Configuring ISDN Services for B-STDX

Ascend Communications, Inc.

Product Code: 80039
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

List of Figures

List of Tables

About This Guide

This guide describes the ISDN services available on the B-STDX 8000 and 9000 switches and gives instructions on how to configure those services. The B-STDX switches provide two types of ISDN support:

- WAN remote access through its HyperPATH ISDN remote access software and its B-STDX 8000 and 9000 hardware platforms
- ISDN trunk backup through its B-STDX 8000 and 9000 hardware platforms

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. This guide assumes you have:

- Installed the Cascade switch hardware. Refer to the *B-STDX 8000/9000 Hardware Installation Guide* for more information.
- Installed the NMS software. Refer to the *Network Management Station Installation Guide*.

- Configured the Cascade switch software. Refer to the *Network Configuration Guide for B-STDX/STDX*.

This document should be used in conjunction with the B-STDX hardware and software documentation mentioned in the previous list.

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. The following table highlights the chapters and contents in this guide.

Read	To Learn About
Chapter 1	Integrated Services Digital Network (ISDN) technology
Chapter 2	WAN remote access switching and its applications
Chapter 3	The HyperPATH ISDN remote access features available on Acsend's 8000 or 9000 B-STDX switch
Chapter 4	Configuring the HyperPATH ISDN remote access software on Ascend's 8000 or 9000 B-STDX switches
Chapter 5	The operation and configuration of ISDN backup trunks on Ascend's 8000 or 9000 B-STDX switches
Chapter 6	Monitoring and troubleshooting ISDN remote connections

Conventions

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

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 materials not contained in this manual.

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

HP OpenView Menus

This manual shows HP OpenView SNMP Management Platform, Version 4.11 menu options. In HP OpenView, 4.11, CascadeView/UX menu options appear on different menus than in HP OpenView, 3.3.1. This guide references the location of the menu options for HP OpenView, Version 4.11.

Terminology for ISDN Modules

The module that is used to provide the B-STDX 8000/9000 switches with ISDN remote access capability is referenced by the following terms:

- ISDN I/O Module
- I/O Module
- PRI I/O Module

Related Documentation

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

Ascend

- B-STDX 8000/9000 Hardware Installation Guide (80005)
- Network Management Station Installation Guide (80014)
- Network Configuration Guide for B-STDX/STDX (80017)
- Diagnostic and Troubleshooting Guide for B-STDX/STDX (80018)
- Cascade Networking Services Technology Overview (80001)

Third Party

1. *Solaris 2.4 System Configuration and Installation Guide or Solaris 2.5 System Configuration and Installation Guide (depending on the version of Solaris that you are using)*
2. *HP OpenView Windows User's Guide (for HP 9000 Series and Sun SPARCstation)*
3. *SYBASE Commands Reference Manual*
4. *SYBASE System Administration Guide*
5. *ISDN and Broadband ISDN with Frame Relay and ATM*, Third Edition, William Stallings
6. *ISDN Does it All*, Network Computing, May 1 1995
7. *ISDN Nailed-up Access to Frame Relay PVC Service*, SR-NWT-002447
8. *CCITT Blue Book*, DSS 1 Network Layer, Recommendations Q.931, November 14-25, 1988.
9. *CCITT Blue Book*, DSS 1 Data Link Layer, Recommendations Q.920-Q.921, November 14-25, 1988

10. *Bellcore ISDN Exchange Termination to Frame Handler Interface*, Framework Generic Criteria, FA-NWT-001328, Issue 1, December 1992

11. *Bellcore ISDN Nailed-up Access to Frame PVC Service*, SR-NWT-002447, December 1992

12. *Pillars of PPP*, Network Computing, September 1, 1995

13. *Multilink PPP: One Big Virtual WAN Pipe*, Data Communications, September 21 1995

14. *The PPP Multilink Protocol (MP)*, RFC 1717, November 1994

15. *The Point-to-Point Protocol (PPP)*, RFC 1661, July 1994

16. *PPP Authentication Protocol*, RFC 1334, October 1992

17. *The PPP Compression Control Protocol (CCP)*, PPP Extensions Working Group

18. *PPP LCP Extensions*, RFC 1570, January 1994

19. *Remote Authentication Dial In User Service (RADIUS)*, May, 1995, draft-ietf-nasreq-radius-02.txt

20. *Multiprotocol Interconnect over Frame Relay*, RFC 1490, July, 1993

21. *PPP over ISDN*, RFC 1618, May, 1994

22. *PPP in HDLC-like Framing*, RFC 1662, July, 1994

23. *PPP Reliable Transmission*, RFC 1663, July 1994

24. *The PPP Internet Protocol Control Protocol (IPCP)*, RFC 1332, May 1992

25. *Multiprotocol encapsulation over ATM adaption Layer 5*, RFC 1483, July, 1993

26. *The translation of IP Datagrams over the SMDS service*, RFC 1209, March, 1991

27. *IP Dynamic Address Assignment*, Functional Specification May 25, 1995

28. *ISDN/SMDS Interworking: PPP-to-1209 Translation Lport*, Functional Specification, September, 20, 1995

29. *Dynamic Virtual Circuits*, Functional Specification, August, 10, 1995, Rev: 0.2

30. *The Internet-Draft for the RADIUS Protocol*, RFC 2058, January 1997

31. *The Merit AAA Server Documentation*

1

ISDN Services

This chapter describes the fundamentals of ISDN technology, and gives a brief description of Ascend's implementation of ISDN services on the B-STDX switches.

Background

Integrated Services Digital Network (ISDN) is a digital network architecture that has been in use by various telephone companies for almost 30 years.

ISDN was initially deployed during the 1960s in an effort to increase the speed and quality of existing communications. Today, ISDN is being brought into homes and offices to replace conventional analog telephone service and redefine local and business communications throughout the world.

Technology Fundamentals

ISDN communications provides many types of benefits and services. The following sections describe ISDN and the various benefits and services that it provides.

What is ISDN

ISDN is a set of network protocols that enables a wide range of digital communication services. Some of the benefits derived from ISDN include:

- Improved Remote Access
- Faster Call Setup
- Improved Quality of Service
- Device Integration
- Dynamic ISDN Connections
- Bandwidth on Demand

Improved Remote Access

With an ISDN, dial-in digital communications is achieved at a rate that surpasses conventional analog service.

Analog communications is limited to 56 Kbps. An ISDN exceeds 56 Kbps with an ISDN Basic Rate Interface (BRI). Using one of two B-channels on the BRI, dial-in communications is increased from 56 to 64 Kbps. Using both B-channels, an effective bit rate of 128 Kbps is achieved. Figure 1-1 illustrates how a BRI is used for remote access communications.

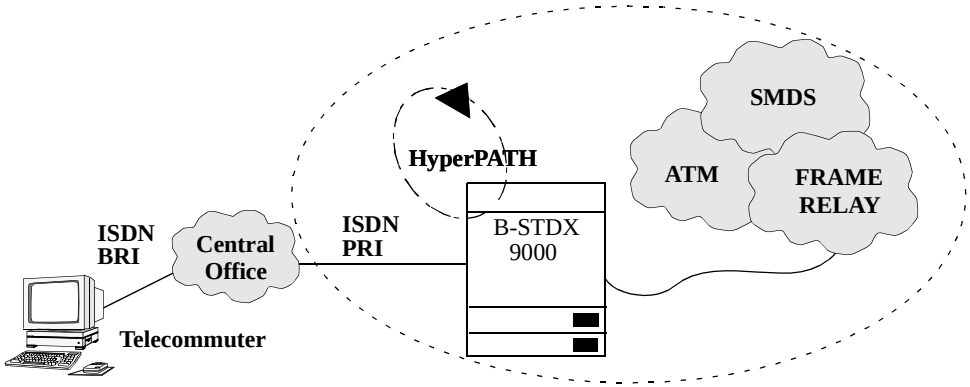

Figure 1-1. ISDN and Remote Access

Faster Call Setup

An ISDN connection is set up much faster than a typical analog connection since no modem is involved and no negotiation process takes place.

Improved Quality of Service

Analog communications are known to be error prone due to the nature of the analog signal and the method used to transfer the signal across the copper wire. With ISDN, the signal produced is more reliable, resulting in a higher Quality of Service.

Device Integration

One of the most important ISDN benefits is device integration. Using the same copper wire that links most homes and businesses to the existing telephone network, ISDN provides the integration of digital signals from various devices over a single network interface. Communication that once required numerous wire pairs can now take place over one wire pair passing digital signals through logical B-channels. Figure 1-2 illustrates how devices send their signals across an ISDN BRI.

.

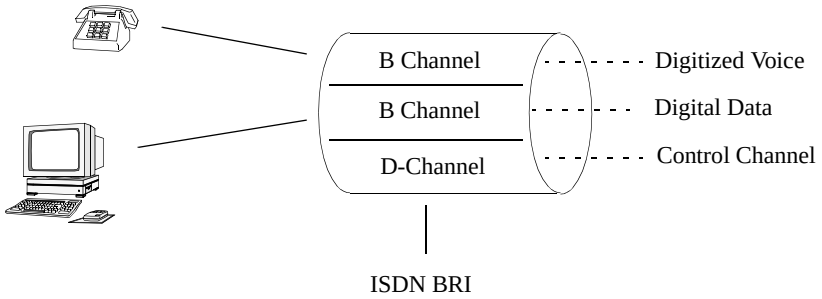

Figure 1-2. ISDN and Device Integration

These devices are connected to an ISDN line using an ISDN Network Termination One (NT-1) device. The ISDN NT-1 device connects up to eight ISDN devices to a single ISDN line. For more information on ISDN NT-1 devices, refer to “ISDN NT-1 Devices” on page 1-7.

Dynamic ISDN Connections

Unlike leased lines, ISDN connections are established on an as-needed basis. A connection is activated only when it is needed, so charges are incurred only for the time the connection is up, plus the call setup charges.

One very common use of ISDN is as a backup to a leased line. An ISDN connection is kept in reserve in case the leased line goes down. When the ISDN connection is no longer needed, it is terminated. Initiating and terminating an ISDN connection is done automatically. Figure 1-3 illustrates ISDN and leased-line backup.

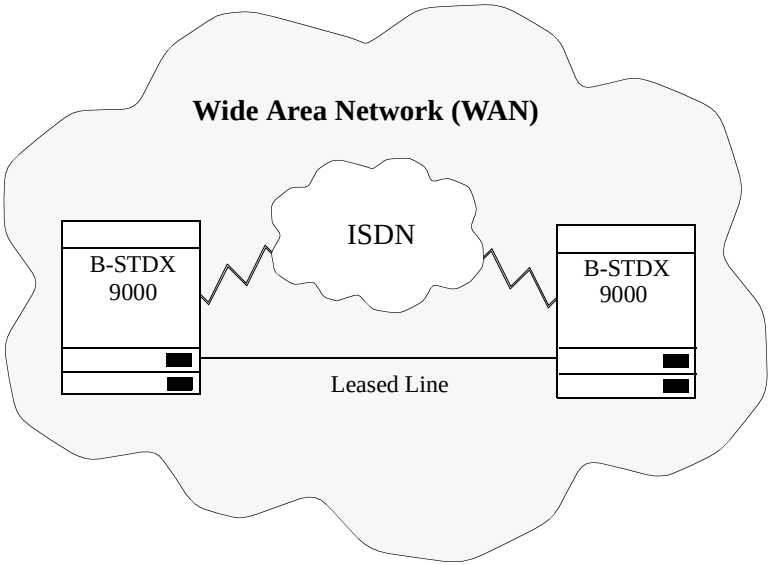

Figure 1-3. ISDN and Leased-Line Backup

Bandwidth on Demand

Since ISDN can automatically initiate and terminate calls, it is a cost-effective way to add capacity to a leased line that at times reaches full capacity. When the leased line is saturated, an ISDN connection is established. When the connection is no longer needed, it is terminated. Refer to Figure 1-3.

How ISDN Works

Using ISDN, a conventional analog signal is replaced with a 64 Kbps digital signal. This digital signal is transported over an ISDN connection using B-and D-channels. B-channels carry digital voice and/or data. D-channels initiate, receive, and control calls.

ISDN is available on two types of interfaces, a basic rate interface (BRI) or a primary rate interface (PRI).

Basic Rate Interface (BRI)

Basic rate is an interface that is most often used in a home or small office. A single BRI services two telephones which can each call a different destination at the same time. Both calls are sent over the same copper wire.

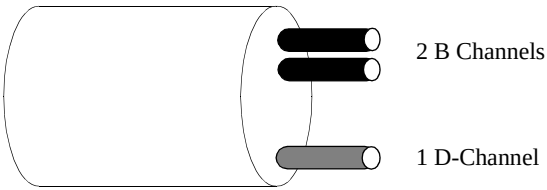

Figure 1-4. Basic Rate Interface

A BRI consists of two B-channels operating at 64 Kbps and one D-channel that operates at 16 Kbps. The total user data rate is 144 Kbps.

A BRI provides better voice quality, higher data rates, lower error rates, faster call setup times, and much more flexibility when compared to the conventional telephone network.

Primary Rate Interface (PRI)

Primary rate is an interface that is most often used in large commercial sites. Primary rate connections are often used as high-speed trunks for transferring large files and other continuous data streams. They can also be subdivided with a multiplexor to provide channels for multiple devices.

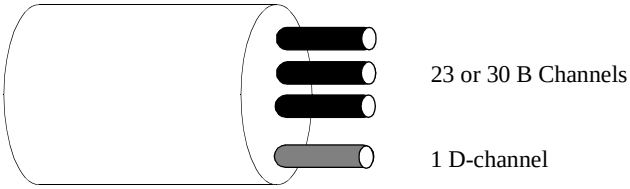

Figure 1-5. Primary Rate Interface (PRI)

A PRI can have one of two configurations:

- The North American PRI configuration consists of 23 B-channels and one D-channel that operate at 64 Kbps. The total data rate is 1.536 Mbps.
- The European PRI configuration consists of 30 B-channels and one D-channel that operate at 64 Kbps. The total bit rate is 1.984 Mbps.

The D-channel

The D-channel provides signaling to initiate and terminate calls. This signaling adheres to the OSI model and operates in the Physical, Data-Link, and Network protocol layers. These protocols are used to define message types that are sent between the customer and the local loop to set up and maintain services.

ISDN NT-1 Devices

The ISDN Network Termination One (NT-1) device is a device used in North America to connect the customer's data or telephone equipment to the local telephone loop. Originally, the ISDN NT-1 device was designed as a piece of equipment that would be owned and maintained by the service provider. With the breakup of AT&T, the Regional Bell Operating Companies (RBOCs) are no longer allowed to own equipment that resides on customer premises. In the United States, the ISDN NT-1 device is purchased, installed, and maintained by the customer.

The ISDN NT-1 device connects terminal equipment and terminal adapter equipment to the local telephone loop. Terminal equipment includes ISDN-compatible telephones and computers. Terminal adapters are devices used to connect non-ISDN-compatible equipment. Figure 1-6 shows how an ISDN NT-1 device connects this type of equipment.

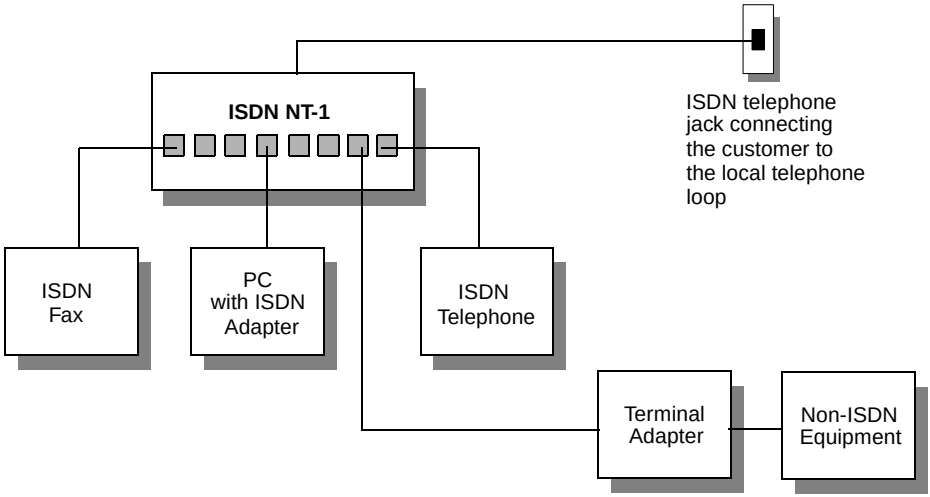

Figure 1-6. ISDN NT-1 Device

In the United States, an NT-1 device interface connects to the customer's equipment on one side and the telephone company's wire on the other side of the device. On the customer's side, up to eight devices can be connected and supported by the ISDN NT-1 device.

