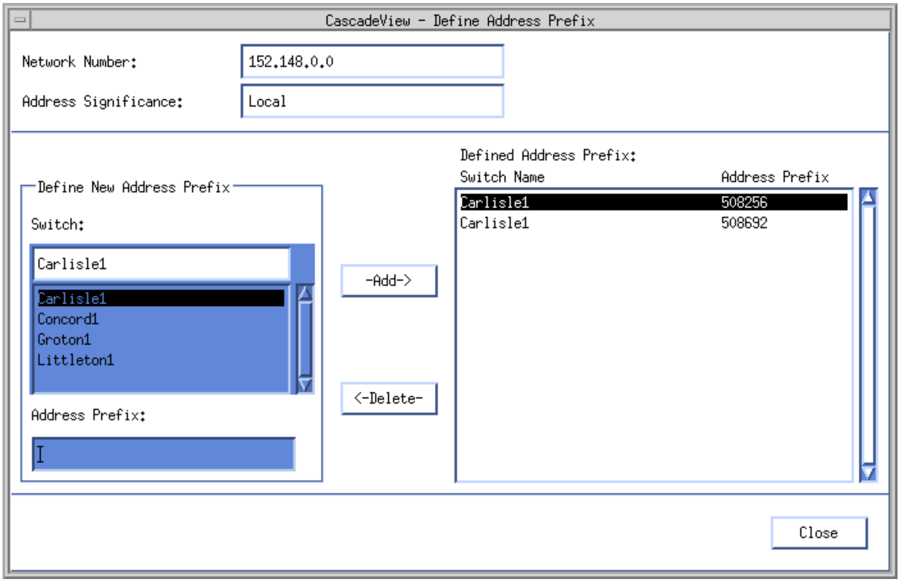


Figure 8-6. Define Address Prefix Dialog Box

This dialog box displays the Network Number and Address Significance (local or global).

2. On the left, select the switch for which you are defining the address prefix(es).
3. In the Address Prefix text box, type a character string of at least three numbers.
4. Choose Add. The address prefix appears in the Defined Address Prefix list box.
5. Repeat Step 3 and Step 4 until you define all address prefixes for the selected switch.
6. When you finish, choose Close.

Setting Networkwide Parameters

This section describes how to modify the individual and group mask parameters. It also describes how to set the group address processing mode.

> *All switches in the network must have the same group masking parameters.*

To modify the masking parameters and set the group address processing mode:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SMDS Parameters ⇒ Set SMDS Networkwide Parameters. The Set SMDS Networkwide Parameters dialog box appears as shown in Figure 8-7.

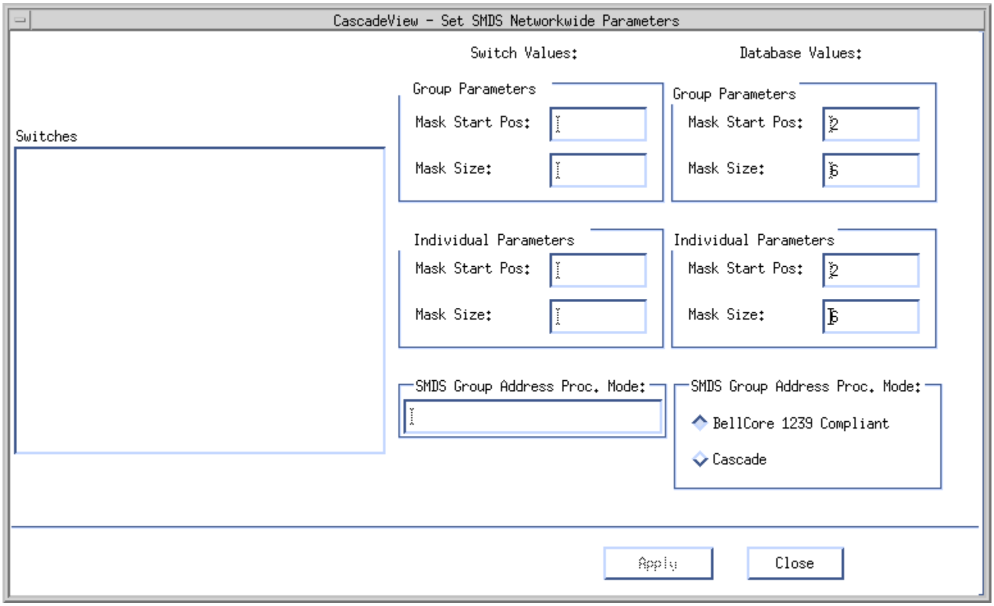


Figure 8-7. Set SMDS Networkwide Parameters Dialog Box

2. Select a switch in the Switches field.

   The system displays the group and individual mask parameters for the switch and database.

3. Modify the group and individual mask parameters database values (displayed on the right side of the dialog box), by completing the fields in Table 8-6.

Table 8-6. Set SMDS Networkwide Parameters Fields

Field	Action/Description
Group Mask Parameters	
Mask Start Pos	Enter a value between 1 and 15. The default start position is 2.
Mask Size	Enter a value between 1 and 15. The default size is 6. ***Note**: If you set the Mask Size to 0, it will disable the switching system.*
Individual Mask Parameters	
Mask Start Pos	Enter a value between 1 and 16. The default start position is 2.
Mask Size	Enter a value between 1 and 16. The default size is 6.
SMDS Group Address Proc. Mode	Select an SMDS switching mode.Options include: *Bellcore 1239 Compliant (default)* – Complies with Bellcore 1239 and determines how frames are processed. *Cascade* – Uses the direct trunk connection and does not rely on the SMDS cloud. The SMDS cloud is used only to communicate with non-Cascade switches. For more information, refer to “Group Address Frame Processing” on page 8-7.

4. Choose Apply to save the changes.

5. Choose Close to exit the dialog box.

Accessing SMDS Logical Port Functions

To access SMDS logical port functions:

1. Select the switch to which you want to add a logical port.
2. Log in to CascadeView/UX using either a provisioning or operator password.
3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
4. Select the physical port you want to configure. The Set Physical Port Attributes dialog box appears.
5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears as shown in Figure 8-8.

The Set All Logical Ports in PPort 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 many logical port functions, such as modify and delete logical ports.

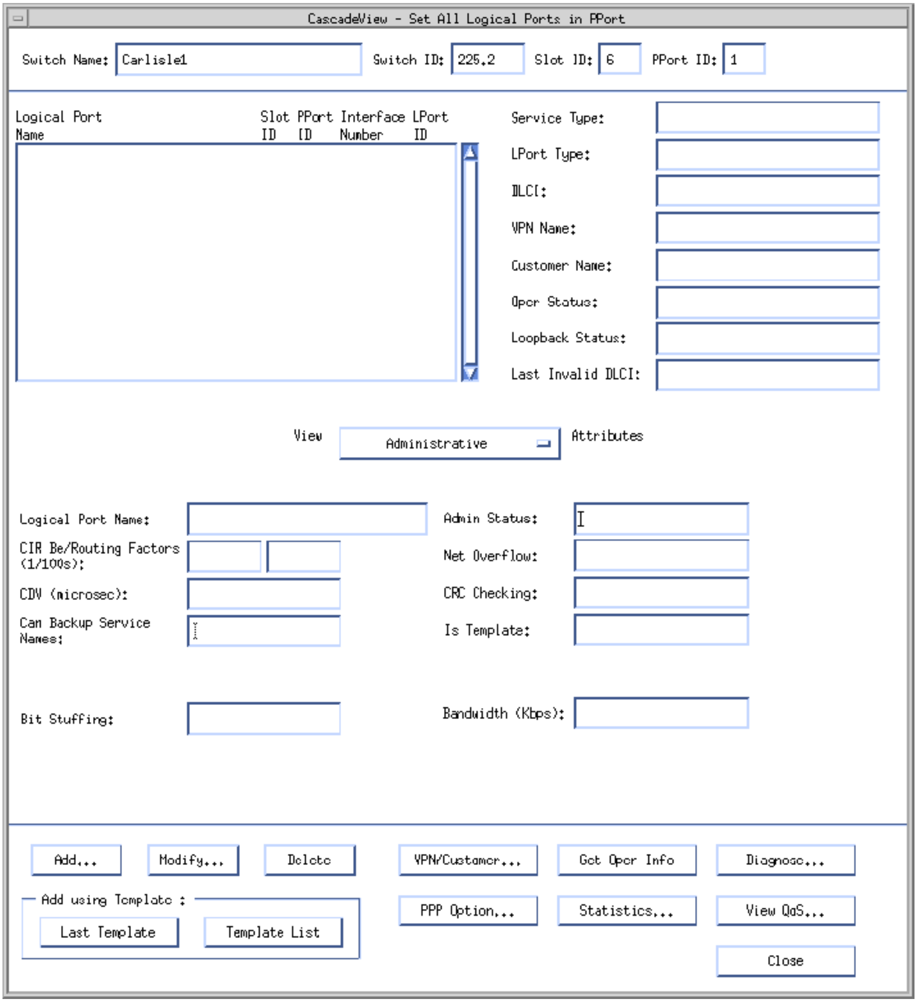


Figure 8-8. Set All Logical Ports in PPort Dialog Box

Table 8-7 lists and describes the Set All Logical Ports in PPort dialog box commands.

Table 8-7. Set All Logical Ports in PPort Dialog Box Commands

Command	Function
Add/Modify/Delete	Enables you to add a new logical port or Modify or Delete an existing logical port configuration. For information about deleting logical ports refer to "Deleting SMDS Logical Ports" on page 8-70.
Diagnose	Accesses diagnostic tests for the selected logical port. For more information about diagnostics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Statistics	Displays the summary statistics for and existing logical port. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Last Template/ Template List	If you have already defined a logical port configuration and saved it as a template, you can use this option to define a new logical port using the same parameters. Refer to the "Administrative Tasks" on page 8-69 for more information.
Get Oper Info	Displays a status message in the *Oper Status* field for the selected logical port.
VPN/Customer	Displays the Virtual Private Network customer's name.
View Qos Parameters	Displays the Quality of Service parameters.

Adding an SMDS Logical Port

To add SMDS logical ports:

1. Perform the steps in "Accessing SMDS Logical Port Functions" on page 8-18.
2. On the Set All Logical Ports in PPort dialog box, choose Add.

   The Add Logical Port dialog box appears as shown in Figure 8-9.

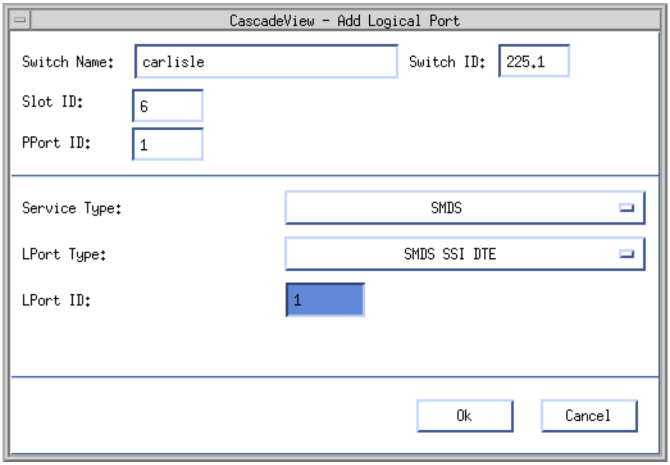


Figure 8-9. Add Logical Port Dialog Box

3. Choose Service Type, SMDS.
4. Choose LPort Type (refer to Table 8-8 for instructions). The supported logical port types vary for each type of I/O module.
5. Choose OK.

6. Set the attributes for the selected logical port as described in the appropriate sections (refer to Table 8-8).

Table 8-8. SMDS Logical Port Configurations

Logical Port Type	Refer to...
SMDS SSI-DTE	"Defining SSI-DTE Logical Ports" on page 8-23.
SMDS OPTimum Trunk	"Defining SMDS OPTimum Trunk Logical Ports" on page 8-39.
SMDS SNI (DTE or DCE)	"Defining DXI/SNI Logical Ports (DCE or DTE)" on page 8-42.

The Set Attributes Options Menu

When you define a new logical port, the Add Logical Port dialog box displays a Set Attributes option menu that enables you to set different attributes for each type of logical port. Attributes include:

Administrative — Sets the admin status, net overflow, and bandwidth parameters.

Congestion Control — Sets the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network.

SMDS — Sets the polling interval and polling thresholds for each logical port.

Trap Control — Sets the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port.

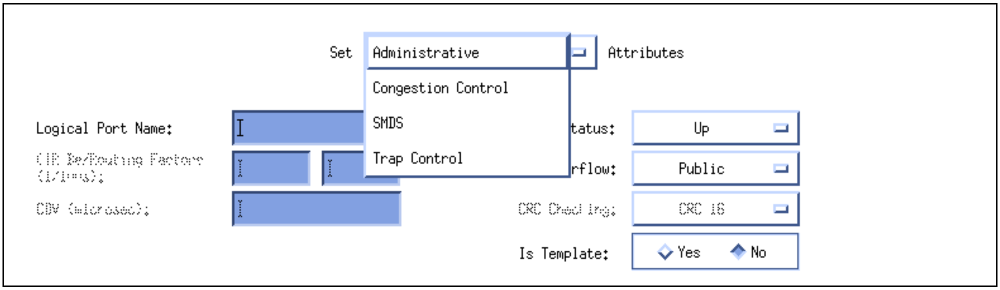


Figure 8-10. Set Attributes Option Menu

Defining SSI-DTE Logical Ports

An SSI-DTE logical port is an SMDS switching system interface. Multiple SSIs can reside on one channelized port, but only one SSI-DTE logical port can reside on a non-channelized physical port. The SSI-DTE is the logical port you configure to multiplex with other SMDS DXI/SNI logical ports.

Use the following configuration sequence to define an SMDS SSI-DTE logical port.

Step 1. Define an SSI-DTE logical port configuration.

Step 2. *(Optional)* Configure an OPTimum trunk logical port on this same physical port.

Step 3. Select a feeder address.

To define an SSI-DTE logical port:

1. Complete the Add Logical Port dialog box fields described in Table 8-9.

Table 8-9. Add Logical Port Fields

Field	Action/Description
Service Type	Select SMDS.
LPort Type	Select SMDS SSI DTE.
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one.

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields shown in Figure 8-11.

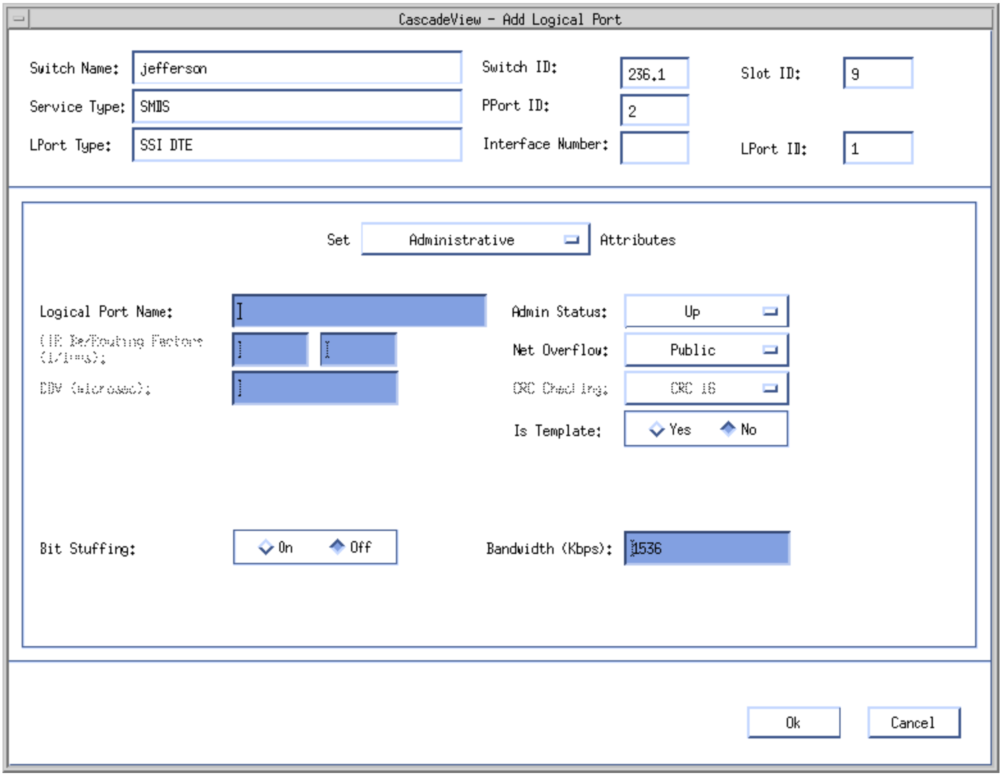


Figure 8-11. Set Administrative Attributes Dialog Box (SSI-DTE)

Administrative Attributes

Complete the administrative attributes fields described in Table 8-10.

Table 8-10. Add Logical Port-Set Administrative Attribute Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Admin Status	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. *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
Is Template	(*Optional*) Save these settings as a template to use again to quickly configure a logical port with the same options. To create a template, choose Yes in the *Is Template* field. Refer to “Using Templates” on page 8-69 for more information.
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth remaining from the physical clock rate, less any logical ports already configured. ***Note**: If you are defining an SMDS OPTimum trunk port on this same physical port, decrease the amount of bandwidth on this logical port to ensure sufficient remaining bandwidth.*

Table 8-10. Add Logical Port-Set Administrative Attribute Fields (Continued)

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	If you are configuring a channelized T1 or E1 module, specify the DS0 (for T1) or TS0 (for E1) channel(s) assigned to the logical port. The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel ***Note**: The logical port bandwidth either increments or decrements depending on the number of channels you select or deselect. You can configure other logical ports with different attributes, to other DS0/TS0 channels on this same physical port.*
Bit Stuffing	Select the bandwidth that matches the bandwidth capability of the customer premise equipment (CPE) connected to this logical port. Enables bit stuffing on T1/E1/DSX-1 ports. Bit stuffing effects the available bandwidth of each DS0/TS0 channel on this port. *On* – Provides 56 Kbps of bandwidth. *Off* – Provides 64 Kbps of bandwidth.

Congestion Control Attributes

1. Set the congestion control attributes for this logical port by selecting *Congestion Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 8-12.

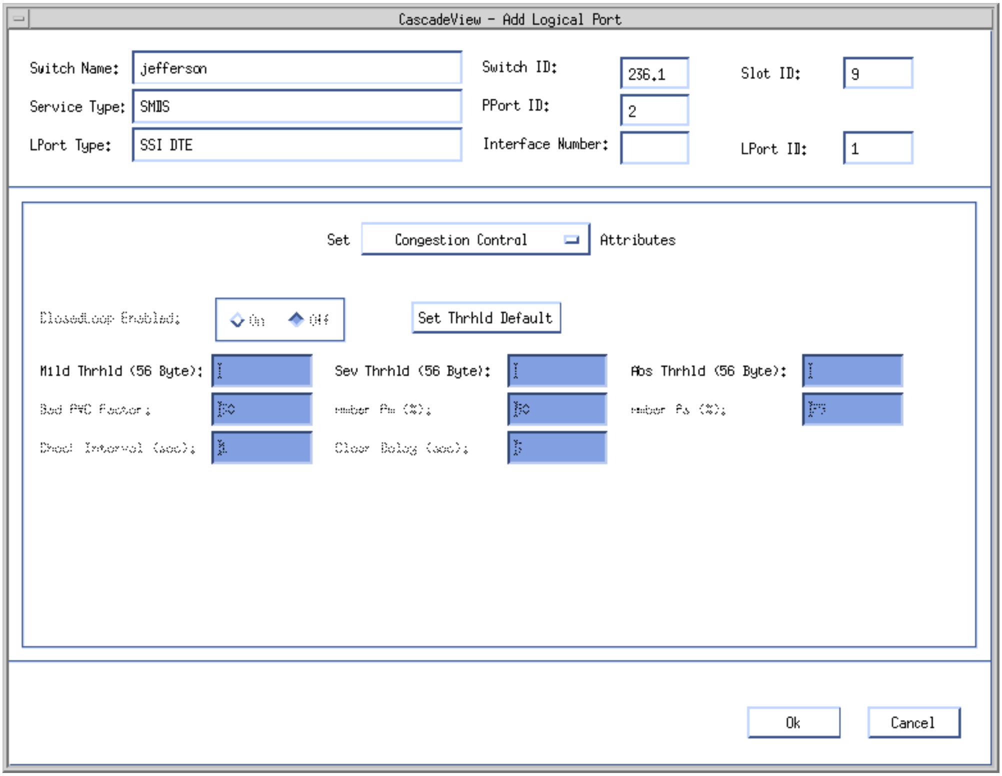


Figure 8-12. Set Congestion Control Attributes Dialog Box (SSI-DTE)

2. Complete the congestion control attributes fields described in Table 8-11.

Table 8-11. Set Congestion Control Fields

Field	Action/Description
Cong. Enabled	Set the congestion control parameters. This field enables/disables OSPF closed-loop congestion control for each logical port. For more information refer to "Closed-Loop Congestion Control" on page 7-7. Options include: *Off (default)* – Disables closed-loop congestion. *On* – Enables closed-loop congestion.
Set Thrhld Default	Sets the Mild, Severe, and Absolute threshold settings to the default settings described in Table 7-5 on page 7-10 through Table 7-5 on page 7-10.
Mild Thrshld (*SSI only*) Severe Thrshld (*SSI only*) Absolute Thrshld	Accept the defaults or enter values for the mild, severe, and absolute threshold fields as defined in Table 7-5 on page 7-10 through Table 7-7 on page 7-11. ***Note****: Do not exceed the maximum threshold value for each card type (see Table 7-4 on page 7-9 for more information). The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.* ***Note****: If you are setting the threshold parameters on a T1/E1 card, the default values will not appear until you set the bit stuffing and bandwidth allocation. Refer to Table 8-10 on page 8-25 for more information.* ***Note****: For Channelized T1/T1 PRI and Channelized E1/E1 PRI cards, if n DS0s are assigned per channel, the maximum value allowed on the number of buffers is n x 225 (T1) and n x 174 (E1).*
Check Interval	Enter and interval. This determines the number of seconds in which the switch monitors the trunk's congestion on the port. The default is one (1) second.

Table 8-11. Set Congestion Control Fields (Continued)

Field	Action/Description
Clear Delay	Enter a value. This determines the number of seconds in which the switch monitors the trunk's non-congestion state. Enter a value. The default is three (3) seconds.

SMDS Attributes

1. Set the SMDS attributes by selecting *SMDS* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 8-13.

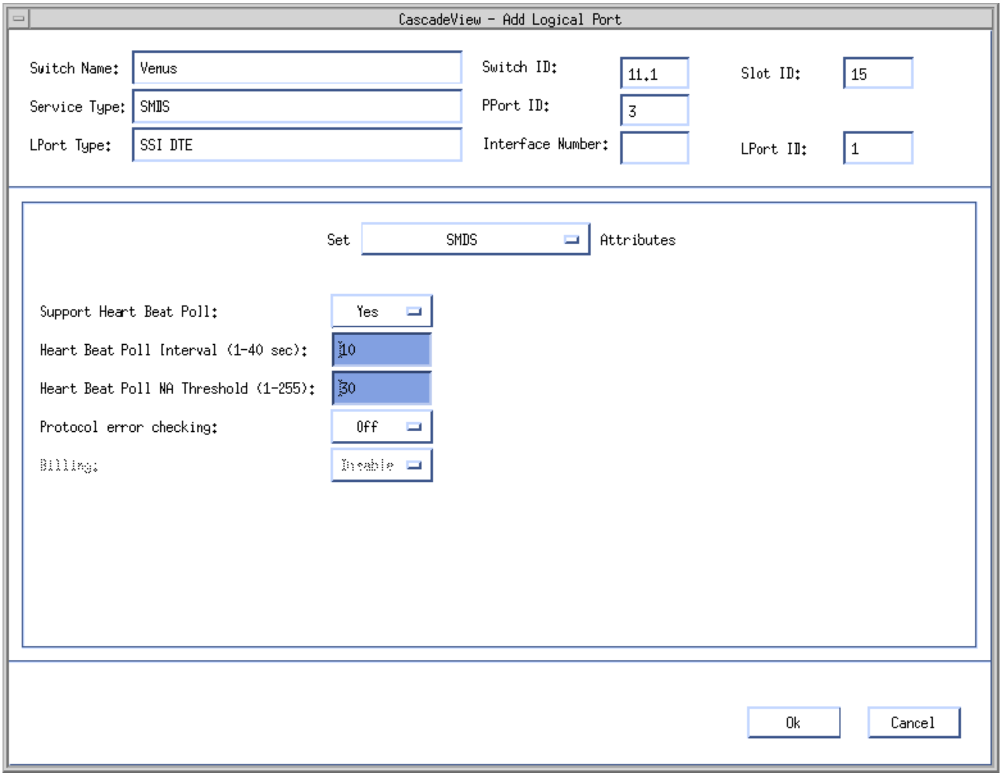


Figure 8-13. Set SMDS Attributes Dialog Box (SSI-DTE)

2. Complete the SMDS attributes fields described in Table 8-12.

Table 8-12. Set SMDS Attributes Fields

Field	Action/Description
Support Heart Beat Poll	Select *Yes* (*default*) only if the CPE connected to this port supports heart beat poll responses; otherwise select *No*. Heartbeat polls check for a keep-alive signal coming from the CPE.
Heart Beat Poll Interval (1-40 sec)	Enter a value between 1 to 40 seconds. The default is 10 seconds. This value specifies the time that occurs between heart beat polling requests sent to the CPE.
Heart Beat Poll NA Threshold (1-255)	Enter a value between 1 and 255; the default value is 30. The configured threshold of heart beat polling requests that can go unanswered before a trap is recorded in the event log. A threshold crossing alert is sent to the NMS each time the threshold for the DXI/SNI is exceeded, within a 15-minute time period. The unanswered heart beat poll count resets every 15 minutes.
Protocol Error Checking	Set the protocol error checking parameter. This field determine the level of protocol error checking on PDUs received by this logical port. **Enable this field for debugging purposes only**. Options include: *Off (default)* – Minimal address checking. *On* – Complete Level 2 protocol error checking. This activates Level 2 protocol error counters for which you can view statistics. There is a slight performance cost if you enable protocol error checking. For information about SMDS statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

Trap Control Attributes

1. Set the trap control attributes by selecting *Trap Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 8-14.

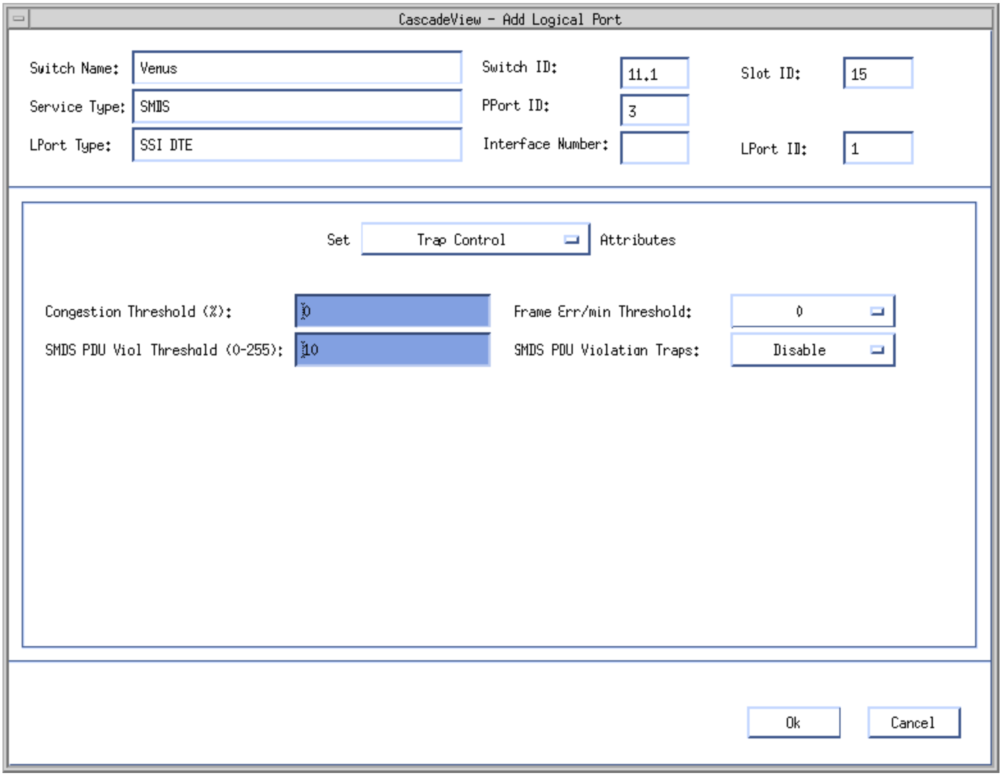


Figure 8-14. Set Trap Control Attributes Dialog Box (SSI-DTE)

2. Complete the trap control attributes fields described in Table 8-13.

Table 8-13. Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold (%)	Enter a value between 0 and 100 to indicate the threshold percentage for generating and sending traps to the NMS for this logical port. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the percentage value you enter. Adjust the entered value according to how sensitive this port needs to be to network congestion. Options include: *Low* – Generates a trap at the first sign of congestion. *High* – Generates traps for serious network congestion. *Zero (default)* – Disables congestion threshold. If you enter zero, no traps are generated for this logical port.
SMDS PDU Viol Threshold (0-255)	Specify the number of PDU violations that can occur before a trap is sent to the NMS. The software increments a counter every time an SMDS PDU violation takes place on a logical port. The software polls these counters every 60 seconds. If a particular counter exceeds the specified SMDS PDU violation threshold for the logical port, then it generates a trap corresponding to that particular violation. The default is 10 PDU violations. Options include: *Low* – Sensitive to SMDS PDU violations. *High* – Issue traps only when there is a significant number of SMDS PDU violations.
CRC Checking (*HSSI modules only*)	Set this value to match the number of error checking bits used by the CPE connected to this port. Performs a cyclic redundancy check (CRC) on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.

Table 8-13. Set Trap Control Attributes Fields (Continued)

Field	Action/Description
Frame Err/Min Threshold	Enter a value from 0 to 16384 to configure the threshold of frame errors on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS. Adjust this value according to how sensitive this port needs to be to frame errors. Options include: *Low* – Port is sensitive to frame errors. *High* – Generates traps when a significant number of frame errors occurs within a one-minute period. *Zero (default)* – Disables this feature, which prevents traps from being generated for this logical port.
SMDS PDU Violation Traps	Enable or disable this field. An SMDS PDU violation can be either an SIP3 SMDS address failure or an invalid DXI2 frame header. These errors mean incoming frames are bad indicating problems with the CPE configuration. Options include: *Disable* (*default*) – Turns off traps. *Enable* – Issues traps for PDU violations.

3. Choose OK. The Set All Logical Ports in PPort dialog box appears, displaying the configured attributes for the logical port.

4. Choose Close. The Set Physical Port Attributes dialog box appears.

5. Configure the remaining logical ports for this physical port. Refer to the instructions that follow for the specific type of logical port you want to add.

6. If you are configuring an OPTimum trunk logical port on this same physical port, define the SSI feeder as described in the next section "Defining the Feeder Address for an SSI-DTE Logical Port".

7. Otherwise, you are ready to configure the DXI/SNI logical port(s). Refer to the section "Defining DXI/SNI Logical Ports (DCE or DTE)" on page 8-42 for more information.

Defining the Feeder Address for an SSI-DTE Logical Port

Before you define an OPTimum trunk (on the SSI-DTE logical port) you must define a feeder address on the logical port. The OPTimum trunk logical port inherits the subscribed address from the SSI feeder address.

> *If you select an individual address to use as the feeder address for an SSI-DTE logical port, a DXI/SNI cannot subscribe to it. An SSI DTE logical port can subscribe to one feeder address only.*

To define the feeder address and select the individual address to which the SSI-DTE logical port subscribes:

1. From the Set Physical Port Attributes dialog box, select Logical Port. The Set All Logical Ports in PPort dialog box appears as shown in Figure 8-15.

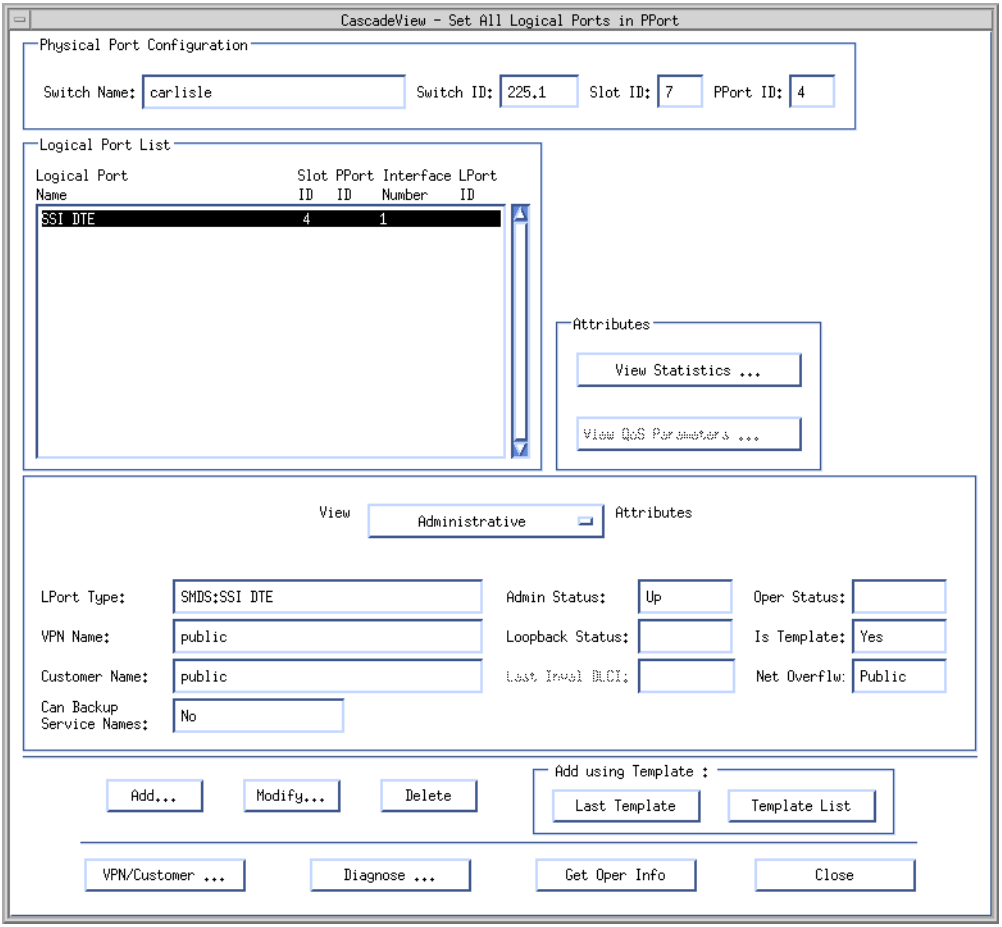


Figure 8-15. Set All Logical Ports in PPort Dialog Box

2. Select the SSI-DTE logical port from the list box and choose Modify. The Modify Logical Port dialog box appears, displaying the attributes for the selected logical port as shown in Figure 8-16.

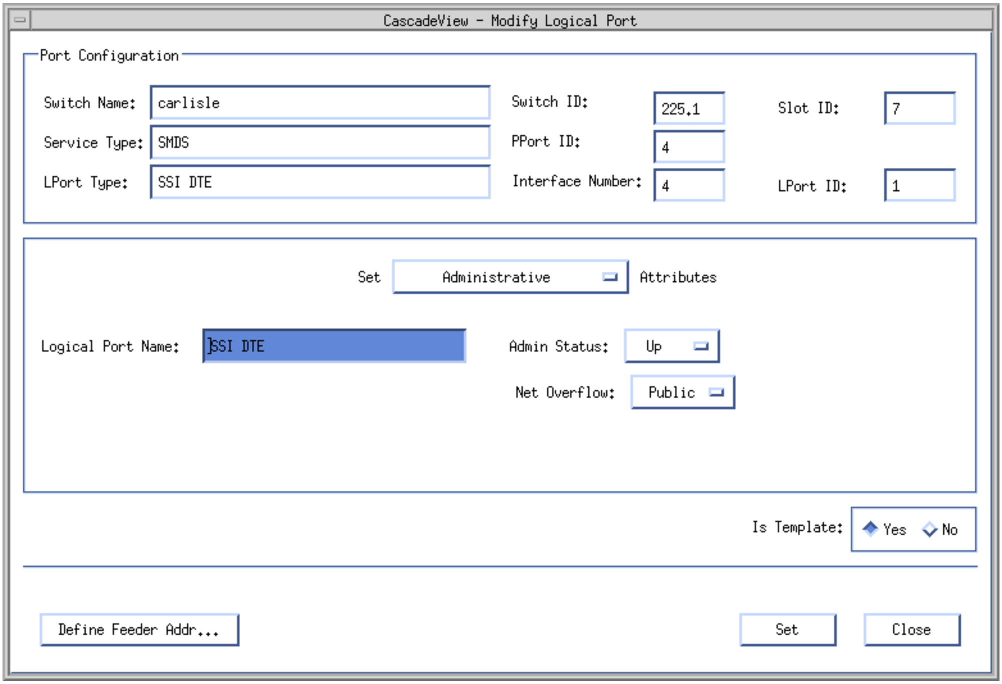


Figure 8-16. Modify Logical Port Dialog Box

3. From the Modify Logical Port dialog box, choose the Define Feeder Addr command. The Define Feeder Address for SMDS SSI LPort dialog box appears as shown in Figure 8-17.

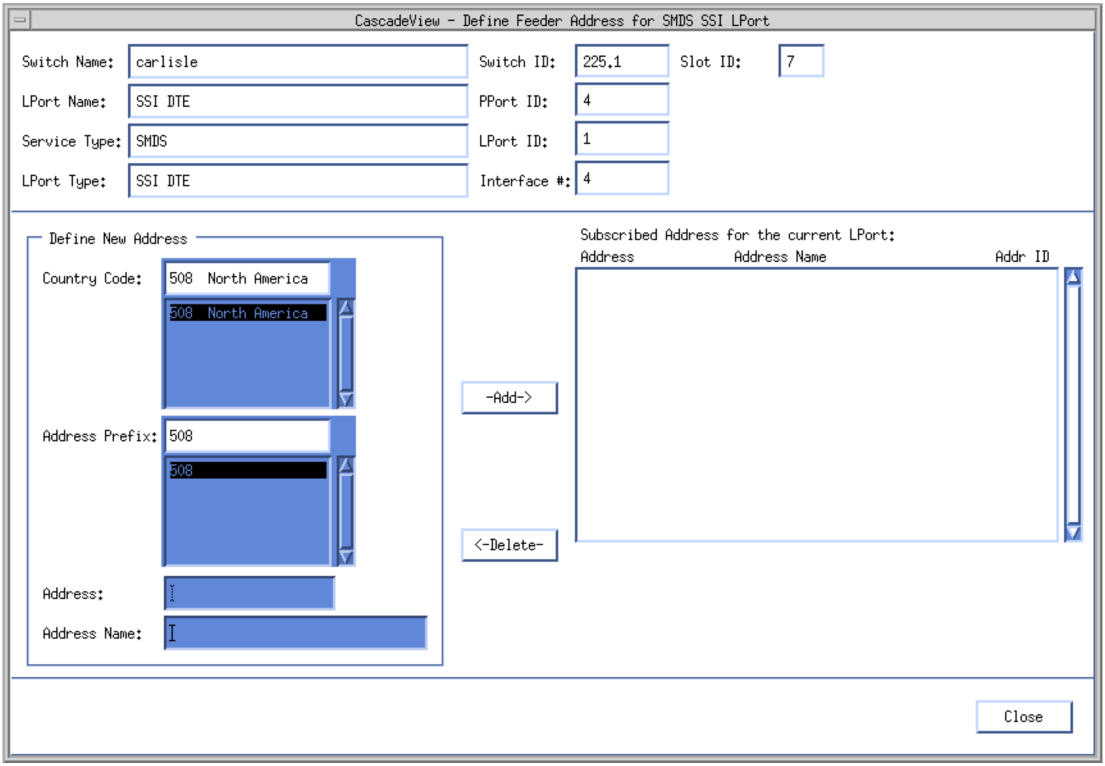


Figure 8-17. Define Feeder Address for SMDS SSI LPort Dialog Box

4. Complete the required fields described in Table 8-14.

Table 8-14. Define Feeder Address for SMDS SSI LPort Fields

Field	Action/Description
Country Code	Select the Country Code to which the SSI-DTE logical port subscribes.
Address Prefix	Select the Address Prefix to which the SSI-DTE logical port subscribes.

Table 8-14. Define Feeder Address for SMDS SSI LPort Fields (Continued)

Field	Action/Description
Address	Type the remainder of the address (address suffix) in the Address field. Refer to "SMDS Addressing" on page 8-3 for more information.
Address Name (*Optional*)	Enter an alphanumeric name to further describe the address. Do not use an apostrophe.

5. Choose Add. The address appears in the Subscribed Addresses for the current LPort list box as shown in Figure 8-18.

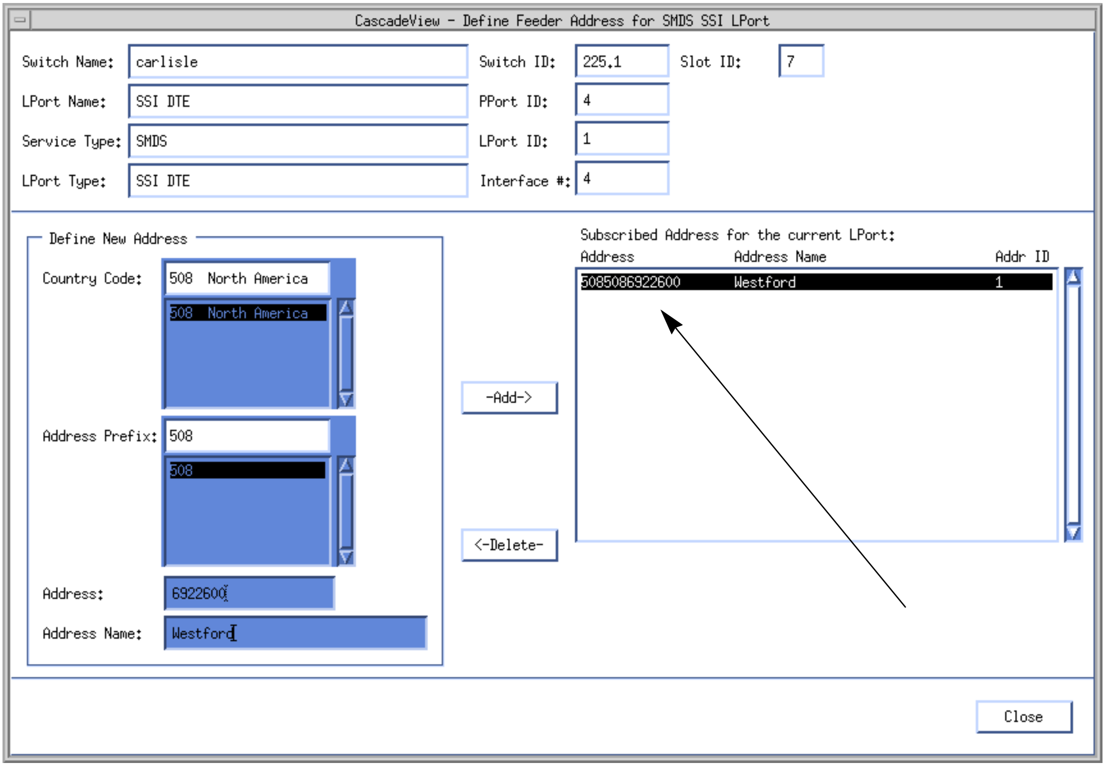


Figure 8-18. Define Feeder Address for SMDS SSI LPort Dialog Box

6. Choose Close. The Modify Logical Ports dialog box reappears.
7. Choose Close. The Set All Logical Ports in PPort dialog box appears.
8. Choose Close to return to the Set Physical Port Attributes dialog box.

Defining SMDS OPTimum Trunk Logical Ports

You can configure an SMDS OPTimum trunk to connect Cascade switches across an SMDS network. This configuration allows several interswitch trunks to share a single physical port. The Cascade OPTimum trunk feature allows private enterprise networks to purchase lower-cost, public-carrier services as the trunk between two Cascade switches, instead of using a more expensive leased line.

The Cascade switch architecture enables you to use Cascade OPTimum trunking for SMDS. You can configure the same physical port with one or more logical ports for SMDS OPTimum path. This allows several interswitch trunks to share a single physical port. All SMDS OPTimum paths are assigned one SMDS individual address, which is terminated at the logical ports. SMDS OPTimum Trunk logical ports inherit their subscribed address from the SSI feeder address that you previously defined on the same physical port. For information about the SSI feeder address, refer to "Defining the Feeder Address for an SSI-DTE Logical Port" on page 8-34.

> *Channelized T1/E1 modules do not support OPTimum trunk logical ports.*

Before you configure an SMDS OPTimum trunk, verify the following tasks are complete:

- ☑ Define an SSI-DTE logical port configuration on the same physical port. (Refer to "Defining SSI-DTE Logical Ports" on page 8-23.)
- ☑ Define an individual address for the SSI feeder.
- ☑ Select the individual address for the SSI feeder. (Refer to "Defining the Feeder Address for an SSI-DTE Logical Port" on page 8-34.)

To configure an SMDS OPTimum trunk, you must first configure a SSI-DTE logical port on the same physical port. Use the following sequence:

Step 1. Configure the physical port you want to use for the OPTimum trunk (refer to "Configuring Physical Ports" on page 6-9).

Step 2. (*Optional*) If you are using individual addresses and group addresses, define the country code (refer to "Defining the Country Code and Address Prefix" on page 8-14).

Step 3. (*Optional*) Modify the SMDS Networkwide Parameters (refer to "Setting Networkwide Parameters" on page 8-16).

Step 4. Configure an SSI-DTE logical port (page 8-23) on the same physical port. Assign this logical port a minimum amount of bandwidth.

Step 5. Configure the OPTimum trunk logical port on this same physical port (refer to page 8-39). You can assign the remaining bandwidth to this logical port.

To define an SMDS OPTimum trunk logical port:

1. Complete the Add Logical Port dialog box fields as described in Table 8-15.

Table 8-15. Add Logical Port (OPTimum Trunk) Fields

Field	Action/Description
Service Type	Select SMDS.
LPort Type	Select SMDS SSI DTE.
LPort ID	The Logical Port ID is a read-only field that automatically defaults to two (2).

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields shown in Figure 8-19.

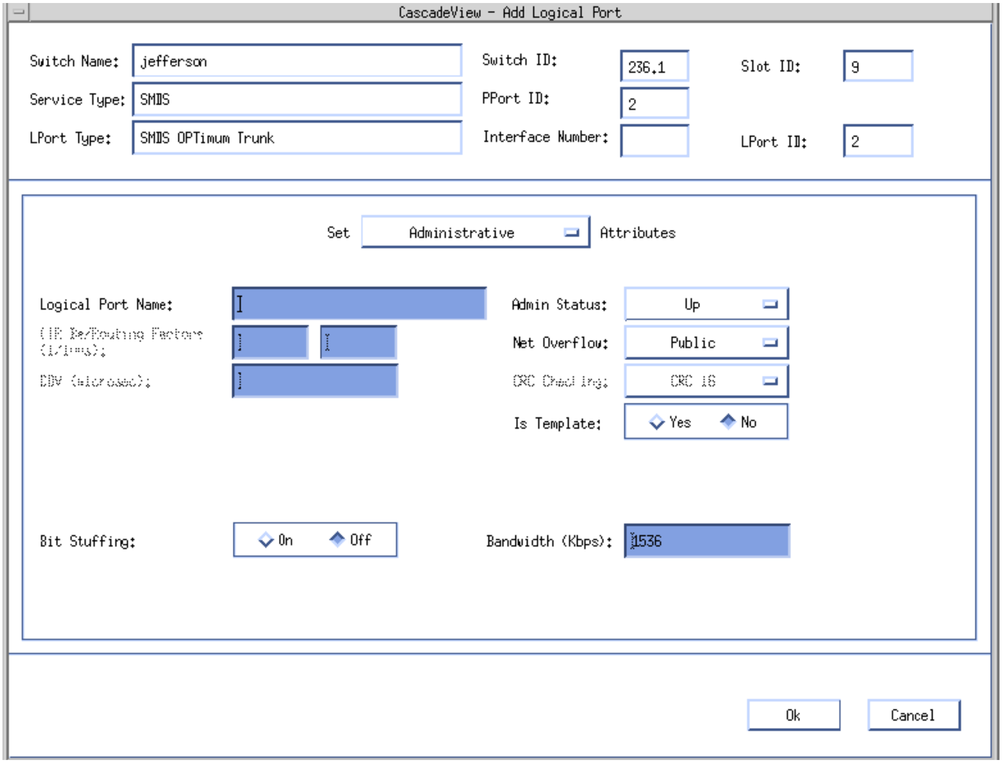


Figure 8-19. Add Logical Port (OPTimum Trunk) Dialog Box

3. Complete the administrative attributes fields described in Table 8-10 on page 8-25.

4. Complete the trap control attributes fields described in Table 8-13 on page 8-32.

5. Choose OK. The Set All Logical Ports in PPort dialog box appears and displays the name of the logical port that you just configured.