ISDN Telephone Services

There are a number of additional telephone services that are provided with ISDN, including the following:

Multiple Telephone Numbers — This service provides a way for a single interface to have multiple telephone numbers. This service is often used in homes or small offices.

Caller Identification — This service provides a way to display the telephone number of an incoming call.

Caller Identification Restriction — This service provides a way for the caller to prevent the display of their telephone number to the called party.

Ascend's Implementation of ISDN Services

Ascend provides two types of ISDN support on the B-STDX switches:

- WAN remote access through the HyperPATH ISDN remote access software and the B-STDX 8000 and 9000 hardware platforms
- ISDN trunk backup through the B-STDX 8000 and 9000 hardware platforms

HyperPATH Remote Access

The HyperPATH remote access software supports ISDN dial-in communications to the B-STDX switch over a BRI connection. The incoming ISDN call connects to a PRI logical port on a B-STDX 8000 or 9000 switch and is then transferred to its destination using internetworking services. The ISDN internetworking support includes PPP to Frame Relay and ATM services.

Refer to the following for a further description of remote access and HyperPATH:

- Chapter 2 for an overview of remote access
- Chapter 3 for a detailed description of the HyperPATH remote access features
- Chapter 4 for instructions on configuring HyperPATH remote access

ISDN Trunk Backup

The ISDN trunk backup feature allows the B-STDX switches to set up one or more backup trunks over an ISDN network to replace a primary trunk. When an ISDN trunk backup is initiated, a call is made over an ISDN network to connect the switches and activate the backup trunk over the ISDN connection.

Refer to Chapter 5 for a description of how the ISDN trunk backup works and for instructions on setting up an ISDN backup trunk.

2

Remote Access Switching Overview

This chapter contains an overview of WAN remote access switching, and includes the following:

- An introduction to WAN remote access
- Limitations of LAN access servers when used for remote access to WANs
- Advantages of the Ascend B-STDX switch with its HyperPATH remote access software
- Application solutions provided by the B-STDX switch with its HyperPATH remote access software

This chapter assumes you have a working knowledge of ISDN. Refer to the Related Documentation section in “About This Guide” for ISDN references.

Refer to Chapter 3 for more details about the HyperPATH remote access features.

Introduction

The demand for remote access to information is voracious. Business travelers want access to updated pricing and inventory levels. Workers at remote branch offices want instant access to remote databases and file servers. Telecommuters want access to electronic mail and remote files. And it seems like everyone wants access to the Internet.

At the same time, wide area networking technology is rapidly evolving. Leased lines and Time Division Mulitplexors are giving way to Frame Relay, ATM, and SMDS switched networks. Public switched WANs have been deployed globally and are growing rapidly.

The success of switched WANs and the demand for remote data access are causing the worlds of WAN switching and remote access to merge (refer to Figure 2-1).

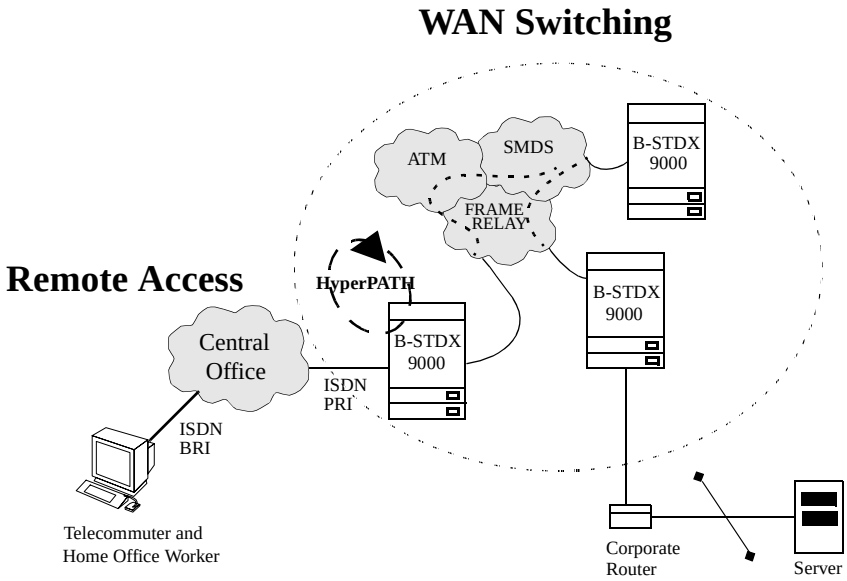

Figure 2-1. Merging of WAN Switching and Remote Access

LAN Access Servers Limitations

The features provided by a traditional LAN access server such as user authentication, compression, and multiprotocol access are now required for WAN access. Early attempts to satisfy these requirements have been met by connecting WAN switches with LAN access servers. LAN servers, however, have some limitations:

- WAN Protocols
- Quality of Service Features
- Scalability

WAN Protocols

LAN access servers are limited in their ability to speak WAN protocols because they were designed for LAN access.

Quality of Service Features

LAN access servers are also unable to offer a guaranteed Quality of Service (QOS) level for each remote access user. First-generation LAN servers are router-based systems. One of the attractive characteristics of router networks — the automatic sharing of bandwidth among traffic sources — can become a liability when a few users or applications cause performance degradation for higher priority traffic. Network planners have few capabilities to work with in the routers for achieving the desired QOS. This limitation is fundamental, and it arises from one of the features of routers that has made them popular: the use of connectionless protocols.

In Figure 2-2, devices A, B, and C desire access to Router D. The remote access router will assign all devices to the same PVC. All devices must therefore share the same PVC resource and, in effect, none of the devices will receive a guaranteed QOS.

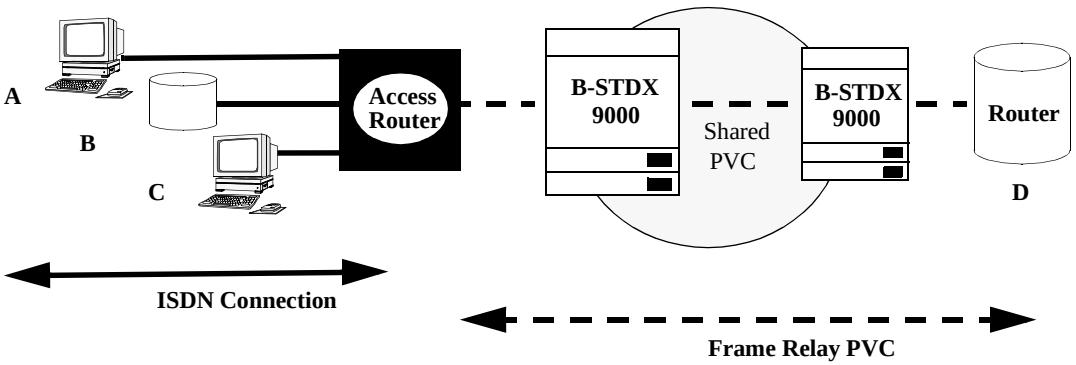

Figure 2-2. Remote Access without QOS

Scalability

Access servers for WAN remote access must be able to handle large-scale remote access designs. There are two aspects of scalability to consider here: latency and port count.

LAN access servers are router-based and must perform route determination with every packet received prior to forwarding the packet to its destination. The most popular protocol uses IP as the Layer 3 protocol. The routing decisions are based on the IP address in the layer 3 header (which is typically 40 bytes long). The Router must examine the IP address of each packet individually and determine the best path for forwarding each packet. For other protocols, such as IPX, a similar decision process is made. In other words, a router-based server must perform *route determination and forwarding with every packet.* Such per-packet processing can tremendously increase the end-to-end latency as the network grows in size.

Current remote LAN servers are targeted at small-scale networks that connect 8 to 48 remote users. Large scale designs with LAN servers require stacking multiple boxes. This is neither cost effective nor manageable.

B-STDX and HyperPATH ISDN Remote Access

The solution for WAN remote access is to integrate remote access with a WAN switch. This new type of product is called a *Remote Access Switch* (refer to Figure 2-3). The Ascend B-STDX, integrated with its HyperPATH remote access software and an ISDN module, is the industry's first remote access switch. It combines remote access and WAN switching functions in a single chassis.

The Ascend B-STDX remote access provides the following advantages over LAN access servers:

- Guaranteed QOS for each remote access user (refer to "Quality Of Service (QOS)" on page 3-3)
- WAN protocol support
- Scalability (refer to "Scalability" on page 3-4)

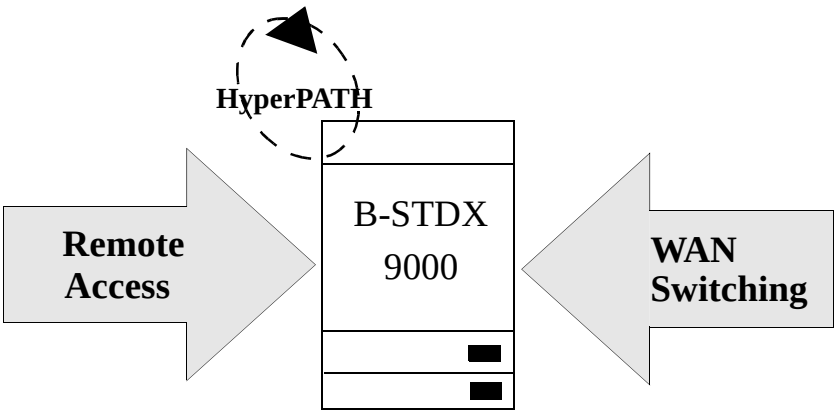

Figure 2-3. Remote Access Switch

Remote Access Applications for the B-STDX and HyperPATH

This section presents some remote access applications for which the B-STDX and HyperPATH remote access is best suited.

Remote User Access

There are two primary remote user access applications in use today. They are:

- Internet Access
- Telecommuting

Internet Access

Internet access (Figure 2-4) is one of the most important remote access applications. Internet use is growing exponentially. The world wide web is becoming a vehicle for mass-market merchandising and entertainment as well as for information access and communication. The “web” is rapidly evolving to support access to text, graphics, video, and sound.

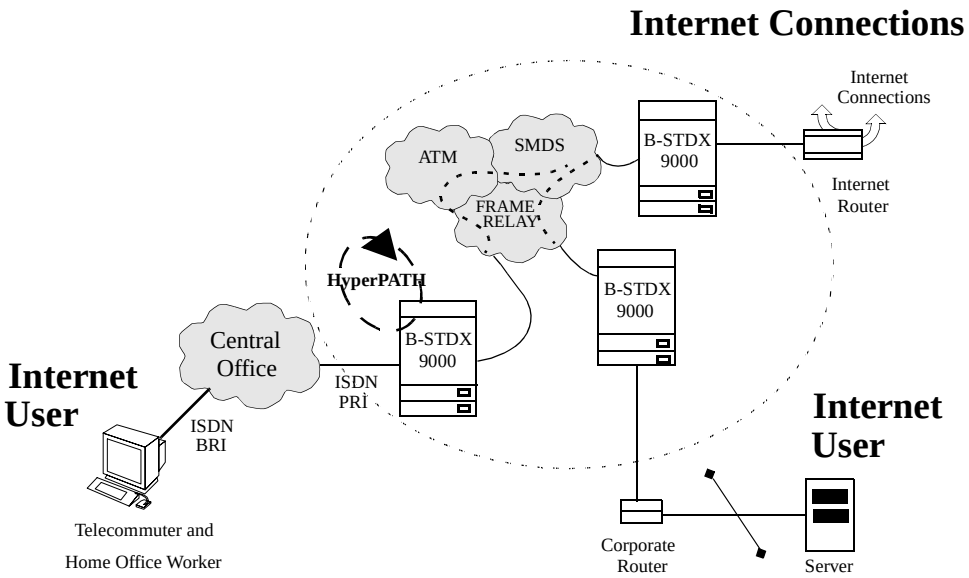

Figure 2-4. Internet Access

ISDN is the *most efficient access technology for Internet access.* This is due to the high bandwidth rate of a Basic Rate Interface (128 Kbps) and also due to the ability of Multilink PPP to bond multiple ISDN bearer channels together into a high-speed link. Refer to the Related Documentation section in “About This Guide” for background information on Multilink PPP.

Telecommuting

The downsizing of the early 1990’s has resulted in leaner corporations with overworked employees struggling to balance professional and family life. Many of these employees are accessing the corporate network in the evening or on weekends after spending time with their family. Other employees are working from home several days per week because a quiet, more focused environment improves overall productivity. Still others telecommute because it is better for the environment. Whatever the reason, telecommuting is a growing trend. Figure 2-5 illustrates a telecommuter connected to a WAN.

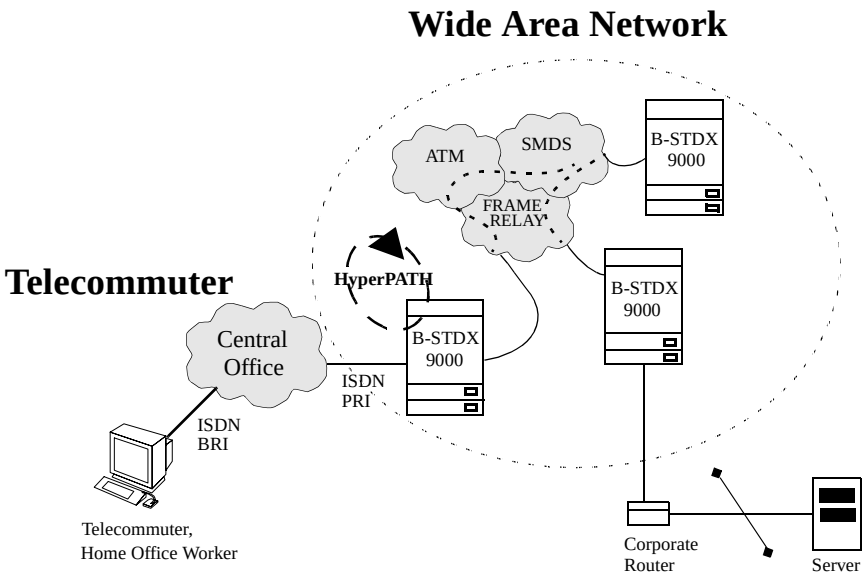

Figure 2-5. Telecommuting

Remote Branch Office Access

Many remote branch offices use leased lines for access to broadband networks. The trouble with leased lines is that they can be very expensive and they offer a static level of bandwidth. Building a fault tolerant network using redundant leased lines becomes cost prohibitive as the number of remote branches grows. Figure 2-6 illustrates a remote branch office connected to a WAN.

ISDN offers leased-line redundancy, without having to buy another leased line. In the event of a leased line failure, an ISDN channel can be established automatically without impact to higher layer protocol sessions. Broadband services such as Frame Relay are supported over the ISDN connection as if the connection were a leased line. In many countries ISDN service is much less expensive than a leased line and is being used not only for redundancy but also instead of leased lines.

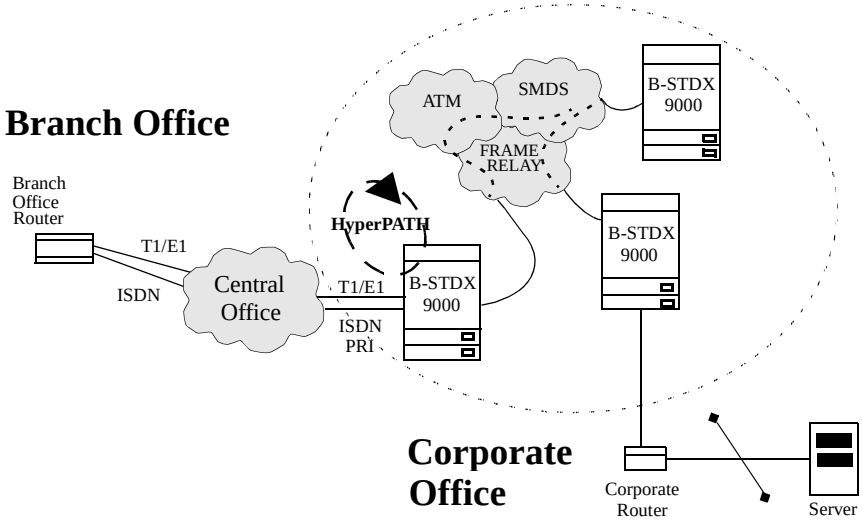

Figure 2-6. Remote Branch Access

Daily *busy hours* can often exceed the capacity of a leased line circuit resulting in degraded network performance due to excessive demand. ISDN allows additional bandwidth to be accessed on demand resulting in smooth network operation even during busy hours. In fact, multiple B-channels can be *bonded* together with the Multilink PPP protocol.

3

ISDN Remote Access Features

Ascend's B-STDX 8000 and 9000 Multiservice WAN switches, integrated with their HyperPATH remote access software and an ISDN module, can function as public remote access switches. With the B-STDX switches, Service Providers can deliver high-performance public remote access services over existing Frame Relay and ATM networks. These services can be configured, managed, and monitored through a single platform, CascadeView/UX.

This section contains a description of the HyperPATH remote access features available with CascadeView Release 2.3 and Release 4.2 of the switch software. Features described include the following:

- Operational Features
- Protocol Support
- Security
- Signaling

Operational Features

The ISDN remote access operational features described in the following sections include:

- WAN Remote Access
- Quality of Service
- Scalability
- Logical Port Configuration
- The ISDN I/O Module
- The B Channel
- The D-Channel
- Monitoring and Troubleshooting Capabilities

WAN Remote Access

First generation remote access server products were designed for remote LAN access. These products support Ethernet and Token Ring access and some have been retrofitted to support T1 or E1 links. In some cases, they might even support Frame Relay.

A remote access switch is designed for remote WAN access. The Ascend B-STDX is a second generation remote access server that supports Frame Relay and ATM access solutions. The B-STDX provides WAN services and a very high-quality communications link (see Figure 3-1).

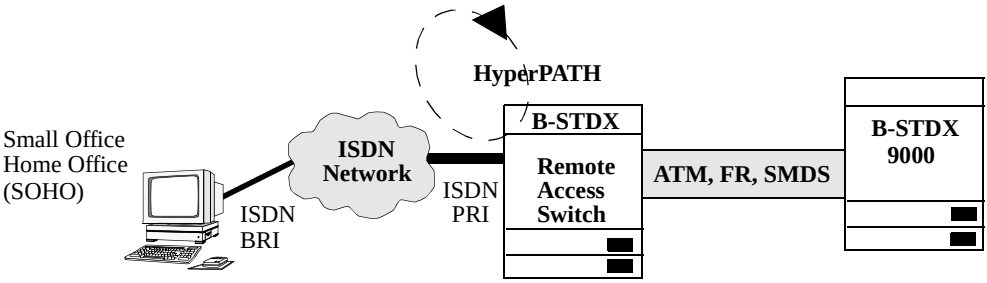

Figure 3-1. Remote Access Switch

Quality Of Service (QOS)

The B-STDX remote access switch provides access for remote branch offices and remote users. A fundamental advantage of the B-STDX solution lies in the ability to provide a guaranteed Quality Of Service (QOS) for each remote access user. There are two aspects of QOS to consider: throughput and latency.

In the case of Frame Relay and ATM, every ISDN connection received by the switch is mapped to a dedicated Permanent Virtual Circuit (PVC). Figure 3-2 illustrates the QOS virtual connections. Each PVC is assigned an appropriate Committed Information Rate (CIR), which provides the remote device with a guaranteed throughput across the WAN. In addition, every PVC can be assigned a priority level (low, medium, and high). High-priority traffic will achieve a lower latency through the switch than low-priority traffic.

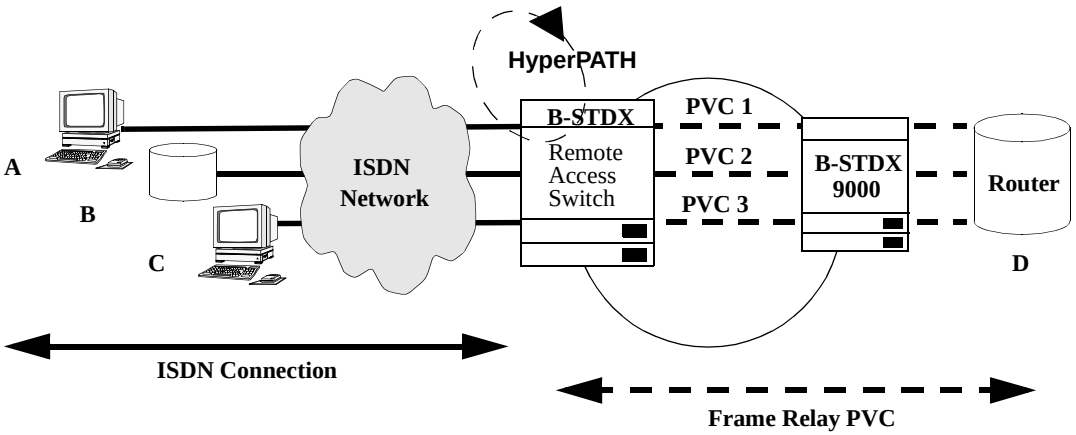

Figure 3-2. Remote Access with QOS

In Figure 3-2, remote user A has a Basic Rate Interface (BRI) connection (i.e., two 64-Kbps B-channels). The B-STDX remote access switch will bond both B-channels using Multilink PPP and map the connection to PVC 1 with a CIR of 128 Kbps. The end-to-end connection (remote user A to Router D) is provided a guaranteed QOS of 128 Kbps. Remote Device B has a Primary Rate Interface (PRI). As B-channels are dynamically bonded together, **the CIR is automatically increased** to the appropriate level, giving the device a high-speed, guaranteed QOS remote access connection. Each device is given their own PVC with the desired QOS.

First generation LAN servers are router-based systems. Network planners have few capabilities to work with in the routers for achieving the desired QOS. This limitation is fundamental, and it arises from one of the features of routers that has made them popular: the use of connectionless protocols (refer to “Quality of Service Features” on page 2-3).

Scalability

The B-STDX remote access switch provides scalability that router-based access servers cannot. This is because switch-based servers operate at layer 2 of the OSI Reference Model. Two types of switching that are of special interest are Frame Relay and ATM. Both protocols operate at Layer 2 of the OSI Reference model and are

connection oriented. This means that rather than determining the path of each packet independently, the switches establish a path between the endpoints and send all packets across that path. For Frame Relay and ATM networks, a switch-based remote access server performs *route determination only once*. As the network grows, switch-based solutions offer a much lower end-to-end latency than router-based solutions.

Logical Port Configuration

The B-STDX supports logical port types with ISDN as follows:

FR UNI-DCE — This logical port selection 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.

FR UNI-DTE — This logical port selection performs the Frame Relay DTE functions specified for link management. Select this option to connect a Frame Relay DCE (network switch) where the B-STDX acts as the DTE. You can also use this logical port type as the link between two B-STDX switches when configuring a Frame Relay OPTimum trunk on the same physical port.

FR NNI — This logical port selection enables you to connect a B-STDX switch to non-Ascend switches or networks using a standard protocol. You can also use an NNI logical port as the link between two B-STDX switches when configuring a Frame Relay OPTimum trunk on the same physical port.

PPP-to-1490 Translation — This logical port selection configures the port to enable a DTE device configured for the Point-to-Point Protocol (PPP) to communicate with another DTE device on the network configured for Frame Relay and encapsulating multi-protocols (according to RFC1490).

Encapsulated FRAD — This logical port selection configures the port to perform Frame Relay encapsulation/de-encapsulation for the HDLC/SDLC-based protocol.

Refer to the *Network Configuration Guide for B-STDX/STDX* for a more detailed description of the logical port services.

The ISDN I/O Module

There are two versions of the ISDN I/O module:

- A 4-port T1/ISDN I/O module
- A 4-port E1/ISDN I/O module

4-Port T1/ISDN I/O Modules

The Ascend 4-Port T1 ISDN I/O module provides T1 (1.544 Mbps) and primary rate ISDN (23 B-channels and 1 D-channel) interface support for the B-STDX 8000 and 9000 Multiservice WAN Switches.

The 4-port I/O module and associated software enables the B-STDX to fully integrate ISDN remote access with Frame Relay and ATM WAN switching.

Configuration

Each port can be configured individually to support Primary Rate ISDN, channelized T1, or Switched 56. Each port can support either 23 ISDN B-channels and one ISDN D-channel or up to 24 x DS0 T1 time slots. Each I/O module contains a RISC processor for high performance and flash memory for easy field installation of new capabilities.

When configured for ISDN, each module offers four primary rate ISDN ports. A fully loaded B-STDX 9000 offers a very high-density, remote access solution supporting 1,288 ISDN B-channels. Refer to Chapter 4 to configure the ISDN module.

Refer to the *B-STDX 8000/9000 Hardware Installation Guide* for a detailed description of the ISDN I/O modules.

Connectivity

The T1 ISDN I/O module contains four integral T1 CSU/DSUs and provides a D4 or Extended Super Frame (ESF) channel format T1 interface. This makes it easy and economical to interface to multiple sites over a single T1 connection. The result is a space and cost savings that increases performance and eliminates the cabling of an external CSU/DSU. Traffic can remain in its original D4 or ESF channel format from a CSU/DSU, eliminating expensive equipment for extra data handling and improving reliability by reducing the introduction of errors.

When operating as a T1 interface, the DS0 channels can be mapped to a maximum of 24 HDLC data links. Contiguous or non-contiguous n x DS0 channels compose each HDLC data link. Each of the n x DS0 data link channels can be configured as DCE or DTE, providing a variety of logical port functions.

4-Port E1/ISDN I/O Modules

The 4-Port E1 ISDN I/O module provides E1 (2.048 Mbps) and primary rate ISDN (30 B-channels and 1 D-channel) interface support for the B-STDX 8000 and 9000 Multiservice WAN Switches.

The 4-Port I/O module and associated software enables the B-STDX to fully integrate ISDN remote access with Frame Relay and ATM WAN switching.

Configuration

Each port can be configured individually to support Primary Rate ISDN or channelized E1. Each port can support either 30 ISDN B-channels and one ISDN D-channel or up to 31 x 64 E1 time slots. Each I/O module contains a RISC processor for high performance and flash memory for easy field installation of new capabilities.

When configured for ISDN, each module offers four primary rate ISDN ports. A fully loaded B-STDX 9000 offers the highest density, remote access solution supporting 1,680 ISDN B-channels. Refer to Chapter 4 to configure the ISDN module.

Refer to the *B-STDX 8000/9000 Hardware Installation Guide* for a detailed description of the ISDN I/O Modules.

Connectivity

The E1 ISDN I/O module contains four integral E1 Network Terminating Units (NTUs) and provides a CRC4 channel format E1 interface. This makes it easy and economical to interface to multiple sites over a single E1 connection. The result is a space and cost savings that increases performance and eliminates the cabling of an external NTU. Traffic can remain in its original CRC4 channel format from an NTU, eliminating expensive equipment for extra data handling and improving reliability by reducing the introduction of errors.

When operating as an E1 interface, the 64 Kbps channels can be mapped to a maximum of 31 HDLC data links. Contiguous or non-contiguous n x 64 Kbps channels compose each HDLC data link. Each of the n x 64 Kbps data link channels can be configured as DCE or DTE, providing a variety of logical port functions.

The B Channel

The B-channel is a user channel that can be used to carry digital data or PCM-encoded digitized voice. Two kinds of connections can be set up over the B-channel; circuit-switched and semi-permanent. The ISDN card supports both connection types. A circuit-switched channel is equivalent to the switched digital service available today.

B-Channel Hunt Groups

It would be nice if all the Telecommuters for a particular corporation could use the same phone number to access the corporate LAN. The Hunt Group feature makes this easy.

A Hunt Group is a group of B-channels that can be accessed using the same phone number. In Figure 3-3, if the number 800-555-1000 is called, an ISDN connection is made to one of the free B-channels in the range 1 to 10 on Port 1 (if a free B-channel exists). Assuming it does, a free DLCI on the egress port will transition to the ACTIVE state establishing a connection from the ISDN access device to the remote device.

B-Channel	Port #	Phone #	DLCI @ Egress Point
1 - 10	1	(800) 555-1000	51 - 60 @ A
11 - 23	1	(800) 555-1001	101 - 113 @ B
1 - 23	2	(800) 555-1002	201 - 223 @ C

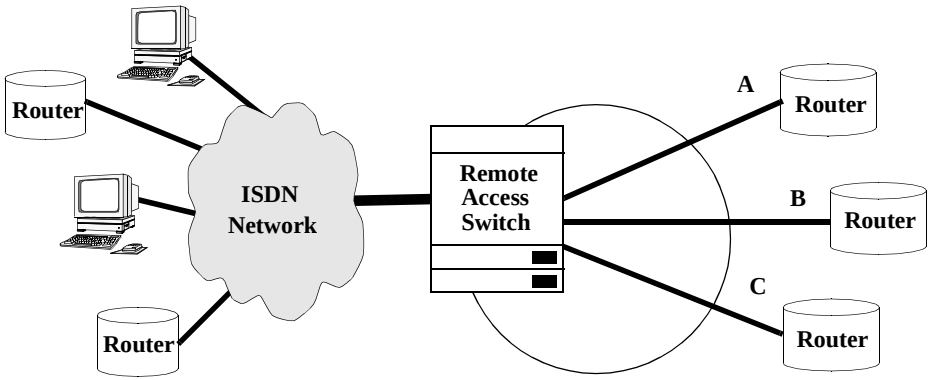

Figure 3-3. B-Channel Hunt Groups

Dynamic IP Address Assignment

The IP Address Assignment option enables the switch to dynamically assign an IP address to the remote user at call establishment time. A block of IP addresses can be configured in the switch on a per Hunt Group basis. This means that there are completely separate address pools for each remote access destination.

Multilink PPP (MP)

The MP and BACP options allow multiple physical links to be combined into one logical link as an *MP Bundle*. Refer to "Multilink PPP (MP)" on page 3-13.

The D Channel

The D-channel serves two purposes:

- It carries common-channel signaling information to control circuit-switched calls on associated B-channels.
- It may be used for packet-switching or low-speed (e.g., 100 bps) telemetry.

The B-STDX supports the use of the D-channel for common-channel signaling only.

There are many similar, but not identical, signaling implementations that are deployed world-wide. can support a wide set of implementations that includes the D-channel protocol stack described in Table 3-1 and the Super D-channel. Note that D-channel signaling is configured for each ISDN I/O module.

The D-Channel Protocol Stack

Table 3-1 describes the D-channel protocol stack supported by HyperPATH.

Table 3-1. The D-Channel Protocol Stack Support

Layer	Protocol
Network	Q.931 (Call Control)
Data Link	Q.921 (LAPD)
Physical	I.431 (Primary Rate Interface)

Super D Channel

A Super D-channel provides signaling support for all of the B-channels on a single ISDN I/O module. HyperPATH supports the Super D-channel for the T1 PRI (US version), but not the E1 PRI (European version). Without the Super D-channel, a D-channel would need to be configured for each physical port on the module. Super D-channel improves scalability by enabling up to 95 B-channels (US version) to be supported on a single card. Super D-channel is sometimes referred to as Non Facility Associated Signaling (NFAS).

Monitoring and Troubleshooting Capabilities

The monitoring and troubleshooting capabilities for ISDN remote access include:

- ISDN Call Status
- Diagnostic Traps for ISDN Remote Access
- Console-Based Call Lookup of Port Statistics

Refer to Chapter 6, “Monitoring and Troubleshooting” for more information.