6. Choose Close. The Set Physical Port Attributes dialog box appears.

When you finish, you are ready to define the trunk line connection. Refer to Chapter 10 for more information.

Defining DXI/SNI Logical Ports (DCE or DTE)

A DXI/SNI logical port configuration performs switching within the SMDS network. You can also configure the DXI/SNI logical port to multiplex to a specific SSI-DTE logical port that provides both local and remote switching capability.

If the DXI/SNI is multiplexed to a specific SSI-DTE, choose an individual address. If, however, the port performs *local switching only*, you must select a defined address prefix and enter a unique address number to create an individual address. You can configure up to 240 DXI/SNI logical ports per IOP, up to a maximum of 3360 per switch.

> *The DXI/SNI-DTE connection is not a typical configuration. Consult the Cascade Technical Response Center before you set up this type of configuration.*

Before you define an SMDS DXI/SNI logical port for either remote or local switching, verify the following tasks are complete:

- ☑ Define an SSI-DTE logical port configuration.
- ☑ Define the individual addresses.

Use the following configuration sequence to define a DXI/SNI logical port:

Step 1. Define the DXI/SNI logical port configuration.

Step 2. Select the addresses to which the DXI/SNI will subscribe.
Or...
Enter an individual address for local switching only.

Step 3. *(Optional)* Define the individual and group address screen for the DXI/SNI.

To define a DXI/SNI logical port:

1. Complete the Add Logical Port dialog box fields as described in Table 8-16.

Table 8-16. Add Logical Port (DXI SNI) Fields

Field	Action/Description
Service Type	Select SMDS.
LPort Type	Select SMDS DXI/SNI DCE or DTE.
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one (1).

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields shown in Figure 8-20.

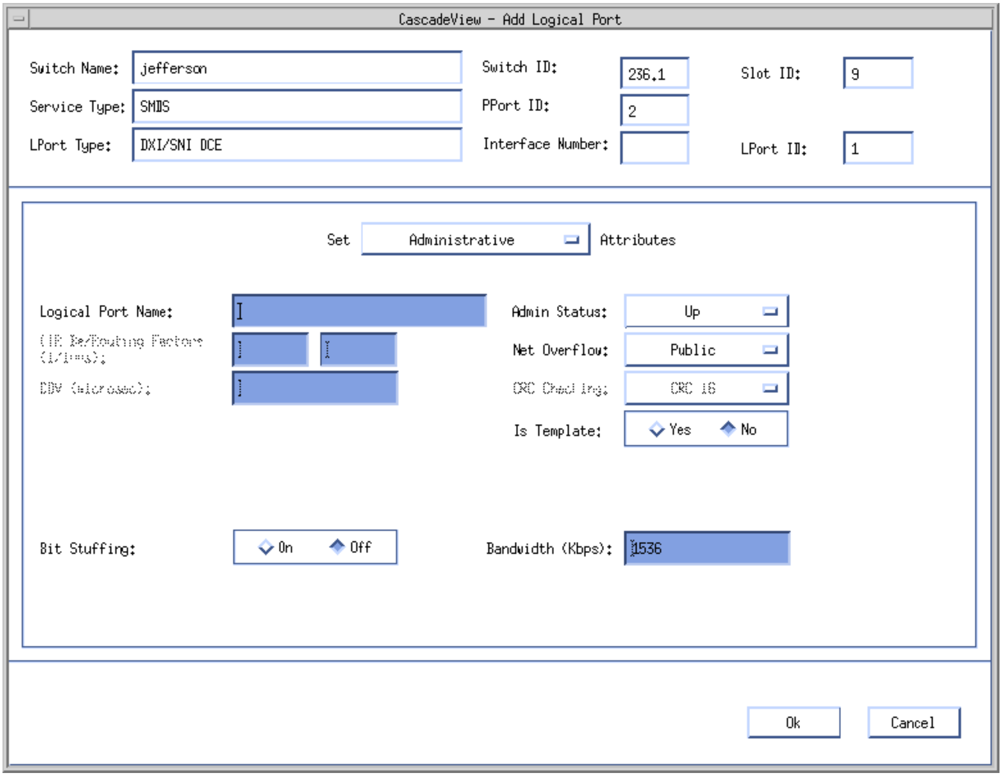


Figure 8-20. Set Administrative Attributes Dialog Box

3. Complete the required fields described in Table 8-10 on page 8-25.

4. Set the congestion control attributes for this DXI/SNI logical port by selecting *Congestion Control* from the Set Attributes option menu. Complete the fields described in Table 8-11 on page 8-28.

5. Set the SMDS attributes for this DXI/SNI logical port by selecting *SMDS* from the Set Attributes option menu. Complete the SMDS attributes fields described in Table 8-12 on page 8-30.

6. (*Optional*) Complete the Multiplex to this SSI field to configure the DXI/SNI to multiplex to an SSI-DTE. Do one of the following:

- If this DXI/SNI is to perform *local switching only*, choose Select. The Select End Logical Port dialog box appears as shown in Figure 8-21. In the Switch Name field, select [None]. Choose OK. Continue with Step 8 on page 8-46.
- If this DXI/SNI is to *multiplex to an SSI-DTE logical port*, choose Select. The Select End Logical Port dialog box appears as shown in Figure 8-21.

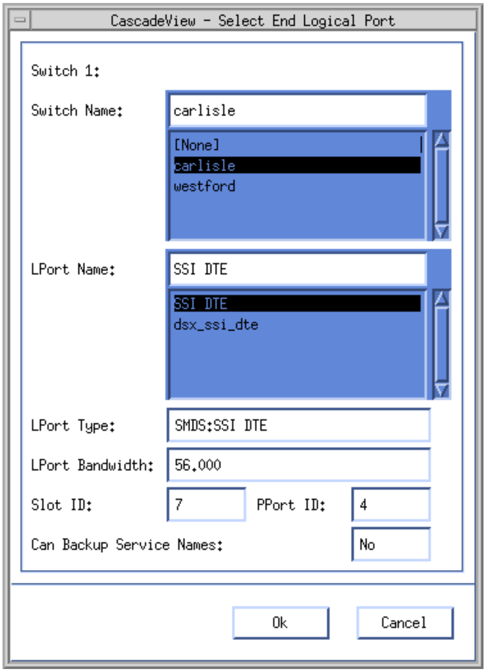


Figure 8-21. Select End Logical Port Dialog Box

7. Complete the required fields described in Table 8-17.

Table 8-17. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the switch (name) where the SSI port resides. The Switch Name field displays a list of the available SSI logical ports residing on the selected switch.
LPort Name	Select the specific SMDS to Access Server Interface (SSI) port to which this logical port will multiplex. Refer to "Defining Individual Addresses for DXI/SNI Multiplexed Logical Ports" on page 8-50 for instructions.

8. Set the trap control attributes for this DXI/SNI logical port by selecting *Trap Control* from the Set Attributes option menu. Complete the fields described in Table 8-13 on page 8-32.

9. Choose OK. The Set All Logical Ports in PPort dialog box appears displaying the name of the configured logical port.

10. Choose Close. The Set Physical Port Attributes dialog box appears.

11. Choose Close to return to the Set Physical Port Attributes dialog box.

12. Do ***one*** of the following:

    - If you configured the DXI/SNI logical port to perform *local* switching only, follow the instructions in "Defining Individual Addresses for DXI/SNI Locally Switched Logical Ports" on page 8-47.

    - If you configured the DXI/SNI logical port to *multiplex* to a designated SSI-DTE, follow the instructions in "Defining Individual Addresses for DXI/SNI Multiplexed Logical Ports" on page 8-50.

Defining Individual Addresses for DXI/SNI Locally Switched Logical Ports

When you configure a DXI/SNI logical port to perform local switching within the map network, you must manually enter the individual addresses to which the port subscribes.

Before you define an SMDS DXI/SNI logical port for either remote or local switching, verify the following task is complete:

- Define an DXI/SNI logical port parameters.

To define the individual addresses for a DXI/SNI logical port:

1. From the Set Physical Port Attributes dialog box, choose the Logical Port command. The Set All Logical Ports in PPort dialog box appears.
2. From the Set All Logical Ports in PPort dialog box, select the name you assigned to the DXI/SNI logical port.
3. Choose the Modify command. The Modify Logical Port dialog box appears, displaying the service and logical port types.
4. Choose OK. The Modify Logical Port dialog box appears, as shown in Figure 8-22, displaying the logical port parameters.

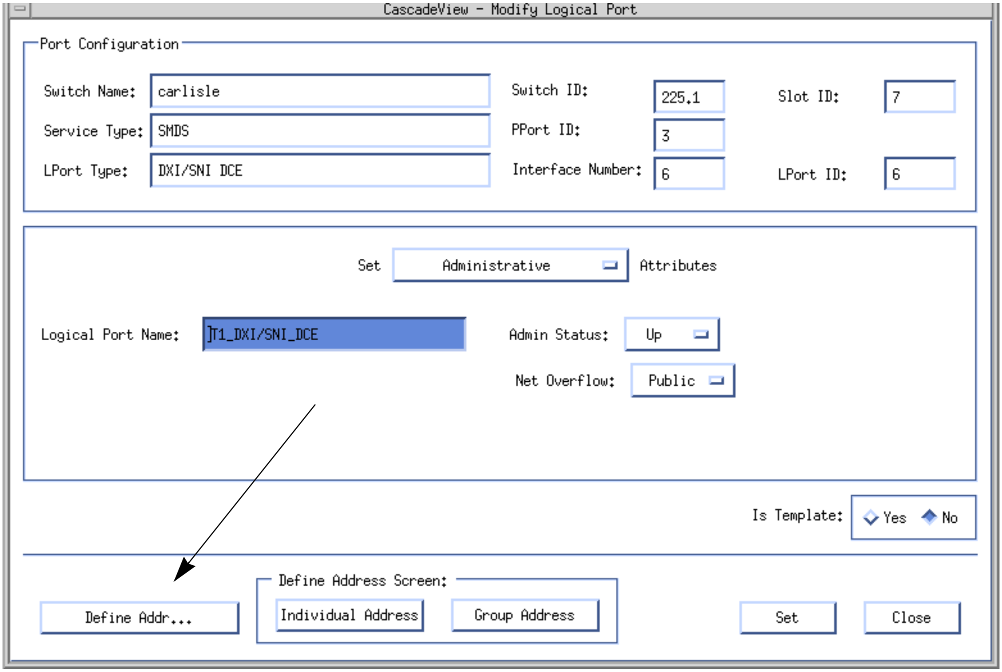


Figure 8-22. Modify Logical Port Dialog Box

5. Choose Define Addr. The Define Individual Address for SMDS DXI/SNI LPort dialog box appears as shown in Figure 8-23.

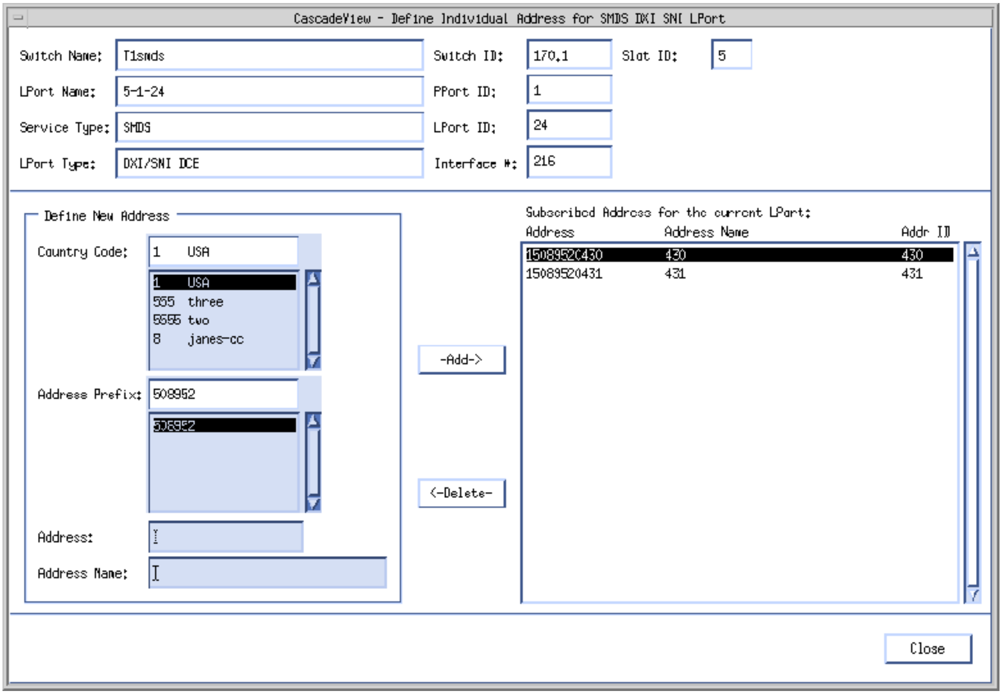


Figure 8-23. Define Individual Address for SMDS DXI/SNI LPort Dialog Box

6. Complete the required fields described in Table 8-18.

Table 8-18. Define Individual Address for SMDS DXI SNI LPort Fields

Field	Action/Description
Address Prefix	In the Define New Address field, select an Address Prefix.
Address	Type the remainder of the address.
Address Name	(*Optional*) Enter up to 16 alphanumeric characters to identify the new subscribed address (for example, westford). Do not use apostrophes.

7. Choose Add. The Subscribed Address for the current Lport list box displays the new address.

8. Repeat Step 6 and Step 7 to create additional individual addresses for the DXI/SNI logical port.

9. When you finish, choose Close. The Modify Logical Port dialog box appears.

10. Choose Close. The Set All Logical Ports in PPort dialog box appears.

11. Choose Close. The Set Physical Port Attributes dialog box appears.

Defining Individual Addresses for DXI/SNI Multiplexed Logical Ports

You do not need to define an address pool for individual addresses. The SSI-DTE logical port to which a DXI/SNI logical port is multiplexed determines the available addresses for the multiplexed DXI. The Define Individual Address for SMDS DXI/SNI LPort dialog box lists the available addresses to which this DXI/SNI port can subscribe.

Before you define an SMDS DXI/SNI logical port for either remote or local switching, verify the following tasks are complete:

- ☑ Define the DXI/SNI logical port parameters.
- ☑ Select the SSI associated with this DXI/SNI logical port.

To enter the individual addresses associated with this DXI/SNI multiplexed logical port:

1. From the Set All Logical Ports for this PPort Port dialog box, select the DXI/SNI logical port and choose Modify. The Modify Logical Port dialog box appears, displaying the service and logical port types.

2. Choose OK. The Modify Logical Port - Set Administrative Attributes dialog box appears as shown in Figure 8-24, displaying the attributes for the selected logical port.

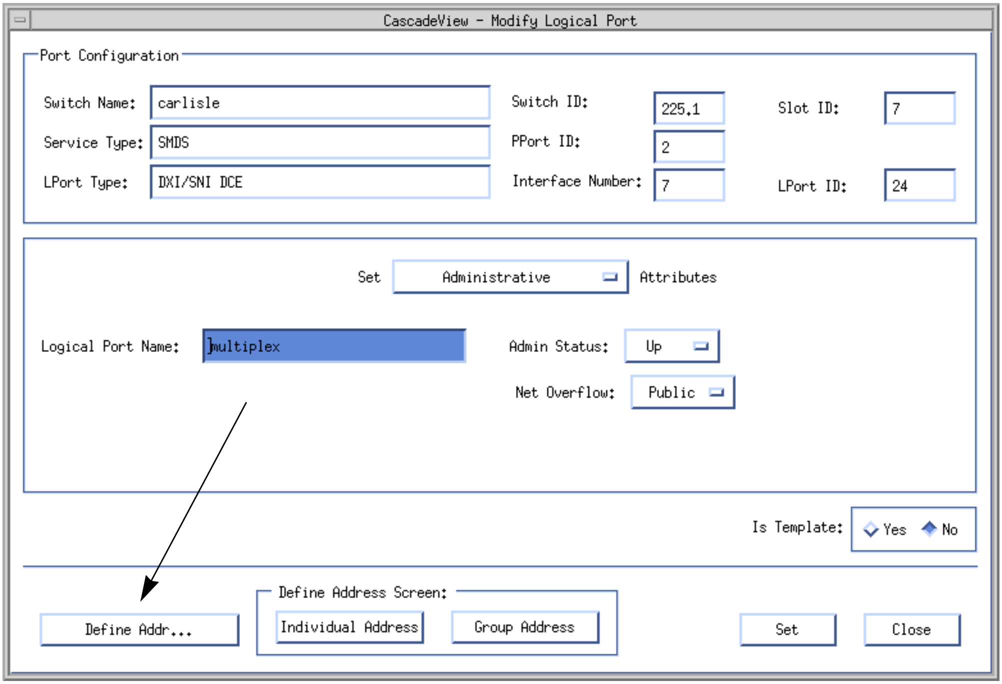


Figure 8-24. Modify Logical Port - Set Administrative Attributes Dialog Box

3. Choose Define Addr. The Define Individual Address for SMDS DXI SNI LPort dialog box appears as shown in Figure 8-25.

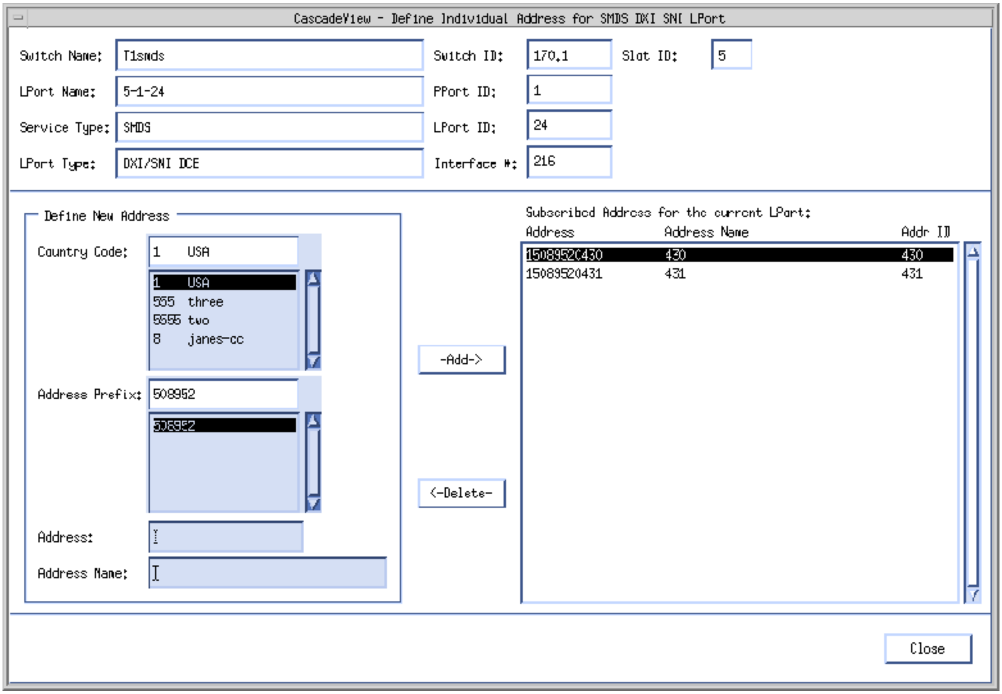


Figure 8-25. Define Individual Address for SMDS DXI SNI LPort Dialog Box

4. Complete the required fields described in Table 8-19.

Table 8-19. Define Individual Address for SMDS DXI SNI LPort Fields

Field	Action/Description
Country Code	Select the Country Code to which the DXI SNI logical port subscribes.
Address Prefix	Select the Address Prefix to which the DXI SNI logical port subscribes.
Address	Type the remainder of the address (address suffix) in the Address field.

Table 8-19. Define Individual Address for SMDS DXI SNI LPort Fields

Field	Action/Description
Address Name	(*Optional*) Enter up to 32 alphanumeric characters to identify the new subscribed address (for example, Boston). Do not use an apostrophe.

5. Choose Add. The Subscribed Addresses for the current LPort box displays the new address as shown in Figure 8-26.

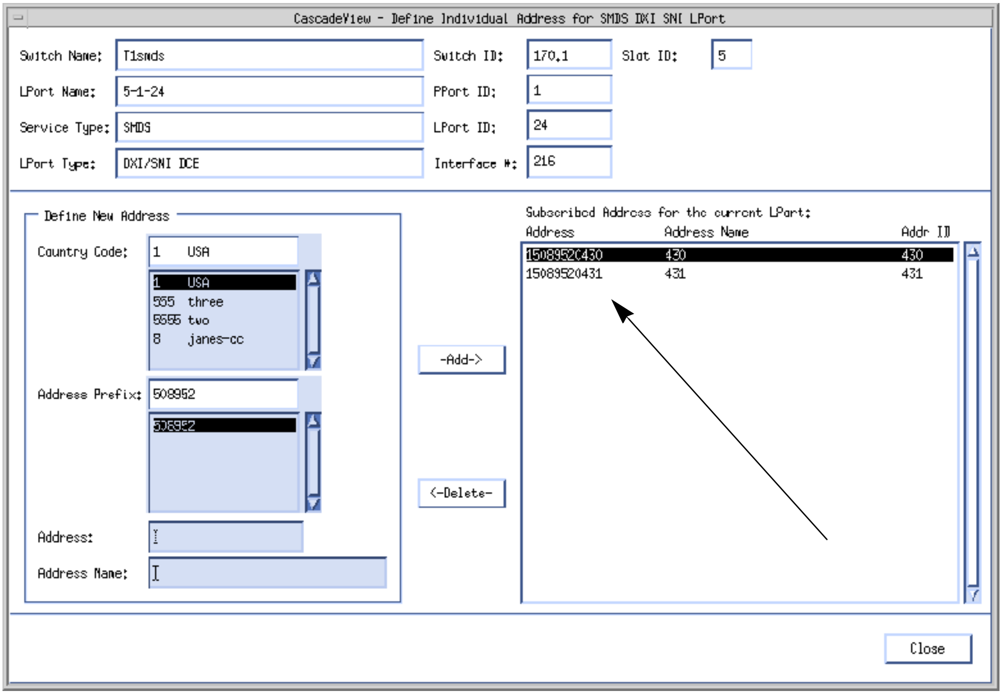


Figure 8-26. Define Individual Address for SMDS DXI SNI LPort Dialog Box

6. Choose Close. The Modify Logical Port dialog box reappears.

7. Repeat Step 4 through Step 6 to subscribe additional addresses.

8. When you finish, choose Close. The Set All Logical Ports in PPort dialog box appears.

9. Choose Close.The Set Physical Port Attributes dialog box appears.

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

11. Choose Close to return to the network map.

Defining a New Group Address

The Define Group Address dialog box displays a list of all group addresses and their members currently defined for a selected switch. From this dialog box, you can add, modify, or delete group addresses from the selected switch, based on the maximum capacities specified in Table 8-5 on page 8-12.

To define a networkwide group address:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SMDS Parameters ⇒ Set All Network Group Addresses. The Set All Networkwide Group Address dialog box appears as shown in Figure 8-27.

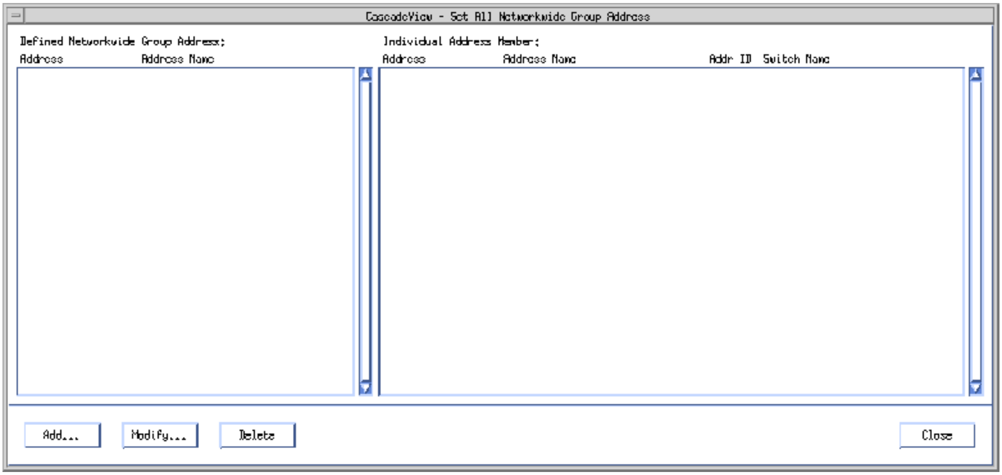


Figure 8-27. Set All Networkwide Group Address Dialog Box

2. Choose Add. The Add Networkwide Group Address dialog box appears as shown in Figure 8-28.

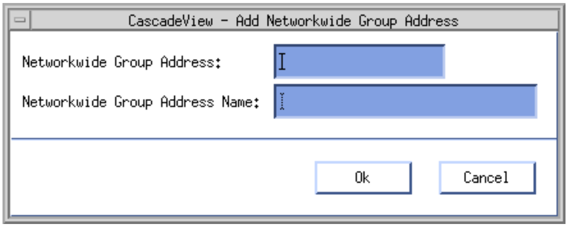


Figure 8-28. Add Networkwide Group Address Dialog Box

3. Complete the fields described in Table 8-20.

Table 8-20. Add Networkwide Group Address Fields

Field	Action/Description
Networkwide Group Address	Enter the complete group address (including the country code and address prefix).
Networkwide Group Address Name (*Optional*)	Enter up to 16 alphanumeric characters to identify the new group address (for example, massachusetts). Do not use an apostrophe.

4. Choose OK. The Set All Networkwide Group Address dialog box reappears, listing the new group address.

5. Repeat Step 2 through Step 4 to define additional group addresses.

6. When you finish, proceed to "Adding Individual Address Members to a Group" to add the individual addresses that make up the group.

Adding Individual Address Members to a Group

To add individual members to a networkwide group address:

1. From the Set All Networkwide Group Address dialog box, select the group address for which you are defining members.

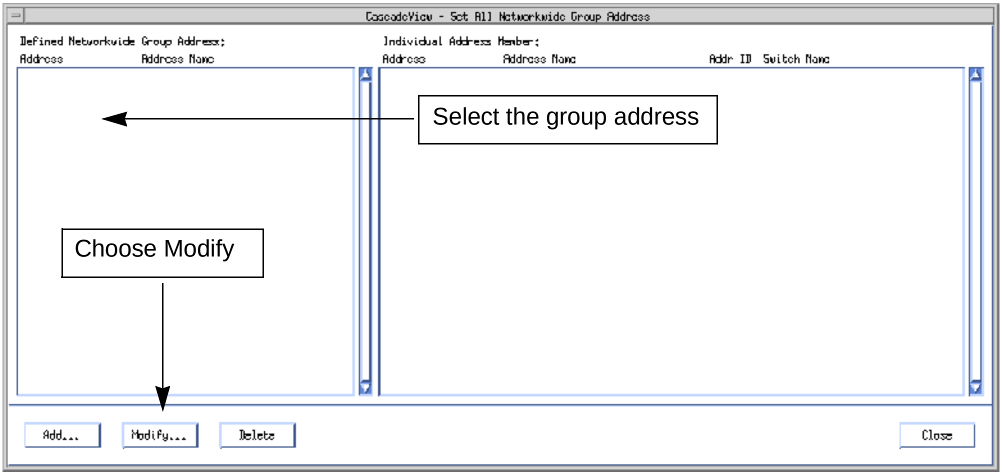


Figure 8-29. Set All Networkwide Group Address

2. Choose Modify. The Modify Networkwide Group Address dialog box appears as shown in Figure 8-30.

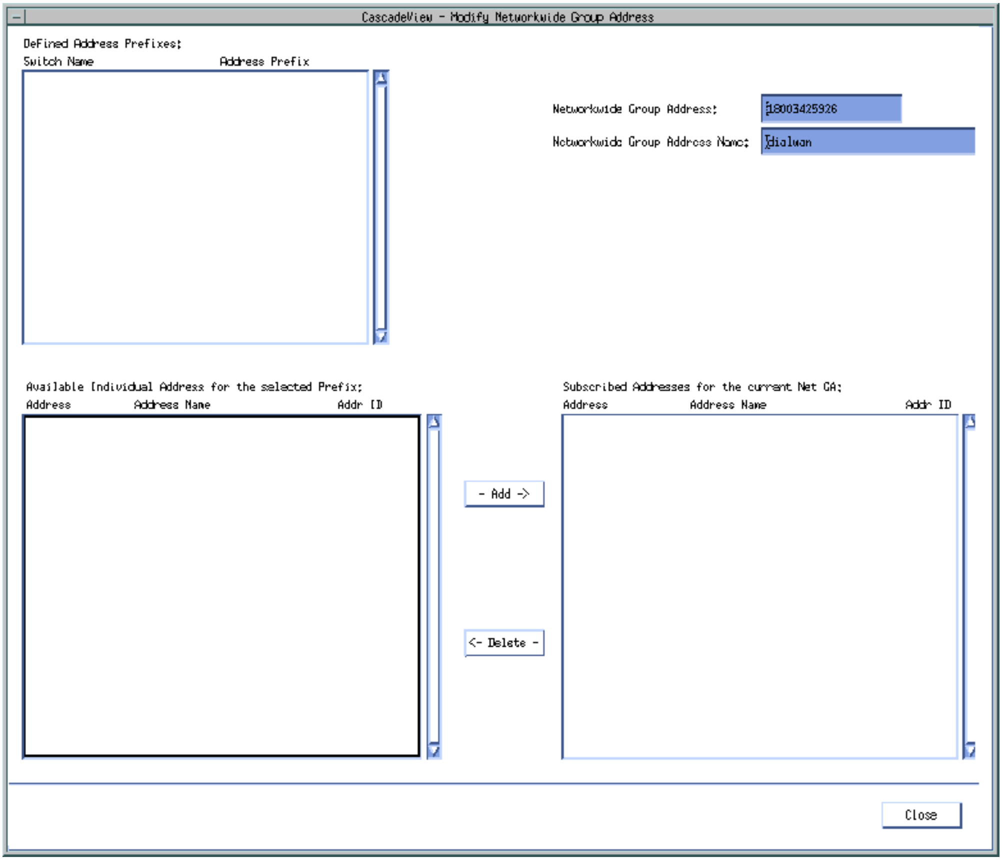


Figure 8-30. Modify Networkwide Group Address Dialog Box

3. In the Defined Address Prefixes list box, select an address prefix.

   The system displays available individual addresses (for the selected address prefix only) in the Available Individual Address for the selected Prefix window. (The system does not display individual addresses from the entire network.)

4. In the Available Individual Address for the selected Prefix list box, select the individual address you want to include as a member of the group, and choose Add.

   The selected individual address appears in the Subscribed Address for the current Net GA list box.

5. Repeat Step 4 until you have added all individual addresses that you want to include in the group.

6. When you finish selecting the individual address members that make up the group, choose Close. The Set All Networkwide Group Address dialog box appears.

7. Choose Close to return to the network map.

Configuring Address Screens

This section describes how to define individual and group address screens. This feature allows you to restrict data exchange on specified DXI/SNI logical ports. For more information about SMDS address screening, refer to "SMDS Addressing" on page 8-3.

Defining an Individual Address Screen

The individual address screen enables you to restrict the data received from the CPE as well as the data transmitted to the CPE. An individual address screen consists of a set of allowed/disallowed addresses.

To define an individual address screen for a DXI/SNI logical port:

1. From the Set All Logical Ports in PPort dialog box, select the DXI/SNI logical port

2. Choose Modify. The Modify Logical Port dialog box appears, displaying the service and LPort types.

3. Choose OK. The Logical Port dialog box displays the attributes for the selected logical port.

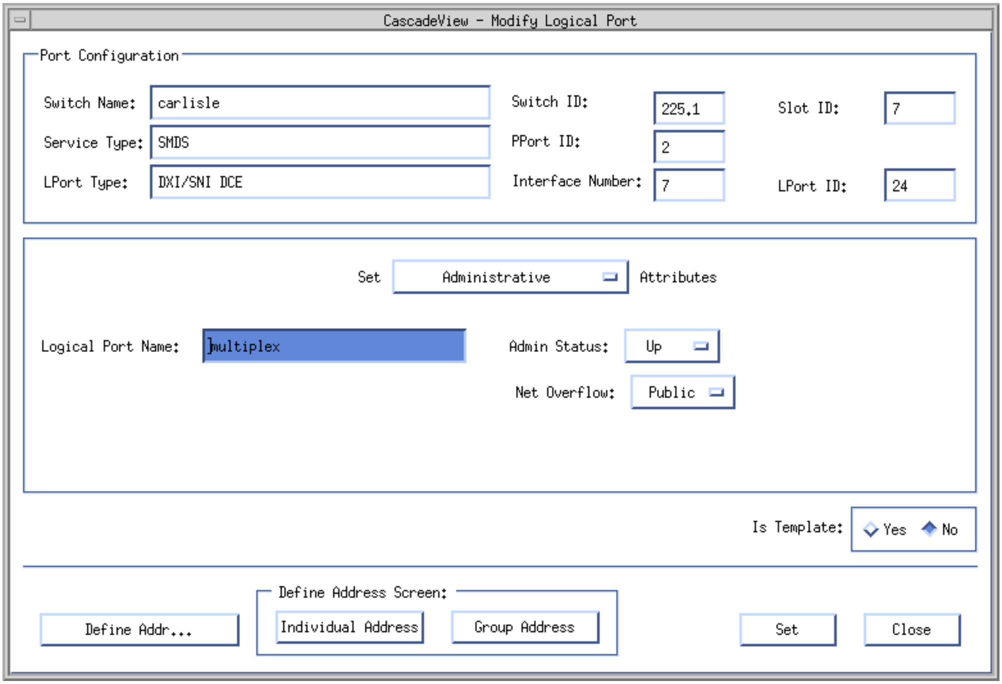


Figure 8-31. Modify Logical Port Dialog Box

4. From the Define Address Screen command group, choose Individual Address. The Define Individual Address Screen dialog box appears as shown in Figure 8-32.

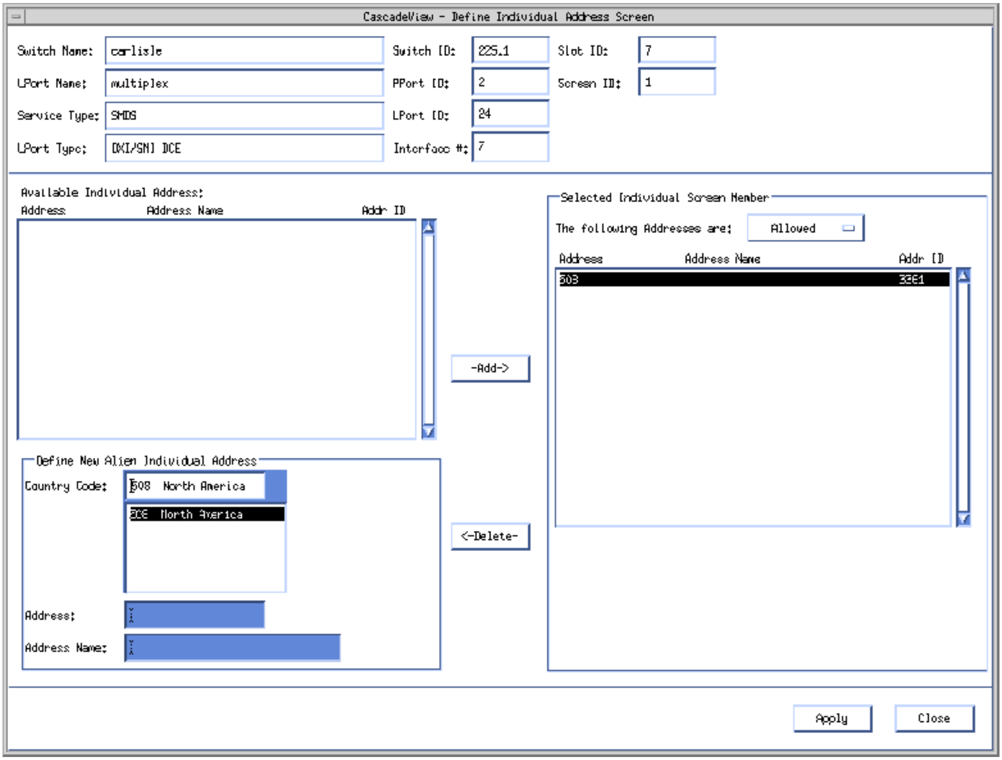


Figure 8-32. Define Individual Address Screen Dialog Box

5. Choose Apply to display the list of available individual addresses.
6. In the “The following Addresses are:” field, select Allowed or Disallowed to specify the desired operation.
7. Choose Apply to enter your selection and activate the Add and Delete command buttons.

8. Do **one** of the following:

   - Select an address from the list of available individual addresses, which includes all addresses to which the DXI/SNI ports on the selected switch subscribes.

     or

   - Enter an alien address in the Define New Alien Individual Address field. If applicable, enter the country code prefix. An alien address is any address not currently defined anywhere in the network. The alien address resides outside the switch and is used for destination screening. The Address Name field is optional.

9. Choose Add. The selected local address (or alien address) now appears in the Selected Individual Screen Member field, along with the address name and assigned address ID number (internal address).

10. When you finish, choose Close. The Modify Logical Port dialog box appears.

11. Choose Close. The Set All Logical Ports in PPort dialog box appears.

Defining a Group Address Screen

The group address screen contains a list of group addresses and an *allowed/disallowed* option. The setting of the allowed/disallowed option globally applies to every group address in the list.

To define a group address screen:

1. From the Set All Logical Ports in PPort dialog box, select the DXI/SNI logical port to which you want to apply the group address screen.

2. Choose Modify. The Modify Logical Port dialog box appears, displaying the service and logical port types.

3. Choose OK. The dialog box displays the attributes for the selected logical port.

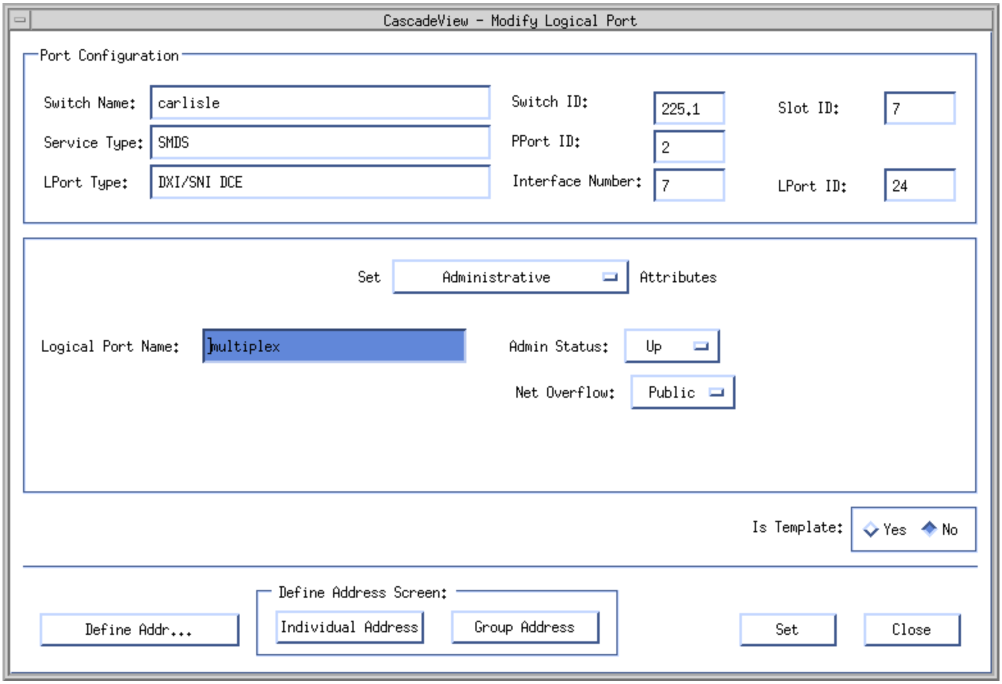


Figure 8-33. Modify Logical Port Dialog Box

4. From the Define Address Screen command group, choose Group Address. The Define Group Address Screen dialog box appears as shown in Figure 8-34.

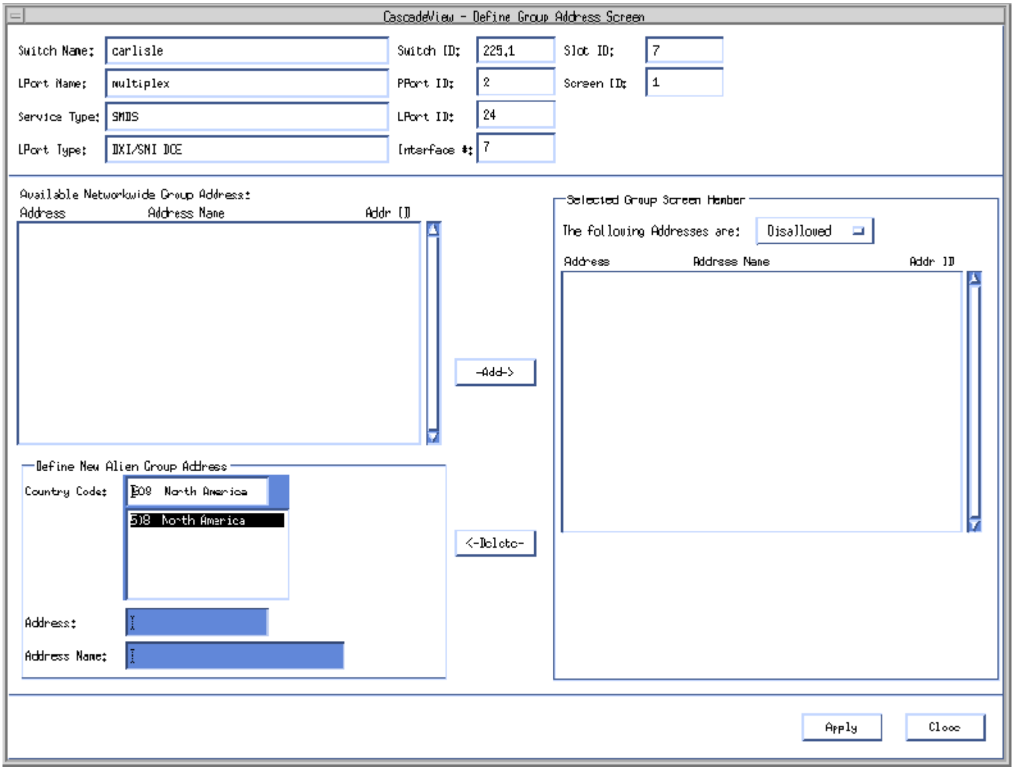


Figure 8-34. Define Group Address Screen Dialog Box

5. Choose Apply to display the list of Available Networkwide Group Addresses.
6. In the “The following Addresses are” field, select Allowed or Disallowed to specify the desired operation.
7. Choose Apply to enter your selection and activate the Add and Delete command buttons.

8. Do **one** of the following:

   - Select an address from the list of Available Networkwide Group Addresses, which includes all group addresses defined for the currently selected network.

     or

   - Enter an alien address in the Define New Alien Group Address field. If applicable, enter the country code prefix. An alien address is any address that is not currently defined for the selected switch. The Address Name is optional.

9. Choose Add. The selected group address or alien address, now appears in the Selected Group Screen Member field, along with the address name and assigned address ID number (internal address).

10. Repeat Step 8 and Step 9 to define more members.

11. When you finish, choose Close. The Modify Logical Port dialog box appears.

12. Choose Close. The Set All Logical Ports in PPort dialog box appears.

13. Choose Close. The Set Physical Port Attributes dialog box appears.

14. Choose Close to return to the network map.

Configuring the In-Band Management Address

An *in-band management address* enables an NMS that is remotely connected to the Cascade network using SMDS, to manage the SNMP/UDP/IP protocol packets.

To configure the In-band management address:

1. From the Administer menu, select Cascade Parameters ⇒ Set All SMDS Parameters ⇒ Set All Management Addresses. The Set All SMDS Management Address dialog box appears as shown in Figure 8-35.

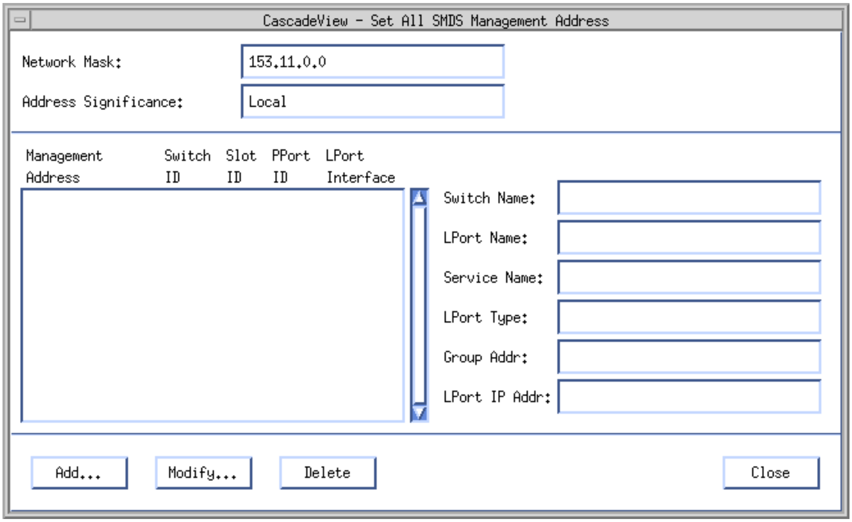


Figure 8-35. Set All SMDS Management Address Dialog Box

> *If you have already configured management addresses, the dialog box displays this information. From the Set All SMDS Management Address dialog box, use the Modify or Delete commands to modify or delete management address configurations.*

2. Choose Add. The Select End Logical Port dialog box appears as shown in Figure 8-36.

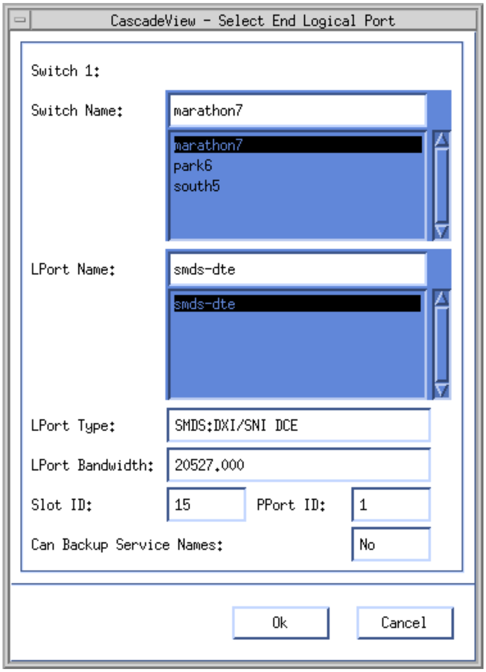


Figure 8-36. Select End Logical Port Dialog Box

3. Complete the required dialog box fields described in Table 8-21.

Table 8-21. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the switch (name) that contains the address pool.
LPort Name	Select the logical port (name) for which you are defining the in-band management address.
LPort Type	Displays the logical port type.
LPort Bandwidth	Displays the logical port bandwidth.

Table 8-21. Select End Logical Port Fields (Continued)

Field	Action/Description
Slot ID	Displays the I/O slot (number) in which the card resides.
PPort ID	Displays the number of the port you are configuring.

4. Choose OK. The Add SMDS Management Address dialog box appears as shown in Figure 8-37.

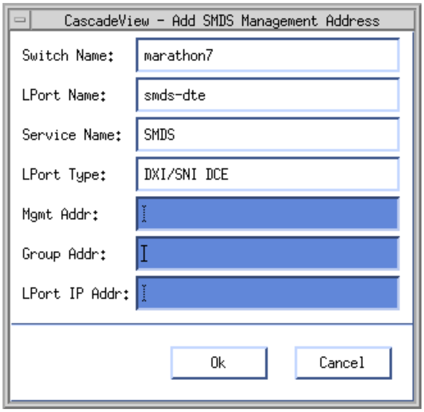


Figure 8-37. Add SMDS Management Address Dialog Box

5. Complete the required fields described in Table 8-22.

Table 8-22. Add SMDS Management Address Fields

Field	Action/Description
Switch Name	Displays the name of the selected switch.
LPort Name	Displays the name of the SSI DTE logical port configuration that contains the address pool.

Table 8-22. Add SMDS Management Address Fields (Continued)

Field	Action/Description
LPort Type	Displays the type of logical port configuration.
Mgmt Address	If the LPort Type is SSI, the management address appears. If the LPort Type is DXI/SNI, enter the individual address to which the logical port subscribes.
Group Address	If applicable, enter the group address to which the logical port subscribes.
LPort IP Address	Enter the IP address of the selected logical port.

6. Choose OK. The Set In-Band Management Addresses dialog box reappears, displaying the in-band management address.

7. Define the NMS path for in-band management as described in “Setting the NMS Path” on page 5-30.

Administrative Tasks

This section describes how to:

- Use Templates to define a new logical port
- Delete circuits
- Delete trunks
- Delete SMDS logical ports
- Disable the SMDS switching system

Using Templates

If you defined a logical port configuration and saved it as a template (see I*s Template* field in Table 8-10 on page 8-25), you can define a new logical port using the same parameters.