Protocol Support

Ascend’s software supports a number of protocols as described in this section.

PPP over ISDN

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol packets over point-to-point links. PPP is comprised of three main components:

- A method for encapsulating and multiplexing different network-layer protocols simultaneously over the same link.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection. The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of users and determination of a failing link.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols. The NCPs handle protocol-specific problems such as assignment and management of IP addresses.

RFC 1661 defines the PPP organization, methodology, and encapsulation, and an extensible option negotiation mechanism that is able to negotiate a rich assortment of configuration parameters and provides additional management functions.

LCP Configuration Options

Table 3-2 lists the LCP configuration options supported by HyperPATH.

Table 3-2. LCP Configuration Option Support

Option	Supported
Maximum-Receive-Unit (MRU)	Yes, with Multilink PPP
Authentication-Protocol	Yes, with PAP/CHAP
Quality-Protocol	No
Magic Number	No
Protocol-Field-Compression (PFC)	Not supported
Address-and-Control-Field-Compression (ACFC)	Not supported

PPP to Frame Relay and ATM

The B-STDX Remote Access Switch supports PPP access to Frame Relay according to RFC 1490. In addition, PPP access to ATM is supported using RFC 1483.

IP Control Protocol (IPCP)

Ascend's software supports RFC 1332, which defines the IP control protocol for establishing and configuring the Internet Protocol over PPP. This release supports IP-Address Assignment.

Bridging Control Protocol (BCP)

Ascend's software supports RFC 1638, which defines the bridging control protocol for the bridging of packets over PPP.

Multilink PPP (MP)

Definition

Ascend's software and the B-STDX remote access switch support RFC 1717, Multilink PPP (MP). MP can combine multiple PPP links into one logical data pipe. For example, MP allows the two B-channels in a Basic Rate Interface (BRI) to be combined into a single 128 Kbps data stream. Additionally, channels can be dynamically added for bandwidth-on-demand applications.

PPP Bandwidth Allocation Protocol (BAP) and PPP Bandwidth Allocation Control Protocol (BACP)

Ascend's software supports the PPP Working Group Internet Draft for BAP/BACP that proposes a method for managing dynamic bandwidth allocations with MP.

Creation, Maintenance, and Deletion of MP Bundles

The following is an overview of how MP bundles are created, maintained, and deleted. Assume that there are currently no PPP connections to the switch.

1. A call comes in from the Remote-System. During PPP negotiations, it says that it supports MP and specifies an 'Endpoint Discriminator,' which will be used in determining the appropriate MP Bundle ID. The ISDN-IOP also says that it supports MP.

2. If Authentication is enabled for the current port, PAP/CHAP RADIUS authentication is performed. If authentication fails, the connection is terminated.

3. The ISDN-IOP determines the MP Bundle ID. If authentication is not enabled, the MP Bundle ID is simply the Endpoint Discriminator (a Remote System specified string of up to 20 bytes) and, if authentication is enabled, the MP Bundle ID is a combination of both the Endpoint Discriminator and the authentication ID, which is simply the Username used during authentication. An Endpoint Discriminator need not be specified by the Remote System. If it is not, the Authentication ID by itself is used as an MP Bundle ID. If Authentication is not enabled and there is no Endpoint Discriminator, a default MP Bundle ID is used.

4. A second call comes in from the Remote-System to the same ISDN-IOP as in Step 3, and it says it also supports MP and specifies an Endpoint Discriminator.

5. The ISDN-IOP says that it supports MP and then determines the MP bundle ID in the same manner as described in Step 3. If the MP Bundle ID of this call matches exactly the MP Bundle ID of the first call, this PPP link is combined with the first PPP link. If it does not match, a new MP bundle is created.

   Therefore, if Authentication is enabled for one of the links, the two PPP links can be combined only if the other link also has Authentication enabled and if both links have the same Authentication ID (Username).

Security

Security is an important feature of any remote access product. The B-STDX 8000/9000 Remote Access Switch supports a tiered security architecture to ensure authorized access to the WAN. The B-STDX offers the following security features:

- Calling Address Screening
- Radius Authentication using Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

Caller Address Screening

Caller Address Screening is a security method that checks the telephone number of the calling party against a preconfigured access list to verify that the calling party is authorized to access the switch. When a call is received the switch will verify that the calling E.164 address matches a preconfigured value. If a match is not found the call is rejected.

Refer to Chapter 4, “Configuring ISDN Remote Access” for instructions on how to set up Caller Address Screening.

PAP, CHAP, and RADIUS

For increased security, the B-STDX Remote Access Switch supports the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP) as described in RFC 1334. The B-STDX Switch also supports the Remote Authentication Dial-In User Service (RADIUS). These protocols and services are described in the sections that follow.

Password Authentication Protocol (PAP)

PAP provides a simple method to authenticate a client's identity using a two-way handshake. This is done only upon initial link establishment.

After the link establishment phase is complete, an ID/Password pair is repeatedly sent by the dial-in user to the Remote Access Switch until authentication is acknowledged or the connection is terminated.

PAP is not a strong authentication method. Passwords are sent over the circuit without encryption and there is no protection from repeated trial and error attacks. The dial-in user is in control of the frequency and timing of the attempts.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is used to periodically verify the identity of a dial-in user using a three-way handshake. This is done upon initial link establishment, and may be repeated anytime after the link is established.

After the link establishment phase is complete, the authenticator sends a "*challenge*" message to the dial-in user. The user responds with a value calculated using a one-way hash function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is terminated.

CHAP is a better authentication method than PAP because it provides protection against playback attack through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a distributed security system that uses an authentication server to solve the security problems associated with remote computing. RADIUS separates user authentication and authorization from the communications process and creates a single, central location for user authentication data. One RADIUS server supports up to tens of thousands of users, making it a very practical service for a rapidly growing network.

Distributed Security Systems

Distributed Security Systems use a client/server design that allows a Remote Access Switch to authenticate a dial-in user's identity through a single, central database located on a RADIUS Authentication Server. The Authentication Server stores all the authentication information about users, including their passwords and access privileges.

A Distributed Security System like RADIUS is more secure than other types of security systems because the authentication data is centrally located and not scattered on a variety of devices throughout the network. The RADIUS system is also scalable and easier to manage because all the data is in one secure place.

RADIUS Client

The RADIUS Client resides on the Control Processor card in the B-STDX. The client passes user information to a designated RADIUS server(s), then grants the dial-in user remote access to the RADIUS server and its authentication/authorization database. It services numerous authentication requests from different switches and ports simultaneously. It uses an "Authentication Session List" (queue) to keep track of numerous requests.

The RADIUS client reports all exceptional events to the NMS via SNMP traps. (Refer to "Diagnostic Traps for ISDN Remote Access" in Chapter 6 for more information). It communicates with PPP protocol machines residing in I/O processors via message manager mailboxes. It also communicates with RADIUS servers via the User Datagram Protocol (UDP). The RADIUS service is a UDP request/response service.

The B-STDX supports the following RADIUS packet types:

- Access Request
- Access Accept
- Access Reject

RADIUS Server

The RADIUS Server receives access requests from the RADIUS client. If the RADIUS server cannot be reached, the RADIUS client can route the request to an alternate server. When an authentication request is received, the RADIUS server validates the request, then decrypts the data packet to access the username and password information. If the username and password are correct, the servers sends an Authentication Acknowledgment that includes information on the user's network system and service requirements.

The RADIUS servers can act as proxy clients to other authentication servers, such as Kerberos.

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms available through published API's such as Kerberos and SafeWord.

The RADIUS Authentication Process

When the user dials into the B-STDX remote access switch, information about the user such as username and password is received by the RADIUS client, then passed to the RADIUS authentication server for acceptance.

- If the access request is accepted, the RADIUS server identifies the calling party and defines an authentication service (PAP or CHAP) and passes that information back to the RADIUS client on the B-STDX switch. The RADIUS client grants access to the calling party.
- If the authentication is rejected, the connection is terminated.

Figure 3-4 illustrates the RADIUS authentication process.

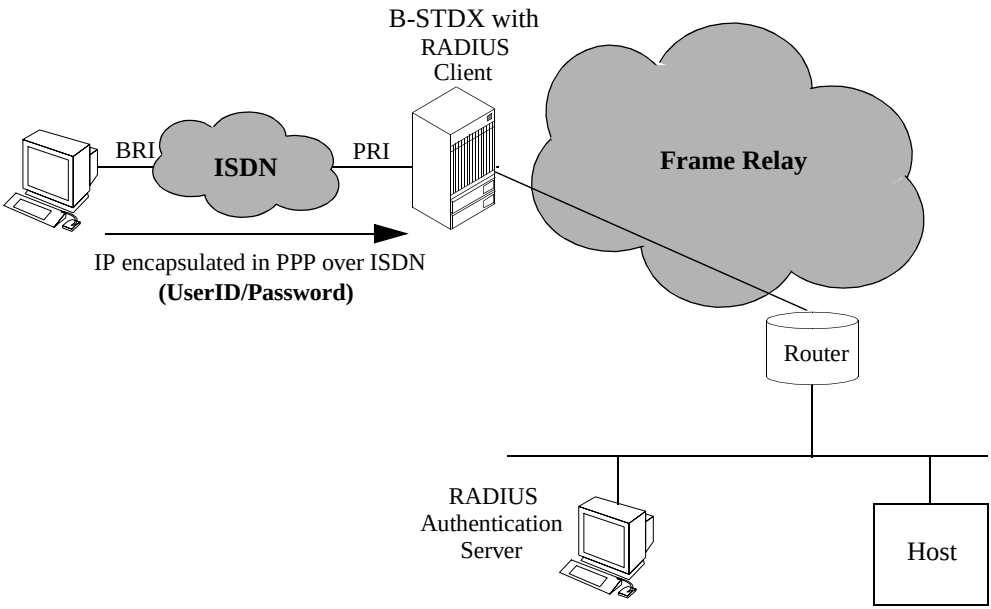

Figure 3-4. The RADIUS Authentication Process

B-STDX's RADIUS Implementation

The B-STDX's support of PAP and CHAP with RADIUS is described in the following sections.

PAP Authentication Process

The following steps explain the PPP PAP RADIUS authentication process:

1. The dial-in user sends a *User ID* and *Password* to the Remote Access Switch's IOP via a PPP packet.
2. The switch's IOP routes this information to the RADIUS client on the control processor card. The RADIUS client sends the *User ID* and *Password* to the RADIUS server via a RADIUS Access-Request packet.

3. The RADIUS server authenticates the user's ID and password. If the access request is accepted, the RADIUS server sends an Access-Accept packet to the RADIUS client. If the user is not authenticated, the RADIUS server sends an Access-Reject packet to the RADIUS client. The Access-Accept packet and Access-Reject packet contain an optional RADIUS reply message.

Although the RADIUS server authenticates a user, the RADIUS client may determine that the user is not authorized to make the connection. In such a case, the RADIUS client changes the pass to fail.

4. The RADIUS client determines if the user is authorized to establish the connection and sends a pass/fail internal message to the switch's IOP (PPP machine).

5. The IOP sends the final results (pass or fail) to the dial-in user via a PPP packet. An optional RADIUS reply message may also be sent at this time. Figure 3-5 illustrates the PPP PAP RADIUS authentication process.

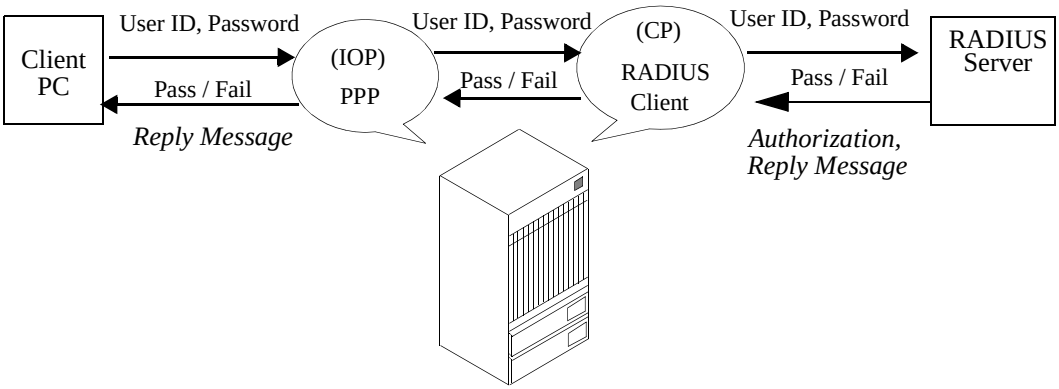

Figure 3-5. PPP PAP RADIUS Authentication

CHAP Authentication Process

The following steps explain the PPP CHAP RADIUS authentication process:

1. The switch generates a string of random characters (challenge) and sends them to the dial-in user via a PPP packet.
2. The dial-in user checks the character string using the user's password and sends the encrypted challenge to the IOP in the switch.
3. The PPP protocol machine (IOP) sends the plaintext string value and the new encrypted value to the RADIUS Client (CP) via an internal message.
4. The RADIUS Client sends the plaintext string and encrypted string to the RADIUS Server via a RADIUS Access-Request.
5. The RADIUS Server authenticates the user's ID and password by encrypting the plaintext challenge (using the user's password stored in the server's database) and comparing it to the original encrypted challenge. The RADIUS server sends an Access-Accept packet or an Access-Reject packet to the RADIUS Client. The Access-Accept packet and Access-Reject packet contain an optional RADIUS reply message.

Although the RADIUS Server authenticates a user, the RADIUS Client may determine that the user is not authorized to make the connection. In such a case, the RADIUS Client changes the pass to fail.

6. The RADIUS Client (CP) determines if the user is authorized to establish the connection and sends a pass/fail internal message to the PPP protocol machine (IOP).
7. The PPP protocol machine (IOP) sends the final results (pass or fail) to the Client (PC) via a PPP packet. An optional RADIUS reply message may also be sent at this time. Figure 3-6 illustrates the PPP CHAP RADIUS authentication process.

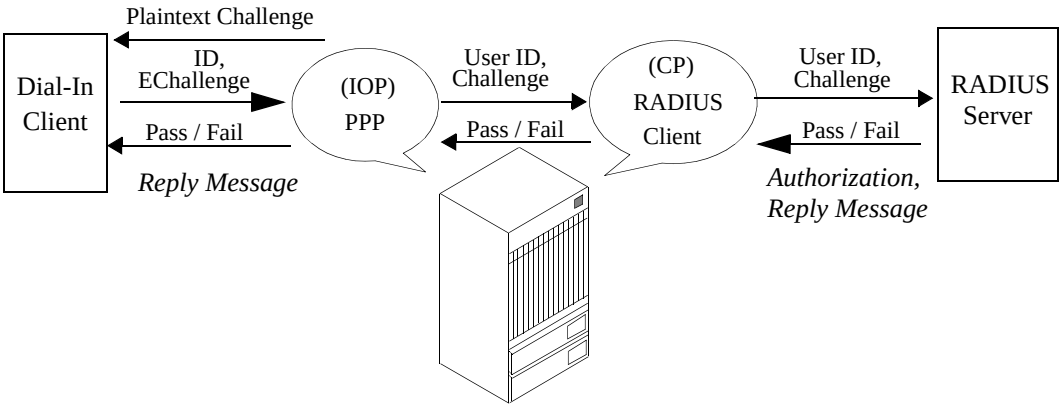

Figure 3-6. PPP RADIUS CHAP Authentication

Signaling

The following paragraphs contain a description of signaling standards that are supported by the ISDN cards.

North American Signaling

The ISDN access card supports the following North American signaling standards and switches commonly found in North America:

- AT&T 4ESS
- AT&T 5ESS
- Northern Telecom DMS 100

European Signaling

The ISDN access card supports the EuroISDN standard (CTR4) as well as switch-specific extensions as required.

Australian Signaling

The ISDN access card supports the Australian signaling standard (TS014) as well as switch-specific extensions as required.