To define a logical port using a template:

1. Choose the Add Using Template command on the Set All Logical Ports in PPort dialog box (see Figure 8-8 on page 8-19).
2. Do one of the following:
   - Choose Last Template to use the last template you defined for this switch.
   - Choose Template List to display a list of templates defined for this map. Select a template and choose OK.

Deleting SMDS Logical Ports

Before you can delete an SMDS logical port, verify:

Step 1. There are no trunks defined on the logical port.

Step 2. There is no SMDS Management Address configured for this logical port.

Step 3. This logical port is not defined as the feeder (SMDS SSI-DTE) for an existing SMDS OPTimum trunk logical port. You must disable the OPTimum trunk or first define another feeder before you can delete this logical port.

Step 4. This is not the SMDS SSI to which other SMDS DXI logical ports can multiplex. Review the Set All Logical Ports dialog box and make sure the “Multiplex to this SSI” field displays *None*.

Step 5. The defined DXI individual address is not a member of a group address. Refer to page 8-56.

Step 6. There is no individual address defined for this logical port. Refer to page 8-47 and page 8-50.

Step 7. There are no SMDS individual/global address screen addresses defined for this logical port. Refer to page 8-58 and page 8-61.

If any of these components exist and use the logical port you want to delete, you must first delete them in the following order:

- Trunks
- SMDS Management Addresses
- Logical port

Deleting Trunks

To delete a trunk:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears. If necessary, select each trunk and review each logical-port endpoint.
2. Select the trunk to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting SMDS Management Addresses

1. From the Administer menu, select Cascade Parameters ⇒ Set All Management Addresses. The Set All Management Address dialog box appears.
2. Choose the Management Address you want to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting the Logical Port

> *If the loopback status field on the Set All Logical Ports screen does not display* ***None****, do not attempt to delete this logical port. refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for more information about loopback testing.*

To delete the logical port:

1. Select the switch on which to delete a logical port.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the port. The Set Physical Port Attributes dialog box appears.
4. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

5. Select the logical port you want to delete. Verify the Loopback Status field displays NONE.

> *Make sure this logical port is not the SSI DTE logical port used as the feeder for an SMDS OPTimum trunk. You must take the OPTimum trunk out of service or first define another feeder address before you can delete this logical port.*

6. Choose Delete.

7. Choose Close.

Disabling the SMDS Switching System

To disable the SMDS switching system feature for the entire Cascade network:

1. Edit the /opt/CascadeView/etc/ cascadeview.cfg file

2. Change the CV_DISABLE_SMDS_SS value from 0 (*enabled*) to 1 (*disabled*).

3. Set the IA and GA mask size parameters to 0. Refer to the steps in Table 8-6 on page 8-17 if necessary.

4. PRAM Sync each CP card in the network. For instructions on how to PRAM Sync a CP card refer, to “Using the Synchronize PRAM Command” on page 12-16.

5. Cold boot the desired switches.

9

Configuring ATM Services

This chapter describes how to configure logical ports for Cascade's Asynchronous Transfer Mode (ATM) Services. ATM is a connection-oriented technology that relays traffic via an address contained within the packet. Unlike Frame Relay, ATM uses short, fixed-length packets called *cells*. Like SMDS, ATM employs a cell relay mechanism. ATM offers scalable rates customized to users' needs from 1.5 Mbps to 155 Mbps or higher. Unlike Frame Relay or other data services, ATM accommodates delay-sensitive traffic such as voice, and constant rate processes such as video. For more information about ATM, refer to the *Networking Services Technology Overview*.

ATM Logical Ports

Table 9-1 lists and describes the types of ATM logical ports you can configure on the B-STDX 8000/9000.

Table 9-1. ATM Logical Port Types

Logical Port Type	Description
ATM UNI DCE	Configures the logical port to communicate with an ATM CPE over ATM PVCs. The Cascade switch acts as an access concentrator feeding multiple Frame Relay and/or ATM PVCs to the CPE via the logical port.
ATM UNI DTE	Configures the logical port to communicate with an ATM switch over ATM PVCs. The Cascade switch acts as an access concentrator feeding multiple Frame Relay and/or ATM PVCs to the ATM network via the logical port.
Network Interworking for Frame Relay Network-to-Network Interface	• Enables an ATM broadband circuit to interconnect two Frame Relay networks. • Enables the logical port to communicate with a peer Frame Relay switch over an ATM PVC. • Multiplexes multiple Frame Relay PVC segments over the ATM PVC. • Supports many-to-one connection multiplexing. • Facilitates inter-LATA FR NNI connections. • Supports Frame Relay/ATM PVC Network Interworking Implementation Agreement FRF.5.
OPTimum Frame Trunk	• Optimizes performance and throughput in situations where both ends are connected by Cascade switches. • Enables the logical port to communicate with a peer Cascade switch over an ATM PVC. • Multiplexes multiple Frame Relay PVCs and SMDS “connections” over the ATM PVC.

Table 9-1. ATM Logical Port Types (Continued)

Logical Port Type	Description
ATM OPTimum Cell Trunk	An OPTimum cell trunk is a virtual path that supports the transmission of virtual circuit connection (VCC) data. Virtual circuits may be established between any B-STDX and Cascade 500 user interfaces via B-STDX 9000 frame/cell trunks and Cascade-500 cell trunks. • Enables a single OSPF routing domain in a mixed network that includes both B-STDX and Cascade 500 switches. Routing decisions allow frame-based traffic to traverse either frame or cell-based trunks. Cell-based traffic is restricted to routes that traverse Direct Cell trunks. OPTimum Cell trunks have no Cascade trunk header. A unique VPI/VCI identifies the circuit and control traffic using a separate channel. A cell trunk uses a virtual path through the ATM cloud as a trunk. • Enables you to create a trunk between either two B-STDX 9000 switches or between a Cascade 500 and a B-STDX. The following modules enable you to create an OPTimum cell trunk logical port from a B-STDX 9000 switch: ATM CS, ATM IWU, or ATM UNI DS3/E3.(You can also create an OPTimum Cell trunk logical port from the Cascade 500 to the B-STDX 9000 on OC3 and DS3 modules.)

Table 9-1. ATM Logical Port Types (Continued)

Logical Port Type	Description
ATM Direct Trunk/ Direct Cell Trunk	Supports the transmission of virtual path connection (VPC) data. Like OPTimum cell trunks, direct cell trunks have no Cascade header. A unique VPI/VCI identifies the circuit and control traffic using a separate channel. A cell trunk uses a virtual path through the ATM cloud as a channel. When configuring a direct cell trunk, no DTE feeder is required and the direct trunk logical port is the only logical port that can be configured since the direct cell trunk uses the entire physical port. • Enables you to create a trunk between either two B-STDX 9000 switches or between a Cascade 500 and a B-STDX. • Enables a single OSPF routing domain in a mixed network that includes both B-STDX and Cascade 500 switches. The following modules enable you to create a direct trunk logical port from a B-STDX 9000 switch: ATM CS, ATM IWU, or ATM UNI DS3/E3. (You can also create a Direct Cell trunk logical port from the Cascade 500 to the B-STDX 9000 on OC3 and DS3 modules.)

I/O Modules for ATM Services

You can configure most ATM logical port types for B-STDX 8000/9000 I/O modules. Table 9-2 lists any limitations.

Table 9-2. I/O Modules for ATM Services

I/O Module Type	ATM Logical Port Support
8-port Universal I/O	ATM UNI-DCE, ATM UNI-DTE, OPTimum Frame trunk, ATM FR NNI
4-port 24 Channel T1	ATM UNI-DCE, ATM UNI-DTE
4-port 30 Channel E1	ATM UNI-DCE, ATM UNI-DTE

Table 9-2. I/O Modules for ATM Services (Continued)

I/O Module Type	ATM Logical Port Support
2-port HSSI	ATM UNI-DCE, ATM UNI-DTE, OPTimum Frame trunk, ATM FR NNI
10-port DSX-1	ATM UNI-DCE, ATM UNI-DTE, OPTimum Frame trunk, ATM FR NNI
1-port channelized DS3	ATM UNI-DCE, ATM UNI-DTE, OPTimum Frame trunk, ATM FR NNI
4-port unchannelized T1	ATM UNI-DCE
4-port unchannelized E1	ATM UNI-DCE
ATM-based I/O Modules	
ATM DS3	ATM UNI-DTE, Direct trunk, OPTimum Cell trunk, OPTimum Frame trunk, ATM FR NNI
ATM CS	ATM UNI-DCE, ATM UNI-DTE, Direct trunk, OPTimum Cell trunk, OPTimum Frame trunk, ATM FR NNI
ATM IWU	ATM UNI-DCE, ATM UNI-DTE, Direct trunk, OPTimum Cell trunk, OPTimum Frame trunk, ATM FR NNI

Configuring Ports for ATM DXI/FUNI and ATM Services

Low Speed ATM *Data Exchange Interface/Frame User-to-Network Interface* (DXI/FUNI) service enables a Cascade switch to interoperate between Frame Relay and ATM technology on a single platform. ATM DXI/FUNI is a frame-based protocol that is designed to map easily to Frame Relay. Initially, Cascade supports ATM DXI/FUNI, Mode 1A features for the ATM DXI/FUNI standard. These features include:

- Provisioning for up to 938 virtual connections per card
- Support for AAL Type 5 data packaging only
- Frame sizes up to 8192 octets (DTE DSU)
- 16-bit frame checking sequence between the DTE and the DCE

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, 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), which 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 bites of VCI). The values have no effect on VPCs, which you can provision anywhere over the VPI = 0 – 255 range.

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 VPI = 0 – 15 and VCI 32 – 1023 range the default values provide.
- When you use the logical port with UNI signalling enabled, you must match the VPI/VCI range settings between the CBX 500 and the attached device *exactly.* The majority of SVC-capable CPE only supports the use of VPI = 0. This means to ensure proper operation, you must also set the CBX 500 logical port for a range of VPI = 0 (VPI bits = 0). You should also match the VCI range with the attached device. Most SVC-capable CPE supports a VCI range of at least 32 – 1023. This translates to a VCI bit setting of 10 on the CBX 500 logical port. If you are not sure about the VPI/VCI range of the attached device, use a conservative CBX 500 logical port setting of VPI = 0 and VCI = 10, to provide close to 1000 VCs over the interface. Refer to Table 9-3 on page 9-8 for more information.
- If you will use this logical port as a feeder for OPTimum trunks, 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 9-3 as a guide to set these values.

> *When you configure an OPTimum trunk between two endpoints, the OPTimum trunk 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 or each endpoint must accommodate this VPI.*

Table 9-3. 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

Table 9-3. Number of Valid Bits in VPI/VCI (Continued)

[1] If Number of Valid VPI Bits =	Valid VPI Range Is	If Number of Valid VCI Bits =	[2] Valid VCI Range Is
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 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. The following table provides a guide to map and convert physical layer bandwidth to logical port bandwidth:

Table 9-4. 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

Table 9-4. Physical and Logical Port Bandwidth Conversions (Continued)

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)
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 amounts of 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 2 cells every second are lost. For these cases, you may want to either adjust the traffic rate or disable UPC for this circuit.

About 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. ILMI also determines the operational status of the logical port. ILMI is available on ATM CS and ATM IWU modules only.

For example, with ILMI enabled on a UNI-DCE port, the logical port polls the attached device every five (5) seconds. Five seconds is the *polling period*. If no response is received after four consecutive polls (*loss threshold)*, the link is considered down.

Table 9-5 describes the differences between UNI DCE and DTE logical ports with ILMI enabled and disabled.

Table 9-5. Logical Ports and ILMI Settings

Port Type	Parameter Effected	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 link is declared down (time period is based on the polling period x loss threshold).	Physical Port state
	Address Registration	• Send node prefixes • Send port prefixes • Accept addresses (qualified against configured prefixes)	None
	Remainder of ILMI MIB	Read-only	None

Table 9-5. Logical Ports and ILMI Settings (Continued)

Port Type	Parameter Effected	With ILMI Enabled	With ILMI Disabled
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).	Physical Port state
	Address Registration	Accept prefixes (and optionally qualify addresses against configured prefixes)	None
	Remainder of ILMI MIB	Read-only	None

Before You Begin

Before you begin, verify the following tasks are complete:

- ☑ Create a subnet and network map (Chapter 4)
- ☑ Add a Cascade switch (Chapter 4)
- ☑ Configure the IP address and set the NMS path (Chapter 5)
- ☑ Configure the I/O module(s) (Chapter 6)
- ☑ Configure the physical port parameter(s) (Chapter 6)

Accessing ATM Logical Port Functions

To access the Logical Port functions in CascadeView, use the following steps:

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.

4. Choose the Logical Port command. The Set All Logical Ports in PPort dialog box appears as shown in Figure 9-1.

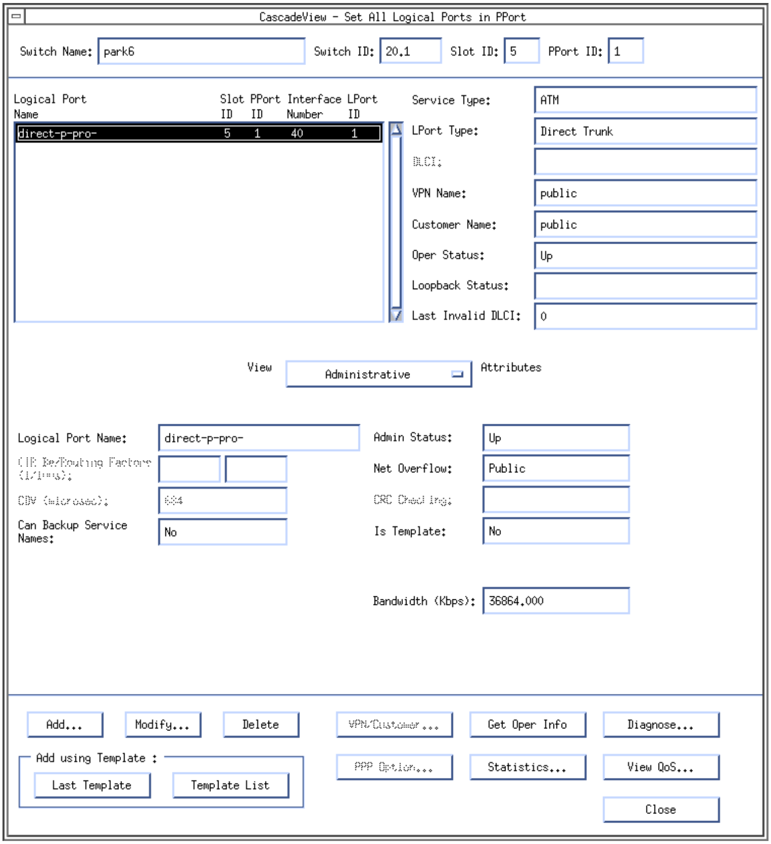


Figure 9-1. Set All Logical Ports in PPort Dialog Box

The Set All Logical Ports in PPort 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 modify and delete logical ports.

Table 9-6 describes the Set All Logical Ports in PPort command buttons.

Table 9-6. Set All Logical Ports in PPort Command Buttons

Command Button	Function
Modify/Delete	*Modify* or *Delete* commands modify or delete logical port configurations. For information about deleting logical ports refer to "Deleting ATM Logical Ports" on page 9-60.
Get Oper Info	A status message appears in the *Oper Status* field displaying a brief status for the selected logical port.
Diagnose	Accesses diagnostic tests for the selected logical port. For more information about diagnostics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Statistics	Displays the summary statistics for the selected logical port. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Add using Template (Last Template Template List)	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 the same parameters. Refer to "Administrative Tasks" on page 9-59 for more information.
VPN/Customer	Displays the Virtual Private Network customer's name.
View Qos Parameters	Displays the Quality of Service parameters.

Adding an ATM Logical Port

1. To add an ATM logical port, perform the steps in "Accessing ATM Logical Port Functions" on page 9-13.

2. On the Set All Logical Ports in PPort dialog box, choose Add. The Add Logical Port dialog box appears as shown in Figure 9-2

.

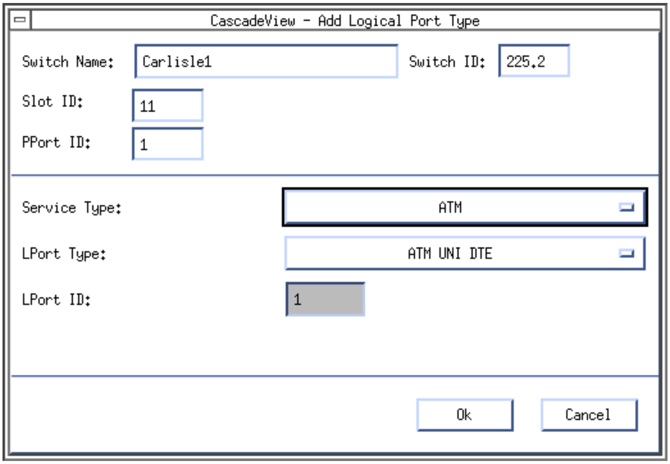


Figure 9-2. Add Logical Port Dialog Box (DTE)

3. Define the specific logical port. Refer to Table 9-7 for specific instructions.

Table 9-7. ATM Logical Port Configurations

LPort Type	Refer to...
ATM UNI DTE or ATM UNI DCE	"Defining ATM UNI DCE/DTE Logical Ports" on page 9-18.
ATM Network Interworking for FR NNI	"Defining Network Interworking for FR NNI Logical Ports" on page 9-41.
ATM OPTimum Frame Trunks	"Defining ATM OPTimum Frame Trunk Logical Ports" on page 9-50.

Table 9-7. ATM Logical Port Configurations (Continued)

LPort Type	Refer to...
ATM OPTimum Cell Trunk	"Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports" on page 9-34.
ATM Direct Trunk	"Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports" on page 9-34.

The Set Attributes Option Menu

When you define a new logical port, the Add Logical Port dialog box displays a Set Attributes option menu (Figure 9-3) that enables you to set different attributes for each type of logical port. Attributes include:

Administrative — Determines the number of channels allocated to each port and sets the admin status, net overflow, and bandwidth parameters. The administrative attribute fields may vary, depending on the type of service and card type.

Congestion Control — Set the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network.

Link Mgmt — *(ATM Interworking for FR NNI only)* Sets the DCE and DTE polling timer and interval values.

ATM — Set the ATM parameters which include the number of valid bits in the VPI/VCI, the ATM protocol, and the UNI type.

ILMI/Signaling/OAM — The ILMI/Signaling, and OAM information.

> **ILMI** — Management information base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep-alive protocol.
>
> **Signaling** — Signalling is a protocol that supports the dynamic creation of ATM virtual circuits. For more information, refer to the CBX 500 Network Administrator's Guide.
>
> **OAM** — Sets the alarm functions that generate operations, administration, and maintenance (OAM) alarms.

Trap Control — Sets the congestion threshold percentage in which traps are generated, and the number of frame errors per minute on each logical port.

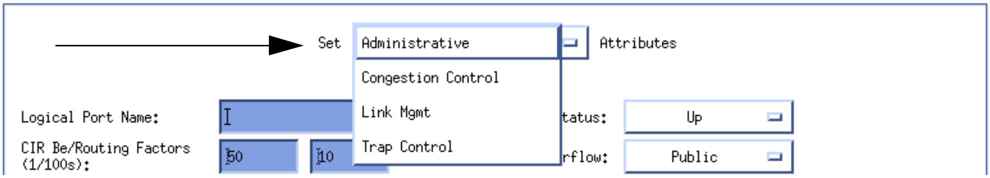


Figure 9-3. Set Attributes Option Menu

Defining ATM UNI DCE/DTE Logical Ports

To define an ATM UNI-DCE or ATM UNI-DTE logical port:

1. Complete the Add Logical Port dialog box (Figure 9-2) fields described in Table 9-8.

Table 9-8. Add Logical Port (UNI-DCE) Fields

Field	Action/Description
Service Type	Select ATM.
LPort Type	Select ATM UNI DCE (Network Side) or ATM UNI-DTE.
Logical Port ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one.

2. Choose OK. The Set Administrative Attributes dialog box appears and displays the fields shown in Figure 9-4.

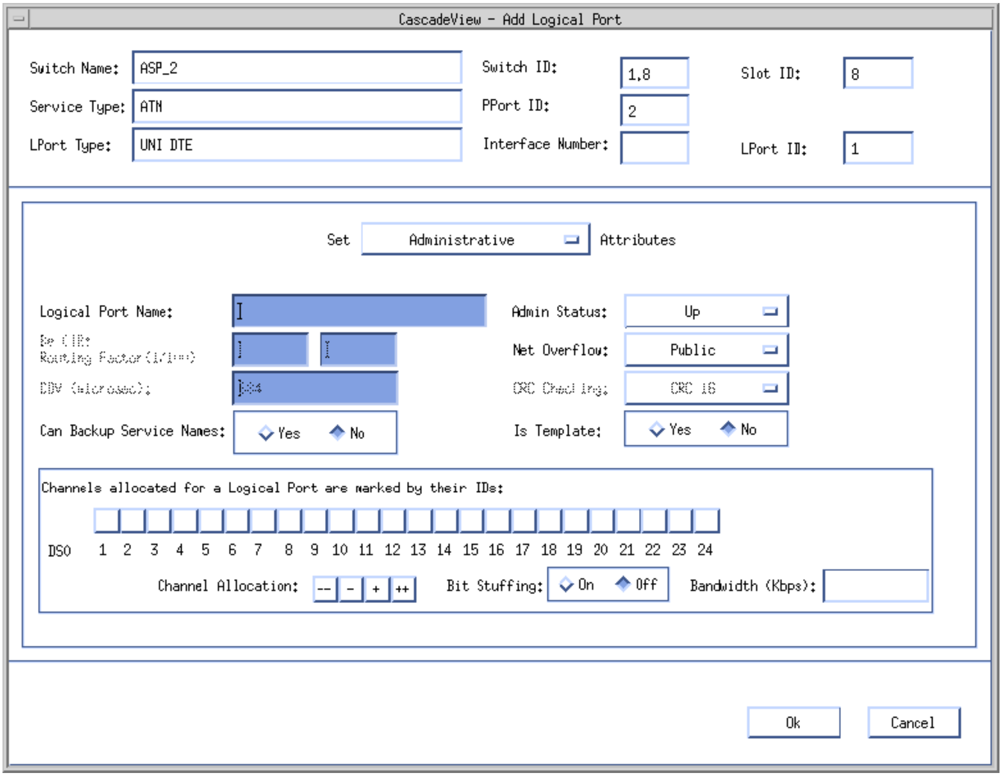


Figure 9-4. Set Administrative Attributes Dialog Box (ATM UNI DCE/DTE)

Administrative Attributes

1. Complete the required fields described in Table 9-9.

Table 9-9. Set Administrative Attributes Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Can Backup Service Names	*(Fault-tolerant PVC only)* Select Yes to configure a logical port for backup service. For more information, refer to "Configuring Fault-Tolerant PVCs" on page 7-44.
Admin Status	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. *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
CRC Checking (HSSI modules only)	Set this value to match the number of error checking bits used by the CPE connected to this port. Performs a cyclic redundancy check (CRC) on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.
Is Template	(*Optional*) You can save these settings as a template, which you can use again to quickly configure a logical port with the same options. To create a template, choose Yes in the *Is Template* field. Refer to "Administrative Tasks" on page 9-59 for more information.

Table 9-9. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	Specify the DS0 (for T1) or TS0 (for E1) channel(s) allocation for this logical port. The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel ***Note****: The logical port bandwidth either increments or decrements depending on the number of channels you select or deselect. You can configure other logical ports with different attributes, to other DS0/TS0 channels on this same physical port.*
Bit Stuffing	Select the bandwidth that matches the bandwidth capability of the customer premise equipment (CPE) connected to this logical port. Enables bit stuffing on T1/E1/DSX-1 ports. Bit stuffing effects the available bandwidth of each DS0/TS0 channel on this port. *On* – Provides 56 Kbps of bandwidth. *Off* – Provides 64 Kbps of bandwidth.

Table 9-9. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth remaining from the physical clock rate, less any logical ports already configured. To define a trunk logical port on this same physical port, decrease the amount of bandwidth on this logical port to ensure sufficient remaining bandwidth. For example: *Physical port clock speed*: 1536 Kbps *Logical port UNI-DTE/NNI Feeder Bandwidth*: 56 Kbps *Logical port Frame Relay Trunk Bandwidth*: 1480 Kbps The example configuration allocates a PDN trunk with 1480 Kbps bandwidth between two Cascade switches, each attached to a PDN network.

Congestion-Control Attributes

1. Set the congestion control attributes by selecting *Congestion Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 9-5 on page 9-23.

The congestion-control attributes do not apply to ATM CS and ATM IWU modules. Proceed to "ATM Attributes" on page 9-26 and "ILMI and OAM Attributes" on page 9-28.

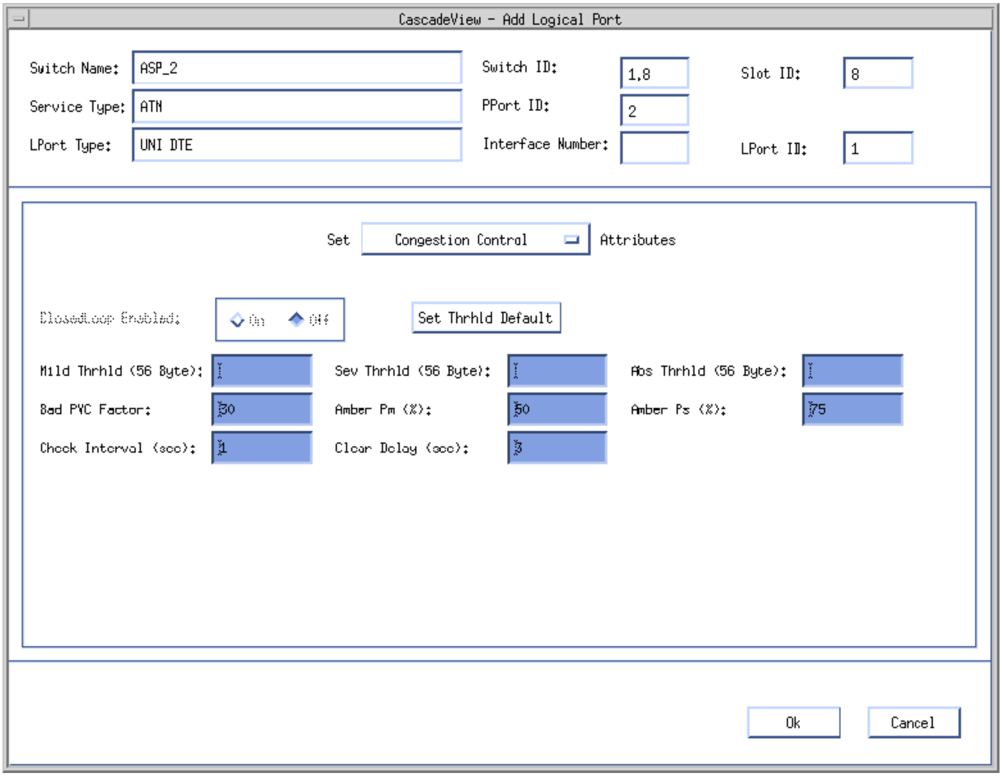


Figure 9-5. Set Congestion Control Attributes Dialog Box (UNI DCE/DTE)

> *Do not exceed the maximum threshold value for each card type. The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.*

> *For channelized T1/T1 PRI and channelized E1/E1 PRI modules, if **n** DS0s are assigned per channel, the maximum value allowed on the number of buffers is n x 225 (T1) and n x 174 (E1).*

2. Complete the required dialog box fields described in Table 9-10.

Table 9-10. Set Congestion Control Attributes Fields

Field	Action/Description
ClosedLoop Enabled	Set the congestion control parameters. This field enables/disables OSPF closed-loop congestion control for each logical port. For more information refer to "Closed-Loop Congestion Control" on page 7-7. Options include: *Off (default)* – Disables closed-loop congestion. *On* – Enables closed-loop congestion.
Set Thrhld Default	Set the Mild, Severe, and Absolute threshold settings to the default settings described in Table 7-5 on page 7-10 through Table 7-5 on page 7-10.
Mild Thrshld (56 Byte) Severe Thrshld (56 Byte) Absolute Thrshld (56 Byte)	Accept the defaults or enter values for the mild, severe, and absolute threshold fields as defined in Table 7-5 through Table 7-7. ***Note**: If you are setting threshold parameters on a T1/E1 card, the default values will not appear until you set the bit stuffing and bandwidth allocation. Refer to Table 9-9 on page 9-20 for more information.*

Table 9-10. Set Congestion Control Attributes Fields (Continued)

Field	Action/Description
Bad PVC Factor	Enter a value between 0-32. Determines the threshold for “bad” PVC detection. The following example shows the relationship between the “bad” PVC factor and threshold. $$\text{Threshold} = \frac{Bc+(Be/2)}{2^{(32-F_b)}}$$ The default is 30. ***Note**: If you select simple as the rate enforcement scheme (see Table 11-8 on page 11-23) this feature is disabled.*
Amber Pm (%)	Controls the reduction percentage of Be when mild congestion occurs. Enter a Pm% value. The default is 50%.
Amber Ps (%)	Enter a Ps% value. This value controls the reduction percentage of Be when severe congestion occurs. The default is 75%.
Check Interval (sec)	Enter and interval. This determines the number of seconds in which the switch monitors the trunk’s congestion on the port. The default is one (1) second.
Clear Delay (sec)	Enter a value. This determines the number of seconds in which the switch monitors the trunk’s non-congestion state. Enter a value. The default is three (3) seconds.

ATM Attributes

1. (*ATM IWU and ATM CS modules only*) Set the ATM attributes by selecting *ATM* from the Set Attributes option menu. The Add Logical Port dialog box displays the fields shown in Figure 9-6.

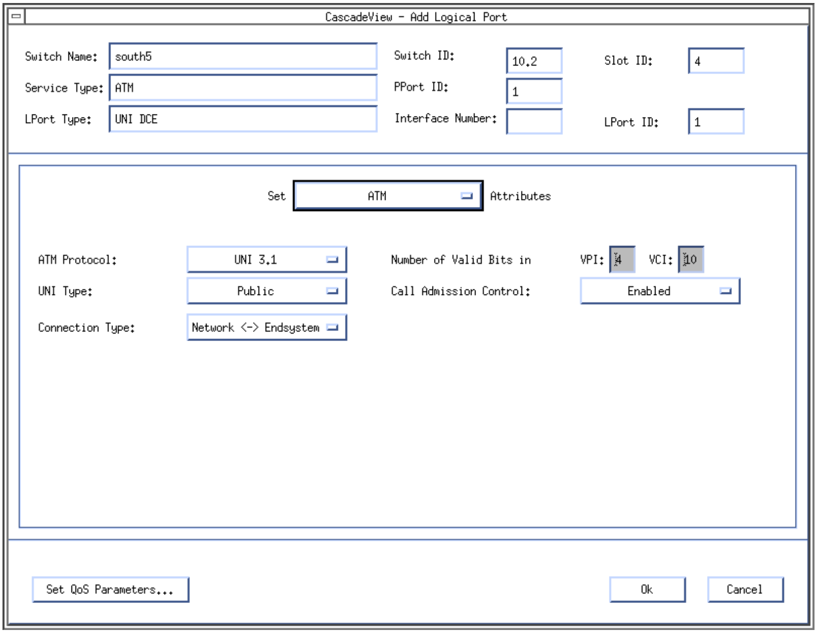


Figure 9-6. Set ATM Attributes Dialog Box (UNI DCE/DTE)

2. Complete the required fields described in Table 9-11.

Table 9-11. Set ATM Attributes Fields

Field	Action
ATM Protocol	Select the ATM protocol. You can use the UNI 3.0 option if IISP 3.1 is the desired protocol. Options include: UNI 3.1 (*default*) UNI 3.0. IISP 3.1

Table 9-11. Set ATM Attributes Fields (Continued)

Field	Action
UNI Type	Select Public or Private. See Table 9-7 describes when to select these options for both DTE and DCE ports.
Connection Type	Select Network <-> Network if this port connects to another switch or an endsystem. Select Network <-> Endsystem if this port connects to a router or host (UNI-DCE ports only).
Number of Valid Bits in VPI	Set the number of valid bits in VPI. This field applies to Virtual Channel Connections (VCCs) only. Specify the number of bits used in the ATM cell header for storing the Virtual Path Identifier (VPI). The total of both values cannot exceed 14. The default of 7 is recommended for both fields, which enables you to configure 127 OPTimum trunks, with up to 96 virtual channels on a given virtual path. The valid range for the VPI field is 0-8. For more information about setting these values, refer to page 9-7.
Number of Valid Bits in VCI	Set the number of valid bits in VCI. This field applies to Virtual Channel Connections (VCCs) only. Specify the number of bits used in the ATM cell header for storing the Virtual Channel Identifier (VCI). The total of both values cannot exceed 14. The default of 7 is recommended for both fields, which enables you to configure 127 OPTimum trunks, with up to 96 virtual channels on a given virtual path. The valid range for the VCI field is 5-14. For more information about setting these values, refer to page 9-7.

Table 9-11. Set ATM Attributes Fields (Continued)

Field	Action
Call Admission Control	Set the call admission control parameter to enabled or disabled. *Enabled* (*default*) – Port rejects a circuit creation request if there is not enough available bandwidth. *Disabled* – Port attempts to create a circuit even if there is not enough available bandwidth (for VBR Non-Real Time and UBR queues 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.*

ILMI and OAM Attributes

1. (*ATM IWU and ATM CS modules only*) Set the ILMI and OAM attributes by selecting *ILMI/Signaling/OAM* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in in Figure 9-7.

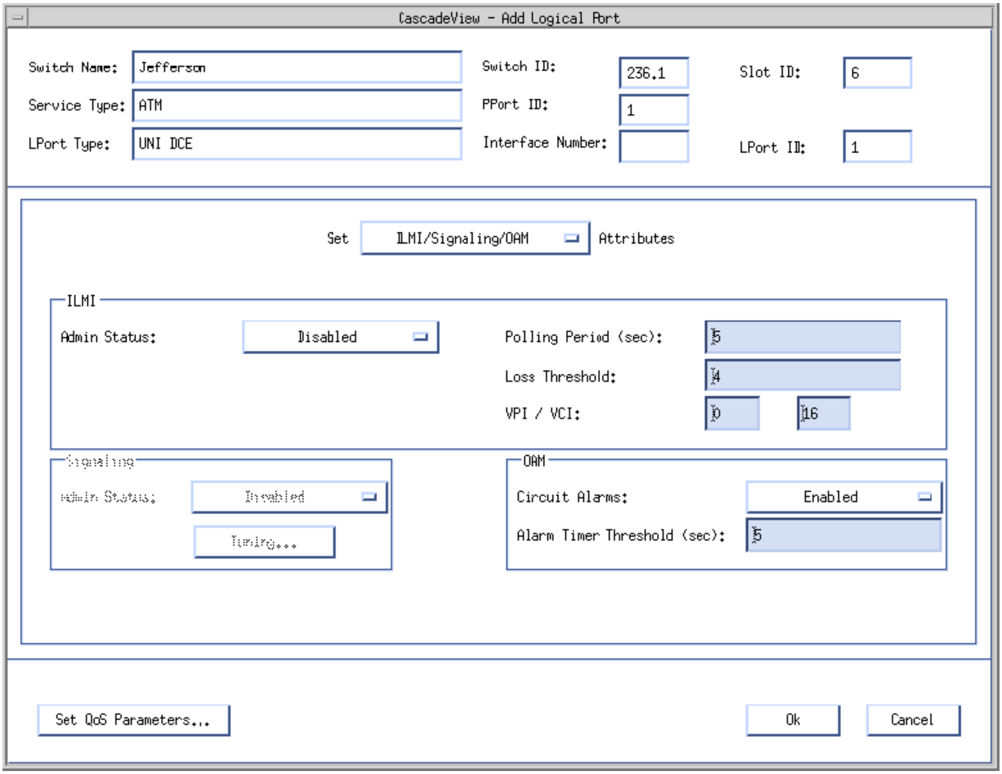


Figure 9-7. Set ILMI/OAM Attributes Dialog Box (UNI DCE/DTE)

2. Complete the required fields described in Table 9-12.

Table 9-12. Set ILMI and OAM Attributes Fields

Field	Action
Admin Status	Enable or disable the admin status. *Enabled* – Provides ILMI support. When ILMI is *Disabled* (default), the logical port state is the same as the physical port state. For information about ILMI support, refer to "About Interim Local Management Interface (ILMI)" on page 9-11. *Disabled* – Disables ILMI support. If you are using line loopback diagnostics, you must disable ILMI support. See the *CascadeView/UX Diagnostics and Troubleshooting Guide for B-STDX/STDX* for more information on loopbacks.
Polling Period (sec)	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*.
Circuit Alarms	Set the circuit alarm status. *Enabled* (*default*) – Allow this logical port to generate OAM alarms. The switch uses these alarms to signal when the circuits have gone down or come back up. Select Disabled – Disables OAM alarms on this logical port.

Table 9-12. Set ILMI and OAM Attributes Fields (Continued)

Field	Action
Alarm Timer Threshold (sec)	Set the alarm timer threshold in seconds. The switch waits until the circuit has been down for the time period you specify in this field before generating an OAM alarm. The default is *5 seconds*.

Trap-Control Attributes

1. Set the trap control attributes by selecting *Trap Control* from the Set Attributes option menu.

   The Add Logical Port dialog box displays the fields shown in Figure 9-8.

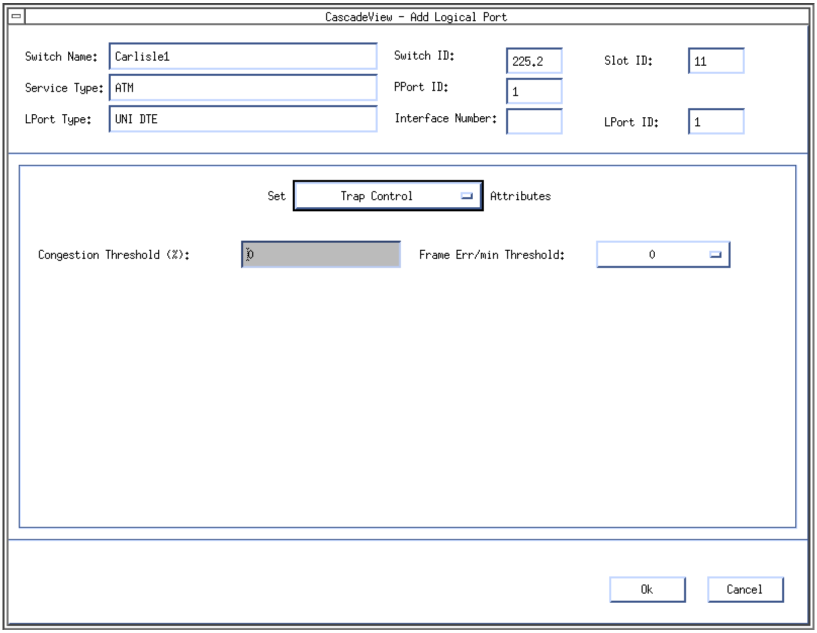


Figure 9-8. Set Trap Control Attributes Dialog Box (UNI DCE/DTE)

2. Complete the required fields described in Table 9-13.

Table 9-13. Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold (%)	Enter a value between 0 and 100 to indicate the threshold percentage for generating and sending traps to the NMS for this logical port. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the percentage value you enter. Adjust the entered value according to how sensitive this port needs to be to network congestion. Options include: *Zero (default)* – Disables congestion threshold. If you enter zero, no traps are generated for this logical port. *Low* – Generates a trap at the first sign of congestion. *High* – Generates traps for serious network congestion.
Frame Err/Min Threshold	Enter a value from 0 to 16384 to configure the threshold of frame errors on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS. Adjust this value according to how sensitive this port needs to be to frame errors. Options include: *Zero (default)* – Disables this feature, which prevents traps from being generated for this logical port. *Low* – Port is sensitive to frame errors. *High* – Generates traps when a significant number of frame errors occurs within a one-minute period.

3. *(Optional)* Choose Set QoS Parameters to set Quality of Service (QoS) parameters. The Set Logical Port QoS Parameters dialog box appears. For instructions on setting these parameters, refer to page 9-56. When you finish, return to this section and proceed to Step 4.

> *If you want to use the default settings for each service class, skip Step 3. By default, Bandwidth Allocation is set to Dynamic and over-subscription Factor is set to 100%. The Routing Metric setting does not apply to trunks.*

4. Choose OK. The Set All Logical Ports in PPort dialog box appears.

5. Choose Close. The Set Physical Port Attributes dialog box appears.

   Configure the remaining logical ports for this physical port. Refer to the instructions that follow for the specific type of logical port you want to add.

   When you finish configuring a DTE logical port, you can add either a FR NNI logical port or an OPTimum trunk logical port. Refer to page 9-50 for information about ATM OPTimum trunk logical ports.

6. To configure logical ports on another physical port, select the port, then refer to the appropriate section for the logical port type you want to configure.

   After you configure both endpoints of an ATM UNI logical port connection, you can add PVCs between the logical port endpoints.

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. Before you can configure an ATM OPTimum Cell trunk logical port, you must first configure an ATM UNI DTE logical port on the same physical port.

Using Direct Cell Trunks

You can configure an ATM direct trunk to create a connection between two B-STDX 9000 switches or between a B-STDX 9000 switch and a Cascade 500 switch.

To configure a direct cell trunk, use the following sequence:

Step 1. Configure the physical port you want to use for the direct trunk (refer to "Configuring Physical Ports" on page 6-9). You can configure direct trunks on any of the following ATM modules:

- ATM CS
- ATM IWU
- ATM DS3

(You can also create a Direct Cell trunk logical port from the Cascade 500 to the B-STDX 9000 on OC3 and DS3 modules.)

Step 2. Configure an ATM Direct trunk logical port on the physical port.

Using ATM OPTimum Cell Trunks

You can configure an ATM OPTimum trunk to create a switch-to-switch Cascade trunk through a public data network (PDN) into another Cascade network. The Cascade OPTimum trunk allows private enterprises to purchase lower-cost public-carrier services as the trunk between two Cascade switches, rather than use a more expensive leased-line service.

To implement the OPTimum trunk, first configure a UNI-DTE feeder logical port on the same physical port. To configure an OPTimum trunk, use the following sequence:

Step 1. Configure the physical port you want to use for the OPTimum trunk (refer to "Configuring Physical Ports" on page 6-9).

Step 2. Configure a UNI-DTE feeder logical port (page 9-18) for the OPTimum trunk on this physical port.

Assign this logical port a minimum amount of bandwidth.

Step 3. Configure the OPTimum trunk logical port on the same physical port. Assign the remaining bandwidth to this logical port (if there is only one OPTimum trunk configured on the physical port).

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

1. Complete the Add Logical Port dialog box fields as follows:

   Service Type — Select ATM. The available ATM Logical port types appear.

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

   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 9-3 on page 9-8).

   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 which shares this physical port (refer to page 9-7).

   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).

   VCI —The number of valid bits in the Virtual Channel Identifier. Refer to "Setting the Number of Valid Bits in the VPI/VCI" on page 9-7 for further details.

> *Virtual Path ID 0 is reserved and cannot be used.*
>
> *You have to provision a VPC in another ATM network between two Cascade switches. This VPC acts like a physical line. Specify the VPI of this VPC in the Virtual Path ID field.*

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields shown in Figure 9-9.

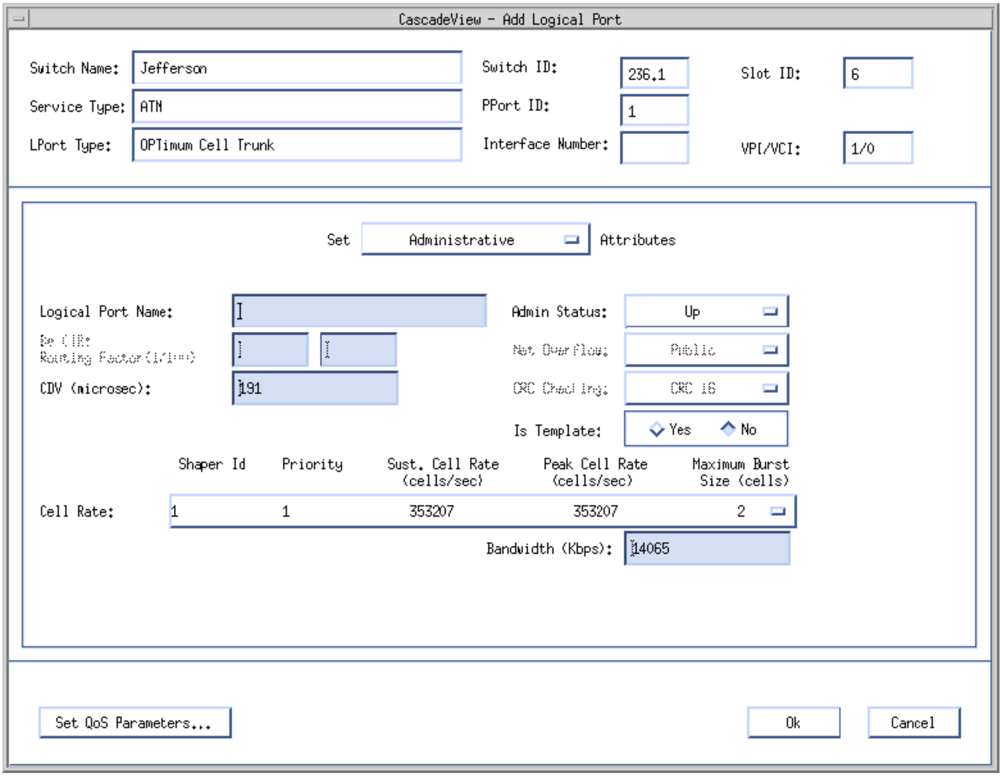


Figure 9-9. Set Administrative Attributes (Direct/OPTimum Cell, ATM CS/IWU Card)

Administrative Attributes

Complete the administrative attributes fields as described in Table 9-14. Note that Table 9-14 lists all possible administrative attributes for a Direct and OPTimum Cell logical port. The attributes vary depending on your type of I/O module.

Table 9-14. Direct and OPTimum Direct Cell Administrative Attributes

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Admin Status	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. *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
CDV (microsec)	(*OPTimum Direct Cell Trunks, ATM CS/IWU modules only*) Specify the maximum cell delay variation (in µsecs) for this logical port. This value applies only to CBR traffic, and specifies the maximum variation in time delays between cells going out of this logical port. The default value is 684 for DS3 ports, or 191 for OC3c ports. To change the default, you need to know the maximum CDV for PVCs on the port, as well as the traffic requirements of the hardware at the other end of the connection.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
Is Template	(*Optional*) You can save these settings as a template, which you can use again to quickly configure a logical port with the same options. To create a template, choose Yes in the *Is Template* field. Refer to “Administrative Tasks” on page 9-59 for more information.

Table 9-14. Direct and OPTimum Direct Cell Administrative Attributes

Field	Action/Description
Shaper ID	*(OPTimum Direct Cell Trunks, ATM CS/IWU modules only)* Choose a value from 1 through 15 to specify the Shaper ID and associated priority, sustainable cell rate, peak cell rate, and maximum burst size values.
Peak Cell Rate (cells/sec)	*(ATM UNI DS3 modules only)* Specify the maximum allowed cell transmission rate (expressed in cells per second). The PCR defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
Sustainable Cell Rate (cells/sec)	*(ATM UNI DS3 modules only)* Specify the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. SCR 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 traffic.
Maximum Burst Size (cells)	*(ATM UNI DS3 modules only)* Specify 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 CBR or UBR traffic.

Table 9-14. Direct and OPTimum Direct Cell Administrative Attributes

Field	Action/Description
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. 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 currently configuring. Leave enough bandwidth for any remaining OPTimum trunks you need to configure on this logical port. ***Note:*** *Multipoint VCCs are limited over OPTimum trunks. You cannot configure more than one circuit leaf of a point-to-multipoint circuit on the same logical port, since multiplexing cannot be performed at the port level. If you configure more than one OPTimum trunk on a logical port, set up a circuit leaf for a given circuit root on only one of the OPTimum trunks.*

Trap Control Attributes

1. Complete the trap control attributes fields for ATM direct trunks as described in Table 9-13 on page 9-32.

2. (*Optional*) Choose Set QoS Parameters to set Quality of Service (QoS) parameters. The Set Logical Port QoS Parameters dialog box appears. For instructions on setting these parameters, refer to page 9-56. When you finish, return to this section and proceed to Step 3.

> *If you want to use the default settings for each service class, you can skip Step 2. By default, Bandwidth Allocation is set to Dynamic and Over-subscription Factor is set to 100%. The Routing Metric setting does not apply to trunks.*

3. Choose Close to return to the Set Physical Port attributes dialog box.

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

5. To configure logical ports on another physical port, select the port, then choose Set Attr. Refer to the appropriate section for the logical port type you want to configure.

   After you configure both logical port endpoints for a trunk, you can add the trunk line connection between them. Refer to Chapter 10, “Configuring Trunks”.