4

Configuring ISDN Remote Access

The HyperPATH Remote Access software resides on the B-STDX 8000/9000 switch. The B-STDX switch supports two Primary Rate Interface (PRI) I/O modules that enable ISDN remote access communications.

When an I/O module is configured, you can dial into the B-STDX switch over an ISDN telephone line using a Basic Rate Interface (BRI). Using the D-channel for signaling, a connection is established between a dial-in user's B-channel and a B-channel on the ISDN I/O module.

You can implement ISDN remote access services using the following I/O modules:

- A 4-Port T1/ISDN I/O Module (contains a standard T1 interface for North American ISDN communications)
- A 4-Port E1/ISDN I/O Module (contains an E1 interface for European ISDN communications)

This section describes how to configure the PRI I/O modules and their physical and logical ports.

In addition to configuring the Ascend equipment, there are many issues you must address when you configure customer premise equipment for ISDN access.

For example, the user device contains a third-party ISDN network access card and software, which must be configured with an IP address. The network to be accessed by this device must recognize the IP address.

For complete information, carefully review the documentation for all network equipment you need to use in this ISDN configuration.

Configuring PRI I/O Modules Overview

Use the following sequence of steps to set up ISDN remote access to the B-STDX 8000/9000 switch:

Step 1. Configure the T1/ISDN I/O Module (page 4-11) or the E1/ISDN I/O Module (page 4-44).

Step 2. Access the Modify Logical Port — Set ISDN Attributes Dialog Box (page 4-77).

Step3. Configure E.164 Called Addresses (page 4-82).

Step 4. Configure Caller ID Screening (page 4-86).

Step 5. Configure PAP, CHAP, and RADIUS (page 4-89).

Step 6. Enable the Echo Request Function (page 4-98).

Step 7. Enable and Configure MP with BAP/BACP (page 4-101).

Before You Begin

Before you begin to configure the PRI module, read this section for background information you will need. This section includes:

- Accessing network maps (page 4-3)
- Accessing logical port functions with the Set All Logical Ports in PPort dialog box (page 4-3)
- Accessing the Switch Back Panel Dialog Box (page 4-9)

Accessing Network Maps

The procedures in this section assume that you know how to log on to CascadeView and open a network map. These tasks are described in the *Network Configuration Guide for B-STDX/STDX*.

Accessing Logical Port Functions

When you perform procedures that configure logical port functions, you must access and use the Set All Logical Ports in PPort dialog box. This section describes:

- How to access the Set All Logical Ports in PPort dialog box (page 4-3)
- The *Set Attributes option menu* (page 4-7)
- *The command buttons on the* Set All Logical Ports in PPort dialog box (page 4-7)

Access the Set All Logical Ports in PPort Dialog Box

To access the Set All Logical Ports in PPort dialog box:

1. On the network map, select the switch object that contains the PRI T1 module.
2. From the Misc menu, select CascadeView ⇒ Logon. Enter the operator or provisioning password and choose OK.
3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (see Figure 4-1).

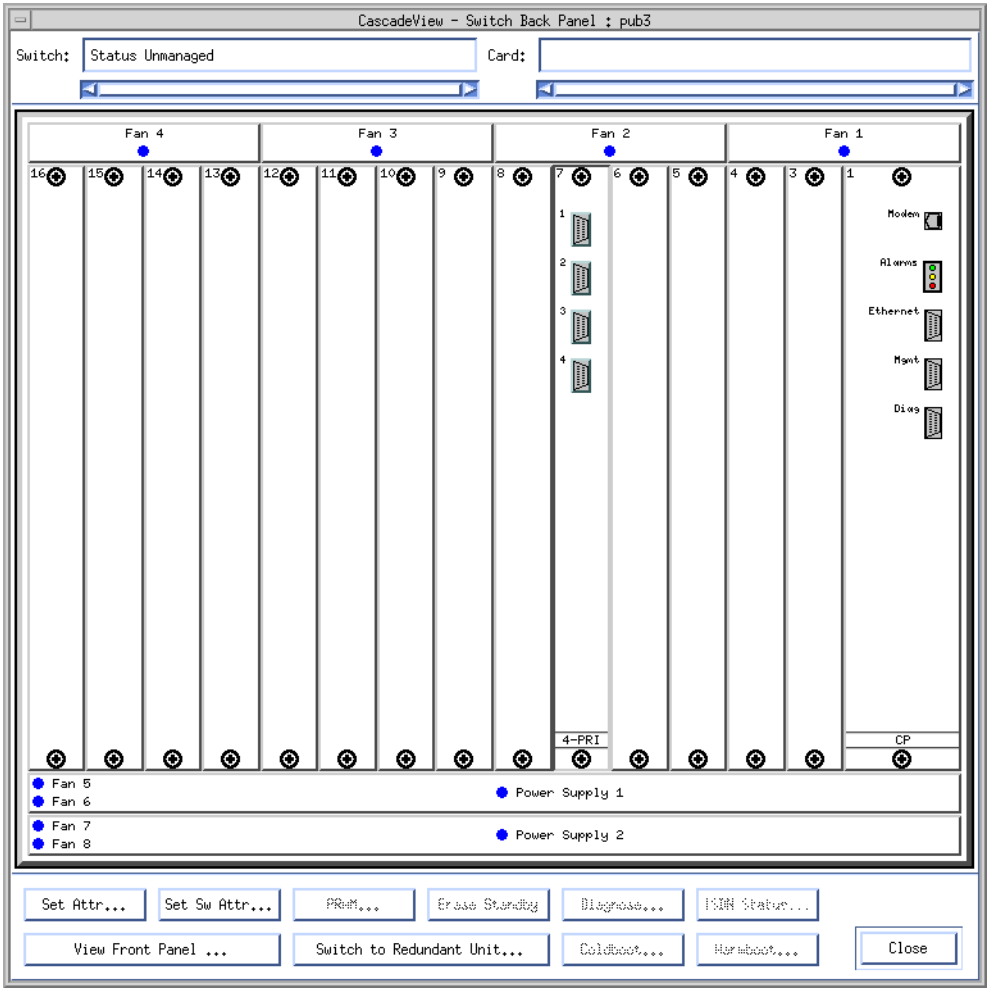

Figure 4-1. Switch Back Panel Dialog Box

4. Select the physical port you want to configure by placing the cursor on the port you want to configure and double-clicking on the left mouse button.

   The Set Physical Port Attributes dialog box appears (see Figure 4-2).

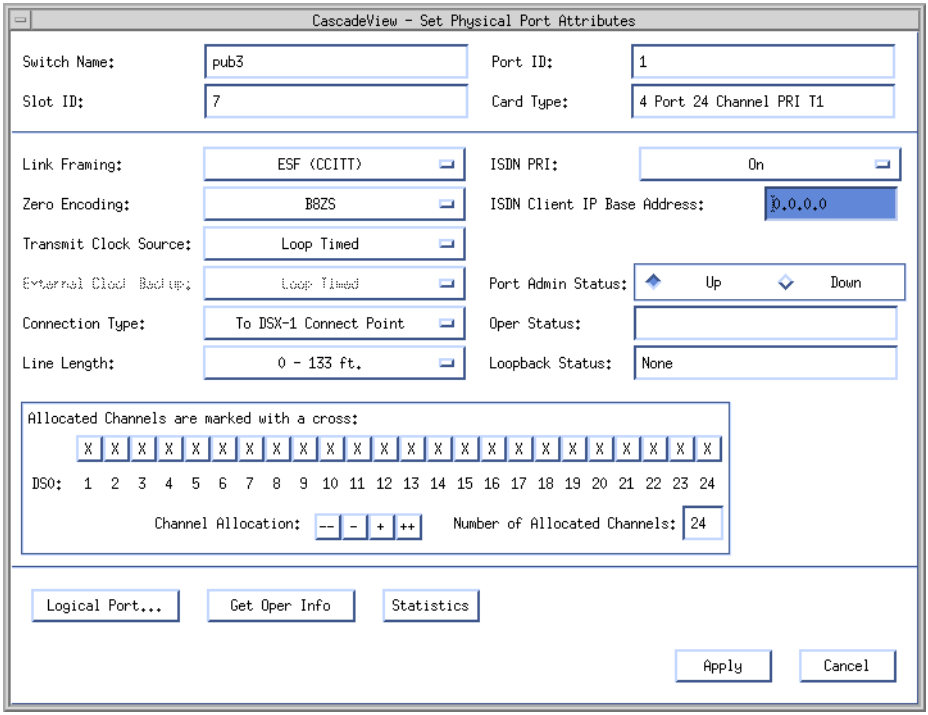

Figure 4-2. Set Physical Port Attributes Dialog Box

5. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears (see Figure 4-3).

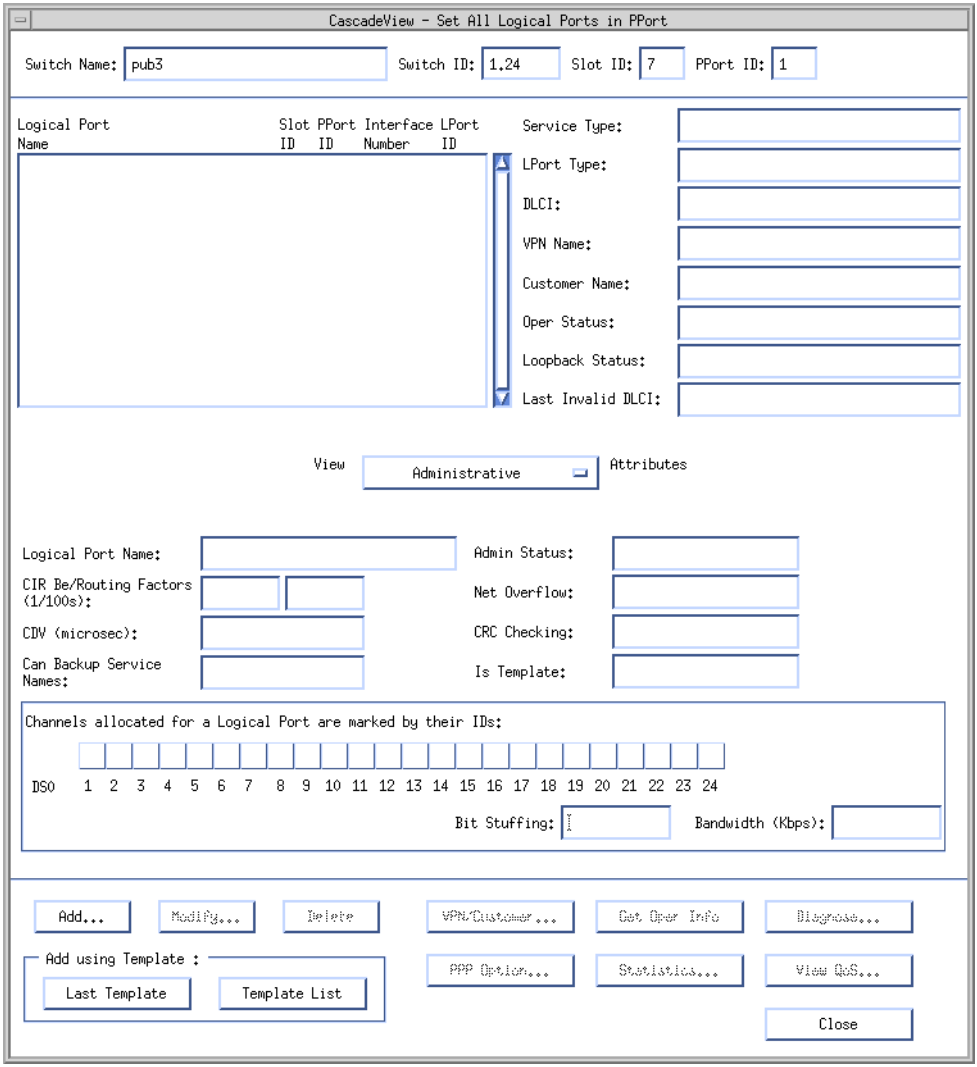

Figure 4-3. Set All Logical Ports in PPort Dialog Box

Set Attributes Option Menu

The Set All Logical Ports in PPort dialog box includes a *Set Attributes option* pull-down menu *(*shown in Figure 4-4). Each choice in the menu results in different fields being displayed. Table 4-1 gives a description of each pull-down option used in this chapter.

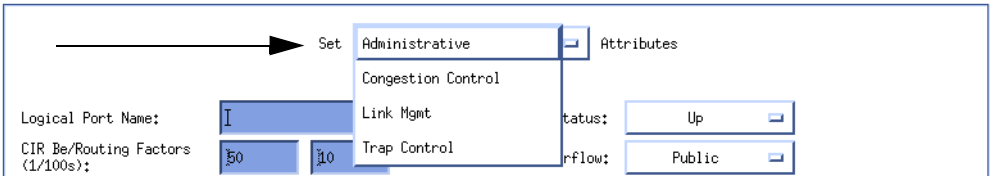

Figure 4-4. Set Attributes Option Menu

Table 4-1. Set Attributes Menu Options

Set [option] Attributes	Description
Administrative	The administrative attributes determine the number of channels allocated to each port and the amount of bit stuffing and bandwidth available on each DS0/TS0 channel on each port. The administrative attribute fields may vary, depending on the type of service.
Trap Control	The trap control attributes determine the congestion threshold in which traps are generated and the number of frame errors per minute on each logical port.

Set All Logical Ports in PPort Dialog Box Command Buttons

The Set All Logical Ports In PPort dialog box displays information about the logical port you select from the Logical Port list. It also provides several command buttons that you can use to access many logical port functions.

Table 4-2 describes the command buttons in the Set All Logical Ports in PPort fields.

Table 4-2. Set All Logical Ports in PPort Command Buttons

Command Button	Description
Modify/Delete	Modifies or deletes logical port configurations. For information about deleting logical ports, refer to the *Network Configuration Guide for B-STDX/STDX*.
Get Oper Info	Displays a status message in the *Oper Status* field that shows 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, you can use this option to define a new logical port using the same parameters.
VPN/Customer	Displays the Virtual Private Network customer's name.
View Qos Parameters	Displays the Quality of Service parameters.

Accessing the Switch Back Panel Dialog Box

The procedures for setting the E1 and T1 PRI module attributes and for configuring the E1 and T1 PRI module physical port attributes require that you first access the Switch Back Panel dialog box with the Set Parameters command.

To access the Switch Back Panel dialog box with the Set Parameters command:

1. On the network map, select the switch object that contains the PRI T1 or E1 module.
2. From the Misc menu, select CascadeView ⇒ Logon. Enter the operator or provisioning password and choose OK.
3. From the Administer menu, select Cascade Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears (see Figure 4-5).

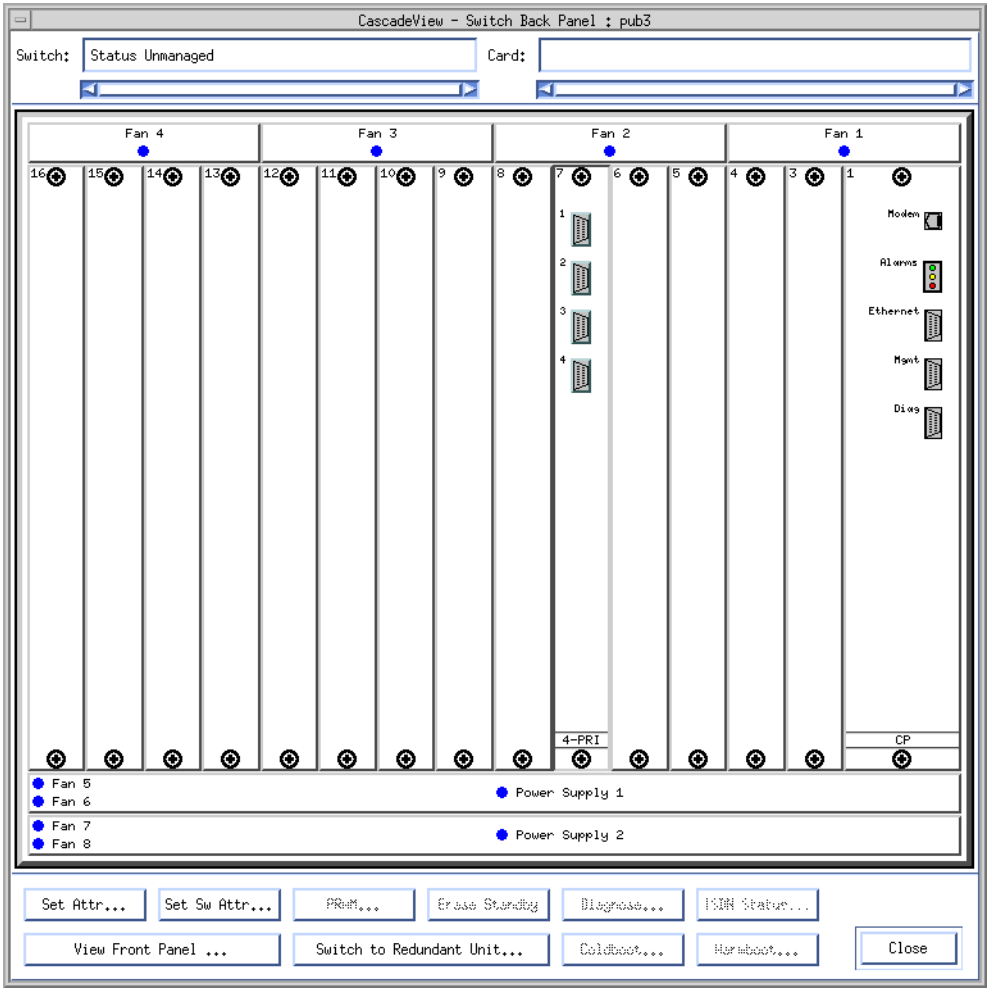

Figure 4-5. Switch Back Panel Dialog Box

Configuring the T1/ISDN I/O Module

Configuring the T1/ISDN I/O module consists of the following tasks:

- Determining the type of D-Channel configuration you want to use (page 4-11)
- Setting the T1/ISDN I/O module Attributes (page 4-12)
- Configuring the Module's Physical Port Attributes (page 4-17)
- Configuring the D-Channel(s) (page 4-24)
- Defining the B-Channels (page 4-33)

Determining the D-Channel Configuration

The ISDN modules have four PRI ports that connect to ISDN PRI lines. The module's signaling is controlled by the D-channel, which can be configured in the following two ways:

- Super D-Channel
- Four D-Channels

The next two sections describe how the D-channel can be configured. Review these sections and decide how you will configure the D-channel before you configure the ISDN I/O module.

Make your choice carefully, it is difficult to reconfigure the switch to enable Super D-channel (NFAS) at a later date.

Super D-Channel

A Super D-channel configuration means that you will configure one D-channel to handle all of the signaling information for all four ports on the I/O module. This configuration gives you the largest amount of data throughput since it makes use of three additional B-channels. This configuration also reduces the amount of signaling overhead. The total channels available with this configuration include one D-channel and 95 B-channels.

Four D-Channels

A four-D-Channel configuration means that you configure one D-channel for each PRI port on the I/O module. This configuration reduces data throughput since it reserves four channels for signaling. It does, however, provide a little more flexibility when provisioning the ISDN service. The total channels for this configuration include four D-channels and 92 B-channels.

Setting the T1/ISDN I/O Module Attributes

Configure the T1/ISDN I/O module (PRI TI module) as follows:

1. Access the Switch Back Panel dialog box with the Set Parameters command (refer to "Accessing the Switch Back Panel Dialog Box" on page 4-9).
2. Select the specific PRI I/O module you want to configure by placing the cursor on the module and double-clicking on the left mouse button.
3. The Set Card Attributes dialog box appears (see Figure 4-6).

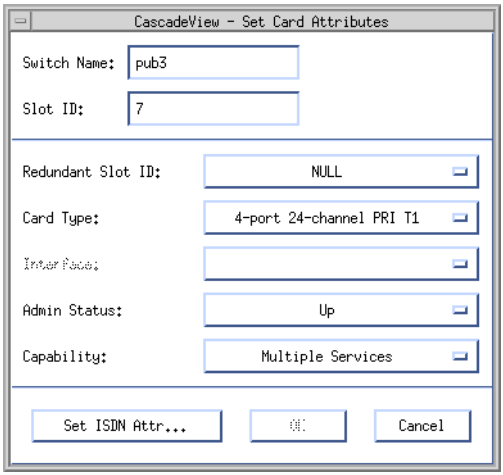

Figure 4-6. Set Card Attributes Dialog Box

4. Complete the Set Card Attributes dialog box fields described in Table 4-3.

Table 4-3. Set Card Attributes Fields

Field	Action/Description
Card Type	Select 4-port 24-channel PRI T1.
Redundant Slot ID	(*Optional*) Set if this PRI I/O module is to have a redundant standby partner installed. The default setting is NULL. You must always install and configure the redundant PRI I/O module in the next higher slot from its main partner. For additional information on configuring B-STDX modules and redundancy, refer to the *Network Configuration Guide for B-STDX/STDX*.
Admin Status	Set to *Up* for normal operation. *Up* — This PRI I/O module becomes fully operational when you start the switch. *Down* — This PRI I/O module does not come on-line when you start the switch. The configuration is saved in the database but is not downloaded to the switch. Use this option when you run foreground diagnostics. Maintenance — This PRI I/O module does not receive the application software when you start the switch. A module in this state only has its boot flash loaded. Application code is not running. This setting enables you to reset the PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a hardware problem.

5. Choose Set ISDN Attr.

   The Set ISDN Card Attributes dialog box appears (see Figure 4-7).

   The ISDN Card Attributes dialog box enables you to specify the signaling to be used between the Central Office and the B-STDX switch.

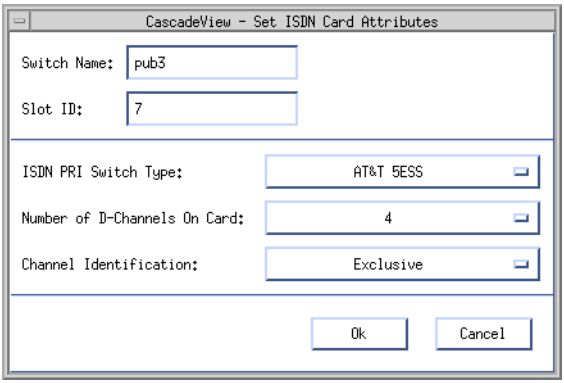

Figure 4-7. Set ISDN Card Attributes Dialog Box

6. Complete the Set ISDN Card Attributes dialog box fields described in Table 4-4.

Table 4-4. Set ISDN Card Attributes Fields

Field	Action/Description
ISDN PRI Switch Type	Select the type that corresponds to the signaling standard used by the ISDN central office switch. *AT&T 5ESS* *AT&T 4ESS* *NT-DMS-100* (Northern Telecom) The TPH and NET 5 selections are gray and are not available, since they are for E1 PRIs.

Table 4-4. Set ISDN Card Attributes Fields (Continued)

Field	Action/Description
Number of D-Channels On Card	Select the number according to the signaling configuration you plan to use. *1* — Select 1 to configure a *Super D-channel* (NFAS). The Super D-channel supports all the B-channels on the module. *4* — Select 4 to configure four D-channels, one for each of the four physical ports. The switch uses the remaining DS0 channels as B-channels, for a total of 92 B-channels.
Channel Identification	Select *Exclusive.* The Channel Identification method defines how the central office will handle the incoming ISDN call. *Exclusive* — Enables the central office switch to assign the B-channel as soon as the call is received. *This is the standard method of operation.* *Preferred* — Enables the Ascend switch to assign the B-channel.

It is difficult to reconfigure the switch to enable Super D-channel (NFAS) at a later date. Carefully choose the Number of D-channels according to your network needs. If you anticipate needing up to 95 B-channels, select 1 to enable Super D-channel.

7. Choose OK to return to the Set Card Attributes dialog box.
8. Choose OK to return to the Switch Back Panel dialog box.

   The PRI I/O module you configured is displayed (see Figure 4-8).

Proceed to the following section to configure the module's physical port attributes.

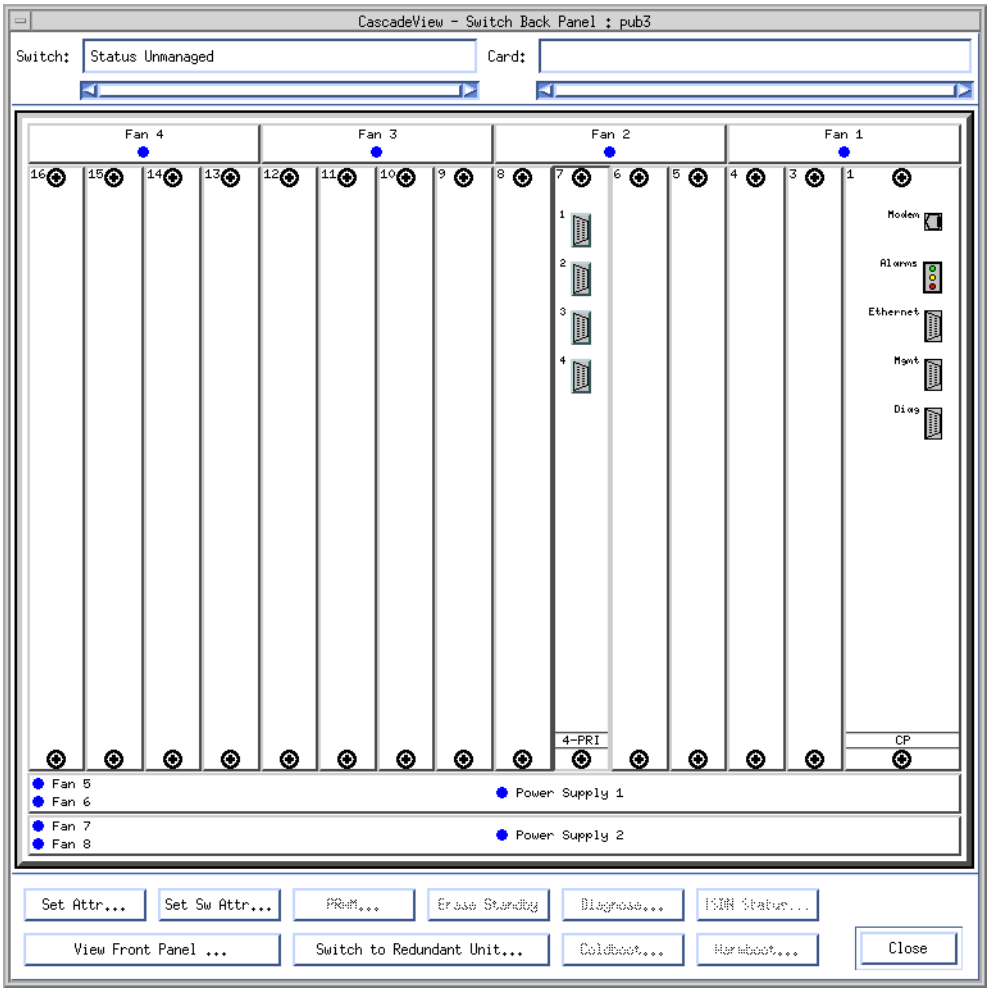

Figure 4-8. Switch Back Panel Dialog Box

Configuring the T1/ISDN/I/O Module's Physical Port Attributes

This section describes how to configure those attributes that are specific to each physical port on the PRI I/O module. Some attributes define the framing and encoding of the data passing through the module. Others are used to define the clock source, the connection type, and the length of the ISDN line used to connect the Central Office to the B-STDX switch.

To configure the physical port attributes:

1. Access the Switch Back Panel dialog box with the Set Parameters command (refer to "Accessing the Switch Back Panel Dialog Box" on page 4-9).

2. Select the physical port you want to configure by placing the cursor on the port you want to configure and double-clicking on the left mouse button.

   The Set Physical Port Attributes dialog box appears (Figure 4-9).

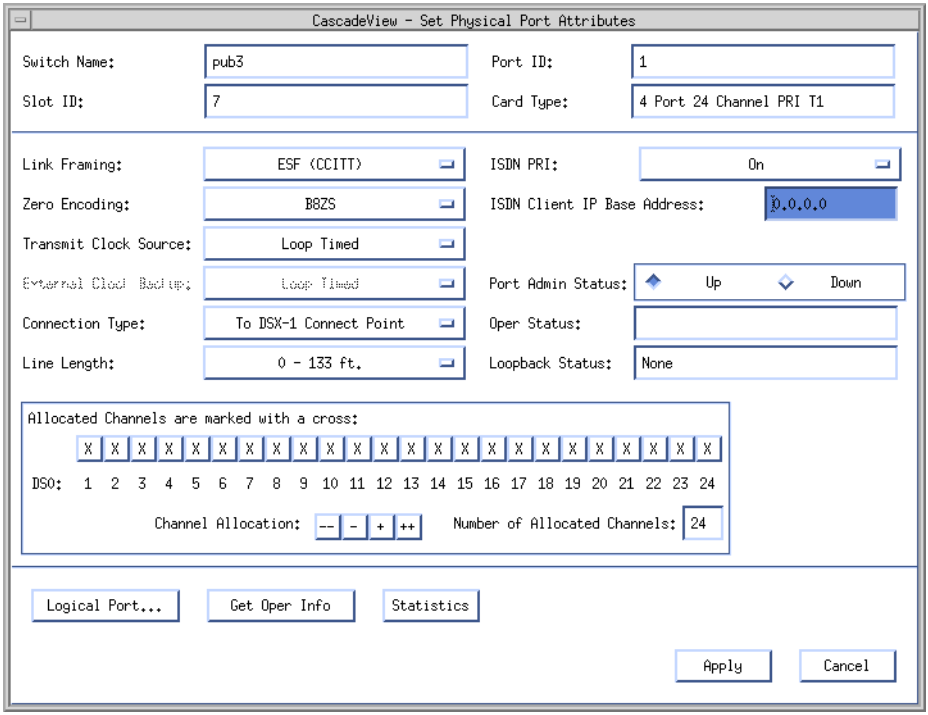

Figure 4-9. Set Physical Port Attributes Dialog Box

*If **none** is not displayed in the **loopback status** field, 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.*

3. Complete the Set Physical Port Attributes dialog box fields described in Table 4-5.

Table 4-5. Set Physical Port Attributes Fields

Field	Action/Description
Link Framing	Link Framing defines a framing specification. Framing provides a method of distinguishing between the individual channels; it is accomplished by adding one additional bit to each frame. The default is ESF (CCITT). Make sure you configure the customer premise equipment (CPE) to use the same framing specification as the Ascend physical port. Select one of the following options. *D4 Framing* — A frame format that consists of twelve frames (also referred to as "*Superframe*"). It provides end-to-end synchronization and signaling associated with a particular channel. *ESF (CCITT and AT&T)* — Extended Superframe. A framing format that extends the D4 framing format from 12 frames to 24 frames and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel, and data link. The advantage of ESF framing over D4 framing is that it enables the Ascend equipment to monitor and respond to a maintenance message from the network. Facility Data Link (FDL) for *CCITT* is the European standard, and *AT&T* is the US standard. *ESF (None)* — No Facility Data Link (FDL) messaging support.

Table 4-5. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Zero Encoding	Zero Encoding indicates whether the T1 interface uses the Jammed Bit (AMI) or the B8ZS encoding method. 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. The default is B8ZS. Refer to your facility service provider for more information about selecting a zero encoding method. Select one of the following options. *Jammed Bit* — Refers to the jammed bit zero encoding indicated in the AT&T specification. 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. *B8ZS* **(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 placed in and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment.

Table 4-5. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Transmit Clock Source	This option defines the source of the transmit clock. Select one of the following options. *Looped Time* — This is the default. The clock source is derived from the network timing received. *Internal* — The internal T1 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 *Looped Time* or *Internal* clock source. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about external clock source and backup for a T1 module.
ISDN PRI	Select ON to enable this T1 physical port to use ISDN PRI services. If you select *Off*, the physical port behaves as a standard T1. Refer to the *Network Configuration Guide for B-STDX/STDX* if you need to configure this module for standard T1 access.