Defining Network Interworking for FR NNI Logical Ports

An ATM Network Interworking for FR NNI logical port enables an ATM broadband circuit to interconnect two Frame Relay networks. This configuration enables the logical port to communicate with either a Cascade or a non-Cascade Frame Relay switch over an ATM PVC.

Before you configure a Network Interworking for FR NNI logical port, first configure an ATM UNI DTE logical port on the same physical port.

You can configure more than one Network Interworking for FR NNI logical port on a single physical port.

To define a Network Interworking for FR NNI logical port,

1. Complete the Add Logical Port dialog box (Figure 9-10) fields described in Table 9-15.

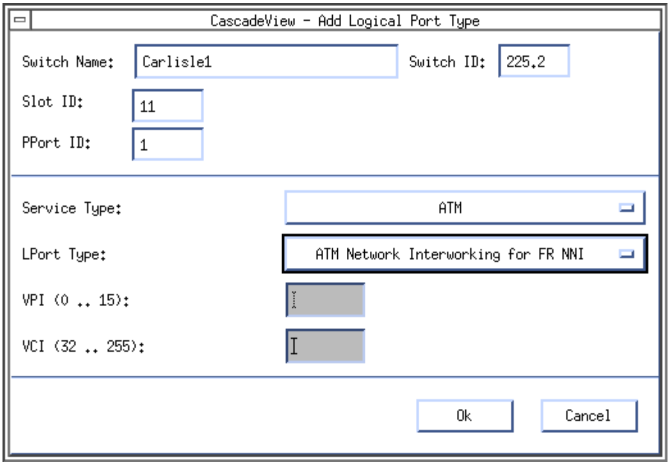


Figure 9-10. Add Logical Port Type (ATM FR NNI) Dialog Box

Table 9-15. Add Logical Port Fields (FR NNI)

Field	Action/Description
Service Type	Select ATM.
LPort Type	Select ATM Network Interworking for FR NNI.
VPI	Enter the VPI of the ATM VCC that carries the NNI data. Refer to "Virtual Paths and Virtual Channels" on page 9-6 for more information about this field.
VCI	Enter the VCI of the ATM VCC used to carry the NNI data. (NNI is a single ATM circuit that can be used to carry a single Frame Relay circuit or many Frame Relay circuits multiplexed over a single ATM circuit.) Refer to "Virtual Paths and Virtual Channels" on page 9-6 for more information about this field.

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields as shown in Figure 9-11.

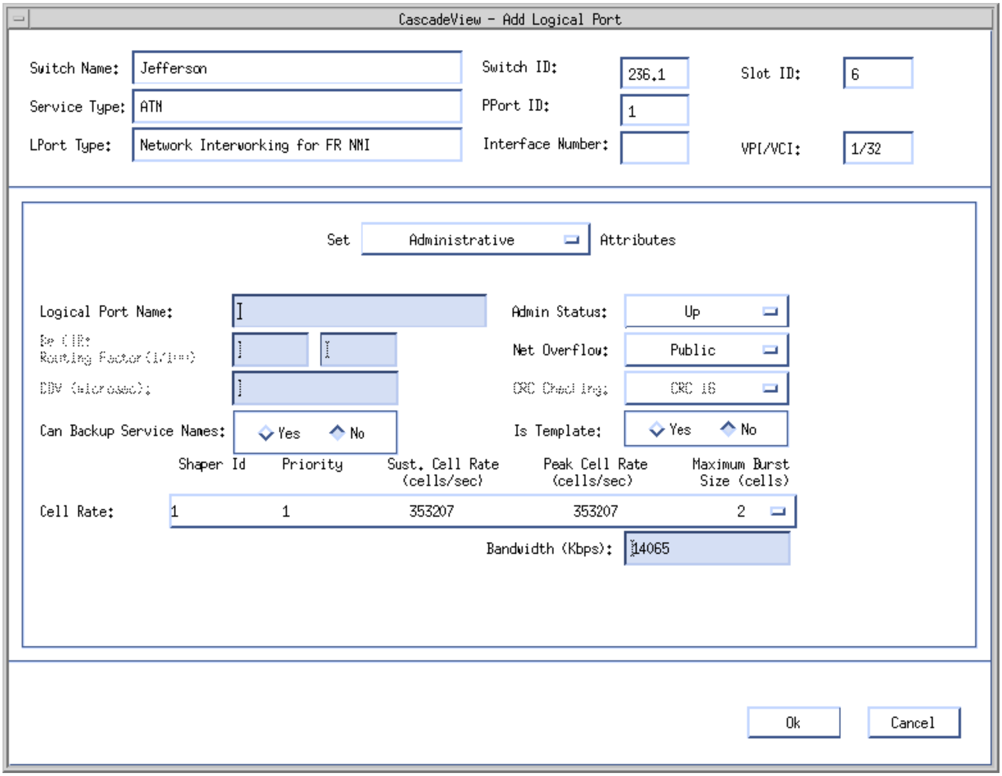


Figure 9-11. Set Administrative Attributes Dialog Box (ATM CS/IWU)

Administrative Attributes

Complete the required fields described in Table 9-16. Attributes vary depending on the type of module and logical port.

Table 9-16. ATM FR NNI Administrative Attributes

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Admin Status	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. *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
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 "Configuring Fault-Tolerant PVCs" on page 7-44.
Is Template	(*Optional*) Save these settings as a template to use again to quickly configure a logical port with the same options. To create a template, choose Yes in the *Is Template* field. Refer to "Administrative Tasks" on page 9-59 for more information.
Shaper ID	*(ATM CS/IWU modules only)* Choose a value from 1 through 16 to specify the Shaper ID and associated priority, sustainable cell rate, peak cell rate, and burst tolerance values.

Table 9-16. ATM FR NNI Administrative Attributes (Continued)

Field	Action/Description
Peak Cell Rate (cells/sec)	*(ATM UNI DS3 modules only)* Select a PCR between 0 and 7. 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.
Sustainable Cell Rate (cells/sec)	*(ATM UNI DS3 modules only)* Specify the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. The SCR 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 traffic.
Maximum Burst Size (cells)	*(ATM UNI DS3 modules only)* Specify the maximum number of cells that can be received at the Peak Cell Rate. MBS 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.
Bandwidth (kbps)	Enter the amount of bandwidth you want to configure for this logical port. 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 for the OPTimum trunk you are currently configuring. Remember to leave bandwidth for any remaining OPTimum trunks you need to configure on this logical port.

Link Management Attributes

1. Set the link management attributes by selecting *Link Mgmt* from the Set Attributes option menu.

   The Add Logical Port dialog box appears displaying the link management attributes and fields shown in Figure 9-12.

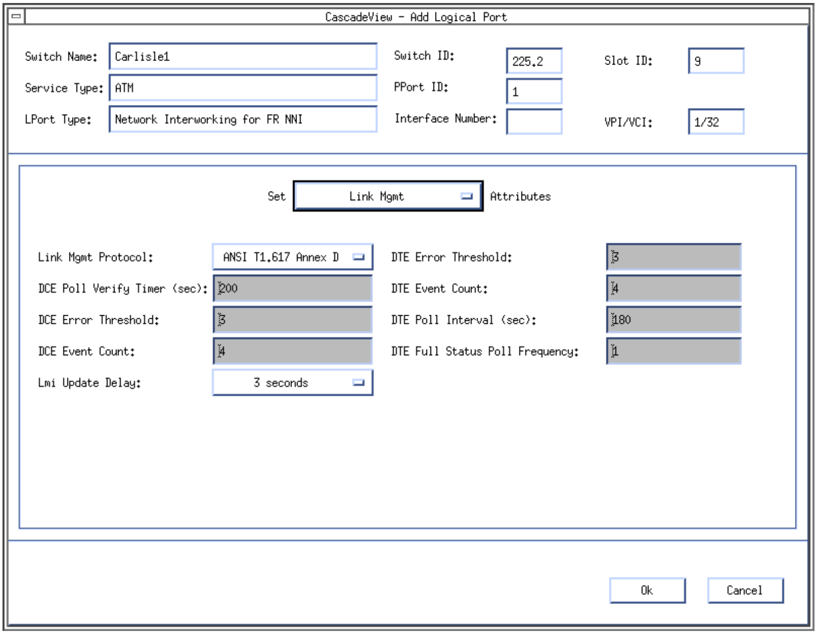


Figure 9-12. Link Management Attributes Dialog Box

2. Complete the required fields described in Table 9-17.

Table 9-17. ATM FR NNI Link Management Attributes

Field	Action/Description
Link Mgmt Protocol	Select the link management protocol used by the Frame Relay equipment connected to this port. Options include: *ANSI T1.617 Annex D (default)* – The network uses DLCI 0 for link management. *LMI Rev1* – The network uses DLCI 1023 for link management. *CCITT Q.933 Annex A* – For international standard (European) use only. The network uses DLCI 0 for link management. *Auto Detect* – Use this option only if the attached customer premise equipment (CPE) provides the link management protocol. This logical port can then automatically detect which protocol is in use. *Disabled* – Use this option only if the attached CPE does not support link management or to disable link management for troubleshooting.
DCE Poll Verify Timer (Sec)	Specify the value of the T392 timer, which sets the length of time the network should wait between status enquiry messages. If the network does not receive a status enquiry message within the number of seconds you specify, the network records an error. The default value is 200 seconds. Increase this value if the DTE device has a poll frequency that is greater than or equal to the DCE Poll Verify Timer. Decrease this value if the DTE's poll frequency is less than or equal to 1/2 of the DCE poll verify timer.

Table 9-17. ATM FR NNI Link Management Attributes (Continued)

Field	Action/Description
DCE Error Threshold	Specify the DCE error threshold. This parameter is used with the DCE Events Count (N393) parameter. The Local Management protocol monitors the number of events you specify for the DCE Event Count. If the number of events found in error exceeds the DCE Error Threshold you specify, the link is declared inactive. The default value is three.
DCE Event Count	Specify the DCE event count. This field specifies the number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or invalid status enquiry message or expiration of the T392 timer. For example, use the default DCE Error Threshold value of three and the default DCE Event Count value of four. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.
LMI Update Delay	Set a timer from 1 to 9 seconds to enable asynchronous LMI updates. The default is three (3) seconds. When you set this timer, the switch sends a signal (known as an *event*) to notify other network equipment (CPE) when a circuit on this logical port goes up or down. The specified time interval creates a buffer. If the circuit recovers within this period of time, no event is issued. If you choose *No Updates*, the switch does not send a signal to the CPE. If you choose *No Delay*, the switch sends an update immediately to the CPE. For example, if the network takes a significant amount of time to recover from trunk outages, increase the LMI update delay. This delay minimizes network downtime visibility to end-users.

Table 9-17. ATM FR NNI Link Management Attributes (Continued)

Field	Action/Description
DTE Error Threshold	Specify an error threshold.This parameter is used with the DCE (DTE) Events Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DCE (DTE) Event Count. If the number of events found in error exceeds the specified DCE (DTE) Error Threshold, the link is declared inactive. The default value is three (3).
DTE Event Count	Specify the number of events in a sliding window of events monitored by the network. The default is four. An event is the receipt of a valid or invalid status inquiry message or expiration of the T392 timer. For example, use the default DCE (DTE) Error Threshold value of 3 and the default DCE (DTE) Event Count value of 4. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events. ***Note***: *The DCE (DTE) Error Threshold and the DCE (DTE) Event Count work together. The lower you set these values, the more sensitive the logical port is to LMI poll errors. To make the logical port less sensitive to errors, increase these values.*
DTE Poll Interval (sec)	Specify the number of seconds between the transmission of status enquiry messages. Set the DTE poll interval to a value that is less than the DCE poll verify timer on the attached device. (This value must be greater than 1/2 the value of the DCE poll verify timer.) The default is 180 seconds for one-to-one mapping.
DTE Full Status Poll Frequency	Specify the number of T391 polling cycles between full status enquiry messages. Reduce this value to absorb more bandwidth, since the more frequent full status requests increase overhead. The default value is one for one-to-one mapping.

3. Complete the congestion-control attributes fields described in Table 9-10 on page 9-24.

4. Complete the trap-control attributes fields described in Table 9-13 on page 9-32.

5. Choose OK. The Set All Logical Ports in PPort dialog box reappears.

6. Choose Close to return to the Set Physical Port Attributes dialog box.

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

8. To configure logical ports on another physical port, select the port, then choose Set Attr. Refer to the appropriate section for instructions as described in Table 9-7 on page 9-16.

   After you configure both logical-port endpoints for a trunk, you can add the trunk-line connection. Refer to Chapter 10, “Configuring Trunks”.

Defining ATM OPTimum Frame Trunk Logical Ports

An ATM Open Packet Trunking (OPTimum) logical port enables you to use public ATM networks as trunk lines between two Cascade switches. You can configure an ATM OPTimum trunk logical port to:

- Connect to a peer Cascade switch over an ATM PVC.

- Connect to a peer Cascade switch over an ATM PVC, using an ATM DSU.

You can multiplex Frame Relay PVCs and SMDS “connections” over the ATM PVC.

Using ATM OPTimum Frame Trunks

You can configure an ATM OPTimum trunk to create a switch-to-switch Cascade trunk through a public data network (PDN) into another Cascade network. The Cascade OPTimum trunk allows private enterprises to purchase lower-cost public-carrier services as the trunk between two Cascade switches, rather than use a more expensive leased-line service.

To implement the OPTimum trunk, first configure a UNI-DTE feeder logical port on the same physical port. To configure an OPTimum trunk, use the following sequence:

Step 1. Configure the physical port you want to use for the OPTimum trunk (refer to "Configuring Physical Ports" on page 6-9).

Step 2. Configure a UNI-DTE feeder logical port (page 9-18) for the OPTimum trunk on this physical port.

Assign this logical port a minimum amount of bandwidth.

Step 3. Configure the OPTimum trunk logical port on the same physical port. Assign the remaining bandwidth to this logical port.

To configure an ATM OPTimum Frame trunk logical port:

1. Complete the Add Logical Port Type dialog box fields as follows:

   Service Type — Select ATM. The available ATM Logical Port Types appear.

   LPort Type — Select ATM OPTimum Frame Trunk.

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

   Virtual Path ID — Enter a number from 1-*nnnn* to identify the virtual path for the ATM logical port. 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. For more information, refer to Table 9-3 on page 9-8.

   VCI —Enter the number of valid bits in the Virtual Channel Identifier. If this logical port is on an ATM-based I/O module (ATM DS3/E3, ATM IWU/CS modules), enter a value from 32 to 255. Enter a number that matches the VCI value of the equipment connected to this port. You may have received this value from the ATM network provider. You can use the following range of values depending on the I/O module you are configuring:

   Refer to "Setting the Number of Valid Bits in the VPI/VCI" on page 9-7 for for information.

> *Virtual Path ID 0 is reserved and cannot be used.*
>
> *You must provision a VPC in another ATM network between two Cascade switches. This VPC acts like a physical line. Specify the VPI of this VPC in the Virtual Path ID field.*

2. Choose OK. The system displays the Add Logical Port dialog box and displays the Set Attributes option menu and fields shown in Figure 9-13.

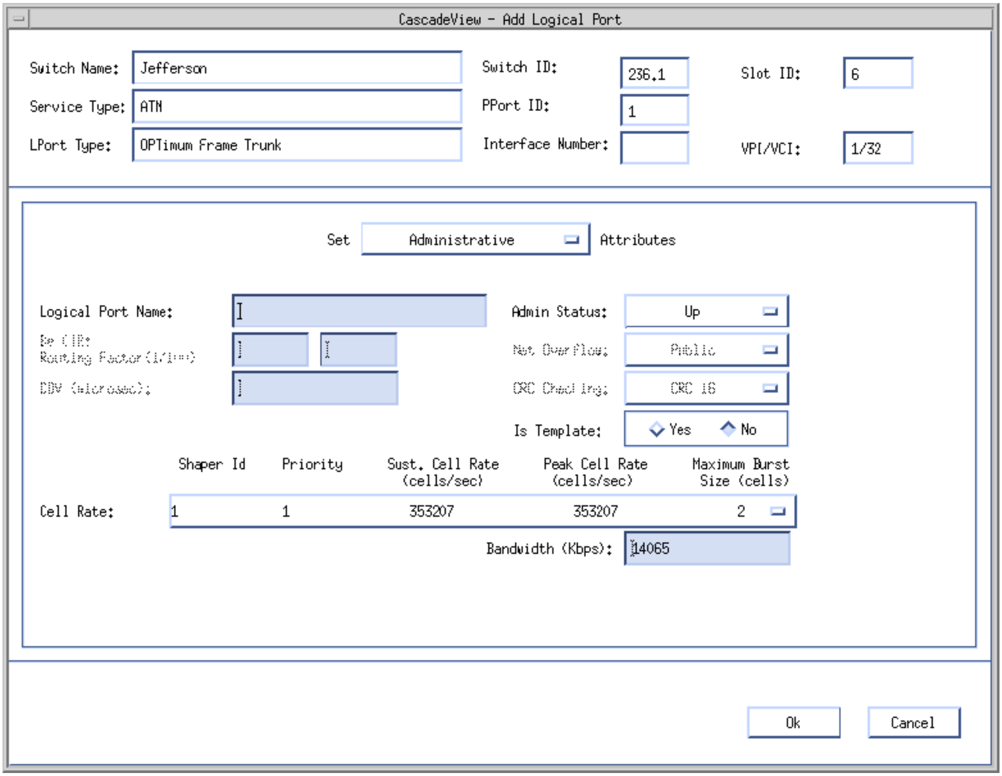


Figure 9-13. Set Administrative Attributes Dialog Box (OPTimum Frame)

3. Complete the administrative attributes fields described in Table 9-16 on page 9-44.
4. Complete the trap control attributes fields described in Table 9-13 on page 9-32.
5. Choose OK. The Set All Logical Ports in PPort dialog box reappears.
6. Choose Cancel to return to the Set Physical Port Attributes dialog box.
7. Choose Close to return to the Switch Back Panel dialog box.

8. To configure logical ports on another physical port, select the port, then choose Set Attr. Refer to the appropriate section (described in Table 9-7 on page 9-16) for instructions.

   After you configure both logical-port endpoints for a trunk, you can create a trunk and add the trunk-line connection. Refer to Chapter 10, “Configuring Trunks”.

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 bandwidth of a port 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 VC. 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 considered to occupy zero bandwidth, since it is a “Best Effort” service.

> *Appendix C 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.*

PVC routing is determined by either an OSPF algorithm or the network administrator (if you manually define the circuit path). Each time a PVC attempts to come up after configuration, OSPF reserves the required bandwidth on the port. It 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 more circuits can be configured 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 may even be dropped.

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

Setting Quality of Service Parameters

The *Set QoS Parameters* option enables you to set the Quality of Service (QoS) parameters for a logical port. You can use the default values listed in Table 9-18, or modify these settings. (You cannot modify the over-subscription Factor for CBR service.)

Table 9-18 briefly describes each class of service.

Table 9-18. QoS Class of Service Descriptions

Field	Description
Constant Bit Rate (CBR)	Handles digital information, such as video and digitized voice requires a continuous stream of bits. CBR traffic requires guaranteed throughput rates and service levels.
Variable Bit Rate (VBR) Real Time	Used for packaging special delay-sensitive applications, such as packet video, which 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.
Unspecified Bit Rate (UBR)	Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic.

Table 9-19 describes the default Quality of Service values for ATM UNI logical ports.

Table 9-19. 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 set the Quality of Service (QoS) Parameters:

1. From the Add Logical Port dialog box, choose Set QoS Parameters. The Set Logical Port QoS Parameters dialog box appears as shown in Figure 9-14.

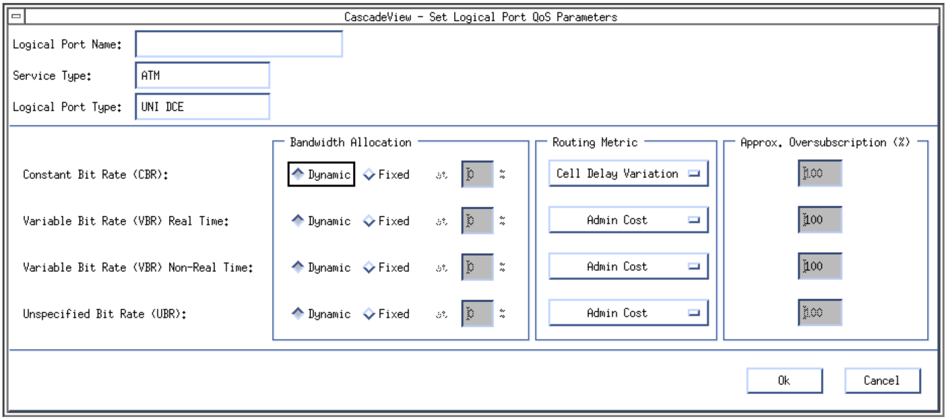


Figure 9-14. Set Logical Port QoS Parameters Dialog Box

2. Configure the *Bandwidth Allocation* fields for each service class. Options include:

   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 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.*

3. In the Routing Metric field, select one of the following *Routing Metrics* for each class of service. Routing metrics apply only if the port is configured as UNI DCE or UNI DTE logical port. Options include:

   Cell Delay Variation (CDV) — This routing metric measures the average variation in delay between one cell and the next, expressed in fractions of a second. When emulating a circuit, CDV measurements allow the network to determine if cells are arriving too fast or too slow.

   End-to-End Delay — This routing metric measures the static delay of the logical port, which consists of both propagation and transmission delay. It is measured when the port initially comes up. It does not include queuing delays, and therefore does not account for port congestion.

   Admin Cost — This parameter measures the Administrative Cost associated with the logical port.

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

   In general, you can leave these values set to 100%, since Cascade's Call Master Connection Admission Control (CAC) algorithm ensures that you can pack circuits on a port without losing data or quality of service. If, however, after monitoring your network, you determine that 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.

Administrative Tasks

This section describes how to:

- Use Templates to define a new logical port
- Delete circuits
- Delete trunks
- Delete ATM logical ports

Using Templates

If you defined a logical port configuration and saved it as a template (see *Is Template* field in Table 9-9 on page 9-20), you can define a new logical port using the same parameters.

To define a logical port from a template:

1. Choose the *Add Using Template* command on the Set All Logical Ports in PPort dialog box (see Figure 9-4 on page 9-19).
2. Do one of the following:
   - Choose *Last Template* to use the last template you defined for this switch.
   - Choose *Template List* to display a list of templates defined for this map. Select a template and choose OK.

Deleting ATM Logical Ports

Before you can delete an ATM logical port, verify the following:

Step 1. An ATM DTE logical port is not defined as part of a circuit. If it is, you must first delete this circuit.

Step 2. There are no trunks defined on this logical port.

Step 3. This logical port is not defined as the feeder (ATM UNI DTE or ATM Transport for Frame Relay NNI) for an existing ATM OPTimum trunk logical port.

If any of these components exist and use the logical port you want to delete, you must first delete them in the following order:

- Circuits
- Trunks
- Logical port

Deleting Circuits

To delete a circuit:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits. The Set All Circuits On Map dialog box appears.
2. To view the list of circuits, select the *Search by Name* field and press Return. If necessary, select each circuit and review each logical port endpoint.
3. Select the circuit to delete.
4. Choose Delete.
5. Choose Close to return to the network map.

Deleting Trunks

To delete a trunk:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears. If necessary, select each trunk and review each logical port endpoint.
2. Select the trunk to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting the Logical Port

To delete the logical port:

1. Select the switch from which to delete a logical port.
2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the physical port. The Set Physical Port Attributes dialog box appears.
4. Choose the Logical Port command. The Set All Logical Ports in PPort dialog box appears.
5. Select the logical port to delete. Make sure the Loopback field displays NONE.

> *Make sure this logical port is not the UNI DTE or ATM NI for Frame Relay NNI logical port used as the feeder for an ATM OPTimum trunk. You must first take the OPTimum trunk out of service or first define another feeder before you can delete this logical port.*

6. Choose Delete.
7. Choose Close.

10

Configuring Trunks

A Cascade trunk is the communications circuit between two switches. The trunk provides the means for two Cascade switches to pass data to each other and exchange internal control messages.

About Trunks

The *Trunk Over-subscription Factor* and the *OSPF Trunk Administrative Cost* parameters enable you to better manage trunk traffic. The over-subscription factor enables you to configure more circuits to a trunk than can be supported at one time *(over-subscribe)*. Over-subscription assumes that due to the bursty nature of network traffic, not all circuits on the trunk are operating at the committed information rate (CIR) at the same time. Therefore, trunk bandwidth should remain sufficient.

The trunk administrative cost enables you to assign a cost value for the trunk. When multiple trunks are available, a circuit will use the trunk with the lowest administrative cost.

Trunk Over-subscription Factor

The trunk over-subscription factor percentage enables you to optimize the aggregate committed information rate (CIR) allowed over the trunk. The over-subscription factor represents the V value for this trunk. The bandwidth on trunks is reserved at runtime based on the CIR value of the PVCs that traverse that trunk.

The routing for PVCs is either determined by an OSPF algorithm, or by the network administrator if you manually define the circuit path. Each time a PVC attempts to come up, OSPF reserves bandwidth equal to the CIR of the PVC on the trunk with the shortest path. The amount of reserved bandwidth is deducted from the available virtual bandwidth pool. The formula used to determine virtual bandwidth is only used for allocating the *initial* path for the PVC. The system periodically reviews each PVC to optimize network resources according to reroute tuning parameters (refer to Chapter 5, "Managing a Cascade Switch").

OSPF uses the following two formulas to determine the available virtual bandwidth value:

Formula 1

This formula determines the initial value of the available virtual bandwidth:

Initial Value = 0.95 (configured bandwidth) x V(%)

Note: V = trunk oversubscription factor

Formula 2

Available Virtual Bandwidth = Initial Value – (Sum of PVC CIR)

It is important to note that the available virtual bandwidth can become negative in extreme situations. 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.

If you configure the trunk over-subsrciption factor at a higher percentage, you increase the available virtual bandwidth (more PVC CIR) over the trunk. An over-subscription value of 200% effectively doubles the available virtual bandwidth. Cascade reserves 5% bandwidth for network management, routing updates, and other management traffic.

If all network traffic attempts to use the network resources at the same time, for example, during multiple file-transfer sessions over the same trunk, the overhead will degrade network performance.

OSPF Trunk Administrative Cost

OSPF trunk administrative cost is a function of OSPF that gives you more control over the specific path a virtual circuit will take through the network. Through OSPF, a circuit can choose the shorter hop path (most direct route across network), regardless of the available bandwidth.

> *OSPF trunk administrative cost only works in networks where all switches are running Release 4.1 or higher, switch software. If some switches are running an earlier release, OSPF only selects the path with the greatest amount of available bandwidth. This is not necessarily the most direct route (minimum hop) through the network.*

When you first define a circuit, the circuit looks for a path that has enough virtual bandwidth available to handle its committed information rate (CIR). If the circuit finds more than one path with the available bandwidth, the circuit chooses the path with the lowest administrative cost. If there is more than one path with the same administrative cost, the circuit chooses the path that has the largest available bandwidth.

Circuits are automatically rerouted around a trunk or switch failure. If the circuit cannot find a path with sufficient bandwidth, it chooses the path with the lowest administrative cost, even if this trunk has a negative bandwidth value. (The negative bandwidth indicates that the trunk is over-subscribed). The use of a path with a negative bandwidth only occurs at the time of a trunk failure.

Configuring Minimum Hop Paths

If you use the default administrative cost value of 100, OSPF selects minimum-hop paths that respect the circuit's Quality of Services values. You can also use the following guidelines to configure this value:

- To minimize end-to-end delay, configure an administrative cost that is proportional to the propagation delay of the trunk. Set the cost of each trunk to the length of the trunk's physical media (in miles or kilometers).
- Set the administrative cost relative to the speed of the physical port. For example, a single T1 trunk hop may be equal to four HSSI trunk hops. You would set the HSSI trunk's cost to 25 and the T1 cost to 100. Keep in mind that since OSPF routing considers available bandwidth, administrative cost is not necessarily a function of bandwidth.

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 10-1 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.

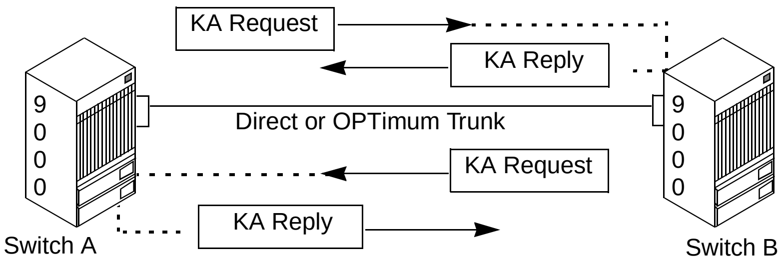


Figure 10-1. Trunk Delay - OSPF Metric and Keep-Alive Messaging

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.

Trunk Backup

The Cascade B-STDX 8000/9000 switch supports a trunk backup option. Trunk backup enables you to setup one or more backup trunks to replace a primary trunk. If a Cascade switch trunk line fails or requires maintenance, you can reroute PVCs from the primary trunk to the backup trunk. You can define primary and backup trunks on any I/O module.

You define a normal, primary or backup trunk in the Add Trunk dialog box (see Figure 10-4 on page 10-15). A backup trunk can have a total bandwidth that is less than that of the primary trunk. To avoid congestion, you can configure multiple backup trunks to backup a single primary trunk. The Cascade switch allows you to define up to eight backup trunks for a single primary trunk.

Once you configure the primary and backup trunk(s), you can configure the primary trunk to automatically back up upon failure. If a trunk line requires maintenance, you can manually initiate and terminate a trunk backup.

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 add a trunk, you can dedicate trunks to specific customers and, if desired, allow customers to monitor their own networks. However, control and configuration of the switches stays with you as the network provider.

A VPN provides a dedicated bandwidth to the network customer, however the management of the network is done by the provider. You create a VPN when you first configure a new switch (Chapter 4.)

Private Net Overflow

The *private net overflow* parameters determine whether circuits originating from a logical port will be restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. You configure the private net overflow parameters when you add a trunk (see Table 10-3 on page 10-16).You can set the private net overflow parameters to two modes:

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

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

Before You Begin

Before you define the trunk connections, verify the following tasks are complete:

- ☑ Create a network map with at least two Cascade switches (Chapter 4)
- ☑ Configure the switch (Chapter 5)
- ☑ Configure the I/O module(s) and physical ports (Chapter 6)
- ☑ Configure the trunk logical port(s) (Chapter 7, Chapter 8, and Chapter 9)

Trunk Definition

Trunk definition is a three-step process:

Step 1. Configure a trunk logical port type. Refer to one of the following sections:

"Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 7-39

"Defining Other Types of Frame Relay Logical Ports" on page 7-41 (Describes Direct Line Trunks)

"Defining SMDS OPTimum Trunk Logical Ports" on page 8-39

"Defining ATM OPTimum Frame Trunk Logical Ports" on page 9-51

Step 2. Define a trunk configuration between the two switches. Refer to "Adding a Trunk" on page 10-13.

Step 3. Create the map line connection that corresponds to the trunk configuration. Refer to "Creating a Trunk-Line Connection" on page 10-20.

Configuring a Trunk for a VPN

Use the following steps to configure a trunk for a VPN:

Step 1. Create the VPN (refer to page 4-22).

Step 2. Add customers to a specific VPN (refer to page 4-23).

Step 3. Create the UNI logical port and specify the net overflow parameters (refer to page 7-21).

Step 4. Dedicate the PVC logical port endpoints to a specific VPN and customer (refer to page 7-43).

Step 5. Specify the trunk parameters (refer to Table 10-3 on page 10-16).

Accessing the Trunk Functions

The Set All Trunks function specifies the two endpoints for a Cascade-to-Cascade switch trunk. When you configure a trunk, you select endpoints that use the same type of logical port (such as Direct Line Trunk) and the same bandwidth.

To access the trunk functions:

From the Administer menu, select Cascade Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears as shown in Figure 10-2.

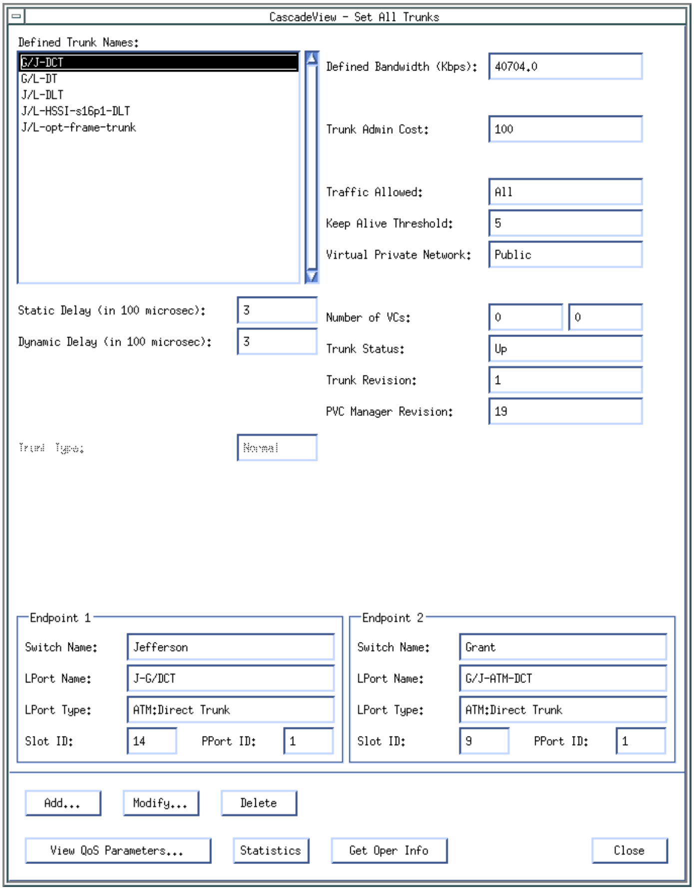


Figure 10-2. Set All Trunks Dialog Box

The Set All Trunks Dialog Box

The Set All Trunks dialog box shown in Figure 10-2 displays information about the trunk you select from the Defined Trunk Names list. It also provides several command buttons that enable you to access additional trunk functions.

Table 10-1 describes the Set All Trunks dialog box fields and command buttons.

Table 10-1. Set All Trunks Fields and Command Buttons

Field/Command Button	Description
Defined Trunk Names	Displays the names of the configured trunks.
Defined Bandwidth (Kbps)	Displays the amount of bandwidth, in Kbps, for the selected trunk.
Subscription Factor (%)	Displays the percentage used to calculate the available virtual bandwidth for the selected trunk.
Trunk Admin Cost	Displays the cost of using this trunk for a virtual circuit when a virtual circuit is dynamically created on the switch.
Virtual Bandwidth (Kbps)	Displays the amount of virtual bandwidth in Kbps. The value*.95* is used because*.05%* of the bandwidth is reserved for network management, routing updates, and other management traffic.
Allowed Traffic	Displays the type of management traffic allowed on this trunk.
Keep Alive Threshold	Displays the number of seconds that the trunk protocol will exchange keep alive (KA) control frames without getting a response from the remote node. ***Note****: Service is disrupted if you change this value after the trunk is online.*

Table 10-1. Set All Trunks Fields and Command Buttons (Continued)

Field/Command Button	Description
Virtual Private Network	Displays the virtual private network name.
Private Net Overflow	Displays *Public* if the customer is allowed to use a public trunk in the event of traffic overflow or trunk failure. Displays *Restrict* if the customer is restricted to only other private trunks during overflow or trunk failure.
Avail Virtual BW (Kbps)	Displays the amount of bandwidth, in Kbps, available for circuit configuration and allotment on the selected trunk.
Number of VCs	Displays the number of virtual channels.
Trunk Status	Displays the current status of the selected trunk. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information on trunk status values.
Trunk Revision	Displays the trunk revision.
PVC Manager Revision	Displays the PVC manager software revision.
Trunk Type	Displays the trunk type. *Normal* – Indicates a common trunk. *Primary* – Indicates that the trunk has a backup for fault tolerance. *Backup* – Indicates that it is the backup trunk (when failure occurs on the primary trunk).
Modify/Delete	If you have already configured some trunk-line connections, the dialog box displays the names. The *Modify* or *Delete* commands enable you to modify or delete trunk configurations.

Table 10-1. Set All Trunks Fields and Command Buttons (Continued)

Field/Command Button	Description
Get Oper Info	Displays a brief status for the selected trunk connection and a status message appears in the Oper Status field.
View QoS Parameters	*(ATM Direct Cell Trunks only)* Displays the Show Logical Port QoS Parameters window.
Statistics	Displays the summary statistics for the selected trunk configuration. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

Adding a Trunk

Complete the following steps to add a trunk.

1. Access the Set All Trunks dialog box shown in Figure 10-2. See “Accessing the Trunk Functions” on page 10-9 if you’re not sure how to do this.

2. Choose Add. The Select Logical Ports dialog box appears as shown in Figure 10-3.

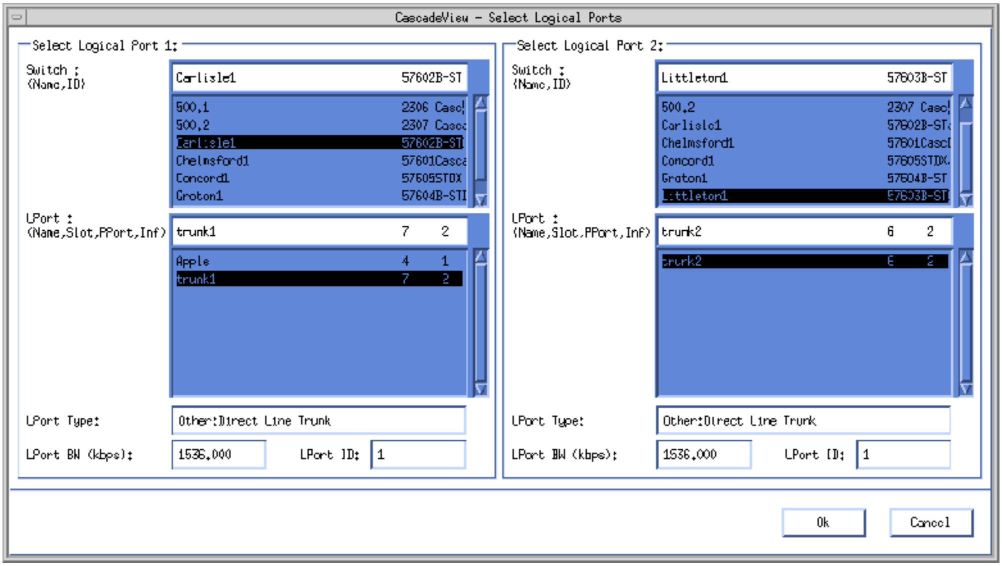


Figure 10-3. Select Logical Ports Dialog Box

3. From the Select Logical Port window, select the switch and Lport for logical port 1 and logical port 2. Table 10-2 describes each of the Select Logical Ports fields.

Table 10-2. Select Logical Ports Fields

Field	Action/Description
Switch (Name, ID)	Select a switch for each endpoint. The dialog box displays the parameters for the selected switch.
LPort (Name, Slot, PPort, Inf)	Select the same trunk logical port type for each endpoint. Choose from the following logical port types depending on the type of logical port service: • Frame Relay OPTimum Trunk • Other:Direct Line Trunk • SMDS OPTimum Trunk • ATM: Direct Trunk • ATM OPTimum Frame Trunk • ATM OPTimum Cell Trunk This field also displays the ifnum, physical port number, I/O slot (number) in which the module resides. ***Note****: Review the LPort Bandwidth field for each endpoint to make sure the bandwidth is identical.*
LPort Type	Displays the configured logical port type.
LPort BW (kbps)	Displays the bandwidth configured for the logical port. This must be the same for both endpoints.
LPort ID	Displays the logical port number.

4. Choose OK. The Add Trunk dialog box appears, displaying the parameters for both switches in the trunk configuration.

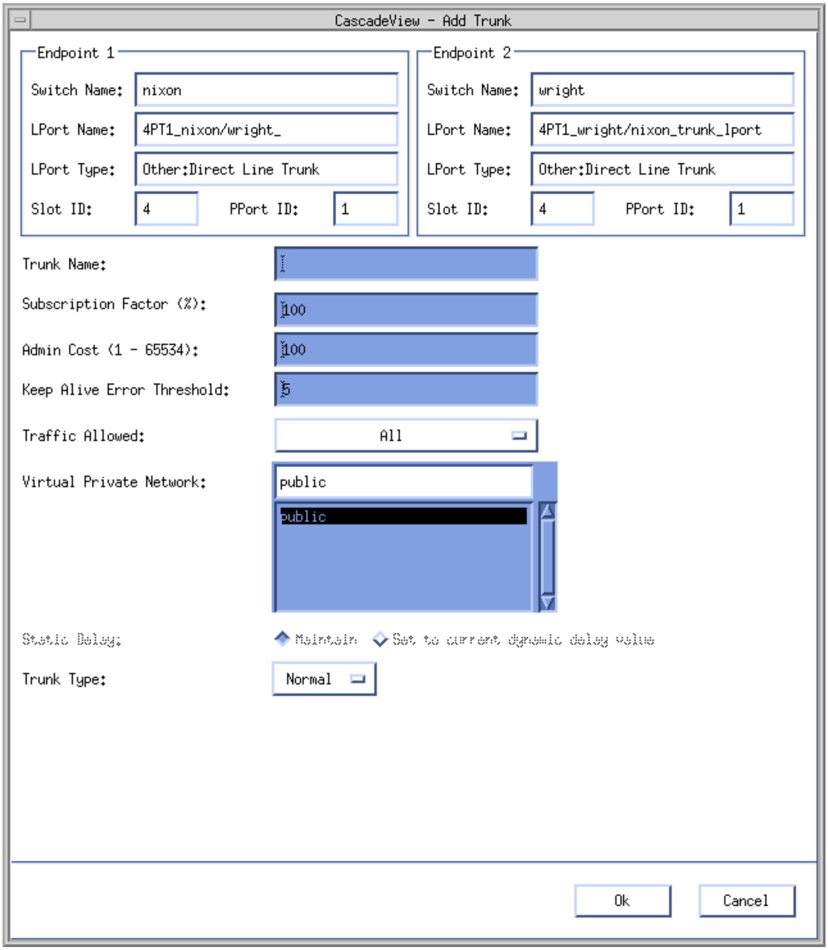


Figure 10-4. Add Trunk Dialog Box

5. Complete the Add Trunk fields described in Table 10-3.

Table 10-3. Add Trunk Fields

Field	Action/Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk. You use this same name when you create the trunk connection (refer to page 10-20).
Subscription Factor (%)	The trunk over-subscription factor percentage enables you to optimize the aggregate CIR you can configure on the trunk, by allowing you to over-subscribe the trunk. The over-subscription factor represents the V value for this trunk. The bandwidth on a trunk is reserved at runtime, based on the configured CIR value of the PVCs that traverse that trunk. For example, you can set this factor to 200% to produce a virtual bandwidth that is two times greater than the defined bandwidth. For a detailed explanation of this parameter, refer to page 10-2. ***Note***: *You can not over-subscribe an ATM Direct Trunk.*

Table 10-3. Add Trunk Fields (Continued)

Field	Action/Description
Admin Cost (1-65534)	Assign an admin cost value of 1 to 65534. The lower the admin cost of the path, the more likely OSPF will select it for circuit traffic. *The default admin cost value is 100.* For a detailed explanation of this parameter, refer to page 10-3. ***Note**: When you increase or decrease the administrative cost of a trunk, the reroute tuning parameters control the rate at which the switch adds or removes circuits from the trunk. Refer to page 5-24 for information about reroute tuning. You cannot use trunk admin cost to force a trunk down.*
Keep Alive Threshold (%)	Configure the keep-alive threshold for a value between 3 and 255 seconds. *The default is 5 seconds*. For a detailed explanation of this parameter, refer to page 10-5. ***Note**: If you are running different switch code versions in your network, for example Version 4.1 and Version 4.2, you must accept the default value of 5 seconds.* ***Note**: Service is disrupted if you change this value after the trunk is online.*

Table 10-3. Add Trunk Fields (Continued)

Field	Action/Description
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – The trunk can carry network management traffic, user traffic, and OSPF address distribution. *Mgt Only* – The trunk can carry *only* network management traffic, such as SNMP communication between a switch and the NMS. *Mgt & User* – The trunk can carry network management traffic and user traffic. ***Note**: To calculate the most efficient route for network management traffic, OSPF uses Trunk Admin Cost. OSPF ignores trunk bandwidth when it selects the best path or a route for management traffic. Management traffic can use a negative bandwidth trunk.*
Virtual Private Network	Select a Virtual Private Network. The default is *Public*.
Static Delay	Defaults to maintain.

Table 10-3. Add Trunk Fields (Continued)

Field	Action/Description
Trunk Type	Select *Normal*, *Primary,* or *Backup*. • Normal is a common trunk. • Primary indicates that the trunk has a backup for fault tolerance. • Backup indicates that it is a backup trunk (when failure occurs on the primary trunk). If you select Backup, complete Step 7. ***Note****: This parameter is not supported on trunks between CBX 500 and B-STDX 9000 switches.* *If you are configuring an ATM Direct Trunk, set this parameter to Normal.*

6. (*Optional*) If you selected *Primary* as the Trunk Type, complete the parameters that appear on the Add Trunk dialog box or accept the default parameters.
7. (*Optional*) If you selected *Backup* as the Trunk Type, complete the additional parameters that appear on the Add Trunk dialog box:

   Primary Trunk of the backup — Select the name of the trunk to back up this configuration.

   Switch Initializing the Call Setup — Select the name of the switch initializing the call setup.
8. When you complete the add trunk dialog box fields, choose OK.
9. Choose Close to return to the network map.

   The next step is to create a trunk-line connection. Proceed to the next section, “Creating a Trunk-Line Connection”.

Creating a Trunk-Line Connection

You must define the trunk configuration between two switches before you create the trunk-line connection on the network map (refer to page 10-13). 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 Add Connection dialog box appears as shown in Figure 10-5.

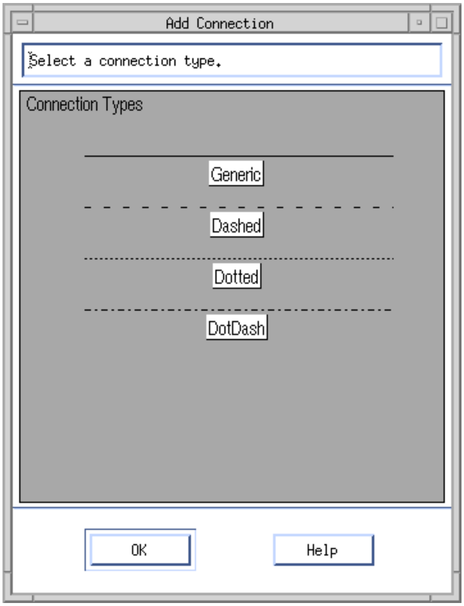


Figure 10-5. Add Connection Dialog Box

2. Select a Connection Type from the palette.

3. To create a trunk-line connection between the two Cascade switches on the network map, click on the first switch object (source symbol) and then the second switch object (destination symbol).

4. The Add Object dialog box appears as shown in Figure 10-6.

Figure 10-6. Add Object Dialog Box

5. Complete the fields described in Table 10-4.

Table 10-4. Add Object Fields

Field	Action/Description
Symbol Type	Displays the type of connection you are adding to the map.
Label	Enter the trunk name you specified on the Add Trunk dialog box (page 10-15).

Table 10-4. Add Object Fields (Continued)

Field	Action/Description
Display Label	Select *Yes* to have the label name appear beneath the trunk line object on the network map. Select *No* if you do not want the label name displayed.
Behavior	Select *Explode* to create the basic CascadeView/UX 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 Add Object – Set Attributes dialog box appears as shown in Figure 10-7.

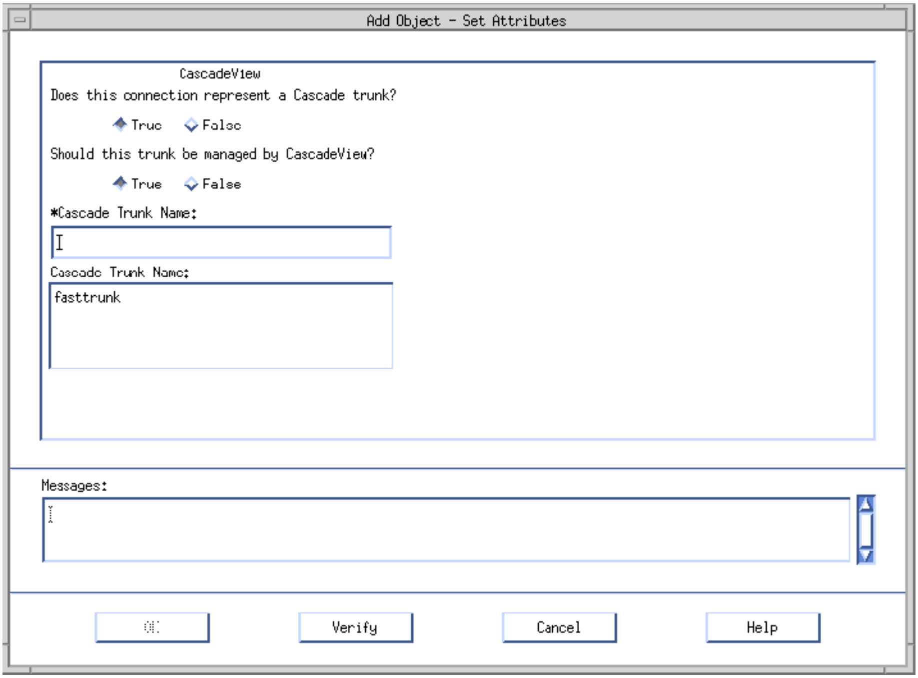


Figure 10-7. Add Object - Set Attributes Dialog Box

6. Complete the required dialog box fields described in Table 10-5.

Table 10-5. Add Object - Set Attributes Fields

Field	Action/Description
Does this connection represent a Cascade Trunk?	Select *True*.
Should this trunk be managed by CascadeView?	Select *True*.
Cascade Trunk Name	Enter the name you assigned to the trunk. This should be the same name you entered for the label in the Add Object dialog box on page 10-21.