Table 4-5. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
ISDN Client IP Base Address	Leave the default address of 0.0.0.0 to disable this feature. When this feature is disabled, the IP address of the remote user will be used. If you want the switch to maintain a pool of IP addresses for the physical port and dynamically assign a temporary IP address to a remote user, enter the base IP address for this physical port. This address comes from the end-user LAN administrator. If you configured the PRI T1 module to use four D-channels (refer to page 4-15), the Ascend switch will maintain a pool of IP addresses for the physical port that range from the base address you enter (x.y.z.n) to (x.y.z.n + 22). This provides 23 distinct IP addresses per physical port. If you configured one Super D-channel (refer to page 4-15), the Acend switch will maintain a pool of IP addresses on the physical ports that do not contain the D-channel that range from the base address you enter (x.y.z.n), to (x.y.n + 23). The range of addresses for the physical port that contains the D-channel is (x.y.z.n) to (x.y.z.n + 22). The subnet mask is set on the ISDN CPE.

Table 4-5. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Port Admin Status	Select *Up*. *Up* — This option enables the port. *Down* — This option saves the configuration in the database without activating the port or to take the port off-line to run diagnostics. Each time you modify the Port Admin Status, choose Apply to send the change to the switch.
Connection Type	Field does not affect the PRI T1 module.
Line Length	Field does not affect the PRI T1 module.
Allocated Channels are marked with a cross	Ensure that the channels you want to allocate are marked with an X, and remove the X from any channels you want to disable. By default, all DS0 channels are selected. To add or remove an X in a channel, click the left mouse button on the channel. You can also add and remove X's by using the four editing buttons: -- Deselects all channels. – Deselects the highest numbered channel that is allocated. + Selects the lowest numbered channel that is not allocated. ++ Selects all channels.

4. Notice the Number of Allocated Channels.

This number is subject to change according to the number of DS0 channels you enable.

If you configure the PRI T1 module to use four D-channels, each DS0 channel 1 through 23 corresponds to a B-channel; the 24th DS0 channel corresponds to the D-channel. However, if you configured the ISDN PRI module to provide only one D-channel ("Super D-channel"), you can use DS0 24 as a B-channel on physical ports 2, 3, and 4. For more information about configuring the number of D-channels, refer to page 4-15.

5. Choose Apply and then OK to save the physical port attributes.

   This sends an SNMP Set command to the switch.

6. Choose Cancel to exit the dialog box.

Configuring the D-Channel(s)

The D-channel carries common channel-signaling information to control circuit-switched calls on the associated B-channels. You use DS0 channel 24 for D-channel support. When you define attributes for the PRI T1 module, you specify the number of D-channels this module can use.

- If you configured the PRI T1 module for a Super D-channel (NFAS), define one D-channel only (DS24) on the *first physical port*.
- If you configured this module to use four D-channels, define one D-channel logical port (DS24) on each of the four physical ports.

To define the D-channel for ISDN services:

1. For the physical port on which you are defining the D-channel, access the Set All Logical Ports in PPort dialog box (see Figure 4-10). Refer to "Access the Set All Logical Ports in PPort Dialog Box" on page 4-3.

If the LOOPBACK field displays "loopback", do not modify or delete the selected logical port.

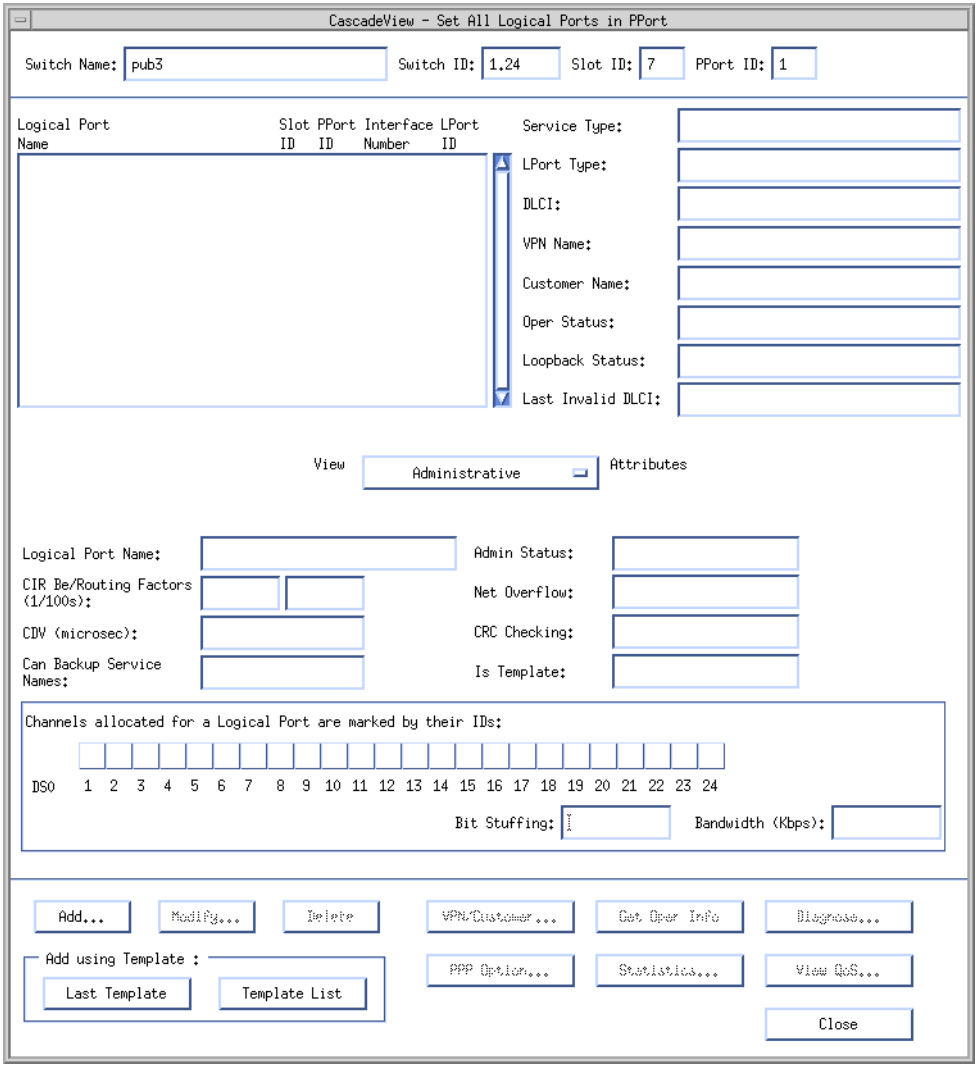

Figure 4-10. Set All Logical Ports in PPort Dialog Box

2. Choose Add if you are not using a template to enter values for the logical port. If you want to base the values for the logical port on a template, choose:

   - Last Template to use the last template you created
   - Template List to choose from a list of the templates you have created

   The Add Logical Port dialog box appears (see Figure 4-11).

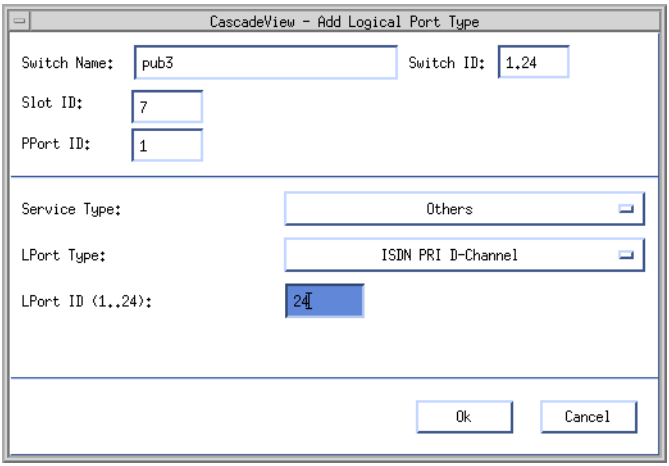

Figure 4-11. Add Logical Port Dialog Box

3. Complete the Add Logical Port dialog box fields described in Table 4-6.

Table 4-6. Add Logical Port Fields

Field	Action/Description
Service Type	Select Others.
LPort Type	Select ISDN PRI D-Channel.
LPort ID	Type 24 to reserve DS0 channel 24.

4. Choose OK. The Add Logical Port dialog box reappears (see Figure 4-12).

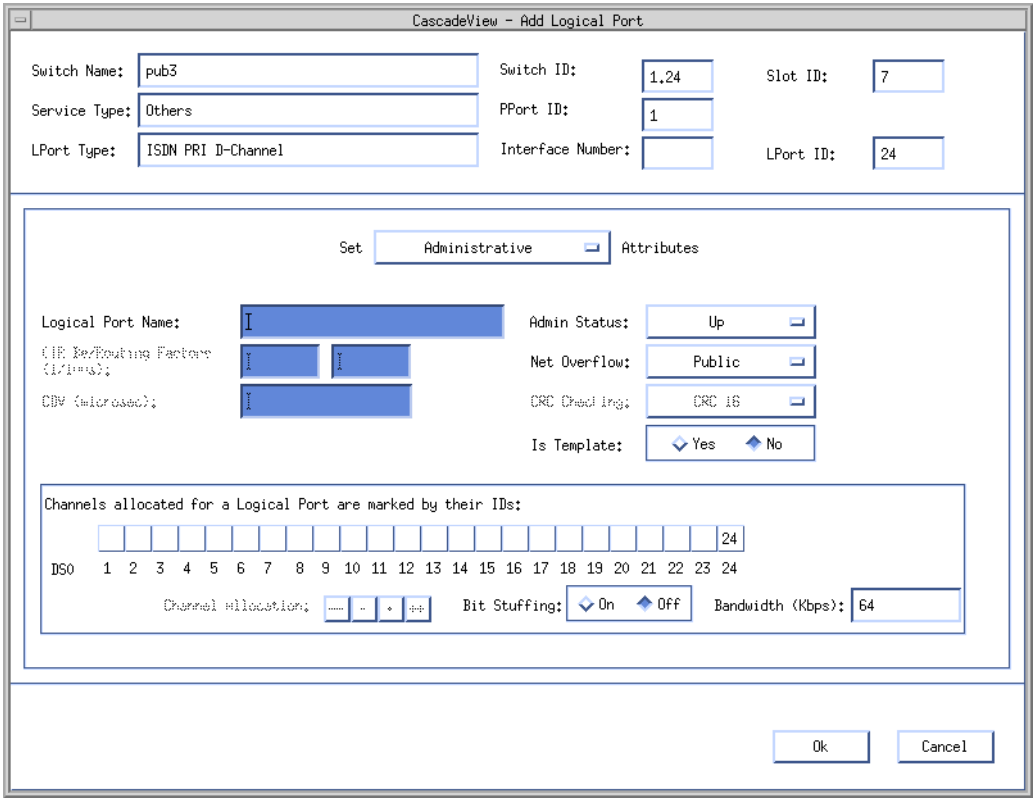

Figure 4-12. Add Logical Port Dialog Box — Set Attributes

5. Complete the Add Logical Port dialog box fields described in Table 4-7.

Table 4-7. Add Logical Port Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric name for this logical port. CascadeView/UX uses this name to reference the logical port.

Table 4-7. Add Logical Port Fields (Continued)

Field	Action/Description
Admin Status	Set the Admin Status to *Up*. *Up* — This option places the port in an active state. This is the default setting. *Down* — This option places the port in an inactive state. You can 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.

6. Select *Trap Control* from the Set Attributes menu. The Add Logical Port — Set Trap Control Attributes dialog box appears (see Figure 4-13).

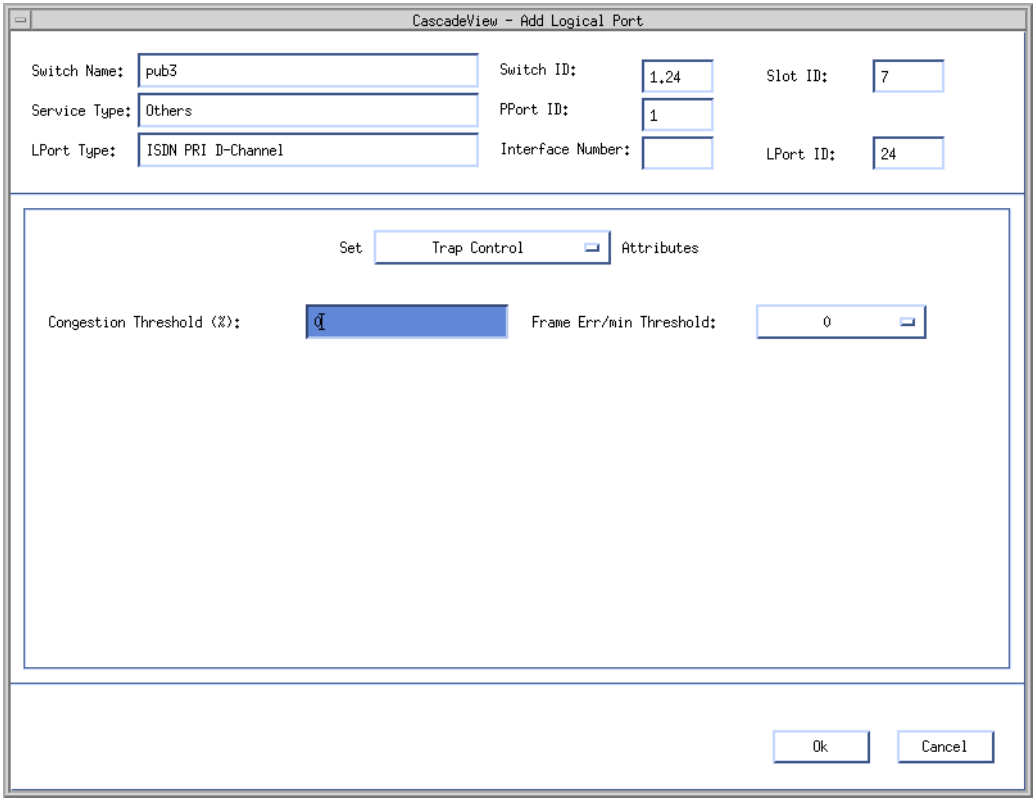

Figure 4-13. Add Logical Port — Set Trap Control Attributes Dialog Box

7. Complete the Add Logical Port — Set Trap Control Attributes dialog box fields described in Table 4-8.

Table 4-8. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold	Enter a value between 0 and 100 (%). This percentage is used 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 this value depending on how sensitive this port needs to be to network congestion. • Set this value low to generate a trap at the first sign of congestion. • Set this value high to generate traps only for serious network congestion. • Use the default of zero to disable this feature — no traps are generated for this logical port.

Table 4-8. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Frame Err/Min Threshold	Select a value between 0 and 16384. The pull-down list includes 0, 1, and powers of 2 up to 16384. The value you enter defines the threshold of frame errors on this logical port and triggers a trap to be sent to the NMS. If the number of frame errors received in one minute exceeds the number you specify, a trap is sent to the NMS. The default setting is zero. Adjust this value depending on how sensitive this port needs to be to frame errors. This logical port becomes more sensitive to frame errors if you configure a low threshold. Set this value *high* to only generate traps when a significant number of frame errors occur within a one-minute period. Use the default of zero to disable this feature. If you enter zero, no traps are generated for this logical port.

8. Select *Administrative* from the Set Attributes menu. The Add Logical Port — Set Administrative Attributes dialog box appears (see Figure 4-14).