7. Choose Verify to confirm your selections.

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

9. Choose OK to return to the network map. The trunk line appears between the two switches on the network map.

Displaying Multiple Trunks Between Switches

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

To display all trunk connections between two switches:

1. Double-click the left mouse button on the solid line between the switches.

   A trunk submap window appears as shown in Figure 10-8.

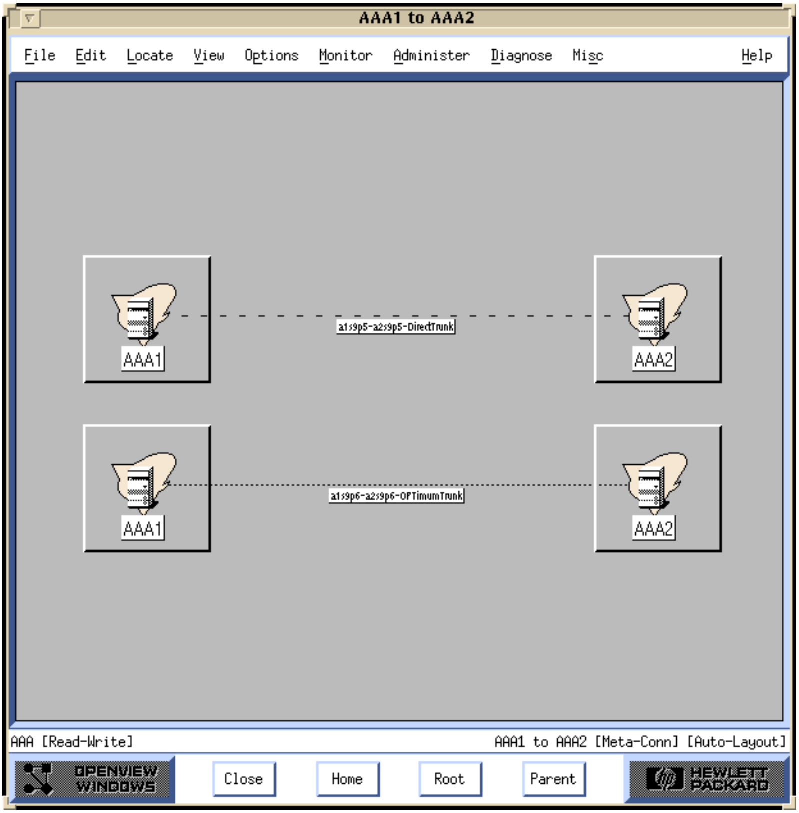


Figure 10-8. Displaying Multiple Trunks-Trunk Submap Dialog Box

2. Choose Close to return to the network map.

Trunk Coloring

All associated trunks are polled for status according to the trunk poll timer. The trunk lines on the network map change color. These colors indicate trunk status according to the polled status and the traps received by the Cascade Event Log. Table 10-6 documents the color scheme that identifies the status of a trunk connection on the network map.

Table 10-6. Trunk Color Status Indicators

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

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

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

$ export XUSERFILESEARCHPATH

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

If you define more than one trunk connection between the same two switches, HP OpenView combines the status to display an orange, yellow, or cyan trunk-line. To display a view of the individual connections, double-click on the trunk line and refer to Table 10-6 to interpret trunk-color status.

When you finish defining your trunk configuration(s) and trunk line connection(s), proceed to Chapter 11, “Configuring Circuits”, to complete the network configuration.

11

Configuring Circuits

Once you configure the switches, physical ports, logical ports, and trunks, you can define the *Permanent Virtual Circuits (PVCs)*. A circuit or PVC defines an end-to-end connection between two logical ports within the Cascade network. The Set All Circuits function enables you to add, modify, or delete circuit configurations.

This chapter describes how to configure circuits for the following types of connection services:

Frame Relay-to-ATM Service Interworking — This service uses a circuit with a Frame Relay logical port at one endpoint and an ATM logical port at the other endpoint. The circuit uses a 10-bit address called a *Data Link Connection Identifier* (DLCI). DLCIs identify the logical endpoints of a virtual circuit and have local significance only.

ATM Data Exchange Interface/Frame User-to-Network Interface (DXI/FUNI) — This service uses a circuit with an ATM logical port defined on a frame-based I/O module, such as the 8-port Universal I/O module. The circuit is identified by a 4-bit *virtual path identifier* (VPI) and a 6-bit *virtual channel identifier* (VCI). Circuits on the ATM DS3/E3 module use an 8-bit VCI.

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

A *virtual channel* (VC) is a connection between two communicating ATM devices. A VC may consist of a group of several ATM links, customer premise equipment (CPE) to central-office switch, switch-to-switch, and switch-to-user equipment.

A *virtual path* (VP) is a group of virtual channels carried between two points. VPs provide a way of bundling traffic headed in the same direction. All communications proceed along this same VC, preserving call sequence and a certain Quality of Service (QoS).

Circuit Routing Priority

A PVC-routing priority enables you to specify the *bandwidth priority* and *bumping priority*, or level of importance, of each circuit in the network. The lower the number, the higher the priority. For example, on the Set All PVCs on Map dialog box, you specify these values as follows:

Bandwidth priority — A value from 0-3, where 0 is the highest priority (default).

Bumping priority — A value from 0-7, where 0 is the highest priority (default).

If you do not override the defaults, all circuits are defined at the highest priority (0, 0), which means all circuits in the network have the same routing priority. However, if you prioritize circuits in your network, the switch assigns circuits with the highest priority to the lowest-cost paths through the network. These high-priority circuits are guaranteed full bandwidth wherever possible. Circuit prioritization occurs at the cost of the lower-priority circuits.

Priority Routing and Path Cost

By assigning specific bumping and bandwidth priorities to circuits, you can guarantee that the needs of high priority PVCs are met first. In addition, you can also accommodate PVCs where the path cost is not important. By assigning a routing priority to specific circuits, you can guarantee that when a link fails or under congestion conditions, the higher priority PVCs are given preference in the network over PVCs with a lower priority.

Example

There are two paths (Path 1 and Path 2) between a pair of nodes (A and B). The cost of Path 1 is 100, while the cost of Path 2 is 200. Multiple circuits within the network are defined with a priority routing of 2,0 and these virtual circuits use all of the bandwidth on the Path 1 link. Without priority routing, additional virtual circuits are forced to use Path 2, which could involve higher delays and more hops.

With priority routing, you can define additional circuits between A and B with a priority of 0,0. The switch running the priority-routing software can detect that Path 1 is entirely populated by the circuits with the 2,0 priority. The switch then forces enough 2,0 priority PVCs from Path 1 to ensure that every trunk in Path 1 has enough bandwidth to satisfy the Quality of Service (QoS) of the highest-priority (0,0) VCs. As a result, some 2,0 priority PVCs are forced to Path 2.

Special Conditions

Routing priority involves the following special conditions, which you should consider when configuring your network.

Low-Priority PVCs

PVCs that have a low bandwidth priority are always at risk in a mixed priority network. For this reason, circuits with a low bandwidth priority can be left without a valid route. The occurrence of this condition depends on the network topology and the amount of available link bandwidth.

ATM Trunk Configuration Guidelines

When you define an ATM trunk, you can reserve bandwidth for each QoS class. This parameter conflicts with routing priority if used on the same circuit. For this reason, if you are using routing priority on ATM trunks, you must specify that 100% of the bandwidth is shared between all of the QoS classes. If you do not do this, and a percentage of the bandwidth is reserved for any given QoS class, the switch ignores the specified routing priority for the ATM trunk and assumes the circuit has 0,0 routing priority.

Routing Priority Rules

The switch uses the following rules when implementing routing priority for circuit provisioning, trunk-failure recovery, and load-balance rerouting of circuits.

Circuit Provisioning

1. When provisioned, a higher-priority PVC selects a path when the circuit is provisioned, that is both cost effective and satisfies QoS.
2. All PVCs with a lower priority are ignored.
3. As the connection is established, higher-priority PVCs force lower-priority PVCs from their selected path until there is enough available link bandwidth to accommodate the higher-priority PVC QoS.
4. CascadeView selects lower-priority PVCs that are forced from their path in the following order.
    a. Bumping priority, where lowest bumping priority VCs are selected first.
    b. Within a group of VCs of the same bumping priority, the order of the Equivalent Bandwidth (EBW or CIR Frame Relay), where VCs with a higher EBW are selected first.
    c. Within a group of VCs that have the same bumping priority and the same EBW, in the order of the channel identifier.

Trunk-Failure Recovery

PVCs always attempt to reroute themselves when a trunk goes down. The Cascade switch software allows a trunk to reach negative bandwidth for PVCs recovering from trunk failure if there is no other available path with positive bandwidth. Priority routing modifies these rules as follows:

1. A higher bandwidth priority PVC selects an optimal path in response to trunk failure without taking into account the bandwidth consumed by lower-bandwidth priority VCs. The lower-priority VCs may be forced to use paths that are not optimal (as defined in the provisioning rules).

2. Lower bandwidth priority PVCs are not allowed to cross trunks where there is at least one higher priority VC and the bandwidth is negative, with the exception of PVCs configured with 0 bumping priority. Bumping priority 0 PVCs are allowed to push a trunk to negative bandwidth and rely on reroute balancing to correct the negative bandwidth at a future time.

3. Higher-priority PVCs may push a trunk to negative bandwidth if there are no more lower priority PVCs to force off the trunk. In this case, all of the lower-priority PVCs (excluding 0 bumping priority PVCs) are forced off the trunk. PVCs configured with 0 bumping priority are given special permission to share the negative bandwidth trunk with higher priority PVCs until the reroute balancing corrects this at a future time.

Balance Rerouting

Balance rerouting is a switch function that periodically tests the efficiency of each PVC route. A PVC that was rerouted due to trunk failure may not be on the most optimal path at any given time or may be traversing a negative bandwidth trunk. Balance rerouting corrects these conditions by rerouting the PVC to a new path.

Priority routing modifies the switch balance-rerouting functions so that a PVC with a higher bandwidth priority is given an optimal path, and the bandwidth used by the lower-priority PVCs is not considered by the switch. For this reason, the PVCs with the lower priority may be forced onto a path that is not optimal. Refer to "Circuit Provisioning" on page 11-4 for details about path selection.

Interoperability with Previous Releases

To use circuit-routing priority in your network, the following interoperability restrictions apply:

- All switch software must be at least Release 4.1 or higher for B-STDX switches and Release 2.4 on STDX switches.

- On a trunk, if either end resides on a 4.1 B-STDX switch or a 2.4 STDX switch, the trunk treats all PVCs equally (assumes all have a 0,0 priority).

- On a circuit, if either end belongs to a 4.1 B-STDX switch or a 2.4 STDX switch, the circuit is automatically assigned a 0,0 priority. The NMS does not support any routing priority other than 0,0 on switches running Release 4.1 or lower.

Rate Enforcement

Rate enforcement prevents network congestion and allocates network resources to ensure the commitment of service contracts. Rate enforcement measures the actual traffic flow across a connection and compares it to the configured traffic flow parameters for that connection. Traffic outside the acceptable configured level (CIR) is tagged and discarded if congestion develops.

Rate enforcement is implemented on a per DLCI basis on all circuits on ingress switches. When the switch receives data over time interval *Tc* (Tc=Bc/CIR), it classifies the frame as follows:

- Under the committed burst size (Bc)
- Over the committed burst size but under the excess burst size (Be)
- Over the excess burst rate

Color designators (green, amber, and red) identify packets travelling through the network. Congested nodes use the designators to determine which frames to discard first in various congested states or congestion conditions. Table 11-1 describes the designators (traffic colors) and discard policy.

Table 11-1. Rate Enforcement and Discard Policy

Traffic Color	Description	Discard Eligible (De)
Green	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, less than Bc.	No
Amber	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, greater than Bc but less than Be.	Frame is eligible for discard if it passes through a congested node.
Red	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, greater than Be.	All red frames are discarded.

Graceful Discard

The *graceful discard* feature enables you to control network behavior and user traffic. You can set the graceful discard parameters as follows:

On — The switch allows some red frames to be transmitted. This maximizes network usage, but may overload the network.

Off — This option avoids potential congestion. This allows strict control of user traffic, but may waste network resources.

When graceful discard is set to On, you can configure the red-frame percent. The red-frame percent is used to limit the number of red frames the network is responsible to deliver. The red-frame percent (pr) is determined as follows.

$$\text{Pr} = \frac{\text{Allowed red frame bits}}{\text{Bc} + \text{Be} + \text{allowed red frame bits}}$$

For more information on the rate-enforcement discard process, refer to the *Networking Services Technology Overview Guide*.

Rate Enforcement Schemes

You can configure the rate enforcement scheme. This option provides more flexibility, increased rate enforcement accuracy, and improved switch performance. You set the rate enforcement scheme in the Add PVC dialog box under the Traffic Type attributes (Refer to Table 11-8 on page 11-23).

Table 11-2 compares the accuracy and switch performance of the Jump and Simple rate enforcement schemes. Number 1 specifies the more accurate scheme and better switch performance, while 2 specifies a less-accurate scheme and slightly degraded switch performance.

Table 11-2. Rate Enforcement Schemes

Scheme	Rate Enforcement Accuracy	Switch Performance
Jump	1	2
Simple	2	1

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 logical port endpoints to a specific VPN and customer. You specify the net overflow parameters that determine whether PVCs originating from this port are restricted to trunks of their own VPN or use public (shared) trunks during overflow or failure conditions. You assign trunks to a VPN when you configure the trunk (described in Chapter 10).

You create a VPN and add customers to a specific VPN when you first configure a switch (refer to Chapter 4).

Using the VPN/Customer View Function

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 customer. When you create a new PVC, the Select End Logical Ports dialog box (Figure 11-24 on page 11-78) only displays the logical ports that belong to the VPN or customer name you select.

> *To give a customer the ability to monitor network resources without the ability to provision, refer to page 4-5.*

To use VPN/Customer view:

1. From the Administer menu, select Cascade Object:Select Customer/VPN. The Select Customer/Virtual Private Network dialog box appears as shown in Figure 11-1.

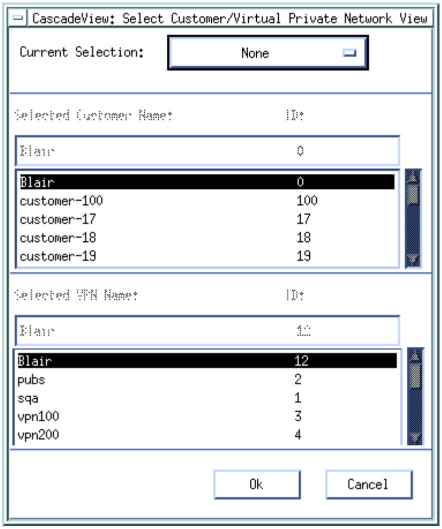


Figure 11-1. Select Customer/Virtual Private Network Dialog Box

2. Use the Current Selection button to select either Customer or VPN. None (*default*) disables the VPN/Customer view.

   If you choose None, 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.

About DLCI Numbers

A data link connection identifier (DLCI) number is a 10-bit address that identifies PVCs. This DLCI number corresponds to the DLCI number the Frame Relay trunk uses to access the PDN. The PDN recognizes this as a normal PVC carrying user traffic.

Depending on your link management type, use the guidelines in Table 11-3 to define DLCI numbers.

Table 11-3. DLCI Number Guidelines

DLCI Number Range	Description
0-15	Reserved
16-991	Available for all link management types
992-1007	Available for LMI Rev 1 only
1008-1023	Reserved

Before you Begin

Before you define the circuits for your network, verify the following tasks are complete:

- ☑ Create a network map and add a Cascade switch (Chapter 4)
- ☑ Configure the IP address and set the NMS path (Chapter 5)
- ☑ Configure the I/O module(s) and physical ports (Chapter 6)
- ☑ Configure the logical port(s) (Chapter 7, Chapter 8, and Chapter 9)
- ☑ Define the trunk parameters and trunk line connections (Chapter 10)

Accessing Circuit Functions

To access circuit functions:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits⇒ Point-to-Point. The Set All PVCs On Map dialog box appears as shown in Figure 11-2.

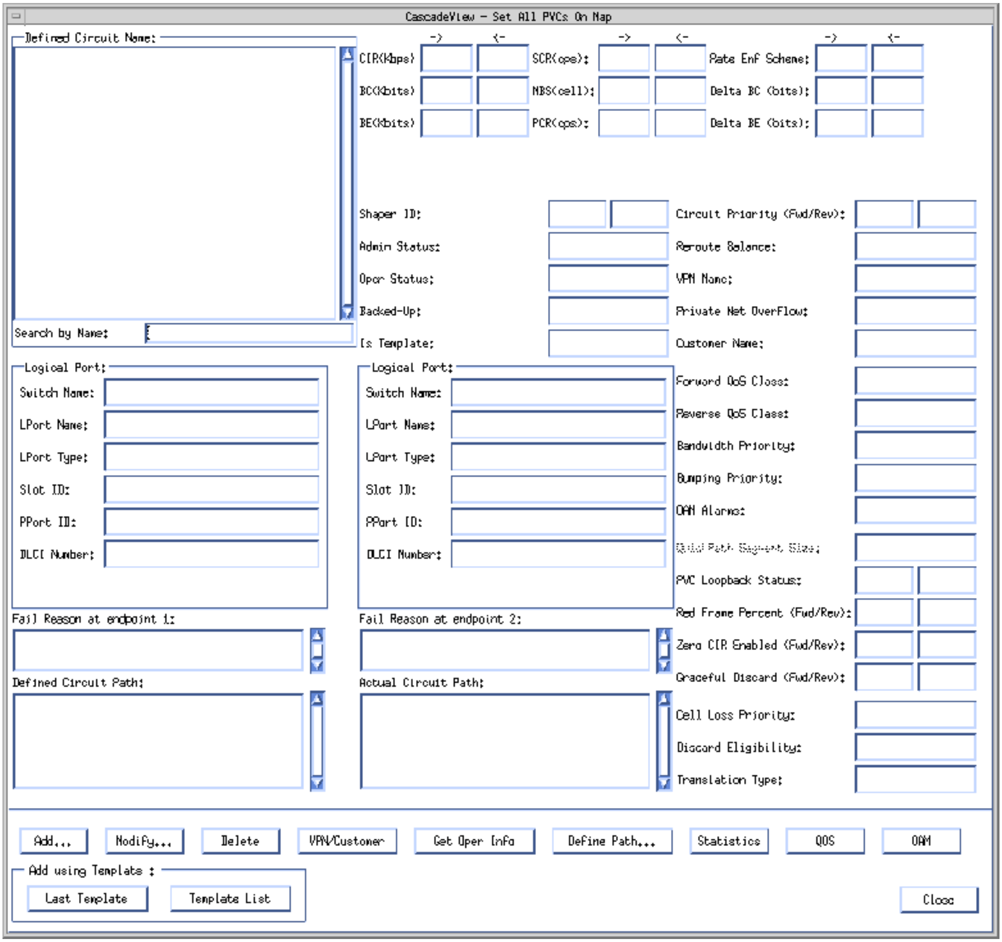


Figure 11-2. Set All PVCs On Map Dialog Box

The Set All PVCs On Map Dialog Box

The Set All PVCs On Map dialog box displays status information for the circuit name you select from the *Defined Circuit Name* list. To view a list of configured circuits, you must first position the cursor in the *Search by Name* field and press Return.

Table 11-4 describes the command buttons on the Set All PVCs dialog box.

Table 11-4. Set All PVCs Status Indicators and Command Descriptions

Command Button	Description
Add/Modify/Delete	Enables you to add a new circuit or Modify or Delete an existing circuit. ***Note**: If the PVC loopback status field does not display NONE, do not attempt to modify or delete the selected circuit. Refer to the* Diagnostic and Troubleshooting Guide for B-STDX/STDX *for more information about loopback testing.*
VPN/Customer	Displays the Virtual Private Network customer's name.
Get Oper Info	Displays a status message in the *Oper Status* field for the selected circuit. For more information, refer to the table of Inactive Operational Status Codes in the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
Statistics	Displays the summary statistics for the selected circuit. For more information about summary statistics, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.
QoS	Displays the Quality of Service values for the selected circuit. For more information about QoS, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

Table 11-4. Set All PVCs Status Indicators and Command Descriptions

Command Button	Description
OAM Alarms (*ATM CS and IWU modules only*)	Displays the OAM alarms for this circuit which indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up.
Add Using Template	If you have already defined a circuit configuration and saved it as a template, use this option to define a new circuit. 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.

Searching for Circuits

To view information for a specific circuit, select the name of the circuit and press Return. You can also use the *Search by Name* field to use wild card characters to search for a specific circuit name. To do this:

- 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 \\.

Adding a Circuit Connection

1. Access the circuit functions as described in "Accessing Circuit Functions" on page 11-12.

2. Choose Add. The Select End Logical Ports dialog box appears as shown in Figure 11-3.

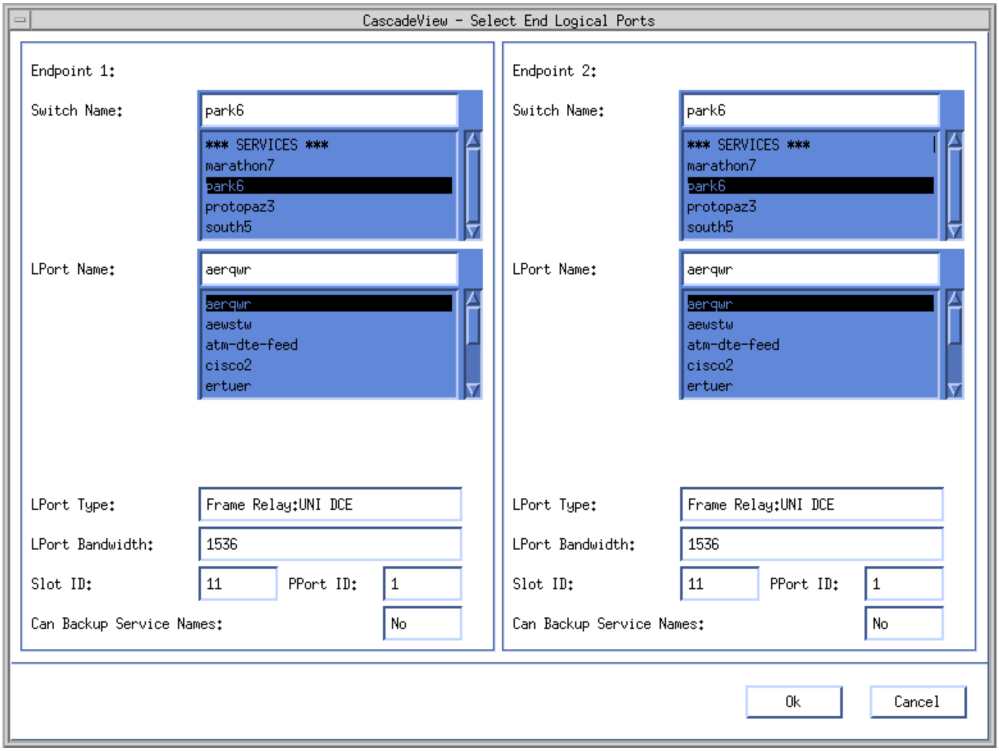


Figure 11-3. Select End Logical Ports Dialog Box

3. Configure Endpoint 1 and Endpoint 2 as follows:

For a fault tolerant PVC Configuration

a. Select *** SERVICES *** from the switch name list box.

b. Select a Service name from the list. You can configure a fault-tolerant PVC only for the following Frame Relay logical port types:

- UNI DCE
- UNI DTE
- UNI NNI.

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 a switch name from the list.

b. Select an lPort name from the list of logical ports. Table 11-5 lists logical port configurations.

c. Continue with Step 4.

Table 11-5. Logical Port Endpoints for Circuits

Endpoint 1	Endpoint 2
Frame Relay to Frame Relay	
FR UNI DCE/DTE, FR NNI	FR UNI DCE/DTE, FR NNI
FR UNI DCE/DTE, FR NNI	Encapsulated FRAD, PPP-to-1490 Translation
Encapsulated FRAD	Encapsulated FRAD
Frame Relay to ATM Network Interworking	
FR UNI DCE/DTE, FR NNI	ATM UNI DCE/DTE, ATM FR NNI

Table 11-5. Logical Port Endpoints for Circuits (Continued)

Endpoint 1	Endpoint 2
Frame Relay to ATM Service Interworking	
FR UNI DCE/DTE,	ATM UNI DCE/DTE
ATM DCE/DTE	Encapsulated FRAD, PPP-to-1490 Translation
ATM FR NNI	Encapsulated FRAD, PPP-to-1490 Translation
ATM to ATM	
ATM UNI DCE	ATM UNI DTE
ATM UNI DCE	ATM UNI DCE
ATM FR NNI	ATM FR NNI

4. The Select End Logical Ports dialog box displays information based on the configuration selections on page 11-16. Table 11-6 describes each field.

Table 11-6. Select End Logical Ports Fields

Field	Description
LPort Type	Displays the logical port type for each port in the circuit configuration.
LPort Bandwidth	Displays the bandwidth for each logical port in the trunk configuration.
Slot ID	Displays the I/O slot (number) in which the module resides.
PPort ID	Displays the port number for the physical port.

5. Choose OK. The Add PVC dialog box appears displaying the current parameters

6. Proceed to the appropriate section to define the circuit attributes.

- "Defining Frame Relay Circuits" on page 11-19.

- "Defining Frame Relay-to-ATM Service Interworking Circuits" on page 11-29. The ATM logical port can reside on either a frame-based I/O module (DXI/FUNI service) or a cell-based ATM I/O module (for example, the ATM DS3/E3 module).
- "Defining ATM Circuits" on page 11-43.

Defining Frame Relay Circuits

To define a circuit for Frame Relay services:

On the Add PVC dialog box, access the Set Attributes option menu shown in Figure 11-4.

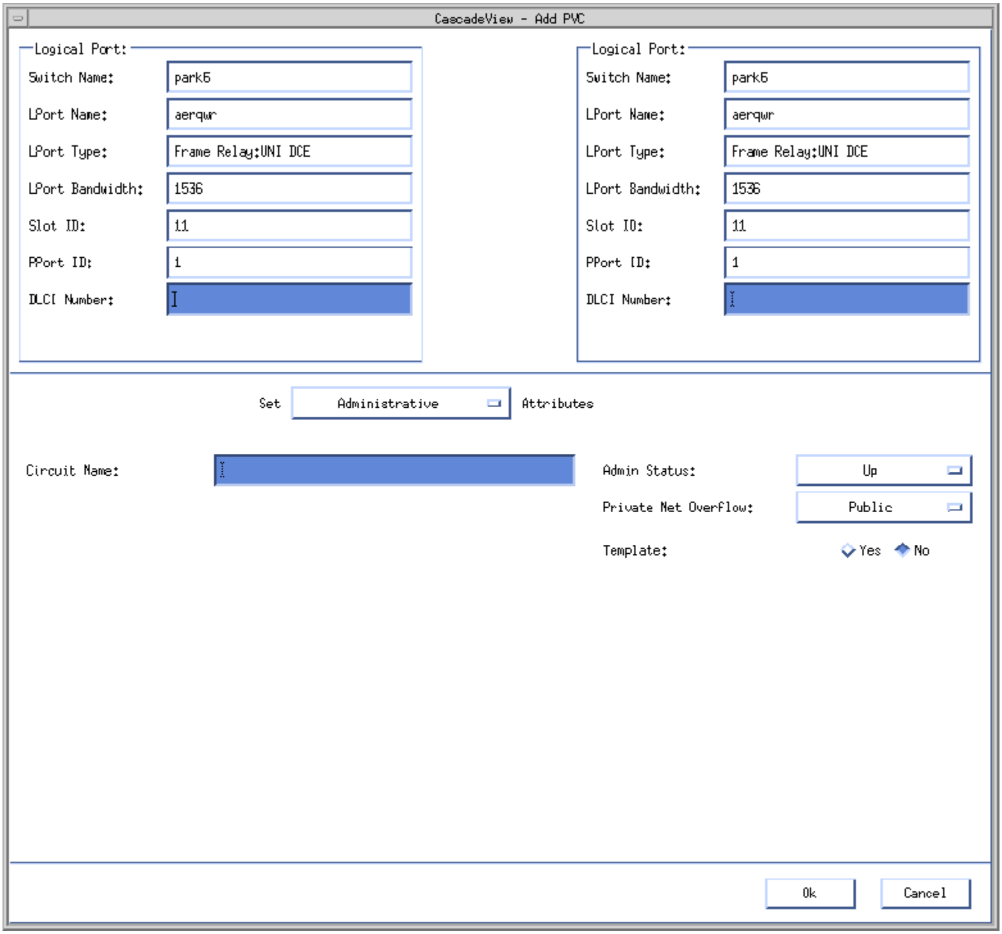


Figure 11-4. Set Administrative Attributes Dialog Box (Frame Relay:UNI DCE)

The Add PVC dialog box displays the parameters for both circuit endpoints and enables you to access the attributes fields through the Set Attributes option menu.

Administrative Attributes

1. Complete the administrative attributes fields described in Table 11-7.

Table 11-7. Set Administrative Attributes Fields

Field	Action/Description
DLCI Number	Enter a unique DLCI for this logical port. For more information, refer to “About DLCI Numbers” on page 11-10.
Circuit Name	Enter any unique, continuous, alphanumeric name to identify the circuit. Do not use parentheses and asterisks.
Admin Status	Select either Up or Down to define whether the circuit is to be activated. *Up (default)* – Activates the circuit. *Down* – Takes the circuit off-line to run diagnostics such as PVC loopback.
Private Net Overflow	(*For Virtual Private Networks*) Set the Private Net Overflow parameters, which determine whether circuits originating from an lport will be restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. For more information refer to “Creating a VPN” on page 4-22. Options include: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.

Table 11-7. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Is Template	(*Optional*) Save these settings as a template to use again to quickly configure a circuit with the same options. To create a template, choose Yes in the *Is Template* field. Refer to "Moving Circuits" on page 11-81 for more information.

Traffic Type Attributes

1. Set the Traffic Type attributes by selecting *Traffic Type* from the Set Attributes option menu.

   The Add PVC dialog box displays the fields shown in Figure 11-5.

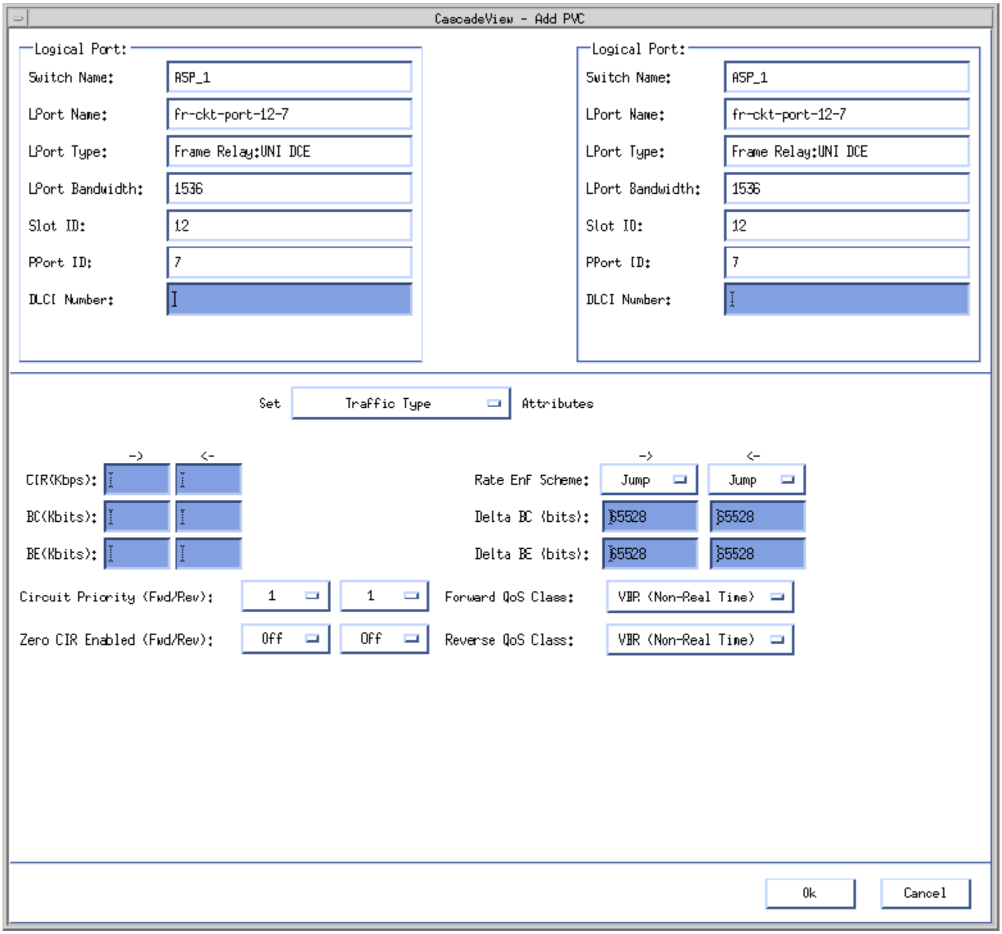


Figure 11-5. Set Traffic Type Attributes Dialog Box (Frame Relay:UNI DCE)

2. Complete the required dialog box fields described in Table 11-8.

> *The left column beneath the (–>) arrow represents the logical port for the circuit that connects Endpoint 1 to Endpoint 2. The right column beneath the (<–) arrow represents the logical port for the circuit that connects Endpoint 2 to Endpoint 1. Enter values in both columns.*

Table 11-8. Set Traffic Type Attributes Fields

Field	Action/Description
CIR (Kbps) (Committed Information Rate)	Enter the rate in Kbps at which the network transfers data under normal conditions. Normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc). The value on each PVC is asymmetric (you can set a different CIR in each direction), which provides more efficient use of bandwidth.
BC (Kbits) (Committed Burst Size)	Enter the maximum amount of data, in Kbits, that the network attempts to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as BC/CIR. This value must be greater than zero and is typically set to the same value as CIR.
BE (Kbits) (Excess Burst Size)	Enter the maximum amount of uncommitted data, in Kbits, the network will attempt to deliver during a specified time interval, Tc. Tc is calculated BC/CIR. The network treats this data as Discard Eligible (DE) data.
Circuit Priority (Fwd/Rev)	Select *1*, *2*, or *3* to configure the priority of data being transmitted on this circuit. Circuit priority determines the data's forward priority. The highest priority is 1 (do not discard data); the lowest is 3 (discards data). Refer to *Networking Services Technology Overview* for more information about congestion control and circuit priority.

Table 11-8. Set Traffic Type Attributes Fields (Continued)

Field	Action/Description
Zero CIR Enabled (Fwd/Rev)	Set the CIR parameter to *On* or *Off*. *On* – Indicates that the PVC has an assigned CIR value of zero and is a best-effort delivery service. Customer data that is subscribed to zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on zero CIR PVCs have DE set to one (1). *Off (default)* – Disables zero CIR. ***Note****: If you set Zero CIR Enabled to On, you can not set the CIR, Bc, and Be values.*
Rate Enf Scheme	Select *Simple (default)* or *Jump*. The configurable rate enforcement scheme provides more flexibility, increased rate enforcement accuracy, and improved switch performance. Refer to “Rate Enforcement Schemes” on page 11-7 for more information. ***Note****: If you select the Simple scheme, the “bad” PVC detection feature (refer to Table 7-12 on page 7-27) is disabled.*
Delta BC (bits)	Set the number of Delta Bc bits for this circuit between 0 - 65528 (*default* 65528). The maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval provided there is positive committed bit (Bc) credits before receiving the frame, but negative Bc credits after accepting the frame.

Table 11-8. Set Traffic Type Attributes Fields (Continued)

Field	Action/Description
Delta BE (bits)	Set the number of Delta Be bits for this circuit between 0 - 65528. (*default* 65528). The maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval provided there is positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame.
Forward QoS Class	Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.
Reverse QoS Class	Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.

User Preference

1. Set the User Preference attributes by selecting *User Preference* from the Set Attributes option menu.

   The Add PVC dialog box displays the fields shown in Figure 11-6.

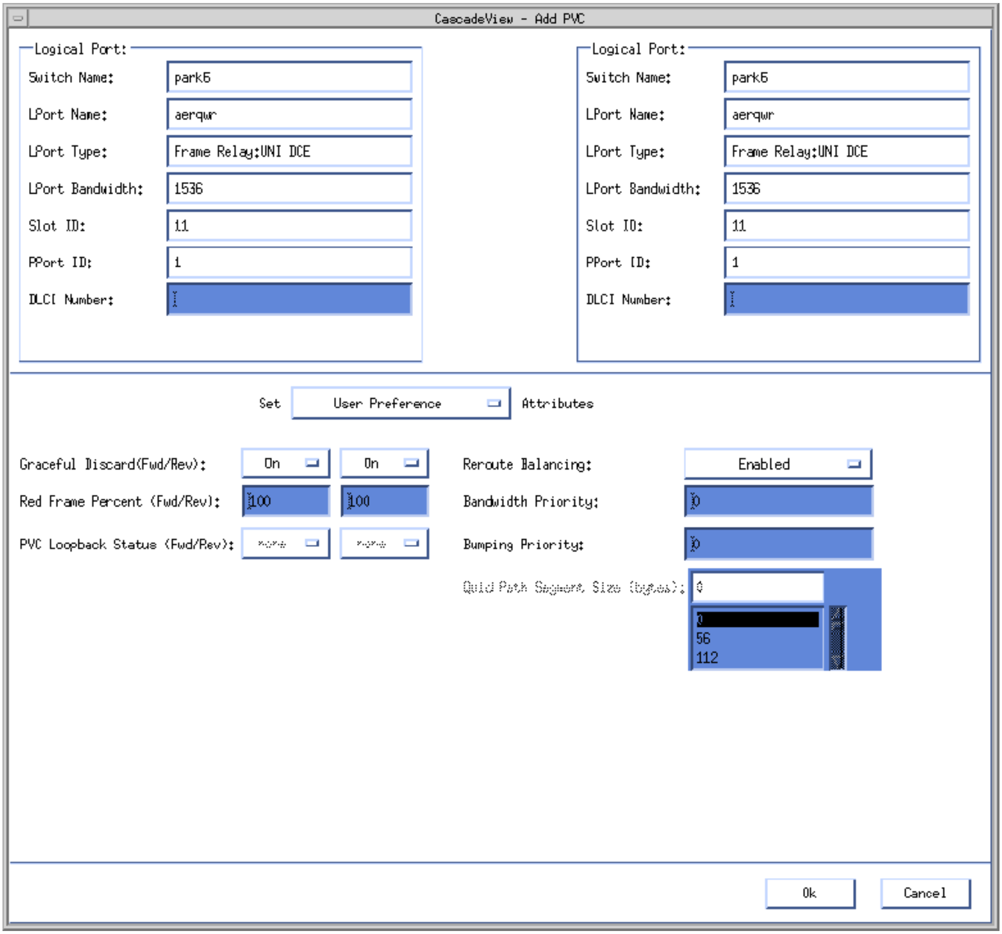


Figure 11-6. Set User Preference Attributes Dialog Box (Frame Relay:UNI DCE)

2. Complete the required fields described in Table 11-9.

Table 11-9. Add PVC-Set User Preference Fields

Field	Action/Description
Graceful Discard (Fwd/Rev)	Select either *On* or *Off* to define how this circuit handles “red” packets. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (BC) and excess burst size (BE) thresholds, including the current frame. The Discard Eligible (DE) bit for a red packet is set to 1, meaning the network can discard this packet unless Graceful Discard is set to On. *On* – Forwards some red packets if there is no congestion. *Off* – Immediately discards red packets.
Red Frame Percent (Fwd/Rev)	Set this value only if Graceful Discard is set to On. Refer to “Graceful Discard” on page 11-7 for more information. The Red Frame Percent limits the number of red frames the network is responsible to deliver.
PVC Loopback Status (Fwd/Rev)	Displays the current loopback state. If the PVC Loopback Status field does not display **None**, do not attempt to modify or delete the selected circuit. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information about loopback testing.

Table 11-9. Add PVC-Set User Preference Fields (Continued)

Field	Action/Description
Reroute Balance	Choose *Enable* to allow this circuit to use reroute tuning. This feature enables the switch to redistribute PVCs across trunks, based on OSPF updates and cost metrics. You must first configure the reroute tuning parameters for the selected switch. For more information, refer to "Defining Circuit Reroute Tuning Parameters" on page 5-24. If you *Disable* this option, this circuit does not use the reroute tuning parameters.
Bandwidth Priority	Set a value from 0 through 3 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.
Bumping Priority	Set a number from 0 through 7 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.
QuickPath Segment Size (Bytes)	Not supported.

3. Choose OK to accept the circuit parameters and send the configuration file to the switch (provided the switch is communicating with the NMS). The Set All PVCs dialog box reappears.

4. (*Optional*) To configure this PVC for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 11-53

5. Choose Close to return to the network map.

Defining Frame Relay-to-ATM Service Interworking Circuits

Frame Relay to ATM Service Interworking enables a Frame Relay device to connect to an ATM user device over a common WAN backbone. Frame Relay to ATM Service Interworking provides a seamless communication between ATM and Frame Relay networks or end-user devices.

> *Cascade supports a maximum of 2000 PVCs on ATM IWU and ATM CS modules.*

To define a circuit for Frame Relay-to-ATM service interworking:

1. On the Add PVC dialog box, access the Set Attributes option menu shown in Figure 11-4 on page 11-19.

   The Add PVC dialog box displays the fields shown in Figure 11-7.

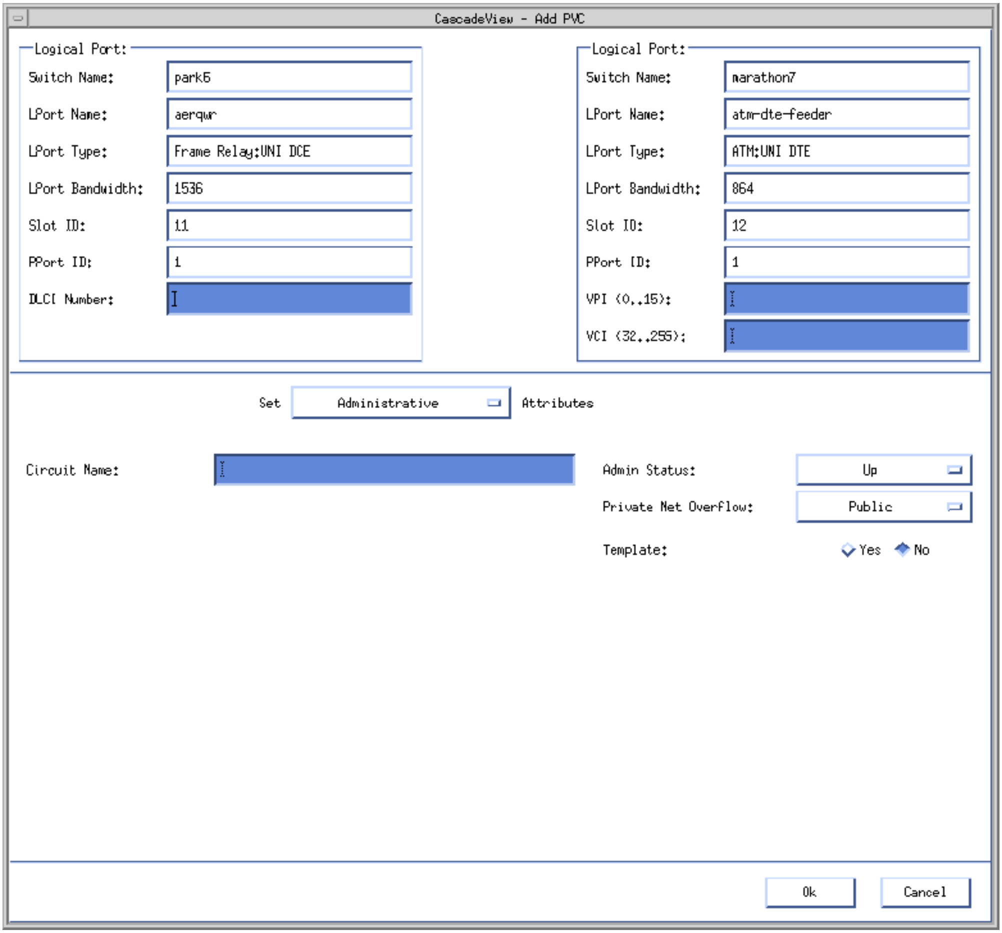


Figure 11-7. Set Administrative Attributes Dialog Box (FR-ATM Service IW)

Administrative Attributes

1. Complete the required fields described in Table 11-10.

Table 11-10. Set Administrative Attributes Fields

Field	Action/Description
DLCI	*(Frame Relay endpoint only)* Enter a unique DLCI for this logical port.
VPI (0..15)	*(ATM endpoint only)* Enter a value from 0 to 15 to represent the virtual path identifier for an ATM circuit. This value is used when the logical port is defined as an ATM OPTimum trunk. ***Note****: If you are configuring the VPI on an ATM CS or ATM IWU module, the VPI range depends on the number of VPI bits selected on the physical port.*
VCI (32..255)	*(ATM endpoint only)* Enter a value to represent the Virtual Channel Identifier for an ATM circuit. When you configure the ATM circuit: • On a frame-based I/O module, enter a value from 32 to 63. • On an ATM-based I/O module (such as the ATM DS3 module), enter a value from 32 to 255. • On an ATM CS or ATM IWU module, the total number of bits available for VPI and VCI is 12 bits. For example, if VPI is set to 1, there are 11 bits available for VCI. If VPI is set to 2, there are 10 bits available for VCI. ***Note****: If you are configuring the VCI on an ATM CS or ATM IWU module, the VCI range depends on the number of VPI bits selected on the physical port.*

Table 11-10. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Administrative Attributes Fields	
Circuit Name	Enter any unique, continuous, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. You can use hyphens.
Admin Status	Select either Up or Down to define whether the circuit is to be activated. *Up (default)* – Activates the circuit. *Down* – Takes the circuit off-line to run diagnostics such as PVC loopback.
Private Net Overflow	(*For Virtual Private Networks*) Set the Private Net Overflow parameters, which determine whether circuits originating from an lport will be restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. For more information refer to "Creating a VPN" on page 4-22. Options include: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.

Traffic Type Attributes

1. Set the Traffic Type attributes by selecting *Traffic Type* from the Set Attributes option menu.

   The Add PVC dialog box displays the fields shown in Figure 11-8.

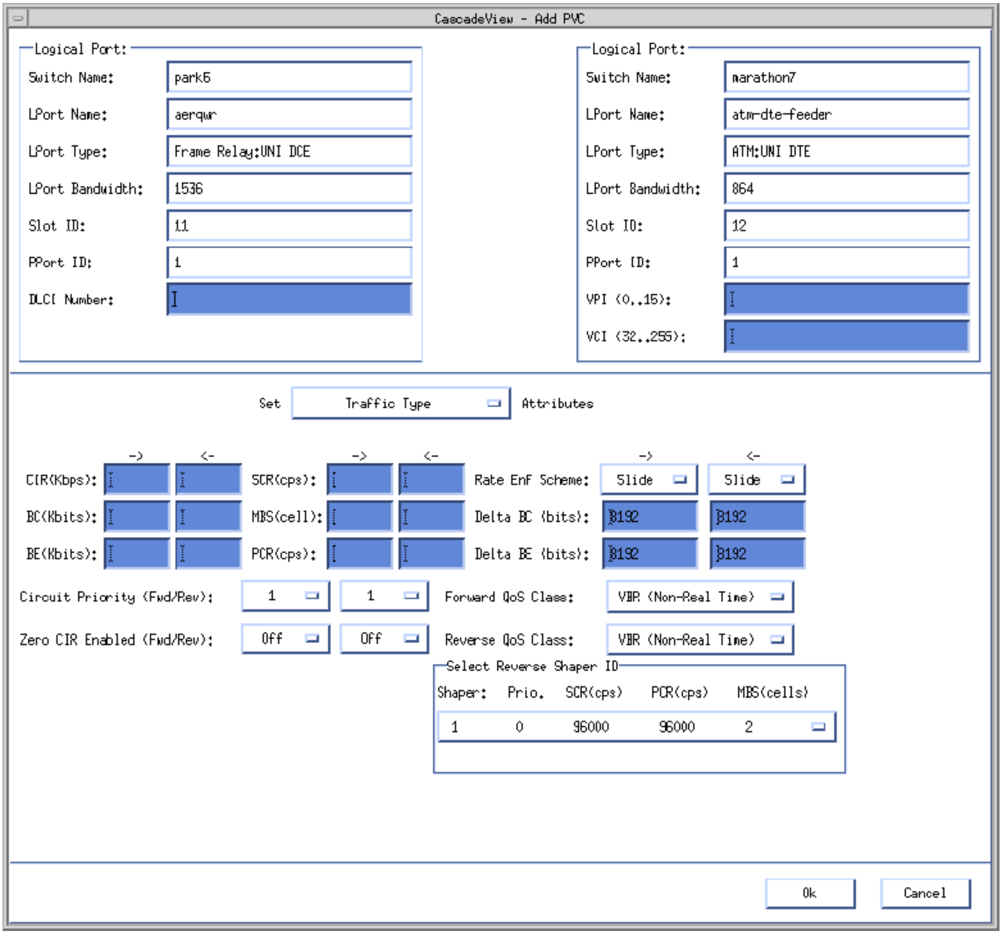


Figure 11-8. Add PVC-Set Traffic Type (FR to ATM IW) Dialog Box

The columns beneath the (—>) arrow represents the logical port for the circuit that connects Endpoint 1 to Endpoint 2. The columns beneath the (<—) arrow represents the logical port for the circuit that connects Endpoint 2 to Endpoint 1.

2. Define the traffic parameters for *one* endpoint of the circuit according to the logical port type. You can enter values in either column. For example, if you enter values for the ATM traffic parameters (SCR, MBS, and PCR), the software calculates the corresponding Frame Relay values (CIR, BC, and BE).

> *Using ATM-based I/O modules (ATM CS and IWU modules), the traffic parameters are a one-way translation. For example, if you change the ATM traffic parameters (SCR, MBS, and PCR), the corresponding Frame Relay values (CIR, BC, and BE) do not change.*

   a. Complete the Frame Relay traffic parameters described in Table 11-11 for the Frame Relay logical-port endpoint.

   b. Complete the ATM traffic parameters described in Table 11-11 for the ATM logical-port endpoint.

Table 11-11. Set Traffic Type Attributes Fields (Traffic Parameters)

Field	Action/Description
Frame Relay Traffic Parameters	
CIR (Kbps) (Committed Information Rate)	*(Frame Relay endpoint only)* Enter the rate in Kbps at which the network transfers data under normal conditions. Normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc).
BC (Kbits) (Committed Burst Size)	*(Frame Relay Endpoint only)* Enter the maximum amount of data, in Kbits, that the network attempts to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as BC/CIR. This value must be greater than zero and is typically set to the same value as CIR.

Table 11-11. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
BE (Kbits) (Excess Burst Size)	*(Frame Relay Endpoint only)* Enter the maximum amount of uncommitted data, in Kbits, the network will attempt to deliver during a specified time interval, Tc. Tc is calculated BC/CIR. The network treats this data as Discard Eligible (DE) data. ***Note***: *If the sum of BC + BE is greater than the value of MBS, you will get an error. If you set BC = CIR and BE to zero, traffic shaping is disabled on the ATM side of the circuit and MBS is forced to equal 32.*
ATM Traffic Parameters	
SCR (Sustainable Cell Rate)	*(ATM endpoint only)* Specify an SCR that is less than or equal to the peak cell rate (PCR). Sustainable cell rate is the average cell transmission rate, measured in cells-per-second. SCR is usually some fraction of the PCR and its value must be greater than or equal to 1/64 of the PCR.
MBS (Maximum Burst Size)	*(ATM endpoint only)* Enter a value between 32 and 2016. Maximum burst size determines the maximum number of cells that can be transmitted at the peak cell rate.

Table 11-11. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
Peak Cell Rate (PCR)	*(ATM endpoint only)* Specify the peak cell rate. Peak cell rate is the maximum transmission rate at which cells are transmitted. It defines the shortest time period between cells. (*Using ATM UNI*) The configured PCR works with the configured physical port PCR queue (refer to page 6-52). The circuit maps to the closest PCR queue whose PCR value is greater than the PCR value you configure here. Traffic shaping uses the PCR value from the PCR queue. ***Note***: *(Using ATM UNI) The SCR is scaled up by the same amount that the configured PCR value is scaled up when it is mapped into a PCR queue. The following formula determines the actual SCR value used for traffic shaping:* SCR (actual) = SCR (configured) * [PCR (actual)/PCR (configured)]
General Fields	
Rate Enf Scheme	Select *Simple (default)* or *Jump*. The configurable rate enforcement scheme provides more flexibility, increased rate enforcement accuracy, and improved switch performance. Refer to "Rate Enforcement Schemes" on page 11-7 for more information.

Table 11-11. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
Delta BC (bits)	Set the number of Delta Bc bits for this circuit between 0 - 53535 (*default* 53535). The maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval provided there is positive committed bit (Bc) credits before receiving the frame, but negative Bc credits after accepting the frame.
Delta BE (bits)	Set the number of Delta Be bits for this circuit between 0 - 53535. (*default* 53535). The maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval provided there is positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame.
Circuit Priority (Fwd/Rev)	Select *1*, *2*, or *3* to configure the priority of data being transmitted on this circuit. Circuit priority determines the data's forward priority. The highest priority is 1 (do not discard data); the lowest is 3 (discards data). Refer to *Networking Services Technology Overview* for more information about congestion control and circuit priority.

Table 11-11. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
Zero CIR Enabled (Fwd/Rev)	Set the CIR parameter to *On* or *Off*. *On* – Indicates that the PVC has an assigned CIR value of zero and is a best-effort delivery service. Customer data that is subscribed to zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on zero CIR PVCs have DE set to one (1). *Off (default)* – Disables zero CIR. ***Note****: If you set Zero CIR Enabled to On, you can not set the CIR, Bc, and Be values.*
Forward QoS Class	Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.
Reverse QoS Class	Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.

User Preference Attributes

1. Set the User Preference attributes by selecting *User Preference* from the Set Attributes option menu.

   The Add PVC dialog box displays the fields shown in Figure 11-9.

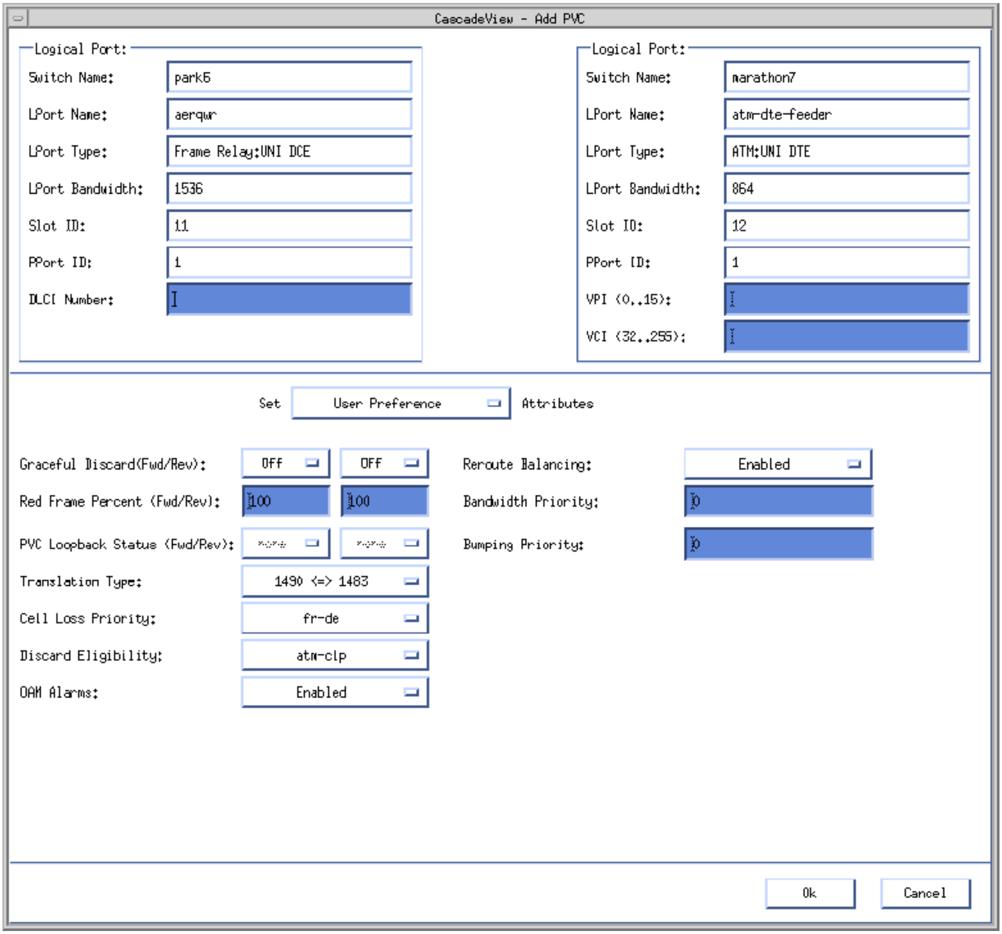


Figure 11-9. Set User Preference Attributes Dialog Box (FR-ATM Service IW)

2. Complete the required fields described in Table 11-12.

Table 11-12. Set User Preference Attributes Fields

Field	Action/Description
Graceful Discard (Fwd/Rev)	Select either *On* or *Off* to define how this circuit handles “red” packets. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (BC) and excess burst size (BE) thresholds, including the current frame. The Discard Eligible (DE) bit for a red packet is set to 1, meaning the network can discard this packet unless Graceful Discard is set to On. *On* – Forwards some red packets if there is no congestion. *Off* – Immediately discards red packets.
Red Frame Percent (Fwd/Rev)	Set this value only if Graceful Discard is set to *On*. Refer to “Graceful Discard” on page 11-7 for more information. The Red Frame Percent limits the number of red frames the network is responsible to deliver.
PVC Loopback Status (Fwd/Rev)	Displays the current loopback state. If the PVC Loopback Status field does not display **None**, do not attempt to modify or delete the selected circuit. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information about loopback testing.

Table 11-12. Set User Preference Attributes Fields (Continued)

Field	Action/Description
Translation Type	*(ATM endpoint only)* Select the ATM Translation Type protocol. Options include: *None* – Each end of the circuit uses the 1490 protocol. *RFC 1490 ⇔ 1483* – If you have a Frame Relay logical port on Endpoint 1 and an ATM logical port on endpoint 2. *RFC 1483 ⇔ 1490* – If you have an ATM logical port on Endpoint 1 and a Frame Relay logical port on Endpoint 2.
Cell Loss Priority	Specify the CLP setting. The CLP bit (Cell Loss Priority) is in each cell's cell header. Options include: fr-de (*ATM CS and IWU modules only*) – Sets the CLP bit to the same value as the Frame Relay frame DE bit on all ATM cells. This maps the DE bit to CLP. 0 – Sets the CLP bit to 0. 1 – Sets the CLP bit to 1.
Discard Eligibility	Select one of the following settings: atm-clp (*ATM CS and IWU modules only*) – Sets the CLP bit received in last cell of the frame to Frame Relay frame De bit. 0 – Sets the DE to 0. 1 – Sets the DE to 1.

Table 11-12. Set User Preference Attributes Fields (Continued)

Field	Action/Description
OAM Alarms (*ATM CS and IWU modules only*)	Choose *Enable* to allow this circuit to generate OAM alarms to indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up.
Reroute Balancing	Choose *Enable* to allow this circuit to use reroute tuning. This feature enables the switch to redistribute PVCs across trunks, based on OSPF updates and cost metrics. You must first configure the reroute tuning parameters for the selected switch. For more information, refer to "Defining Circuit Reroute Tuning Parameters" on page 5-24. If you *Disable* this option, this circuit does not use the reroute tuning parameters.
Bandwidth Priority	Set a value from 0 through 3 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.
Bumping Priority	Set a number from 0 through 7 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.

3. Choose OK to accept the circuit parameters and send the configuration information to the switch (provided the switch is communicating with the NMS).

   The Set All PVCs dialog box reappears.

4. (*Optional*) To configure this PVC for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 11-53.

5. Choose Close to return to the network map.

Defining ATM Circuits

To define an ATM circuit:

1. On the Add PVC dialog box, access the Set Attributes option menu.

   The Add PVC (ATM) dialog box displays the Set Attributes option menu and fields shown in Figure 11-10.

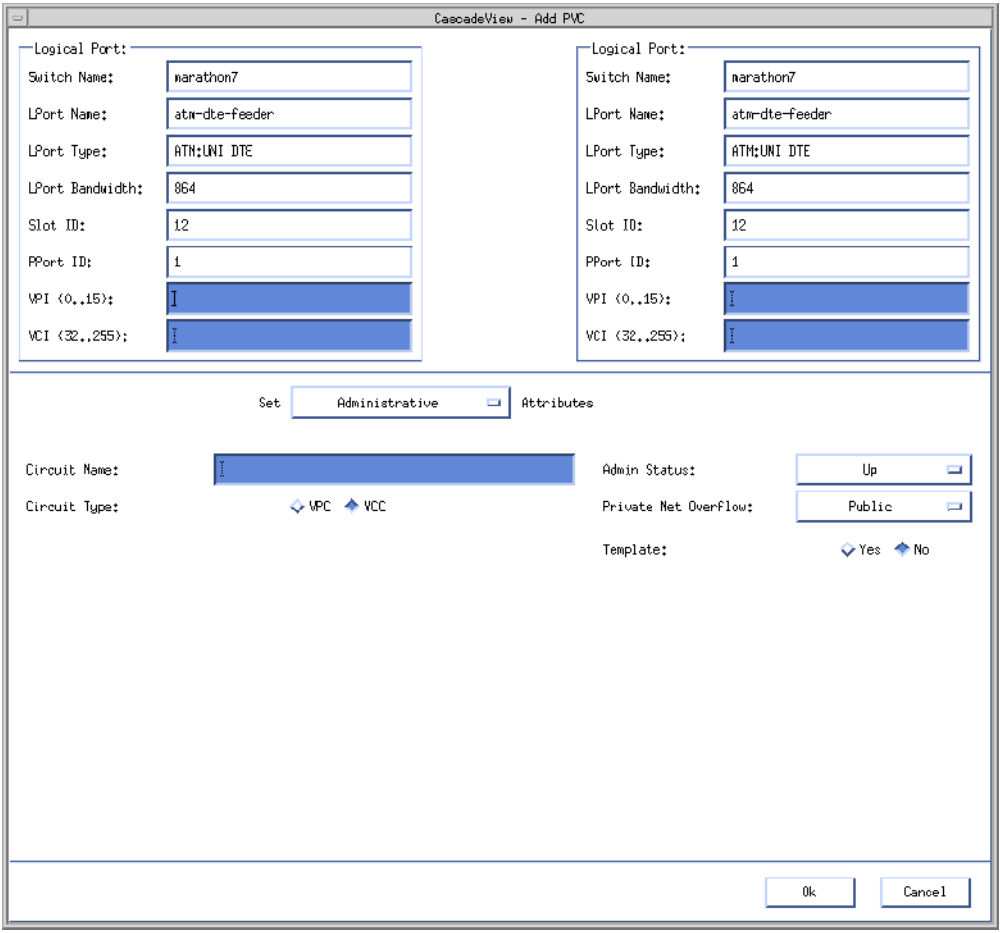


Figure 11-10. Set Administrative Attributes Dialog Box (ATM)

Administrative Attributes

1. Complete the fields described in Table 11-13.

> *Cascade supports a maximum of 2000 PVCs on ATM IWU and ATM CS modules.*

Table 11-13. Set Administrative Attributes (ATM) Fields

Field	Action/Description
VPI (0..15)	*(ATM endpoint only)* Enter a value from 0 to 15 to represent the virtual path identifier for an ATM circuit. This value is used when the logical port is defined as an ATM OPTimum trunk. ***Note****: If you are configuring the VPI on an ATM CS or ATM IWU module, the VPI range depends on the number of VPI bits selected on the physical port.*

Table 11-13. Set Administrative Attributes (ATM) Fields (Continued)

Field	Action/Description
VCI (32..255)	*(ATM endpoint only)* Enter a value to represent the Virtual Channel Identifier for an ATM circuit. When you configure the ATM circuit: • On a frame-based I/O module, enter a value from 32 to 63. • On an ATM-based I/O module (such as the ATM DS3 module), enter a value from 32 to 255. • On an ATM CS or ATM IWU module, the total number of bits available for VPI and VCI is 12 bits. For example, if VPI is set to 1, there are 11 bits available for VCI. If VPI is set to 2, there are 10 bits available for VCI. ***Note****: If you are configuring the VCI on an ATM CS or ATM IWU module, the VCI range depends on the number of VPI bits selected on the physical port.*
Circuit Name	Enter any unique, continuous, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. You can use hyphens.
Circuit Type	Select the type of circuit. Options include: *VPC* – Virtual Path Connection. If you select VPC, the VCI field is set to 0 and cannot be changed. *VCC* (*default*) – Virtual Channel Connection.

Table 11-13. Set Administrative Attributes (ATM) Fields (Continued)

Field	Action/Description
Admin Status	Select either Up or Down to define whether the circuit is to be activated. *Up (default)* – Activates the circuit. *Down* – Takes the circuit off-line to run diagnostics such as PVC loopback.
Private Net Overflow	(*For Virtual Private Networks*) Set the Private Net Overflow parameters, which determine whether circuits originating from an lport will be restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. For more information refer to “Creating a VPN” on page 4-22. Options include: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network.
Is Template	(*Optional*) Save these settings as a template to use again to quickly configure a circuit with the same options. To create a template, choose Yes in the *Is Template* field. Refer to “Moving Circuits” on page 11-81 for more information.

Traffic Type Attributes

1. Set the Traffic Type attributes by selecting *Traffic Type* from the Set Attributes option menu.

   The Set Traffic Type Attributes dialog box displays the fields shown in Figure 11-11.

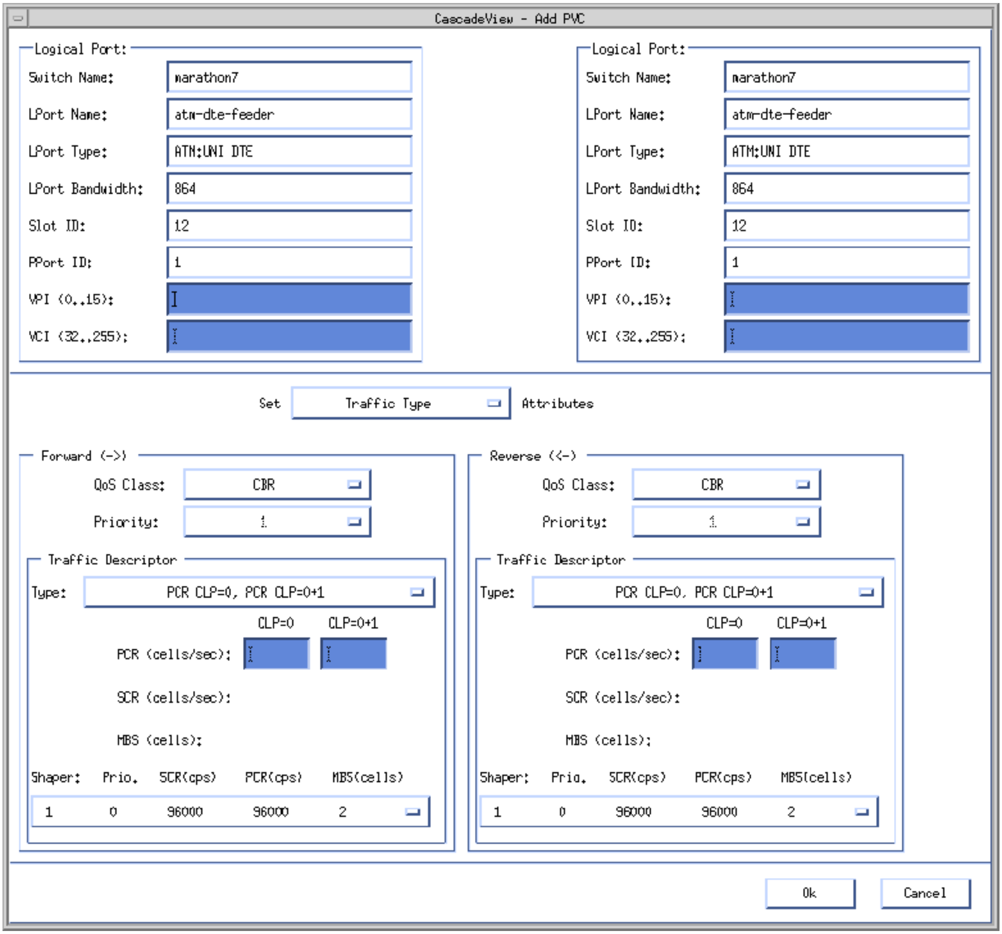


Figure 11-11. Set Traffic Type Attributes Dialog Box (ATM)

> *The example in Figure 11-11 shows an Add PVC dialog box using an ATM IWU module. Shaper information will only appear using an ATM IWU or ATM CS module.*

2. Complete the required fields described in Table 11-14.

Table 11-14. Set Traffic Type Attributes Fields

Field	Description
QoS Class	Set the QoS class. Cascade currently supports only the *VBR non-real time* Class of Service value for non-real time applications. This option enables the circuit to transfer large amounts of data over a long period of time, using a pre-established ATM connection. Class of service values enable you to prioritize circuit traffic.
Priority	Select *1*, *2*, or *3* to configure the priority of data being transmitted on this circuit. Circuit priority determines the data's forward priority. The highest priority is 1 (do not discard data); the lowest is 3 (discards data). Refer to *Networking Services Technology Overview* for more information about congestion control and circuit priority.
Traffic Descriptor Fields	
Type	Select the traffic descriptor type for this circuit.

Table 11-14. Set Traffic Type Attributes Fields (Continued)

Field	Description
Peak Cell Rate (PCR)	Peak cell rate is the maximum transmission rate at which cells are transmitted. It defines the shortest time period between cells. The configured circuit PCR works with the configured physical port PCR (refer to "Configuring Physical Ports" on page 6-9). (*ATM UNI DS3 only*) The circuit maps to the closest PCR queue whose PCR value is greater than the PCR value you configure here. Traffic shaping uses the PCR value from the PCR queue. ***Note****: The SCR is scaled up by the same amount that the configured PCR value is scaled up when it is mapped into a PCR queue. The following formula determines the actual SCR value used for traffic shaping:* SCR (actual) = SCR (configured) * [PCR (actual)/PCR (configured)]
Sustainable Cell Rate (SCR)	*(ATM UNI DS3 only)* Specify an SCR that is less than or equal to the peak cell rate (PCR). Sustainable cell rate is the average cell transmission rate, measured in cells-per-second. SCR is usually some fraction of the PCR and its value must be greater than or equal to 1/64 of the PCR.
Maximum Burst Size (MBS)	*(ATM UNI DS3 only)* Enter a value between 32 and 2016. Maximum burst size determines the maximum number of cells that can be transmitted at the peak cell rate.

User Preference Attributes

1. Set the User Preference attributes by selecting *User Preference* from the Set Attributes option menu.

   The Add PVC dialog box displays the fields shown in Figure 11-12.

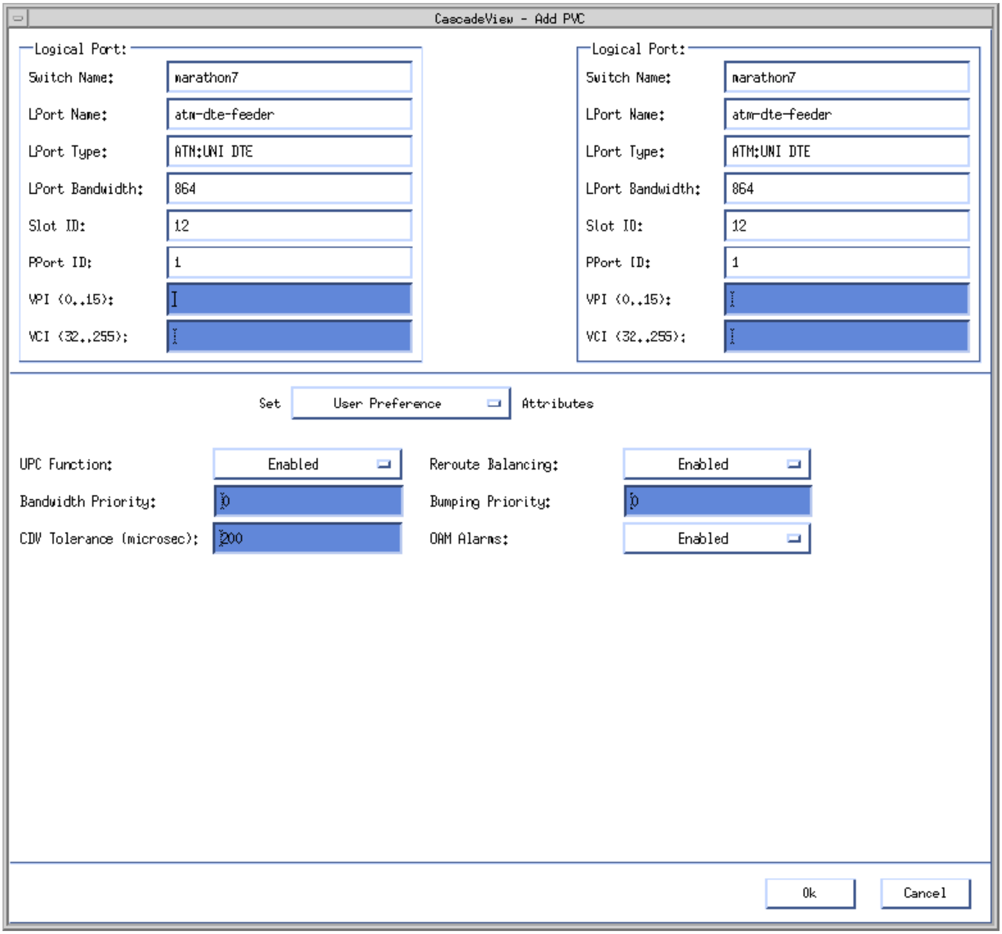


Figure 11-12. Set User Preference Attributes Dialog Box (ATM)

2. Complete the required fields described in Table 11-15.

Table 11-15. Set User Preference Fields

Field	Description
Bandwidth Priority	Set a value from 0 through 3 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.
PVC Loopback Status (Fwd/Rev)	Displays the current loopback state. If the PVC loopback status field does not display NONE, do not attempt to modify or delete the selected circuit. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information about loopback testing.
CDV Tolerance (microsec)	*(OPTimum Direct Cell Trunks only*) Specify the maximum cell delay variation (in µsecs). This value only applies to CBR traffic, and specifies the maximum variation in time delays between cells going out of this logical port. The default value is 684 for DS3 ports, and 191 for OC3c ports. To change the default, you need to know the maximum CDV for PVCs on the port, as well as the traffic requirements of the hardware on the other end of the connection.

Table 11-15. Set User Preference Fields (Continued)

Field	Description
Reroute Balancing	Choose *Enable* to allow this circuit to use reroute tuning. This feature enables the switch to redistribute PVCs across trunks, based on OSPF updates and cost metrics. You must first configure the reroute tuning parameters for the selected switch. For more information, refer to "Defining Circuit Reroute Tuning Parameters" on page 5-24. If you *Disable* this option, this circuit does not use the reroute tuning parameters.
Bumping Priority	Set a number from 0 through 7 where 0 is the default and indicates the highest priority. Refer to "Circuit Routing Priority" on page 11-2 for more information.
OAM Alarms (*AMT CS and ATM IWU modules only*)	Choose *Enable* to allow this circuit to generate OAM alarms to indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up.

3. Choose OK to accept the circuit parameters and send the configuration information to the switch (provided the switch is communicating with the NMS).

   The Set All PVCs dialog box reappears.

4. (*Optional*) To configure this PVC for a specific VPN and customer, refer to "Selecting the VPN and Customer Name" on page 11-53

5. Choose Close to return to the network map.

Selecting the VPN and Customer Name

Before you configure a PVC for a VPN, verify the following tasks are complete:

Step 1. Create the UNI logical port and specify the net overflow parameters (page 7-21).

Step 2. Dedicate the PVC logical port endpoints to a specific VPN and customer (page 7-43).

Step 3. Dedicate a trunk to a specific customer (page 10-6).

Step 4. Specify the PVC's net overflow parameters (page 11-20)

To associate this circuit with a specific VPN and customer:

1. From the Set All PVCs on Map dialog box (Figure 11-2 on page 11-12) select the circuit and choose VPN/Customer.

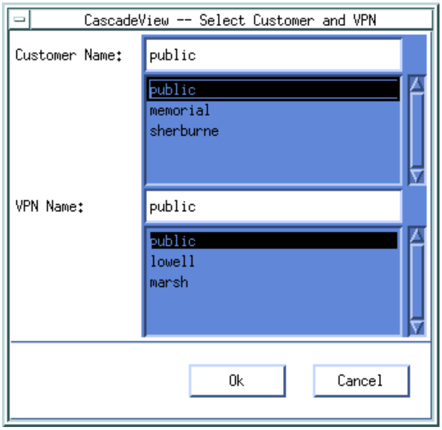


Figure 11-13. Select Customer and VPN Dialog Box

2. Select the customer and VPN name.

3. Choose OK to return to the Set All PVCs on Map dialog box (Figure 11-2 on page 11-12).

4. Choose Close to return to the network map.

Manually Defining the Circuit Path

The Define Path function enables you to manually define a circuit path and bypass the OSPF algorithm to make 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. The Set All PVCs on Map dialog box appears.
2. Select the circuit (name) for which you want to manually define the circuit path.
3. Choose Define Path. The Define Circuit Path dialog box appears as shown in Figure 11-14.

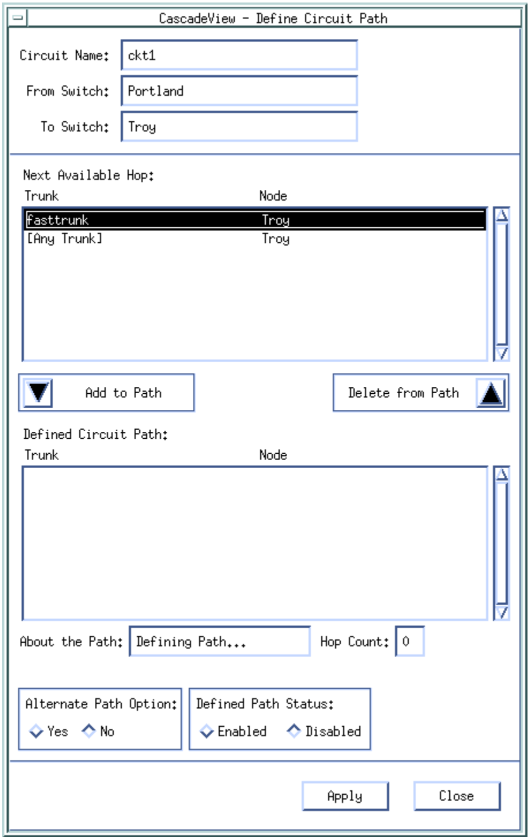


Figure 11-14. Define Circuit Path Dialog Box

4. Complete the Define Circuit Path dialog box fields described in Table 11-16.

Table 11-16. Define Circuit Path Fields

Field	Action/Description
Next Available Hop	Displays a list of the available hops, i.e., trunk-node pairs. Select the trunk-node pair to route the circuit through the network. When there are multiple trunks between two nodes, select [Any Trunk] to route the circuit bases on OSPF. Choose Add to Path. The specified trunk-node pair is added to the Define Circuit Path list, which displays all selected hops.
About the Path	Displays status about the path. For example, after you define a path, this field displays “Path is Completed”.
Hop Count	Displays the number of hops in the selected path.
Alternate Path Option	Select *Yes* or *No* to specify whether OSPF should route the circuit path if the manual route fails. *Yes* – Enables OSPF to route the circuit based on the best available path if the manually defined path fails. *No* – Prevents the circuit from being rerouted; the circuit remains down until the defined path is available.

Table 11-16. Define Circuit Path Fields (Continued)

Field	Action/Description
Defined Path Status	Select *Enabled* or *Disabled* to define whether to use the defined path or to enable the network routing to specify the circuit path. *Enabled* – Routes the circuit based on the manually defined route. *Disabled* – Routes the circuit based on the network's OSPF algorithm.

5. Choose Apply and then choose OK. The specified values are sent to the switch(es), provided the switches are currently communicating with the NMS.

Configuring Point-to-Multipoint Circuits

A point-to-multipoint (PMP) circuit consists of the originating point (circuit root) and endpoints (circuit leaf). 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:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits ⇒ Point-to-Multipoint Circuits. The Set All Point-to-Multiple Point Circuit Roots dialog box appears as shown in Figure 11-15.

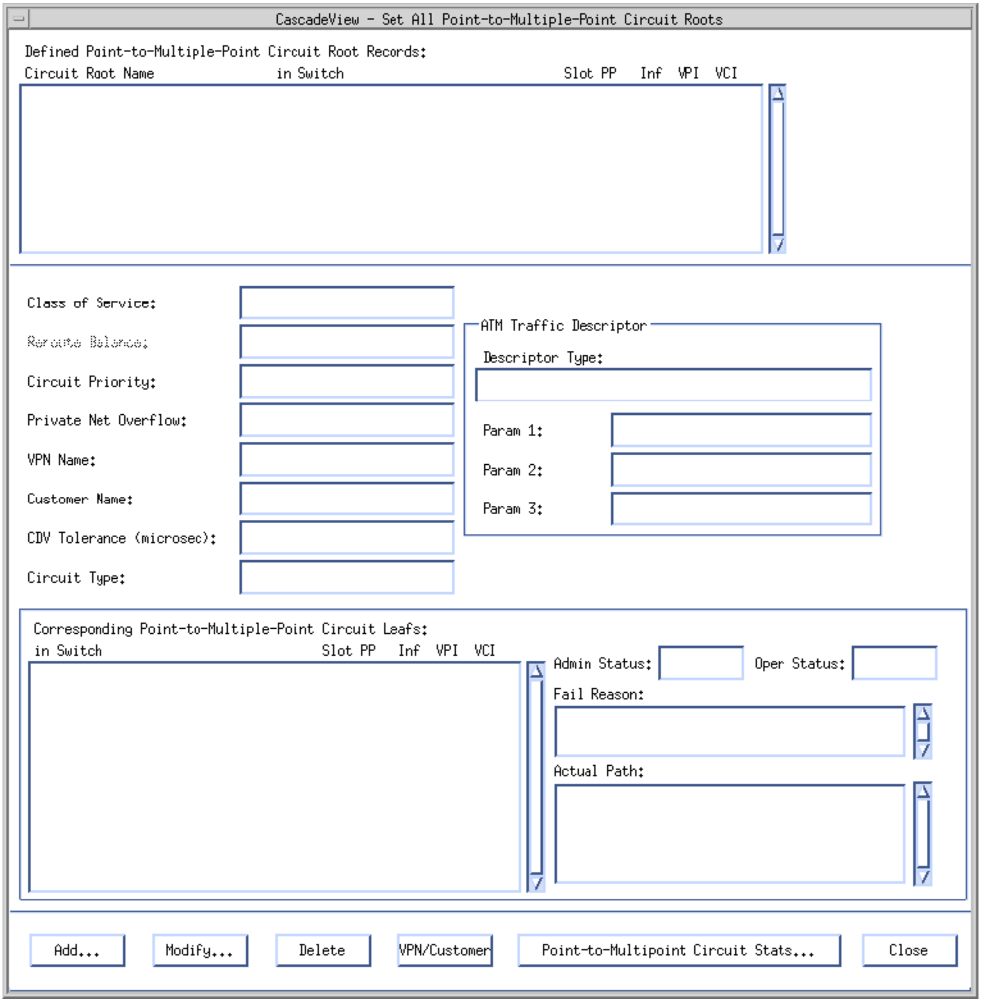


Figure 11-15. Set All Point-to-Multiple-Point Circuit Roots Dialog Box

The Defined Point-to-Multiple-Point Circuit Root Records list box displays any existing PMP circuit roots. The Corresponding Point-to-Multiple-Point Circuit Leafs list box below displays any existing circuit leafs (endpoints) for the selected circuit root.

Table 11-17 describes the commands and circuit root and leaf fields.

Table 11-17. Set All Point-to-Multipoint Circuit Roots Fields and Commands

Field/Command	Description
in Switch	Name and ID of switch on which the root or leaf resides.
Slot	Physical slot for the IOM on which the root or leaf was created.
PP	Number of the physical port on which the root or leaf was created.
Inf	MIB interface number for the logical port on which the root or leaf was created.
VPI	Virtual Path identifier of the logical port assigned to the root or leaf.
VCI	Virtual Channel identifier 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	Displays the switch's current reroute balancing configuration.
Circuit Priority	Displays the circuit's priority.
Circuit Type	Displays the circuit type: VCC (virtual channel connection) or VPC (virtual path connection).

Table 11-17. Set All Point-to-Multipoint Circuit Roots Fields and Commands

Field/Command	Description
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.
Commands	
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.
VPN/Customer	Assigns the selected point-to-multipoint circuit root to a specific VPN and customer name. You assign the circuit to a VPN before you create PMP circuit leafs.
Point-to-Multipoint Circuit 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 B-STDX/STDX*.

Defining a Point-to-Multipoint Circuit Root

This section describes how to configure the originating point (circuit root) for a point-to-multipoint circuit.

To define a point-to-multipoint circuit root:

1. Choose Add. The Add Point-to-Multiple-Point Circuit Root dialog box appears as shown in Figure 11-16.

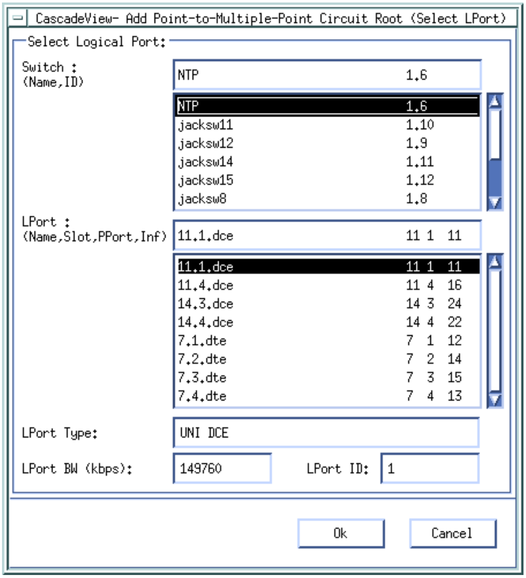


Figure 11-16. Add Point-to-Multiple-Point Circuit Root Dialog Box

2. In the Switch list box, select the switch on which the originating point of the circuit will reside. The selected switch name appears in the text box above the list. The list contains the switch name and ID for all switches the NMS can currently access.

3. In the LPort list box, select the logical port on which the originating point of the circuit will reside. The selected logical port name appears in the text box above the list. The list box displays the logical port name (Name), slot ID (Slot), physical port number (PPort), and MIB interface number (Inf) for all logical ports on the selected switch.

   The following list box displays information for the selected port:

   LPort Type — Displays the type of logical port (ATM UNI DCE or ATM UNI DTE).

   LPort BW (Kbps) — Displays the total logical port bandwidth, in kilobits per second (Kbps).

   LPort ID — Displays the logical port ID.

4. Choose OK. The Add Point-to-Multiple-Point Circuit Root dialog box appears as shown in Figure 11-17.

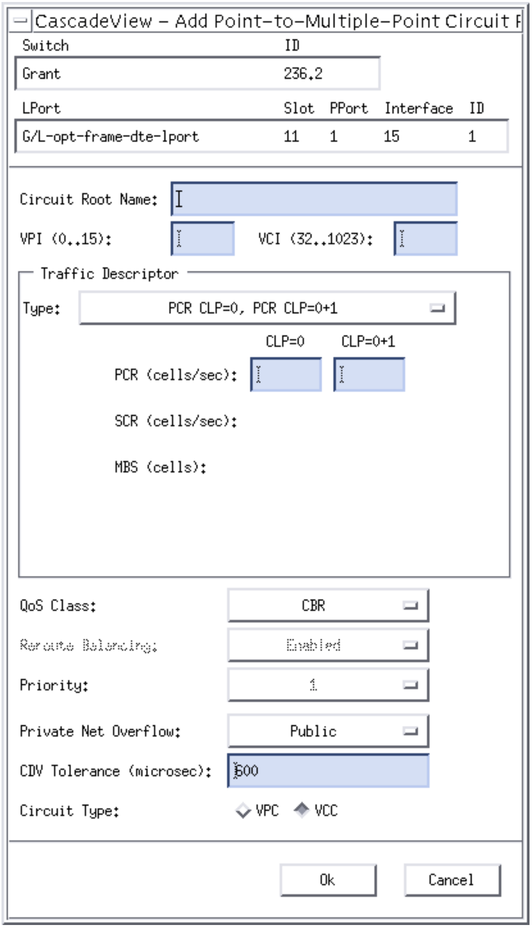


Figure 11-17.   Add Point-to-Multiple-Point Circuit Root Dialog Box

5. Complete the fields described in Table 11-18.

Table 11-18. Add Point-to-Multiple-Point Circuit Root Fields

Field	Action/Description
Circuit Root Name	Enter an alphanumeric name for the circuit root.
VPI (0..15)	Enter a value between 0 and 15.
VCI (32..1023)	Enter a value between 32 and 1023.

6. Select one of the following Traffic Descriptor types. Note that the selected QoS class affects which traffic descriptors are available.

   PCR CLP=0 (cells/sec) — Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. Specify the Peak Cell Rate in cells per second for high-priority traffic (i.e., the CLP=0 cell stream).

   PCR CLP=0+1 (cells/sec) — Specify the Peak Cell Rate, 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. Specify the Sustained Cell Rate, 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. Specify the Sustained Cell Rate, 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. Specify the Maximum Burst Size, 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. Specify the Maximum Burst Size, in cells per second, for the combined high- and low-priority traffic (i.e., the CLP=0+1 cell stream).

7. Complete the fields described in Table 11-19

Table 11-19. Add Point-to-Multiple-Point Circuit Root Fields

Field	Action/Description
QoS Class	Select the Quality of Service class for traffic on this PMP circuit.
Reroute Balancing	Choose *Enable* to allow this circuit to use reroute tuning. This feature enables the switch to redistribute PVCs across trunks, based on OSPF updates and cost metrics. You must first configure the reroute tuning parameters for the selected switch. For more information, refer to "Defining Circuit Reroute Tuning Parameters" on page 5-24. If you *Disable* this option, this circuit does not use the reroute tuning parameters.
Private Net Overflow	(*Virtual Private Networks*) Set the Private Net Overflow parameters, which determine whether circuits originating from an lport are restricted to trunks of their own VPN or use public (shared) trunks during overflow conditions. For more information, refer to "Creating a VPN" on page 4-22. Options include: *Public (default)* – Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own VPN.
CDV Tolerance (microsec)	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.

Table 11-19. Add Point-to-Multiple-Point Circuit Root Fields (Continued)

Field	Action/Description
Circuit Type	Specify the circuit type. Options include: *Virtual Channel Connection (VCC) (default)* *Virtual Path Connection (VPC)* – Sets the VPI field to zero. You cannot change this field.

8. Choose OK to return to the Set All PMP Circuit Roots dialog box (Figure 11-15 on page 11-58).

9. 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 11-53.

Defining Point-to-Multipoint Circuit Leafs

This section describes how to add endpoints to the root circuit.

To define the multiple endpoints of the PMP circuit:

1. Choose Modify. The Modify Point-to Point Circuit Leaf dialog box appears as shown in Figure 11-18.

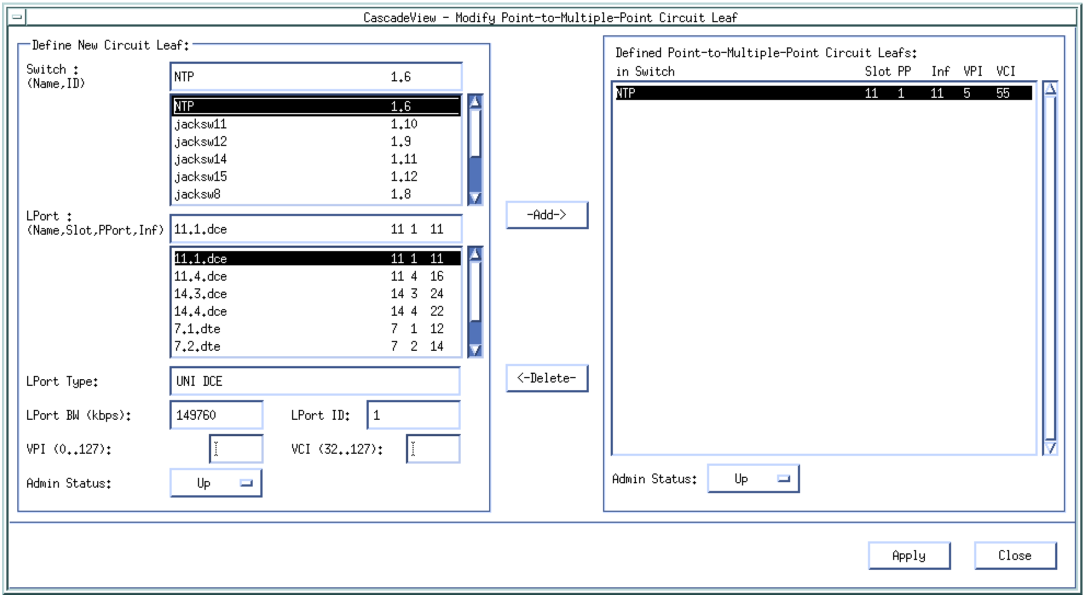


Figure 11-18. Modify PMP Circuit Leaf Dialog Box

The left side of this dialog box enables you to define the endpoints of the PMP circuit. The list box on the right shows the endpoints that have already been defined for the selected originating point.

2. 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.

3. In the LPort list box, select the logical port for the new endpoint. The fields below display the bandwidth and LPort ID for the selected logical port.

4. Complete the fields described in Table 11-20.

Table 11-20. Modify PMP Circuit Leaf Fields

Field	Action/Description
VPI (0..15)	Enter a value between 0 and 15.
VCI (32..1023)	Enter a value between 32 and 127.
Admin Status	Select either Up or Down to define whether the circuit is to be activated. *Up* – Activates the circuit. *Down* – Takes the circuit off-line to run diagnostics such as PVC loopback.

5. Choose -Add-> to add the circuit to the PMP Circuit Leaf list.
6. Choose Apply.
7. Repeat Step 2 through Step 6 for each endpoint you want to create for this PMP circuit.

Do not configure more than one circuit leaf for a given root on the same physical port. If more than one OPTimum trunk is configured on a physical port, only one of the OPTimum trunks will be used for routing only one of the leafs for a given root. (Figure 11-19 shows invalid and valid multiplexing-configuration examples at the port level.)

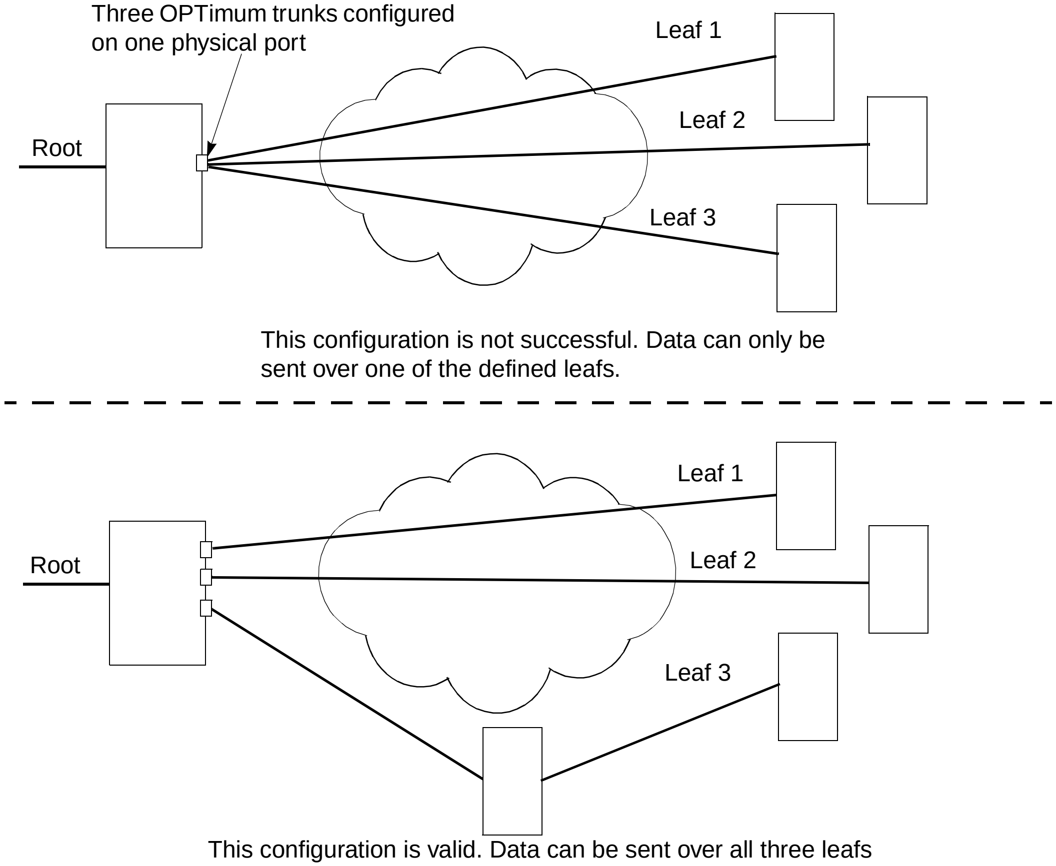


Figure 11-19. PMP Circuit Example

8. Choose Close to return to the Set All Point-to-Multiple Point Circuits dialog box.

9. Choose Close to return to the network map.

Deleting a PMP Circuit Root and Leafs

This section describes how to delete the circuit leafs and root of a PMP circuit, as well as the entire circuit. Before you delete the root of a circuit, you must delete all of the circuit's leafs.

To delete a PMP circuit root and/or one or more of the circuit's leafs:

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 11-15 on page 11-58).
2. From the Circuit Root Name list box, select the PMP circuit root to delete.
3. Choose Modify. The Modify PMP Circuit Leaf dialog box appears (Figure 11-18 on page 11-67).
4. From the Defined PMP Circuit Leafs list box, select the leaf to delete.
5. Choose Delete. A confirmation box appears.
6. Choose OK to continue.
7. Repeat Step 4 through Step 6 for each circuit leaf you want to remove from the PMP circuit. If you are deleting the circuit, delete all leafs.
8. Choose Apply.
9. Choose Close to return to the Modify PMP Circuit Leaf dialog box.
10. In the Circuit Root Name list box, verify the selected circuit is the one to delete. Also, in the Corresponding PMP Circuit Leafs list box, verify that no leafs are listed.
11. Choose Delete. A confirmation box appears.
12. Choose OK to delete the circuit root. The circuit is now deleted from the network.
13. Choose Close to return to the network map.

Configuring Multicast DLCIs

The Set Multicast DLCIs function enables you to add, modify, and delete Multicast DLCI configurations for a Frame Relay network. *You can define up to 32 multicast groups per switch.* You must first configure Frame Relay circuits to define the DLCIs. You then allocate these circuits as member DLCIs in the multicast configuration.

Cascade currently supports one-way multicast. A multicast DLCI enables the network to:

- Accept a frame on a single DLCI
- Replicate the frame
- Distribute the frame to multiple circuit destinations

This configuration requires you to enter a DLCI for a multicast group made up of several circuits. The DLCI represents the circuit endpoints. You must first configure the DLCIs, before you can allocate them as member DLCIs in the multicast group. Refer to Table 11-7 on page 11-20.

Multicast DLCI Member Limits

The number of multicast members supported on a card is a function of the number of bytes available on the card and the frame size being transmitted as follows:

```
member limit = bytes available / frame size
```

This formula determines the maximum number of multicast members supported at the egress card where the multicast DLCI actually occurs. In general, the number of multicast members supported decreases as the frame size increases.

The number of bytes available depends on the card type:

- All IOPA cards (UIO, DSX, T1, E1, etc.) have a maximum of 32000 bytes available.
- All IOPB cards (HSSI, ATM) have a maximum of 9500000 bytes.

> *The ATM CS and ATM IWU I/O modules do not support multicast DLCI.*

Table 11-21 lists common frame sizes and the maximum number of multicast members supported on both card types.

Table 11-21. Multicast DLCI Member Limits

Frame Size (in bytes)	IOPA Card Maximum Multicast Members	IOPB Card Maximum Multicast Members
64	514	14936
128	257	7468
256	128	3734
512	64	1867
1024	32	933
2048	16	466
4096	8	233
8160	4	117

If you have already configured a multicast DLCI, the dialog box displays this information. You can use the Modify or Delete commands to modify or delete multicast DLCI configurations.

Adding a New Multicast DLCI

To configure multicast DLCIs:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Multicast DLCIs. The Set All Multicast DLCIs dialog box appears as shown in Figure 11-20.

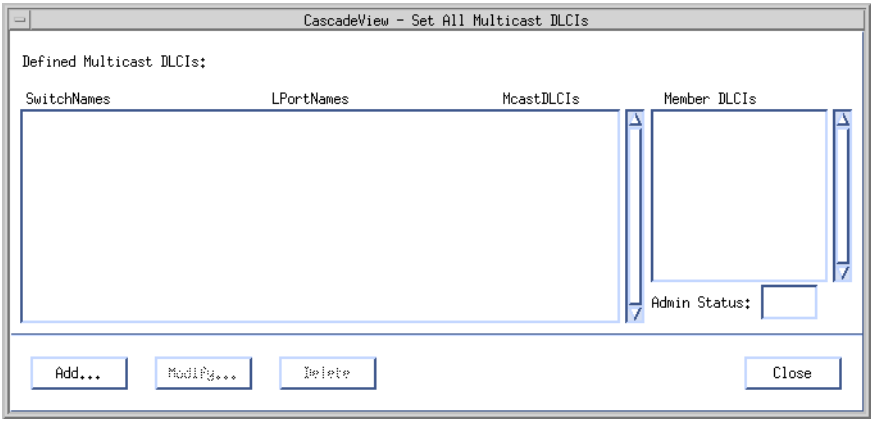


Figure 11-20. Set All Multicast DLCIs Dialog Box

2. Choose Add. The Select End Logical Port dialog box appears as shown in Figure 11-21.

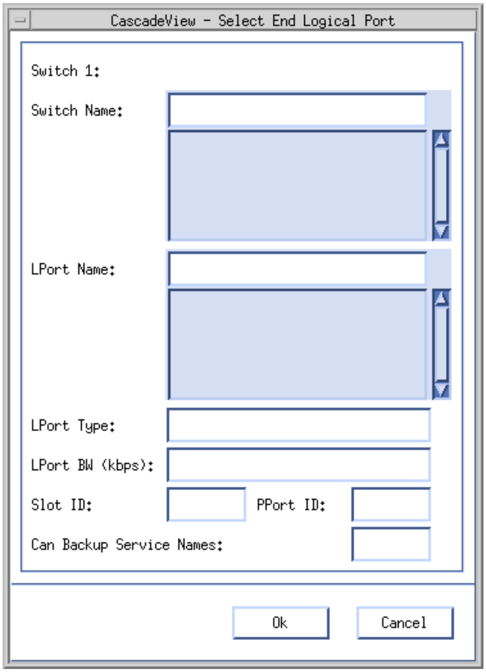


Figure 11-21. Select End Logical Port Dialog Box

3. Choose OK. The Add Multicast DLCI dialog box appears as shown in Figure 11-22.

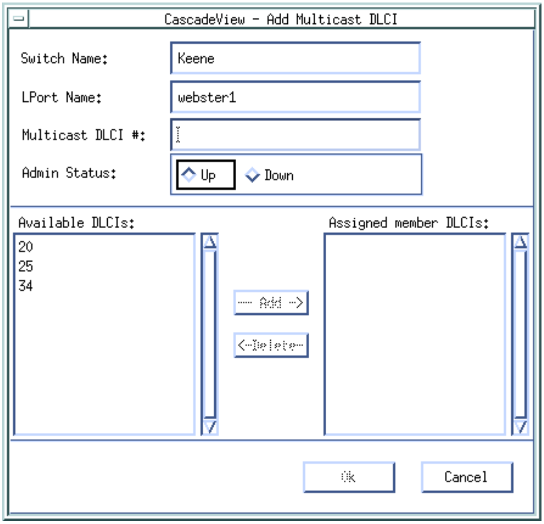


Figure 11-22. Add Multicast DLCI Dialog Box

4. Complete the required dialog box fields described in Table 11-22.

Table 11-22. Add Multicast DLCI Fields

Field	Action/Description
Switch Name	Displays the switch containing the multicast members.
LPort Name	Displays the name of the logical port to receive the multicast frames.
New Multicast DLCI #	Enter a DLCI number to identify the multicast group. For more information, refer to “About DLCI Numbers” on page 11-10.
Admin Status	Select *Down* or *Up* to indicate whether to activate the multicast DLCI when the switch or port comes on-line.

Table 11-22. Add Multicast DLCI Fields (Continued)

Field	Action/Description
Available DLCIs	Select the DLCIs (circuit endpoints) you want to allocate as members of the multicast group and choose Add. This DLCI now appears in the Assigned member DLCI list.
Assigned member DLCIs	Displays a list of the DLCIs you already selected for this multicast group. A multicast group must have at least one member. If you delete a circuit that is a member of a multicast group, the system automatically deletes it from the multicast group.

5. Choose OK to complete the configuration.

Configuring Management DLCIs

You use a Management DLCI when the NMS connects to a LAN via indirect Ethernet, i.e., the router provides the Frame Relay connection to the gateway switch. The NMS accesses the gateway switch through this router.

This access method enables you to monitor the network without the use of an Ethernet module in the switch. It also provides the flexibility to move the NMS from one LAN to another with few reconfiguration requirements.

Adding a New Management DLCI

To configure a Management DLCI:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Management DLCIs. The Set All Management DLCIs dialog box appears, listing the Management DLCIs already configured.

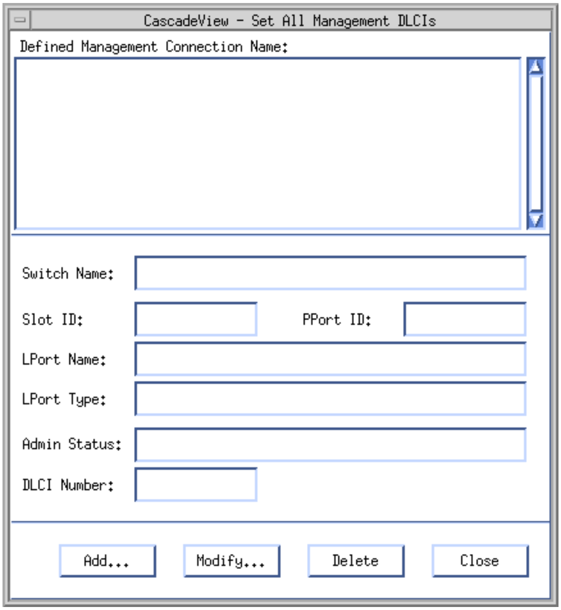


Figure 11-23. Set All Management DLCIs Dialog Box

> *If you have already configured a Management DLCI, the dialog box displays this information. You can use the Modify or Delete commands to modify or delete Management DLCI configurations.*

2. Choose Add. The Select End Logical Port dialog box appears as shown in Figure 11-24.

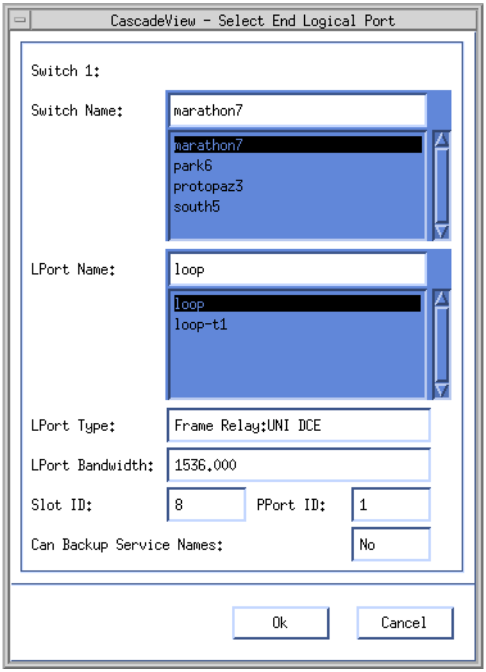


Figure 11-24. Select End Logical Port Dialog Box

3. Complete the required dialog box fields described in Table 11-23.

Table 11-23. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the name of the switch that connects to the router that serves as the Frame Relay interface for the Network Management DLCI.
LPort Name	Select the name of the logical port you configured for the router.
LPort Type	Displays the logical port type.
LPort Bandwidth	Displays the logical port bandwidth.

Table 11-23. Select End Logical Port Fields (Continued)

Field	Action/Description
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 Add Management DLCI dialog box appears as shown in Figure 11-25.

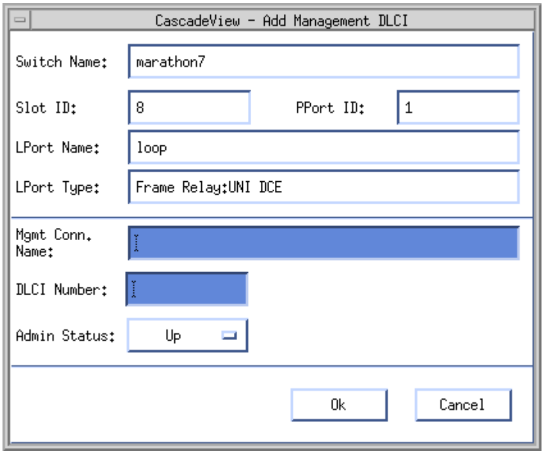


Figure 11-25. Add Management DLCI Dialog Box

5. Complete the dialog box fields described in Table 11-24.

Table 11-24. Add Management DLCI Fields

Field	Action/Description
Switch Name	Displays the name of the switch that connects to the router that serves as the Frame Relay interface for the Network Management DLCI.
Slot ID	Displays the I/O slot (number) in which the card resides.
PPort ID	Displays the port number for the physical port.
LPort Name	Displays the name of the logical port you configured for the router.
LPort Type	Displays the logical port type.
Mgmt Conn Name	Enter a unique, continuous, alphanumeric name to identify the DLCI. Do not use hyphens, dashes, parentheses, and asterisks.
DLCI Number	Enter the number that is used for the Management DLCI. For more information, refer to "About DLCI Numbers" on page 11-10.
Admin Status	Select either *Up* or *Down* to define whether the DLCI is activated when the switch or port comes online.

6. Choose OK to complete the configuration.

After configuring the Management DLCI, add an NMS path for the Management DLCI (refer to "Setting the NMS Path" on page 5-30). Also, enter a static route in the router to access the internal IP network.

Administrative Tasks

This section describes how to:

- Move circuit endpoints
- Use templates to define a new circuit
- Delete circuits

Moving Circuits

The Move Circuit function enables you to move circuit endpoints defined for one logical port (the source) to another logical port (the destination). If you are upgrading a switch and do not want to lose PVC connections, you can use this function to move circuits to another switch.

This function has the following restrictions:

- You cannot move circuits you previously defined as part of a fault-tolerant PVC configuration (defined with a service name or designated as a backup).
- You cannot move a circuit that is currently in use.
- You cannot move a circuit if you receive an error that indicates there is a problem acquiring a lock for the circuit and all associated logical ports.
- You cannot move a circuit that has a manually defined circuit path.
- You cannot define more than one circuit for a Frame Relay FRAD logical port.
- The DLCI must be unique to the destination logical port.
- You cannot move a circuit if the source logical port type is not a valid type for the destination port. For example, you cannot move a Frame Relay or SMDS logical port type to an ATM DS3 module.
- The move circuit function will fail if moving a circuit exceeds the maximum number of circuits allowed for the destination logical port.
- You cannot move a circuit that is a member of a multicast DLCI configuration.

To move a circuit:

1. From the Administer menu, select Cascade Objects:Move Circuit Endpoint. The Select Source & Destination LPorts dialog box appears as shown in Figure 11-26.

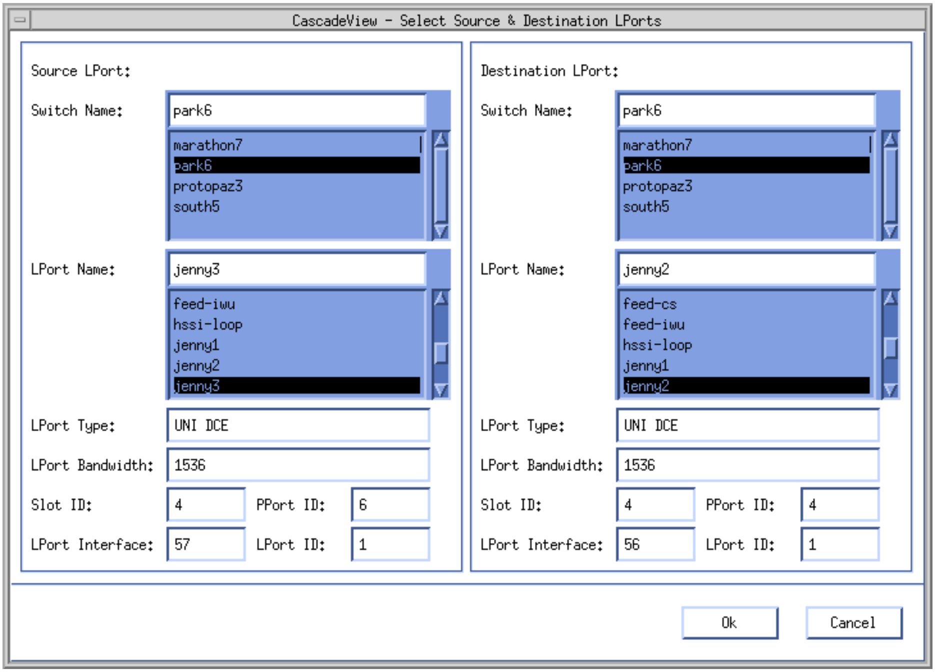


Figure 11-26. Select Source and Destination LPorts Dialog Box

2. Complete the following steps for the source logical port.

   a. Select the switch (name) that contains the circuit you want to move. A list of logical ports defined for this switch appears in the LPort Name field.

   b. Select the logical port (name) on which the circuit is defined. The fields below this list box display information about this port.

3. Complete the following steps for the Destination LPort.

   a. Select the switch (name) to which you want to move the circuit. A list of logical ports defined for this switch appears.

b. Select the logical port (name). The fields below this list box display information about this port.

4. Choose OK. The Move Circuit Endpoint dialog box appears as shown in Figure 11-27.

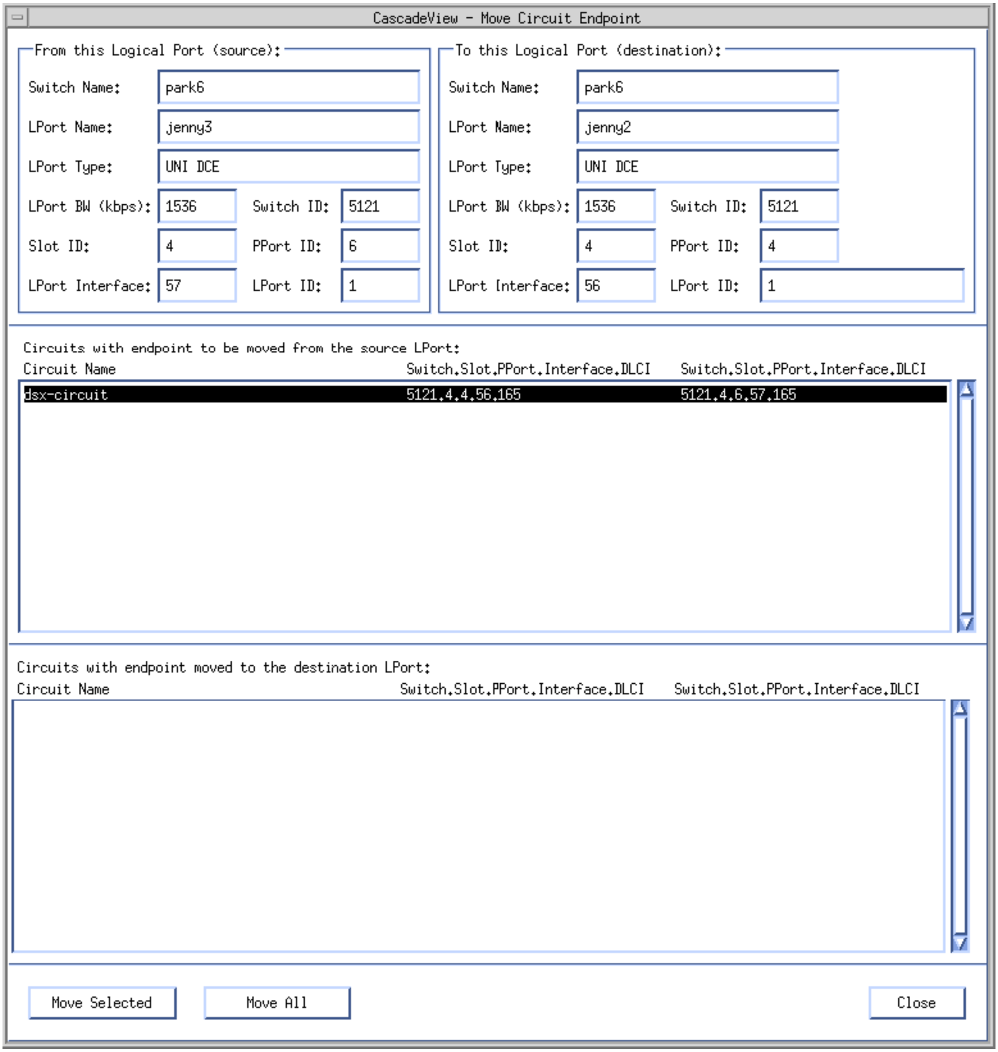


Figure 11-27. Move Circuit Endpoint Dialog Box

5. This dialog box displays the circuits that have the source logical port as an endpoint. From the *Circuits with endpoint to be moved from the source LPort* list box, select the circuit you want to move.

6. Do one of the following:

- Choose Move Selected. The selected circuit appears in the *Circuits with endpoint moved to the destination LPort* list box.

- Choose Move All if you are moving circuits with endpoints on a 10-port DSX or channelized DS3 I/O module. You do not have to highlight all circuits. The Move All command button enables you to move all circuits at the same time. This command button is only enabled if selected endpoints are on a 10-Port DSX or channelized DS3 I/O module.

  This process takes a few minutes, depending on the number of circuits.

7. Repeat Step 5 and Step 6 for each circuit you want to move.

8. If some circuits were not moved in this process, check the restrictions on page 11-81.

9. When you finish, choose Close.

Using Templates

If you defined a circuit configuration and saved it as a template (see *Is Template* field in Table 11-7 on page 11-20), you can define a new circuit using the same parameters.

To define a circuit from a template:

1. Choose the Add Using Template command on the Set All PVCs on Map dialog box (see Figure 11-2 on page 11-12).

2. Do one of the following:

   - Choose Last Template to use the last template you defined for this switch.

   - Choose Template List to display a list of templates defined for this map. Select a template and choose OK.

Deleting Circuits

To delete a circuit:

1. From the Administer menu, select Cascade Parameters ⇒ Set All Circuits. The Set All Circuits On Map dialog box appears.
2. To view the list of circuits, select the Search by Name field and press Return. If necessary, select each circuit and review each logical-port endpoint.
3. Select the circuit to delete.
4. Choose Delete.

12

Downloading the Configuration

This chapter describes how to initialize a switch configuration and download the initialization script file to the switch. The switch stores this configuration information on the Control Processor card, in 64 KB of battery backed-up memory called Parameter Random Access Memory (PRAM). The script download process enables the NMS to communicate with the switch. Once the switch is on-line, you use the Synchronize PRAM command (PRAM Synch) to send the specific configuration information (for logical ports, circuits, etc.) to the switch.

This chapter also describes three additional PRAM functions:

Upload PRAM — Enables you to compare the configuration file in switch PRAM to the configuration file in the NMS database. Refer to page 12-20 for details.

Erase PRAM — Enables you to clear a configuration file from switch memory. Refer to page 12-27 for details.

- **Generate PRAM** — Enables you to generate set commands to configure PRAM but does not upload the switch configuration file to the NMS. This allows you to view the file, before performing an upload. Refer to page 12-20 for details.

Downloading a Switch Configuration

After you define the switch configuration using CascadeView, you must create an initialization-script file and download it to the switch. You download a switch configuration file in the following sequence:

Step 1. Initialize each switch configuration to generate an initialization script file.

Step 2. Make a console connection to the switch.

Step 3. Execute the terminal emulation software.

Step 4. Download the script file to the appropriate switch.

Step 5. Synchronize the switch.

Initializing a Switch Configuration

The Initialize Switches 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 clear PRAM. Refer to either* “Clearing the STDX 3000/6000 Parameter RAM” on page 12-28 or “Clearing the B-STDX 8000/9000 Parameter RAM” on page 12-29.

Generating the Initialization Script File

To initialize switches, use the following steps:

1. 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.

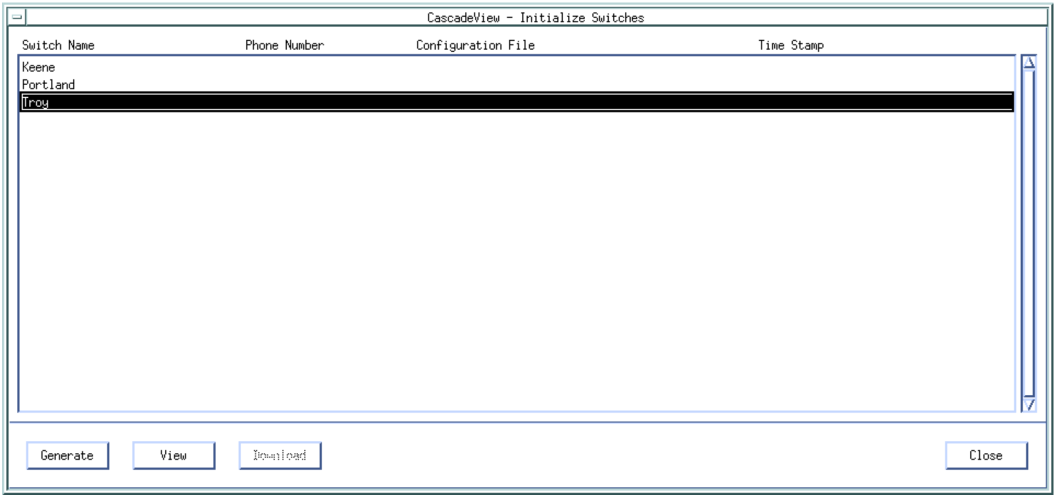


Figure 12-1. Initialize Switches Dialog Box

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. Proceed to the section, "Downloading the File to the Switch" on page 12-5.

Viewing the Initialization Script File

To view the initialization-script file before downloading it to the switch, use the following steps:

1. From the Initialize Switches dialog box, highlight the desired switch.
2. Choose View. The system displays the file contents as shown in the example in Figure 12-2.

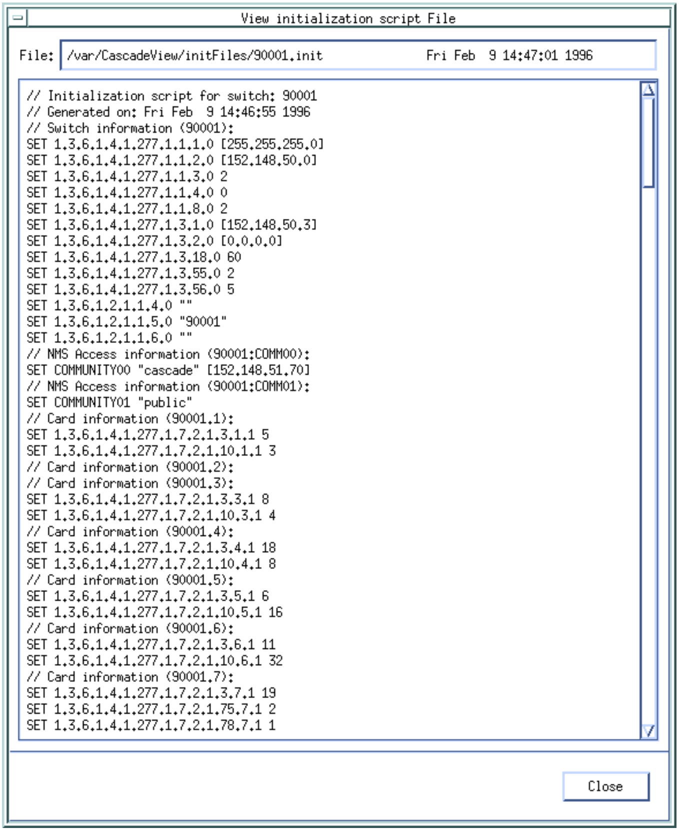


Figure 12-2. View Initialization Script File Dialog Box

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 three methods you can use to download the configuration text file from the NMS to the switch over a serial line:

Tip — The Solaris Tip program. Refer to the next section for instructions.

Terminal Emulation — PC which has a terminal emulation software. Refer to page 12-16 for instructions.

Kermit — Console port with the kermit mode protocol. Refer to page 12-9 for instructions.

Install Program — Enables you to connect to the console using a PC or terminal. Refer to page 12-7 for instructions.

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 d.*

To access the switch using tip, use the following steps:

1. In an xterm window, enter **su - root** and enter the root login and password.
2. Enter **tip hardwire**.

   You should get a connected message.
3. Enter **~#**.

   This command sends a break character to the switch. The console prompt appears.
4. Log in to the switch.
5. At the > prompt, enter the following:

   ```
   enable debug
   password: [your debug password]
   ```

   If you do not know your debug password, contact the Cascade Technical Response Center for assistance.
6. At the ## prompt, enter

   ```
   ## reset pram all
   ```
7. At the "Reset PRAM on all cards? Are you sure (YES/NO)?" prompt, enter **YES**.
8. At the ## prompt, enter

   ```
   ## reset system
   ```
9. At the "Are you sure (YES/NO)?" prompt, enter **YES**.

   The system displays the following message:

   ```
   resetting switch, stand by...
   ```

   Once the switch comes up (approximately 1-2 minutes), the >> prompt appears. This prompt indicates you successfully erased PRAM and the switch can accept a new initialization-script file (refer to "Downloading the Initialization File" on page 12-7). Before you download the file, verify that all IOPs are up by issuing a *show card* console command.

Downloading the Initialization File

You can access the script file in */opt/CascadeView/bin*. If you are using an STDX 3000/6000 switch, you must first convert the file to add a LF to LF-CR, using the unix2dos command. For example, enter

```
unix2dos shuttle38.init shuttle38.init
```

(where *shuttle38.init* is the name of the script file.)

To download the initialization file, use the following steps:

1. Open a second xterm window.
2. Enter the following command:

   ```
   ./script-download -in [ifn] -out [ofn] -linedelay [#in µsec]
   ```

   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*)

   [# in µsec] is the value of the line delay in microseconds (for example, use 300000 to use a 3/10th second line delay). Do not use a value less than 100000.

3. When you finish, type **~^D** in the xterm window to exit the Tip session.

> *Observe the switch on the network map. If the switch remains yellow and does not turn green within a few minutes, refer to the following section to synchronize the switch.*

If You Have Problems

If you have problems using Tip, review the following:

- For an STDX, if you receive the error message **tip:unknown host term**, your workstation may already have the *term* entry in the **/etc/remote** file. To use the Tip program's term command, type **vi /etc/remote** and press Return. Add the following entry to this file:

  ```
  term:\
  :dv=/dev/cua/a:br#19200:el=^C^S^Q^U^D:ie=%$:oe=^D:
  ```

  Type **:wq!** and press Return to exit vi and save your changes.

- If you receive the error "Couldn't open input file" when you ran script-download, enter the following command to change permissions on the /dev/cua/a device:

  ```
  chmod 666 /dev/cua/a
  ```

Using Terminal Emulation Software

You can use any commercially-available terminal emulation package to download the configuration text file from a PC. Refer to the user guide which comes with this package for specific instructions for downloading text files.

Whichever emulation package you use, make sure you set the following variables:

Transfer protocol — Set this to text mode transfer.

Line delay — Set this 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 Kermit

You can use the kermit function to transfer the configuration text file through the console port to the Control Processor card. The advantage of using kermit instead of Tip or a PC terminal emulator is that with kermit, you only have to download the PRAM files needed to establish a connection between the switch and the NMS. For gateway switches, you only need to download the CP PRAM file. For non-gateway nodes, you only download the CP PRAM file and the PRAM file of the IOP that provides the trunk connection to the gateway node.

Another advantage is that after the CP, PP, or IOP reboots with the PRAM file, you do not have to PRAM Sync the CP and IOP(s) that received the new configuration file.

To download the PRAM files to the switch using kermit, use the following steps:

1. Connect a console cable to serial port A on the back of your workstation. Refer to your workstation hardware guide to locate serial port A.

2. Use the Generate PRAM function (refer to page 12-20) to generate a configuration file for the CP and IOP(s).

    - *If this is a gateway switch*, you do not have to Generate PRAM for any IOPs.

    - *If this is not a gateway switch*, you must generate a PRAM file for the IOP that provides the trunk connection to the gateway node.

    - The NMS stores the generated PRAM files in the **/opt/CascadeView.var/cfgSyncFiles** directory. The directory which contains the PRAM files associated with B-STDX 9000 and BTDX 6000 switches running switch software release 04.02.00.00 code may look like the following:

    ```
    9000-04.02.00
    ```

3. When you look in this directory, you see a number of files that include the name of the switch associated with the file followed by a .Pslot number. For example, for switch Westford1, the CP PRAM file would look like **Westford1.P01**. If the PRAM file was from the IOP in slot 14, the PRAM file would look like **Westford1.P14**. These are the files you must transfer down.

4. From either the NMS or a PC, make a console connection to the switch (19200 bps).

5. At the console prompt, type **kermit** and press Return. This puts the console port in the kermit mode for file transfer.

6. Start a kermit session with binary file transfer mode selected.

7. Transfer the CP PRAM file. Once complete, the kermit session automatically closes out and the Diagnostic and CP should automatically warm boot.

8. (*Optional*) To transfer the IOP PRAM file(s), repeat Step 5 through Step 7.

9. Once complete, the NMS should be able to access the switch. If the Switch Back Panel dialog box (Figure 12-10 on page 12-19) displays any of the remaining IOPs in yellow, you can PRAM Synch them. Refer to Figure 12-9 on page 12-18 for instructions for using PRAM Synch.

Using the Install Program

You use the install program to enable a switch with no PRAM to communicate with the NMS. If you are using a direct-line trunk to connect to the NMS, record the information for the remote end of the trunk, port, and switch. You enter this information in "Using a Direct Line Trunk" on page 12-14.

To access the switch using the install program, use the following steps:

1. Using a PC or terminal, connect to the console (for example using Telnet).

2. At the [*switch name*] > prompt, enter the following:

   ```
   enable debug
   password: [your debug password]
   ```

   If you do not know your debug password, contact the Cascade Technical Response Center for assistance.

3. At the [*switch name*]## prompt, enter **Reset Pram all**.

4. At the "Reset PRAM on all cards. ARE YOU SURE <Yes|No>?" prompt, enter **YES**.

5. At the [*switch name*]## prompt, enter **reset system**.

6. At the "ARE YOU SURE <Yes|No>?" prompt, enter **YES**.

The system displays the following message:

```
RESETTING SWITCH, STAND BY ....
```

7. At the [*switch name*]>> prompt, enter **install**.

8. Enter the following information at the prompts:

   a. At the “Enter the node name” prompt, enter the name of the node to which you want to connect.

   b. At the “Enter the network number” prompt, enter the host IP address. (For example, the switch’s internal network number)

   c. At the “Enter the network mask: 255.255.255.0” prompt, do one of the following:

      - If you are using a Class C network, accept the default by pressing Return.
      - If you are using a Class B network, enter **255.255.0.0**

   d. At the “Select the DLCI addressing scheme (Global/Local)” prompt, do one of the following:

      - If you are using global DLCI addressing, enter **G**.
      - If you are using local DLCI addressing, enter **L**.

   e. At the “Enter the address of the switch” prompt, enter the switch’s address.

      By default, the system displays the first switch in the network. For example, if your host IP address is 152.148.50.0, the system displays 152.148.50.1. If this is not the address of the switch to which you want to connect, type the switch’s IP address and press Return.

   f. At the “Enter NMS IP address” prompt, enter the NMS IP address used to manage the switch.

   g. At the “Enter SNMP community name” prompt, enter the default community name **cascade**.

9. The system displays the following prompt and menu as shown in Figure 12-3.

```
Which interface will this switch use to communicate with NMS?
        1       Direct Line Trunk
        2       Direct Ethernet
        3       Indirect Ethernet(through a gateway)
        4       SLIP
        5       Frame Relay Trunk
        6       Management DLCI
Enter choice: █
```

Figure 12-3. Interface Menu

10. Select the type of connection you use to communicate with the NMS and press Return.

11. Do one of the following:

- If you selected 2 Direct Ethernet in Step 10, continue to the next section "Using Direct Ethernet".
- If you selected 1 Direct Line Trunk in Step 10, refer to "Using a Direct Line Trunk" on page 12-14.

Using Direct Ethernet

1. Enter the Ethernet IP address.

   The system displays the selected configuration as shown in Figure 12-4.

```
Configuration selected:
        Switch name:                            mc1
        Network:                                152.148.50.0
        Network mask:                           255.255.255.0
        DLCI scheme:                            Local
        Switch address:                         152.148.50.2
        NMS address:                            152.148.230.16
        SNMP community:                         cascade
        Interface->NMS:                         Direct Ethernet
        Ethernet IP:            152.148.231.137

Is this configuration correct? (Y/N): █
```

Figure 12-4. Direct Line Trunk Configuration Example

2. At the "Is this configuration correct (Y/N)" prompt, do one of the following

- If the configuration is correct, enter **Y**.
- If you need to change any information, enter **N**. Enter the correct information.

The system displays the following message:

```
committing

Preliminary installation completed!

Use NMS to complete the full installation.
```

3. At the “Press RETURN to reboot” prompt, press Return.
4. At the “[*switch name*]>> Press Break” prompt, press Break to disable the Telnet connection.
5. When prompted, enter your login and password.

   The system displays the configuration information for the selected switch.
6. At the > prompt, enter

   `enable debug`
7. At the Debug password prompt, enter your debug password. If you do not know your debug password, contact the Cascade Technical Response Center for assistance.
8. At the ## prompt, enter **next node**.

   The system displays the switch’s internal IP address, Ethernet IP address, and NMS IP address. The install program is complete.

Using a Direct Line Trunk

If you are using a direct line trunk to communicate with the NMS, the system displays the card type menu shown in Figure 12-5.

```
What card type is used for the trunk?
          1       8 port universal I/O
          2       4-port 24-channel Fractional T1
          3       4-port 30-channel Fractional E1
          4       10-port DSX1
          5       2-port HSSI
Enter choice: 1
```

Figure 12-5. Card Type Menu

1. Select the card used for the trunk and press Return.

2. Complete the following information at the prompts:

   a. At the “Enter the slot # of the card” prompt, enter the slot number.

   b. At the “Enter the port # of the trunk” prompt, enter the port number.

   c. At the “Enter the local trunk interface # of the trunk” prompt, enter the local trunk interface number.

   d. At the “Enter the remote trunk interface # of the trunk” prompt, enter the remote trunk interface number.

   e. At the “Enter the IP address of the SWITCH of the remote end [*switch’s IP address*]” prompt, enter the IP address of the remote switch.

   The system displays the menu shown in Figure 12-6.

```
Enter the clock selection:
        1       DCE
        2       Loop Timed DCE
        3       DTE
        4       Direct Trunk
Enter choice: 1
```

Figure 12-6. Clock Source Selection

3. Enter the clock source selection.

4. Select the clock speed in Kbps. The system displays the selected configuration as shown in Figure 12-7.

```
Configuration selected:
        Switch name:                          mc1
        Network:                              152.148.50.0
        Network mask:                         255.255.255.0
        DLCI scheme:                          Local
        Switch address:                       152.148.50.2
        NMS address:                          152.148.230.16
        SNMP community:                       cascade
        Interface->NMS:                       Direct Line Trunk
        IP address of SWITCH at the remote end: 152.148.50.2
        Remote trunk interface #:             1
        Card type:                            8 port universal I/O
        Slot number:                          3
        Port number:                          1
        Local trunk interface #:              1
        Clock source:                         DCE
        Clock speed:                          64 kbps

Is this configuration correct? (Y/N):
```

Figure 12-7. Sample Trunk Configuration

> *You may need to configure additional parameters, depending on the card type you are configuring. Contact the Cascade Technical Response Center for assistance.*

5. Continue with Step 2 on page 12-12.

Using the Synchronize PRAM Command

Whenever you download an initialization-script file from the NMS to the switch for the *first time*, you must synchronize PRAM (*PRAM Sync*) 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).

If you must synchronize a switch, the NMS displays the switch object in yellow. The Synchronize PRAM command enables you to correct inconsistencies between the NMS database and switch PRAM.

Before you synchronize a switch, verify that you have defined the following, as described in Chapter 5:

- ☑ NMS IP Address
- ☑ Community Name
- ☑ Read/Write privileges

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 30. 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/UX and more than 15 switches in the network. This change takes effect when you restart HP OpenWindows.

Refer to the following sections for information about synchronizing a switch:

- "Synchronizing an STDX 3000/6000 Switch" on page 12-17.
- "Synchronizing a B-STDX 8000/9000 Switch" on page 12-18.

Synchronizing an STDX 3000/6000 Switch

To synchronize an STDX 3000/6000 switch:

1. Select the switch to synchronize and from the Misc menu, select CascadeView ⇒ Logon and enter the operator password. (You can only synchronize one switch at a time.)

2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears as shown in Figure 12-8.

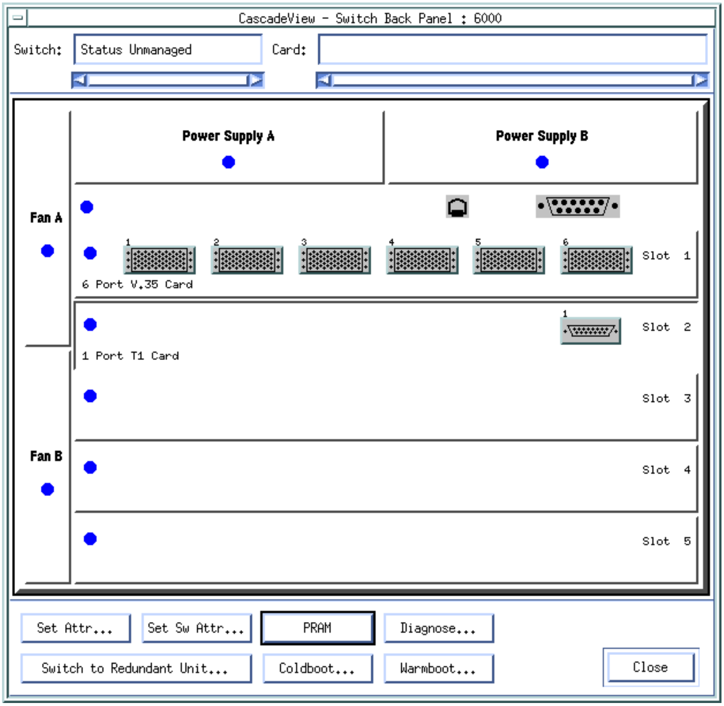


Figure 12-8. Switch Back Panel (STDX) Dialog Box

3. Choose the PRAM command. The Pram Sync dialog box appears.

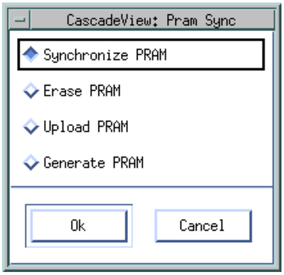


Figure 12-9. Pram Sync Dialog Box

4. Select Synchronize PRAM and choose OK. This sends the binary image of the configuration to the switch, causing it to perform a warm boot. When the switch reboots, all physical ports, logical ports, PVCs, and active sessions stall. If you have a heavily configured switch, it may take several minutes to reboot.

If you made only minimal changes to the switch configuration, you can synchronize PRAM at a later time to avoid interrupting network traffic.

Synchronizing a B-STDX 8000/9000 Switch

To synchronize an STDX 8000/9000:

1. Select the switch to synchronize and from the Misc menu, select CascadeView ⇒ Logon and enter the operator password. (You can only synchronize one switch at a time.)

2. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears as shown in Figure 12-10.

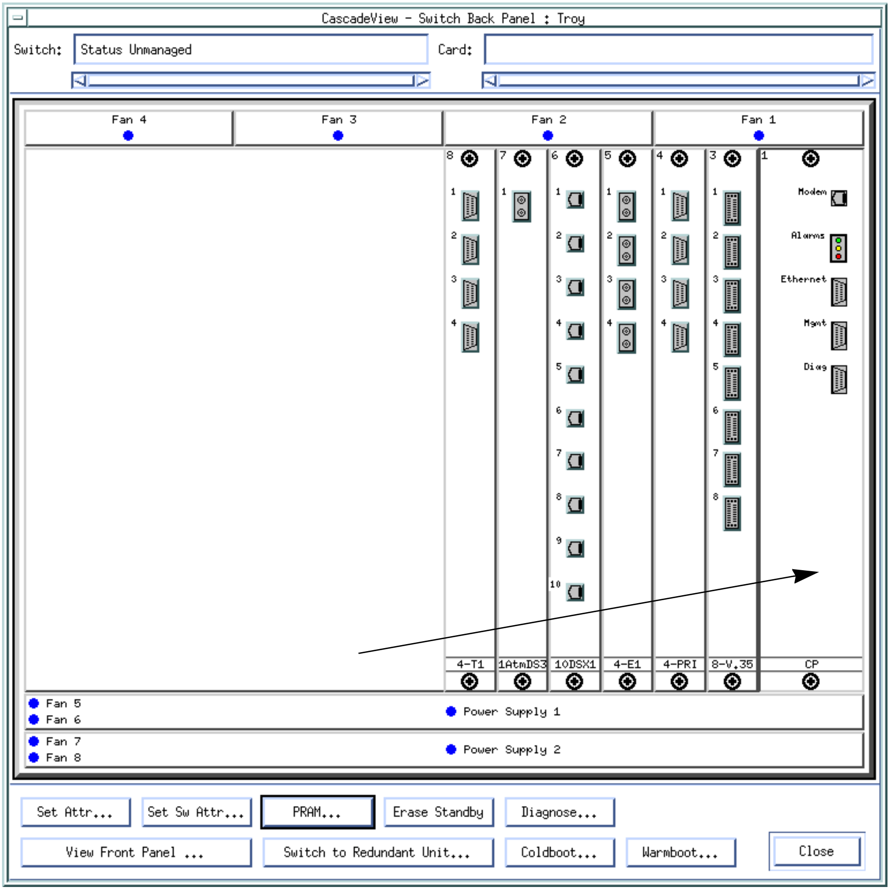


Figure 12-10. Switch Back Panel (B-STDX) Dialog Box

3. Select the I/O module to synchronize. For example, in Figure 12-10, Slot 1 is selected.

If you changed some switch attributes, such as the NMS path, you must synchronize the CP module before you synchronize any I/O modules. If you need to synchronize more than one module, always synchronize from the CP first. Then work your way toward the module that has the highest slot ID.

4. Choose the PRAM... command. The Pram Sync dialog box appears.

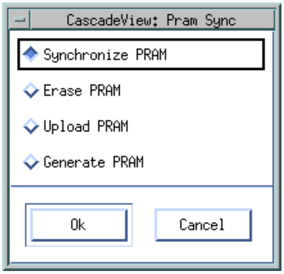


Figure 12-11. Pram Sync Dialog Box

5. Select Synchronize PRAM and choose OK. This sends the binary image of the configuration to the selected module, causing it to perform a warm boot. 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.

If you made only minimal changes to the configuration, you can synchronize PRAM at a later time to avoid interrupting network traffic.

Using the Generate PRAM Command

The Generate PRAM command generates set commands to configure PRAM but does not upload the switch configuration file to the NMS. This feature enables you to view the configuration file before uploading it to the switch.

Using the Upload PRAM Command

Occasionally the switch configuration file for a specific I/O module and the configuration stored in the NMS database do not match. This situation can occur when you upgrade your switch software, use a network management product to manage the switch, or use the MIB to change a switch configuration.

If you remove an I/O Module from one switch and install this module in a second switch, you get a PRAM conflict. This happens because the module contains an unknown configuration. Do not use PRAM upload to clear this condition. Instead, use the Erase PRAM function (page 12-27) to clear PRAM on this module; then reconfigure the module.

To resolve PRAM conflicts, use the Upload PRAM function to view the switch configuration file stored in PRAM. This enables you to compare the configuration file in the switch (PRAM) to the configuration file in the NMS database.

- **Use Upload PRAM** — To replace the configuration file in the NMS database with the switch configuration file.
- **Use Sync PRAM** — To replace the configuration file in switch PRAM with the one in the NMS database. Refer to page 12-8 for information.

The Upload PRAM function requires the following software:

- CascadeView/UX 1.5.x or above.
- Switch Release 4.0.3.xx or 4.1.x or above, where xx is greater than 50 for B-STDX 8000/9000 models.
- Switch Release 2.4 for STDX 3000/6000 models.

Supported Upload PRAM Objects

Upload PRAM currently supports the following objects:

- Physical ports
- Logical ports (except trunk ports)
- SMDS Individual Addresses
- SMDS Group Addresses
- SMDS Alien Addresses
- SMDS Address Screens

Guidelines for Using Upload PRAM

Before you use the Upload PRAM 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.
- If you need to add SMDS Group Addresses and Group Address members, upload PRAM information from the CP before you upload PRAM from an I/O module.
  - The CP upload creates the Group Address in the CP.
  - The I/O module upload adds the members into the Group Address.
- If you need to add SMDS Address Screens and Address Screen members, upload PRAM information from the CP before you upload PRAM from an I/O module.
  - The CP upload creates the Address Screen in the CP.
  - The I/O module upload adds the members into the Address Screen.
- Due to the interdependency of objects with other objects in the database, *be careful* when you use Upload PRAM to delete objects from the database. In general, do not create a situation where there are dangling objects (i.e., an object without a parent) in the switch before applying Upload PRAM.

For example, deleting a logical port without first deleting all associated individual addresses or address screens, creates dangling objects and causes a problem during the Upload PRAM process. Figure 12-12 shows the relationships (parent/child) that exist between CascadeView/UX objects in the database.

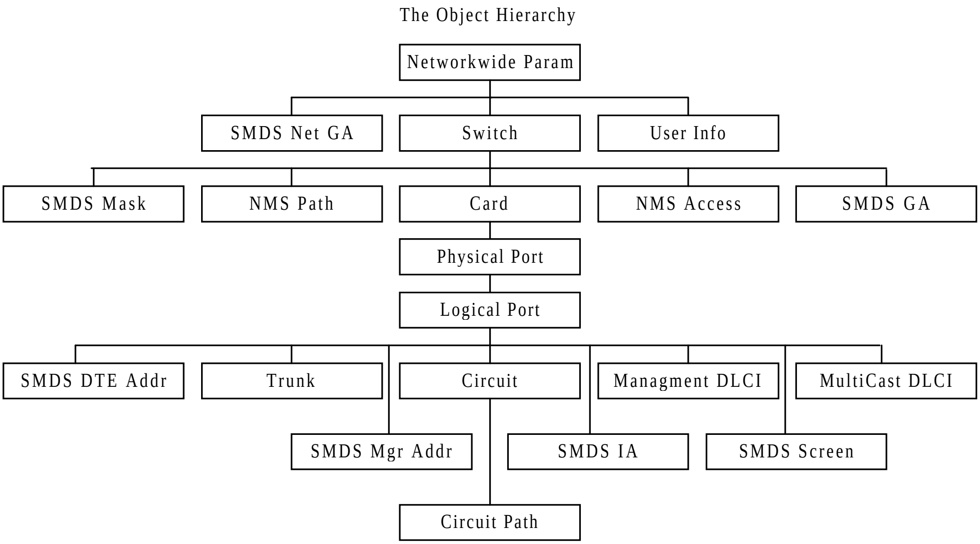


Figure 12-12. CascadeView/UX Object Hierarchy

Uploading a Switch Configuration File

To upload the switch configuration file stored in PRAM, use the following steps:

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, displaying the back panel of the selected switch.
3. Select either the I/O module or the CP module and choose the PRAM command. The CascadeView PRAM Sync dialog box appears.

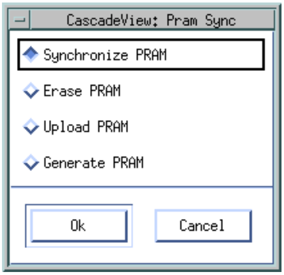


Figure 12-13. Pram Sync Dialog Box

4. Select Upload PRAM and choose OK. The Card PRAM Upload and NMS Synchronization dialog box appears as shown in Figure 12-14.

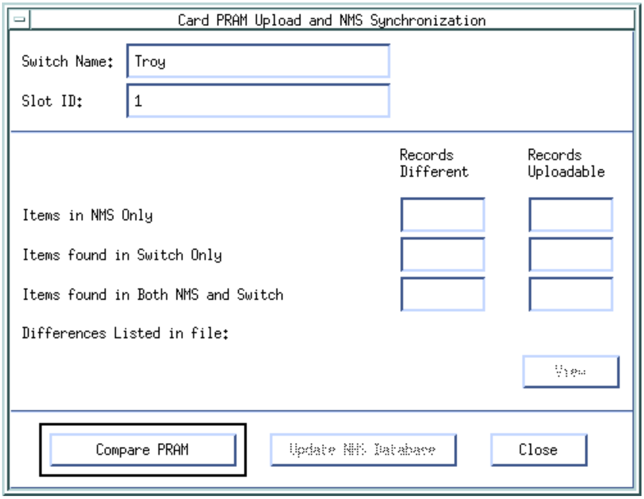


Figure 12-14. Card PRAM Upload and NMS Synchronization Dialog Box

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:

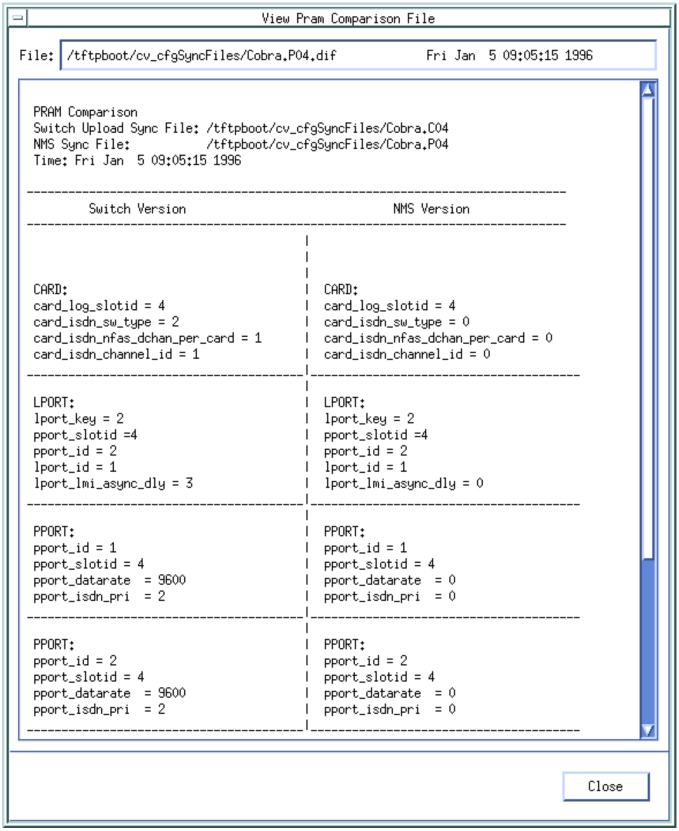
Items in the NMS only — The item exists in the NMS database, but not in the switch PRAM. This situation occurs when you make configuration changes to an unmanaged switch.

Items found in Switch only — The item exists in switch PRAM, but not in the NMS database. This situation occurs when 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 can happen if you modified the configuration directly from the console. For example, if you used console commands to change the admin status of a logical port, the logical port definition in switch PRAM indicates that the logical port is Down; the NMS database records indicate the logical port as Up. These discrepancies can also occur if a PRAM synchronization or SET fails.

The name and location of the file that stores the inconsistencies appears on the dialog box.

7. Choose View to compare the files. (See the example in Figure 12-15).



```
View Pram Comparison File

File: /tftpboot/cv_cfgSyncFiles/Cobra.P04.dif          Fri Jan  5 09:05:15 1996

PRAM Comparison
Switch Upload Sync File: /tftpboot/cv_cfgSyncFiles/Cobra.C04
NMS Sync File:           /tftpboot/cv_cfgSyncFiles/Cobra.P04
Time: Fri Jan  5 09:05:15 1996

------------------------------------------------------------------------------
        Switch Version                            NMS Version
------------------------------------------------------------------------------
                                        |
                                        |
                                        |
CARD:                                   |  CARD:
card_log_slotid = 4                     |  card_log_slotid = 4
card_isdn_sw_type = 2                   |  card_isdn_sw_type = 0
card_isdn_nfas_dchan_per_card = 1       |  card_isdn_nfas_dchan_per_card = 0
card_isdn_channel_id = 1                |  card_isdn_channel_id = 0
----------------------------------------|---------------------------------------
                                        |
LPORT:                                  |  LPORT:
lport_key = 2                           |  lport_key = 2
pport_slotid =4                         |  pport_slotid =4
pport_id = 2                            |  pport_id = 2
lport_id = 1                            |  lport_id = 1
lport_lmi_async_dly = 3                 |  lport_lmi_async_dly = 0
----------------------------------------|---------------------------------------
                                        |
PPORT:                                  |  PPORT:
pport_id = 1                            |  pport_id = 1
pport_slotid = 4                        |  pport_slotid = 4
pport_datarate  = 9600                  |  pport_datarate  = 0
pport_isdn_pri  = 2                     |  pport_isdn_pri  = 0
----------------------------------------|---------------------------------------
                                        |
PPORT:                                  |  PPORT:
pport_id = 2                            |  pport_id = 2
pport_slotid = 4                        |  pport_slotid = 4
pport_datarate  = 9600                  |  pport_datarate  = 0
pport_isdn_pri  = 2                     |  pport_isdn_pri  = 0
----------------------------------------|---------------------------------------

                                                                    Close
```

Figure 12-15. View PRAM Comparison File Dialog Box

8. Choose Close to return to the Card PRAM Upload and NMS Synchronization dialog box.

9. 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.

   - To use the configuration stored in the NMS database, choose Close. Use the Synchronize PRAM command to update PRAM (refer to page 12-8).

10. Repeat Step 3 through Step 9 for each I/O module to complete the configuration upload process.

> *If an error occurs during the upload process, a message dialog appears. After closing this dialog box, you can choose Update NMS Database to continue the upload process for the remaining physical port and logical port definition.*
>
> *If there are problems with the PRAM configuration file, refer to page 12-2 for instructions to download the configuration file stored in the NMS database.*

Erasing Parameter RAM

Occasionally you must download the initialization script file to switch PRAM again. You do this if you suspect the switch PRAM configuration file is corrupt. If you experience problems with a new release of switch software, you might also have to do this as part of a switch downgrade or upgrade procedure. To clear the existing switch configuration file from PRAM, use the Erase PRAM function.

Refer to the following sections for specific information about clearing PRAM on either an STDX 3000/6000 or a B-STDX 8000/9000:

- "Clearing the STDX 3000/6000 Parameter RAM" on page 12-28.
- "Clearing the B-STDX 8000/9000 Parameter RAM" on page 12-29.

Clearing the STDX 3000/6000 Parameter RAM

To remove an existing configuration from the STDX 3000/6000:

1. Install a console terminal to the Serial Management Port on the Packet Processor (PP).
2. Force a line break condition to the switch to display the > prompt.
3. At the > prompt, enter

   `login debug`

   `password: [your debug password]`

   If you do not know your debug password, contact the Cascade Technical Response Center for assistance.
4. At the ## prompt, enter

   `## reset pram`
5. At the "Are you sure (YES/NO)?" prompt, enter **YES**. (YES must be uppercase.)
6. At the ## prompt, enter

   `## reset system`
7. At the "Are you sure (YES/NO)?" prompt, enter **YES**. (YES must be uppercase.)

   The system displays the following message:

   `resetting switch, stand by...`

   Once the switch comes up (approximately 1-2 minutes), a >> prompt appears. This prompt indicates you successfully erased PRAM and the switch can access a new initialization script file download. Verify that all I/O modules are up and active.

Clearing the B-STDX 8000/9000 Parameter RAM

You can clear the existing PRAM configuration from the B-STDX 8000/9000 in the following ways:

Method 1 — Uses the NMS software to clear PRAM. This method is recommended operation.

Method 2 — Requires you to connect a console terminal and clear the PRAM on each I/O module slot number. Use this second method as a backup.

Method 3 —Use as a last resort and only *after consulting a Cascade Technical Response Center representative.*

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.

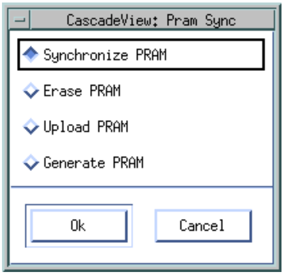


Figure 12-16. Pram Sync Dialog Box

4. 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 CP. (Refer to section “Connecting a Console” in the *B-STDX 8000/9000 Hardware Installation Guide* for details.)

2. Force a line break condition to the switch. Enter a minimum of three characters for login name, and enter a valid community name as the password (“cascade” is the default community name).

> *If you are using Console Authentication, call the Cascade Technical Response Center for assistance. For more information, refer to “Setting Authentication Parameters” on page 5-5.*

3. At the switchname> prompt, enter

```
enable debug
Debug password: [your debug password] (or cascade)
```

> *If you are erasing PRAM on all I/O modules in the switch, including the CP, clear the PRAM on the highest numbered slot first and continue to the lowest numbered slot (left to right).*

4. At the switchname ## prompt, enter

```
reset pram [#]
```

   (where [#] is the module or slot number. [All] will reset all cards.)

5. At the “Reset PRAM. Are you sure (YES/NO)?” prompt, enter **YES**.

6. At the switchname ## prompt, enter

```
reset system
```

   (this step reboots all modules)

7. At the “Are you sure (YES/NO)?” prompt, enter **YES**.

Once the switch comes up (approximately 1-2 minutes), a >> prompt appears. This prompt indicates that the PRAM is erased and the switch is waiting for a new initialization script file download. Verify that all I/O modules are up and in an active state.

Method 3

You should only use the following method as a last resort and only as instructed by a Cascade Technical Response Center representative.

1. Power off the switch.
2. Install a connection from the NMS SPARCstation to the B-STDX 8000/9000 network management port. (Refer to the *Cascade B-STDX 8000/9000 Hardware Installation Guide* for details.)
3. Set both of the two-position dip switches (located on the front of the CP) to the Off position (left).
4. Power on the switch.
5. Execute a terminal emulation session. Set the line parameters as follows: 19,200 baud, 8 bits, no parity.
6. On the terminal emulator, press Return. The following prompt appears:

   ```
   %
   ```

7. At the % prompt, enter

   `erase_pram`

8. Power-off the switch.
9. Set both of the CP's two-position dip switches to the On position, pointing to the right, away from the position numbers on the switch.
10. Power on the switch.

    Once the switch comes up (approximately 1-2 minutes), a >> prompt appears. This prompt indicates that PRAM is erased on the CP only, and the switch is ready for a new text file download.

Monitoring the Network Map

After you download a network configuration, you can monitor the status of a network map using the color-coded status indicators described in Table 12-1. The NMS also provides color-coded status indicators for trunk-line configurations (refer to "Trunk Coloring" on page 10-25).

Table 12-1. Network Map Status Indicators

Object Color	Description
Yellow	An I/O module in the switch may be out of synch. Display the Switch Back Panel dialog box and review the status of each module. If necessary, synchronize PRAM (refer to "Using the Synchronize PRAM Command" on page 12-16). If the switch does not turn green, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* to review background diagnostic statistics.
Wheat	The switch object is not managed. You *unmanage* an object to prevent the NMS from polling the object while you configure it. To manage an object, select Manage Object from the Map menu.
Red	The indicated object is in a failed state and cannot actively communicate with the NMS.
Green	The indicated objects/switches are actively communicating with the NMS.

For more information about monitoring the network, refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX*.

A

Upgrading to a B-STDX Switch

The SQR program *updswch20.sqr* enables you to upgrade an STDX 3000/6000 switch configuration to a B-STDX 8000/9000 configuration. This conversion program changes the graphic representation of the switch back panel to reflect the correct number of slots and CP card type for a B-STDX switch. For example, when you convert an STDX 6000 to a B-STDX 8000, the number of I/O slots changes from six to eight slots.

> *Before you begin the conversion process, back up the Sybase and HP OpenView databases. Refer to* *"ASCII Log File Example" on page 2-10.*

Switch Conversion Program

The switch conversion program converts specific card types from an STDX module to the appropriate B-STDX module and affects the following I/O modules:

STDX Module	Converted to B-STDX Module
6-port V.35	8-port UIO/V.35 interface
6-port UIO X.21	8-port UIO/X.21 interface
1-port channelized T1	4-port channelized T1
1-port channelized E1	4-port channelized E1

This conversion program updates physical port definitions to conform to their new card type. You can define new physical ports as necessary to complete your configuration.

Running the Conversion Script

To run the conversion script, you must know the STDX switch name. To convert attributes for a switch named main3000 to a B-STDX 9000 switch:

1. On the network map, select the switch object.
2. From the Map menu, select Unmanage Objects. The switch object turns to a wheat color indicating that the object is in an unmanaged state.
3. From the command window, type **updswch20.sh main3000 9000**. The conversion script generates a series of messages and reports errors, if any.
4. To remove the STDX switch object from the map, from the Edit menu, select Delete ⇒ From all submaps.
5. To create the B-STDX switch object on your network map, from the Edit menu, select Add Object. The Add Object:Palette dialog box appears.
6. Scroll through the Object Palette to locate the Cascade Object symbol.
7. Select Cascade Object. The Symbol Subclasses for Class Cascade Object appear.

8. Add the Cascade object (B-STDX 8000 or B-STDX 9000) to the network map . To do this, position the mouse pointer on the object, hold down the middle mouse button, drag the object to the map, and then release the mouse button. The Add Object dialog box appears as shown in Figure A-1.

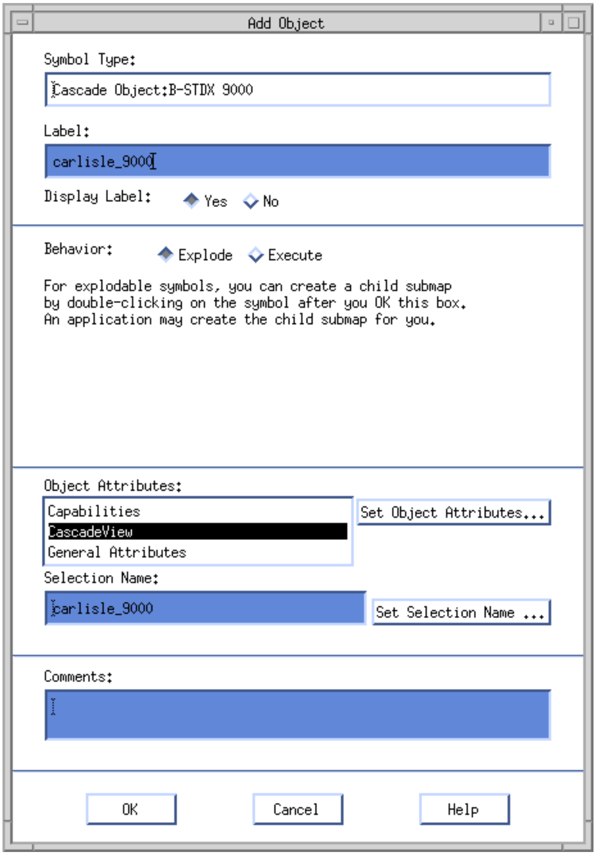


Figure A-1. Add Object Dialog Box

9. Complete the required dialog box fields described in Table A-1.

Table A-1. Add Object Fields

Field	Action/Description
Symbol Type	Displays the type of switch (object) you selected to add to the network map (STDX 3000, STDX 6000, B-STDX 8000, B-STDX 9000 or Cascade 500).
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/UX 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 Add Object – Set Attributes dialog box appears as shown in Figure A-2.

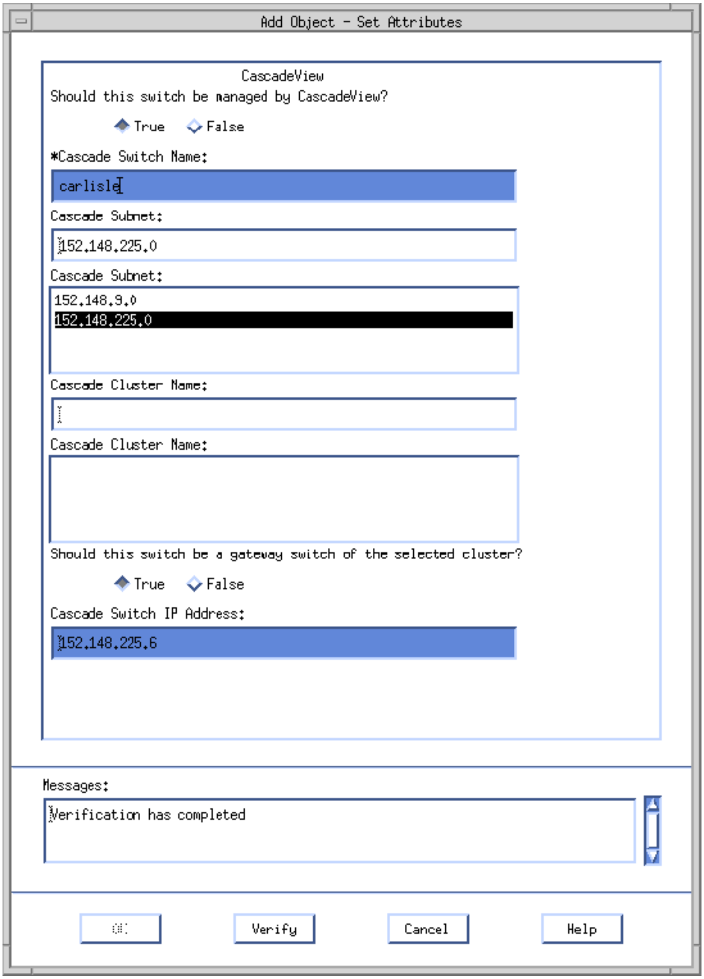


Figure A-2. Add Object - Set Attributes Dialog Box

10. Complete the required dialog box fields described in Table A-2.

Table A-2. Add Object - Set Attributes Fields

Field	Action/Description
Should this switch be managed by CascadeView?	Select *True*.
Cascade Switch Name	Enter a unique name for the switch.
Cascade Subnet	Highlight the Cascade subnet to which this switch belongs.
Cascade Cluster Name	Displays the name of the cluster to which this subnet belongs. Refer to "Creating a Cluster" on page 4-13 for more information.
Should this switch be a gateway switch of the selected cluster?	Select *True* to make this a gateway switch. Select *False* if you do not want this switch to be a gateway switch for the selected cluster.
Cascade Switch IP Address	Displays the switch's IP address. Every time you add an object to the map, CascadeView/UX increments the last octet (host id) by 1. If the next host id number is already used in the network, CascadeView/UX selects the next available number. If you want an IP address other than the displayed address, you can manually change the last octet. If you created a cluster, the IP address range is displayed as shown in Table 4-5 on page 4-13.

11. Choose Verify to confirm your settings. The message appears in the Message field, "Verification has completed".

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.

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

    Notice that the Selection Name field automatically defaults to the value you entered for the Label name. The Selection Name must be a unique name throughout all OpenView objects. Cascade recommends you leave the selection name as it appears. Enter any additional information in the Comments field.

13. Choose OK. The Add Object Palette reappears.

14. Choose OK. The network map displays an object icon representing the switch you just added. At this point the object appears blue and quickly turns to red to indicate that the NMS cannot access the switch.

15. 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.

16. From the Monitor menu, select Cascade Objects ⇒ Show Detail. The Switch Back Panel dialog box should display a B-STDX back panel, with the appropriate I/O modules installed.

B

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.

Table B-1 describes the main parameters used to configure CascadeView to use the Poll Server function.

Table B-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 B-2). ***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 B-2 describes the main parameters used to configure the Poll Server function.

Table B-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 B-1). 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 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 these steps will no longer use the Poll Server.

C

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. This option enables you to control circuit creation on your physical ports based on the specified cell loss ratio objective. If you try to create a circuit which causes the cell loss ratio to exceed the specified objective on a given physical port or exceeds the configured logical port bandwidth, the circuit will not be created.

This section also describes how to configure a customized CAC to optimize your network resources. This option enables you to control the amount of bandwidth that is reserved for VBR-RT and VBR-NRT circuits.You can control the amount of bandwidth reserved based on the physical port type, or based on configurable ranges of SCR requirements for a given circuit, or both.

Quality of service on the network is not guaranteed when using the customized CAC.

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 and VBR-NRT 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.

Tuning the Cascade CAC

The Cascade CAC can be tuned by specifying 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

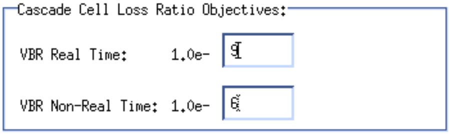
- The creation of the circuit would potentially cause the cell drop ratio to exceed 1 in 100,000

YOU CAN ADJUST THE CAC WHEN YOU FIRST CONFIGURE A SWITCH. DO NOT ADJUST THE CAC ONCE YOU HAVE ACTIVE CIRCUIT TRAFFIC ON THIS SWITCH.

To tune the Cascade 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.

3. If it is not already selected, choose Cascade as the CAC Implementation. The Cell Loss Ratio Objectives area of the screen becomes accessible, and the Customized CAC fields are grayed out.



4. In the 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).

5. When you finish, choose OK to send the values you entered to the selected switch.

To send these values to another switch on the network map, select that switch, access this screen again, and choose OK.

About the CAC Option

The customizable CAC option enables you to control the amount of bandwidth that is reserved for VBR-RT and VBR-NRT circuits.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, the following formula determines the amount of bandwidth that is required for a given circuit:

$$\mathbf{Bwidth_{req} = SCR*F_1*F_2}$$

where F_1 is the physical port factor (entered as a percentage), and F_2 is the SCR range factor (also entered as a percentage). You can configure only an F_1 factor, only an F_2 factor, or both factors. If you do not configure one of these factors, then the value of that factor is, by default, 100%.

Example

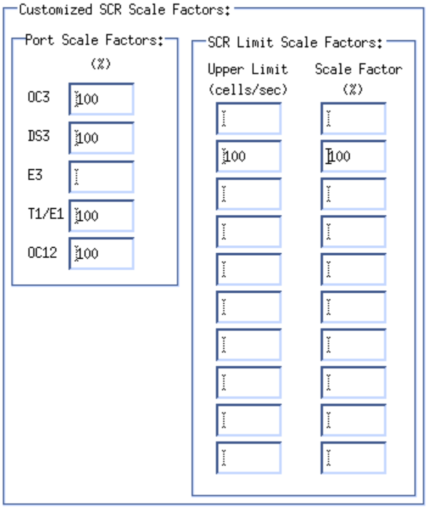
A circuit request is made, and the circuit needs to reserve bandwidth based on an SCR of 10,000 cells/sec. You configure the F1 factor for DS3 ports at 150%, the F1 factor for OC3c ports at 80%, and the F2 factor for circuits with an SCR from 8,001-15,000 cells/sec at 80%.

- 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 bandwidth requirements of the circuit 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.
3. If it is not already selected, choose Custom as the CAC Implementation. The Customized CAC area of the screen becomes accessible, and the Cascade CAC fields are grayed out.



4. *If you want to customize the CAC at the physical port level*:

   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.

5. If you want to customize the CAC based on the SCR of variable bit rate circuits:

   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 charts show 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, and 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 an allocated bandwidth of 15,000 cells/sec (assuming you did not define physical port scale factors).

c. When you finish, choose OK to send the specified values to the selected switch.

To send these values to another switch on the network map, select the switch, access this screen again, and choose OK.

D

DSX to DS3 Conversion

You must run the conversion procedure when you:

- Replace a 10-port DSX card with a channelized DS3 card
- Convert a channelized DS3 card back to a 10-port DSX card

Refer to the following sections for these procedures:

- "Converting a DSX Card to a Channelized DS3 Card" on page D-2
- "Converting a Channelized DS3 card to a DSX Card" on page D-4

Converting a DSX Card to a Channelized DS3 Card

When you convert a 10-port DSX card to a channelized DS3 card, the first 10 logical ports on the DSX card are converted into the first 10 channels on the channelized DS3 card. *Channels 11-28 must not be configured*.

This conversion process requires you to:

1. Install the conversion procedure by running the INSTALL script.

2. Run the conversion procedure.

> *You must be running switch code 4.1.5x.x before you convert a DSX card to a channelized DS3 card. If you are not running 4.1.5x.x, you must upgrade the switch.*

Installing the Conversion Procedure

The INSTALL script creates the *cv_ds3_2_dsx* and *cv_dsx_2_ds3* files. In the database, these files convert a DSX card to a channelized DS3 card, and a channelized DS3 card to a DSX card.

To install the conversion procedure:

1. Verify that you are the root user. You should see a # prompt.

2. Enter the following command to start the INSTALL script:

   ./INSTALL_cv_dsx_2_ds3

   The following message appears:

   ```
   Installing conversion procedures.
   ```

3. Respond to the following prompts:

```
Do you want to Install the conversion procedures [y/n].
```

a. Enter **y**.

```
Enter the Sybase database server name (default: "CASCADE").
```

b. Press Return to accept the default.

```
Enter the Sybase system administrator user name (default:
"sa").
```

c. Press Return to accept the default.

```
Enter the Sybase system administrator password (default:
"").
```

d. Type your sa password.

```
Enter the CascadeView database name (default: "cascview"):
```

e. Press Return to accept the default.

```
Enter the CascadeView database USER name (default:
"cascview").
```

f. Press Return to accept the default.

The following messages appear:

```
Installing cv_dsx2chds3 into Database ...

Installing cv_chds32dsx into Database ...

Done.
```

Running the Conversion Procedure

The *cv_dsx_2_ds3* file converts the DSX card to a channelized DS3 card in the database.

To run the conversion procedure:

1. Verify that you are logged in as the root user. You should see a # prompt.
2. Enter the following command:

   cv_dsx_2_ds3 <CV DB username> <CV DB password> SwitchName Slot#

   for example: ./cv_dsx_2_ds3 cascview cascview Switch1 12

   This string converts the 10-port DSX card in switch 1, slot 12 to a channelized DS3 card.
3. Replace the 10-port DSX card in the switch with a channelized DS3 card. (For replacement instructions, refer to the *B-STDX 8000/9000 Hardware Installation Guide*.)
4. Perform a “PRAM sync” on the CP card and the channelized DS3 card.

Converting a Channelized DS3 card to a DSX Card

When you convert a channelized DS3 card back to a 10-port DSX card, you can move logical ports from the channelized DS3 card that are defined from Channels 1 to 10 only. *Channels 11-28 must not be configured*. This conversion should only be used as a fall-back plan. In the database, the *cv_ds3_2_dsx* file converts the channelized DS3 card to a 10-port DSX card.

To convert a channelized DS3 card to a 10-port DSX card:

1. Install the conversion procedure as described in “Installing the Conversion Procedure” on page D-2.
2. Verify that you are logged in as the root user. You should see a # prompt.

3. Type the following command:

   cv_ds3_2_dsx <CV DB username> <CV DB password> SwitchName Slot#

   for example: ./cv_ds3_2_dsx cascview cascview Switch1 12

   This string converts the channelized DS3 card in switch 1, slot 12 to a 10-port DSX card.

4. Replace the channelized DS3 card in the switch with a 10-port DSX card. (For replacement instructions, refer to the *B-STDX 8000/9000 Hardware Installation Guide*.)

5. Perform a "PRAM sync" on the CP card and the 10-port DSX card.

> *When you convert back to a channelized DS3 card, Multiple Service Values are not available in CascadeView since only FR is recognized. The Application Mode value, DSX Line Length, and DS3 Line Buildout values are lost.*

E

The cascadeview.cfg File

This appendix describes the CascadeView/UX defaults configuration file, cascadeview.cfg. This file contains the default variables for many features used on the STDX 3000/6000, the B-STDX 8000/9000, and the CBX 500 switches. This file is located in the /opt/CascadeView/etc/ directory.

To view the contents of this file, type:

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

Whenever you modify this file, you must stop and then restart CascadeView/UX for the changes to take effect. Refer to the *Network Management Station Installation Guide* if you need instructions for 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-err
ors.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.xxx.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=cascade
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=300
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
#
# 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 60). > 0 - use
this value.
CV_MAX_INTERFACES_PER_STDX=150
export CV_MAX_INTERFACES_PER_STDX
#
# CascadeView Variables for using Poll Server.
#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
#
#  Override default max LPorts per STDX 3000/6000.
#  <= 0 or missing - use default. > 0 - use this value.
CV_MAX_INTERFACES_PER_STDX=0
export CV_MAX_INTERFACES_PER_STDX
#
# Using Poll Server
#CV_POLL_SERVER_PORT=10888
#CV_POLL_SERVER_ADDRESS=localhost
#export CV_POLL_SERVER_PORT CV_POLL_SERVER_ADDRESS
#
#  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
#
# 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/UX 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 Chapter 4 for more information about configuring the network number.

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 (*BSTDX 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, this value may need to be extended 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/UX 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 3.0 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 5-26 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.

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/UX 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/UX. 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/UX, 60 seconds is a good 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_DISABLE_SMDS_SS=0 (*B-STDX only*) — Use this variable to enable (0) or disable (1) the SMDS switching system for the entire CascadeView/UX 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/UX. For more information about the Audit Trail utility, refer to page 2-8.

CV_OUT_OF_SYNC_REFRESH_CNT=0 — The map you display in each session of CascadeView/UX refreshes every N node polls, where N is the number of specified node polls. To refresh, CascadeView/UX checks the database for any out-of-synch 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 t a public network. It is set to Private if this connection resides completely within a private network.

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.

CV_ENABLE_MOVE_ALL_CIRCUIT=TRUE — If this variable is set to True, the Move Circuit functions is enabled for this network. If it is set to False, it is disabled.

CV_POLL_SERVER_PORT=10888 — The port CascadeView polls when using the Polling Server. The default value is 10888. This environment variable is required. The value must match the POLL_SRV_SRV_PORT.

CV_POLL_SERVER_ADDRESS=localhost — IP address (in dot notation) of the node used to run the Poll Server. If the Polling Server runs on the same node as CascadeView, a value of "`localhost`" can be used. This variable is required to use the Polling Server. Setting this and CV_POLL_SERVER_PORT enables the Poll Server.

CV_MV_CKT_CARD_TYPE_CHECKING=TRUE — The Move Circuit function fails if the number of circuits moved exceeds the maximum allowed for the card. 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.

F

Glossary

A

absolute congestion

In Frame Relay, a congested condition in the network that occurs when the queue length reaches a third threshold (64 buffers full), and there is no more room on the queue for any packets, regardless of the type of packet.

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*.

address mask

A bit combination used to describe which portion of an address refers to the network (or subnet) and which part refers to the host. Sometimes referred to as mask. See also *subnet mask*.

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.

alternate mark inversion

A signaling format used in T1 lines that provides for the “one” pulses to have an alternating polarity. 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.

amber frames

Cascade's categorization of packet frames that are forwarded with their Discard Eligible (DE) bit set. If amber packets pass through a congested node, they are eligible for discard. Green, amber, and red frames describe and categorize packet frames for rate monitoring and rate enforcement in Frame Relay networks.

American National Standards Institute (ANSI)

A private, non-governmental, non-profit organization, which develops US standards required for commerce.

American Standard Code for Information Interchange (ASCII)

A code representing characters in binary form.

AMI

See *alternate 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*.

Annex D

A synchronous polling scheme used for the link management of a Frame Relay channel, where the user polls the network to obtain status information on the PVCs configured on the channel. Annex D exchanges this information using DLCI 0.

ANSI

See *American National Standards Institute (ANSI)*.

area id

See *area number*.

area number

One of two portions of the SMDS address, which can start at any digit and the length can be up to eight digits (4 bytes long for BCD encoding).

ASCII

See *American Standard Code for Information Interchange (ASCII)*.

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

A power supply's ability to adapt to the voltage that is being received from the power source.

B

B8ZS

See *bipolar 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 background to provide current operating status for all active switches. These programs do not interfere with switch operations.

Backward Explicit Congestion Notification

A bit in the Frame Relay header that indicates the frame has passed through a congested node from traffic traveling in the opposite direction.

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 users to dial up additional bandwidth as their applications demand.

baud rate

The number of signaling units (in bits per second (bps)) on a serial link.

Bc

See *Committed Burst Size*.

Be

See *Excess Burst*.

BECN

See *Backward Explicit Congestion Notification*.

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 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 (bps)

The number of bits transmitted every second during a data transfer.

blue alarm

An alarm signal, both on the NMS and switch, indicating that an excessive number of one pulses are being received.

BNC connector

A small connector with a half-turn locking shell for coaxial cable. Used with thin Ethernet cabling, E3, and DS3 ATM.

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 (bps)*.

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).

C

Carrier Sense Multiple Access with Collision Detect (CSMA/CD)

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. CSMA/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-switch network.

CascadeView/UX

The UNIX-based graphical user interface used to configure and monitor a Cascade network.

CBR

See *Constant Bit Rate (CBR)*.

cell

Any fixed-length data 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 cell over a packet-switched network. Asynchronous Transfer Mode (ATM) is a type of cell relay 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 56/64K time slots to time-division multiplexed (TDM) signals for transmission within 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.

CIR

See *Committed Information Rate*.

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 with Collision Detect (CSMA/CD)*.

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.

Committed Information Rate

The rate at which the network agrees to transfer information under normal conditions. The rate is averaged over a minimum increment of time, Tc. See also *bandwidth*.

Committed Rate Measurement Interval

The time interval during which the user is allowed to send only Bc committed amount of data and Be excess amount of data. In general, the duration of Tc is proportional to the burstiness of the traffic. Tc is computed from CIR and Bc as Tc=Bc/CIR.

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 operate at their highest utilization. Congestion is handled by employing congestion avoidance and congestion control. See also *mild congestion*, *absolute congestion*, and *severe congestion*.

connectivity

The degree to which any given computer or application can cooperate with other network components in a shared-resource network environment.

Constant Bit Rate (CBR)

A Quality of Service (QoS) class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure cell delivery with constant timing.

Control Processor (CP)

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 IOP modules (IOPs).

CP

See *Control Processor (CP)*.

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 with Collision Detect (CSMA/CD)*.

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.

D

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, that indicates 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 (e.g., Frame Relay to ATM).

Data Link Connection Identifier

A 10-bit address that identifies Frame Relay PVC addresses. See also *Local Management Interface* and *globally significant DLCI*.

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, that indicates 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

In ISDN, the data channel that is used for control signals and customer data. In Primary Rate Interface (PRI) ISDN, the D-Channel operates at 64 KB for E1 and 16 KB for T1.

DE

See *Discard Eligible (DE)*.

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 (versus standard service 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 package (DIP) 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 (DE)

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.

DLCI

See *Data Link Connection Identifier*.

domain

In the Internet (IP), a network community of users sharing the same database information.

DS

See *Digital Signal (Digital Service)*.

DS0

A 64-Kbps channel used in T1 transmission. There are 24 DS0 channels in a T1 line.

DS1

Signaling definition for North American T1 lines, 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 package (DIP) switch

A small mechanical switch or jumper used to set the operating mode of a device.

duplex channel

A channel that can transmit and receive at the same time. This type of transmission is called full-duplex operation.

DXI

See *Data Exchange Interface*.

dynamic routing

A routing technique that allows a message to change its path “en route” through the network.

E

E1

The international 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 placed in the payload 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 with Collision Detect (CSMA/CD)*.

ESF

See *Extended Superframe Format*.

Ethernet

A popular LAN protocol and cabling scheme with a transfer rate of 10/100 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 data-link layer addressing scheme. Compare with *Internet Protocol address*.

Ethernet packet

A variable-length unit of data transmitted on a 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.

Extended Superframe Format

A T1 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 (RBS) 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

In Frame Relay, a set of backup ports (PVCs), defined on the B-STDX 8000/9000 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 Frame Relay circuits to the defined backup ports.

F

FCS

See *Frame Check Sequence*.

FDDI

See *Fiber Distributed Data Interface*.

FDM

See *Frequency-Division Multiplexing*.

FECN

See *Forward Explicit Congestion Notification bit*.

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 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, 56/64-Kbps time slots (DS0s). Customers can lease as many of these channels as needed; they are not required to lease all 24 channels in one circuit.

FRAD

See *Frame Relay Assembler/Disassembler*.

frame

A variable-length block of data transmitted as a single unit. Compare with *cell*.

Frame Check Sequence

In a frame, a field that contains the standard cyclic redundancy check used to detect errors in frames. See also *Cyclic Redundancy Check*.

Frame Relay

A type of data transmission based on a packet-switching protocol with transmission rates up to 45 Mbps. Frame Relay provides statistical multiplexing of data.

Frame Relay Assembler/Disassembler

A function that enables a logical port to perform Frame Relay encapsulation/de-encapsulation for HDLC/SDLC-based protocols. The FRAD function encapsulates HDLC/SDLC traffic entering a Cascade Frame Relay network and de-encapsulates it upon exiting the network. This function is restricted to one point-to-point PVC.

Frame Relay RFC 1294 Multiprotocol Encapsulation

A specification, superseded by RFC 1490, describing encapsulation of multiple protocols over Frame Relay. Rates typically support RFC 1490 to provide connectivity to Frame Relay switches.

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 channel*.

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.

G

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*.

globally significant DLCI

In configuring a Frame Relay network, a feature that requires DLCIs be unique across all ports. Compare with *locally significant DLCI*.

good LED

A green status indicator on a Cascade switch that indicates normal system status and operation during the system-boot process.

graceful discard

When enabled, this function turns “red” frames into best-effort frames. When disabled, this function discards frames.

green frames

Cascade's convention used to identify packet frames as they travel through a Frame Relay network. Green frames are never discarded by the network except under extreme circumstances, such as node or link failure. See also *amber frames* and *red frames*.

group addressing

The ability to send a single datagram/packet to multiple locations simultaneously.

guaranteed packets

Data delivered according to some time constraint with high reliability.

H

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 operate over 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 crossed 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-switch 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.

I

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.

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 IOP and IOP Plus modules in a switch. IOA configurations vary according to the specific IOP module they support.

Input/Output Processor

A module in a switch that manages the lowest level of a node’s trunk or user interfaces. An IOP 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.

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 that enables the Cascade switch to provide the transmit and receive clocks (clock source) to user equipment.

internal testing

A hardware diagnostic that performs internal diagnostic tests on the I/O and processor modules.

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 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 *Internet Control Message Protocol*.

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), which are made up of a network section, an optional subnet section, and a host section.

IOA

See *Input/Output Adapter*.

IOP

See *Input/Output Processor*.

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 connection, for example to establish a backup trunk.

ISO

See *International Standards Organization*.

ITU-T

See *International Telecommunication Union Telecommunication Standard Sector*.

J

jitter

The presence of inconsistent delays in end-to-end data delivery. Excessive jitter may cause difficulty with time-sensitive protocols.

K

Kbps

Kilobits per second.

keep-alives

A series of polling messages used in the Local (or Link) Management Interface (LMI) of a Frame Relay port to verify link integrity between devices.

L

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 *Open Shortest Path First*.

LMI

See *Link Management Interface*.

LMI Rev 1

See *Link Management Interface Rev 1*.

load balancing

A technique that distributes network traffic along alternate paths to the same destination 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 relatively short distances. Compare with *Wide Area Network*.

Local Management Interface

See *Link Management Interface*.

locally significant DLCI

In Frame Relay, an identifier or address that specifies a local router, PVC, SVC, or endpoint device. It is reusable at non-overlapping endpoints and allows for scaleability. Compare with *globally significant DLCI*.

logical port

A software configuration in the Cascade switch (by module type) that defines how a physical port is used. For example, a physical port configured as a Frame Relay direct trunk logical port.

loopback test

A diagnostic that directs signals back toward the transmitting source to test a communications path.

loss of framing (LOF)

A T1 error condition when an out-of-frame condition exists for a normal period of 2 1/2 seconds.

loss of signal (LOS)

A T1 error condition when j175+_75 consecutive zeros are received.

low-level debug

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.

M

management DLCI

A value that specifies a PVC from a LAN connected via a router to a Cascade switch over a Frame Relay network.

Management Information Base (MIB)

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 (MIB)*.

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.

N

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, switch, 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.

O

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 System Interconnection (OSI)

An international standard program created by ISO and ITU-T to develop standards for data networking, such as the OSI model, to facilitate multivendor operating environments.

OPTimum PVC trunk

A logical port type used to create an OPTimum trunk in a Cascade switch network.

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 System Interconnection (OSI)*.

OSPF

See *Open Shortest Path First*.

out of frame (OOF)

A T1 error condition where two or three framing bits of any five consecutive frames are in error.

P

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., character-cell terminal) into packets suitable for transmission. It also disassembles packets into character format for transmission to a character device.

packet processor (PP)

The Cascade STDX 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 (PRAM)

In the switch, memory that contains a module's configuration file, 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. Compare with *active hub*.

path

In the network, a set of trunks over which a PVC/SVC travels . See also *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

Public Data Network.

Permanent Virtual Circuit (PVC)

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 typically provides dial-up 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 (PRAM)*.

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, which consists of a single 16-KB (T1) /64-KB (E1) 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 (PVC)*.

Q

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 Statistics report describes the lost packets and round-trip delay measurements.

R

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 failure.

Receive Data

A hardware signal, defined by the RS-232-C standard, that carries data from one device to another. Compare with *Transmit Data*.

red alarm

A T1 alarm condition indicating a loss of signal or loss of frame at the device's local termination point.

red frames

In Frame Relay, a type of frame to be discarded. Color designators green, amber, and red identify packets as they travel through the network. See also *amber frames* and *green frames*.

redundancy

The duplication of hardware or software within a network to ensure fault-tolerant or backup 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, that a device sends to request permission to transmit.

RFC

See *Request For Comment*.

RFC 1294

See *Frame Relay RFC 1294 Multiprotocol Encapsulation*.

RIP

See *Routing Information Protocol*.

route recovery

In Frame Relay, an OSPF routing function in the Cascade switch. When a redundant trunk is down, new shortest-path routes for 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 segment 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 *Request To Send*.

RXD

See *Receive Data*.

S

SCR

See *Sustainable Cell Rate*.

SEAL

See *Simple and Efficient Adaption Layer*.

Serial Line over Internet Protocol (SLIP)

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 PP or CP module in a Cascade switch.

severe congestion

In Frame Relay, a state or condition that occurs when the queue size is greater than a second predetermined threshold (32 buffers full by default). In this state, the continued forwarding of amber and red packets jeopardize the successful delivery of green packets.

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.*

SIG

See *SMDS Interest Group*.

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.

SIP

See *SMDS Interface Protocol*.

SLIP

See *Serial Line over Internet Protocol (SLIP)*.

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*.

SMDS In-Band Network Management

The NMS manages the SMDS network traffic using SMDS In-Band Network Management. To be managed from this NMS, all SMDS Access Servers/Switches must be in the same IP subnet.

SMDS Interest Group

A consortium of vendors and consultants committed to advancing worldwide SMDS as an open, interoperable solution for high-performance data connectivity.

SMDS Interface Protocol

The protocol defined at the network and end-user interface connection.

SNMP

See *Simple Network Management Protocol*.

SNMP commands

The SNMP protocol supports three important commands: GET, SET, and NEXT. A *GET* command enables an NMS to query one or more objects or variables in an agent MIB. A *SET* command enables an NMS to modify a value of a MIB object or variable and may be used to boot or reboot devices. A *NEXT* command enables an NMS to query agent MIB tables and lists.

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 (SVC)*.

Switched Multimegabit Data Services

A WAN service based on the 802.6 standard for a high-speed, cell-relay, ring-based network. SMDS also offers a low-speed, frame-based interface.

Switched Virtual Circuit (SVC)

A logical connection across a packet-switched network providing as-needed connections to any other node in the network. See also *Virtual Circuit*.

synchronization

Use of a timing source (clock) to synchronize data transmission.

synchronous transmission

A data transmission method that uses a clock signal to regulate data flow.

T

T1

A long-distance circuit that provides 24 channels at 56/64 Kbps each (for a total of 1.544 Mbps). See also *E1*.

T3

A long-distance circuit that provides up to 28 T1 channels. T3 can carry 672 channels of 64 Kbps each (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 volume of data transported through a network connection, expressed in bits per second.

Time Division Multiplexing

A timing mechanism that allocates bandwidth for multiple channels onto one physical channel based on preassigned 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. Compare with *Receive Data*.

trap

An unsolicited message generated by an SNMP agent on a network device (e.g. switch) due to a predefined 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 on the backup trunk.

TXD

See *Transmit Data*.

twisted-pair cable

Cable that consists of two or more pairs of insulated wires twisted together.

U

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 multiport module offered with different physical connections, such as V.35 or X.21.

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 Network Interface Data Communications Equipment

A device that performs the Frame Relay DCE functions for link management and expects a Frame Relay DTE device (e.g., Cascade switch) to be attached to it.

User Network Interface Data Terminal Equipment

A device that performs the Frame Relay DTE functions for link management. The user specifies this option on the NMS to connect to a Frame Relay DCE, where the Cascade switch acts as the DTE.

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

V.35

An industry standard for physical layer communication between a network access device and a packet network. Cascade V.35 modules support up to 4096 Mbps (STDX) and 8192 Mbps (B-STDX).

VC

See *Virtual Channel*; *Virtual Circuit*.

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 *PVC* and *SVC*.

Virtual Circuit Identifier

A field in the ATM cell header that is used as an addressing identifier to route cell traffic.

Virtual Path

A group of VCs carried between two points that provides a way to bundle traffic headed in the same direction.

Virtual Path Identifier

A field in the ATM cell header that is used as an addressing identifier to route cell traffic.

VPI

See *Virtual Path Identifier*.

VP

See *Virtual Path*.

W

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.

Y

yellow alarm

A T1 alarm that is generated when the interface receives a red alarm signal from the remote end.

Index

D

M

U

V

W

X

Z