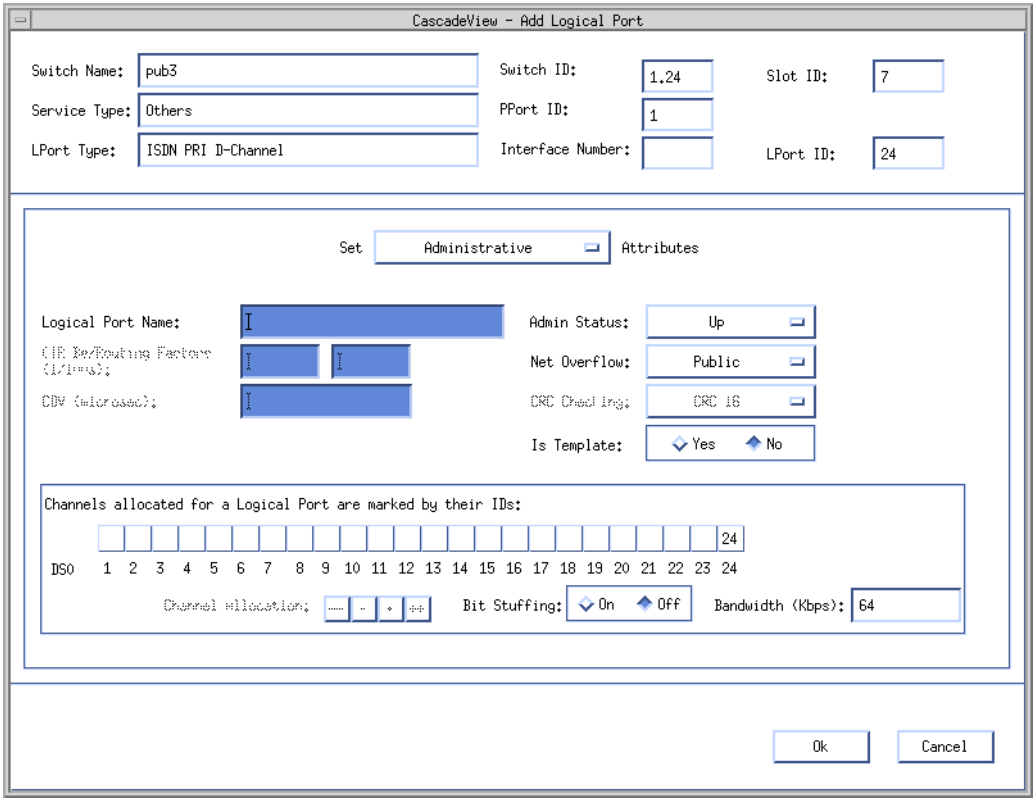

Figure 4-14. Add Logical Port — Set Administrative Attributes Dialog Box

9. Complete the Add Logical Port — Set Administrative Attributes dialog box fields described in Table 4-9.

Table 4-9. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	Verify the field displays Lport ID 24 in the box for DS0 24. When you configure a D-channel, the box for DS0 24 displays the LPort ID you entered in Step 3 on page 4-26. This channel performs all ISDN signaling.

Table 4-9. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Bit Stuffing	Bit stuffing defaults to Off for the D-channel, and 64 Kbps of bandwidth is reserved for the D-channel.
Is Template	(*Optional*) Choose *Yes* if you want to save these settings as a template that you can use again to quickly configure a logical port with the same options.

10. Choose OK to return to the Set All Logical Ports in PPort dialog box.

    The name of the logical port you just configured appears in the list.

11. Repeat this procedure if there is a need to define a D-channel for each of the remaining physical ports. If you are using Super D-channel, or when you are done defining the other D-channels, the next step is to define the B-channels. Continue with the following section.

Defining the B-Channels

B-channels are referred to as *bearer* channels or *data* channels. When a D-channel receives the ISDN call setup message, a B-channel associated with this D-channel is selected to handle the call.

Select the B-channel logical port type to correspond to the network protocol of the CPE connected to this port. This chapter provides an example using a PPP-to-1490 logical port configuration.

The following example configures a B-channel for PPP over ISDN to Frame Relay. You can use similar steps to configure any service and LPort type.

To define the B-channel logical port:

1. For the physical port on which you are defining the B-channel, access the Set All Logical Ports in PPort dialog box (see Figure 4-15). Refer to “Access the Set All Logical Ports in PPort Dialog Box” on page 4-3.

If the LOOPBACK field displays “loopback”, do not modify or delete the selected logical port.

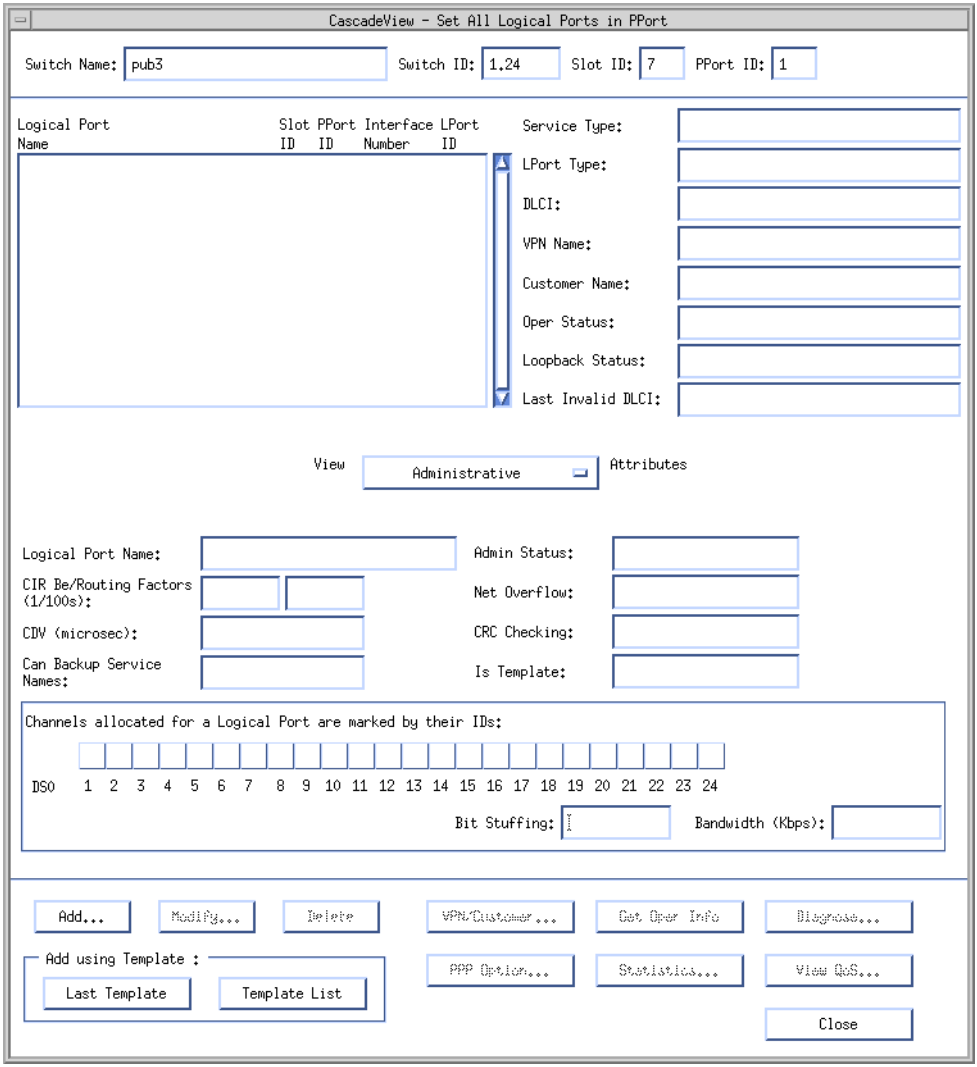

Figure 4-15. Set All Logical Ports in PPort dialog box

2. Choose Add if you are not using a template to enter values for the logical port.

   If you want to base the values for the logical port on a template, choose:

   - Last Template to use the last template you created
   - Templates list to choose from a list of the templates you have created

   The Add Logical Port dialog box appears (see Figure 4-16).

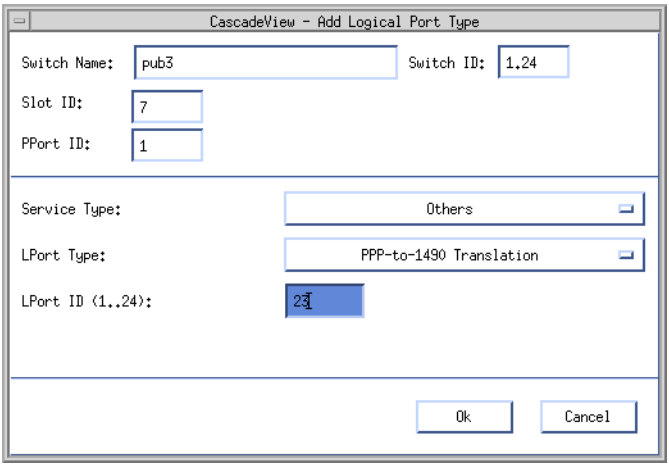

Figure 4-16. Add Logical Port Dialog Box

3. Complete the Add Logical Port dialog box fields described in Table 4-10.

Table 4-10. Add Logical Port Fields

Field	Action/Description
Service Type	Select Others to configure PPP-to-1490.
LPort Type	Select the LPort Type (PPP-to-1490)
LPort ID	Type a logical port ID between 1 and 23. This ID should correspond to the DS0 channel you are using.

4. Choose OK. The Add Logical Port dialog box reappears (see Figure 4-17).

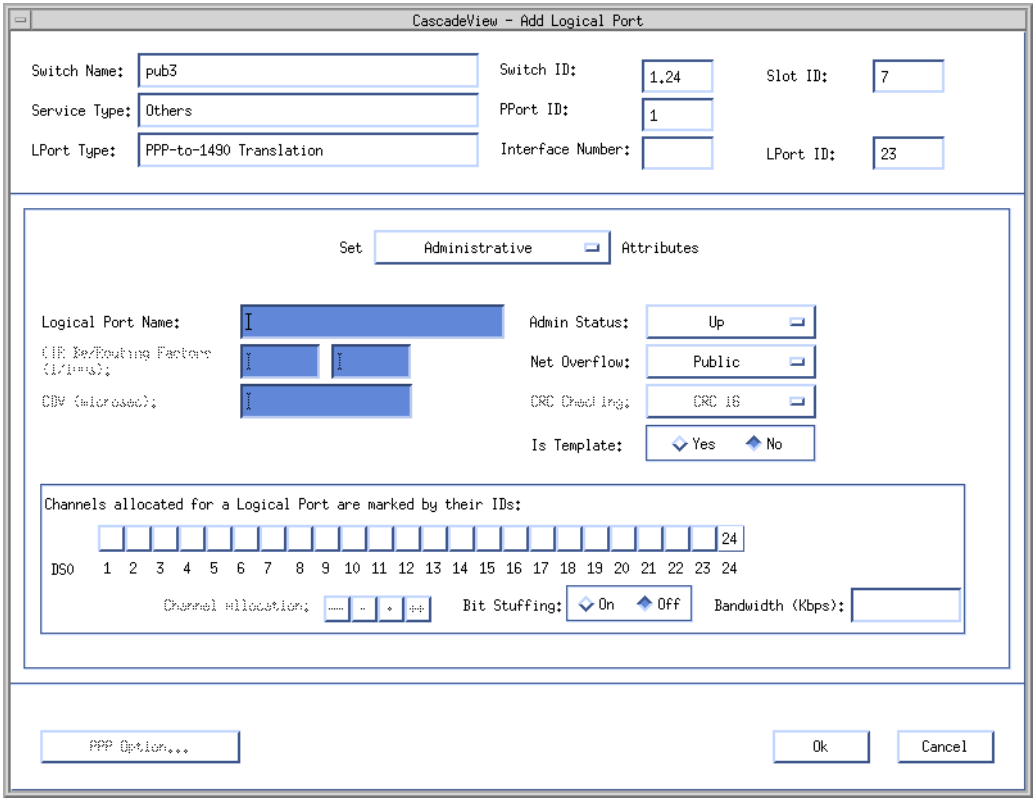

Figure 4-17. Add Logical Port Dialog Box — Set Attributes

5. Complete the Add Logical Port dialog box fields described in Table 4-11.

Table 4-11. Add Logical Port Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric name for this logical port. CascadeView/UX uses this name to reference the logical port.

Table 4-11. Add Logical Port Fields (Continued)

Field	Action/Description
Admin Status	Set the Admin Status to *Up*. *Up* — This option places the port in an active state. This is the default setting. *Down* — This option places the port in an inactive state. You can 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.

6. Select *Trap Control* from the Set Attributes menu. The Add Logical Port — Set Trap Control Attributes dialog box appears (see Figure 4-18).

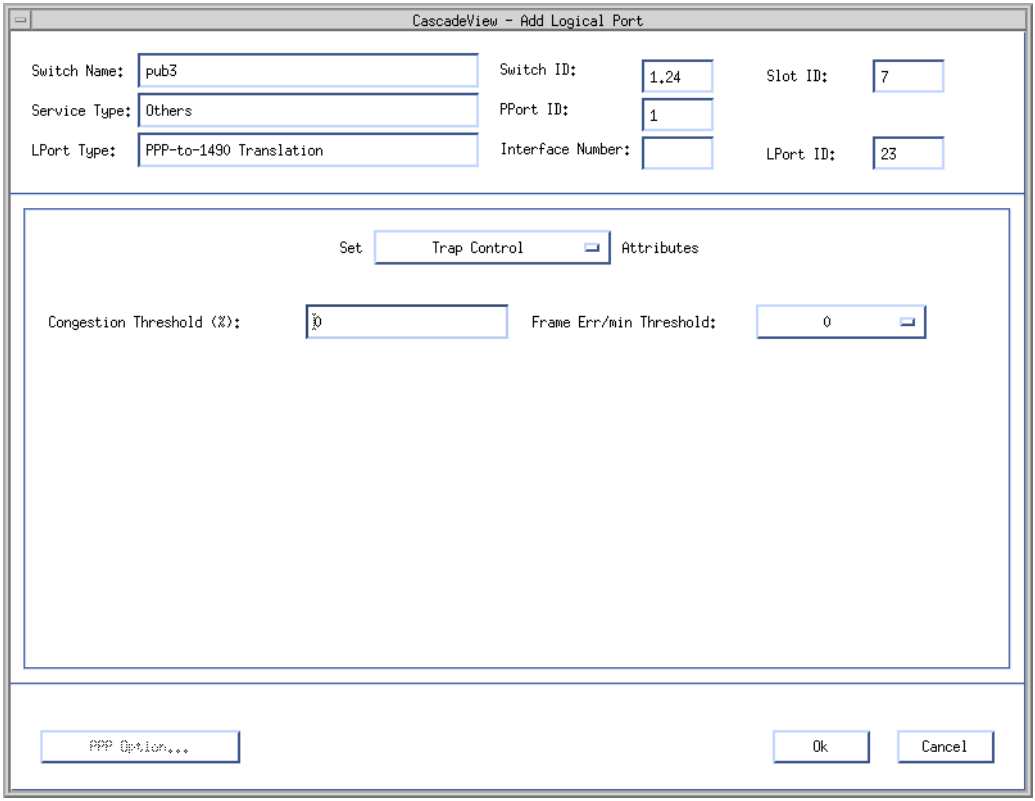

Figure 4-18. Add Logical Port — Set Trap Control Attributes Dialog Box

7. Complete the Add Logical Port — Set Trap Control Attributes dialog box fields described in Table 4-12.

Table 4-12. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold	Enter a value between 0 and 100 (%). This percentage is used 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 this value depending on how sensitive this port needs to be to network congestion. • Set this value low to generate a trap at the first sign of congestion. • Set this value high to generate traps only for serious network congestion. • Use the default of zero to disable this feature — no traps are generated for this logical port.

Table 4-12. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Frame Err/Min Threshold	Select a value between 0 and 16384. The pull-down list includes 0, 1, and powers of 2 up to 16384. The value you enter defines the threshold of frame errors on this logical port and triggers a trap to be sent to the NMS. If the number of frame errors received in one minute exceeds the number you specify, a trap is sent to the NMS. The default setting is zero. Adjust this value depending on how sensitive this port needs to be to frame errors. This logical port becomes more sensitive to frame errors if you configure a low threshold. Set this value *high* to only generate traps when a significant number of frame errors occur within a one-minute period. Use the default of zero to disable this feature. If you enter zero, no traps are generated for this logical port.

8. Select *Administrative* from the Set Attributes menu. The Add Logical Port — Set Administrative Attributes dialog box appears (see Figure 4-19).

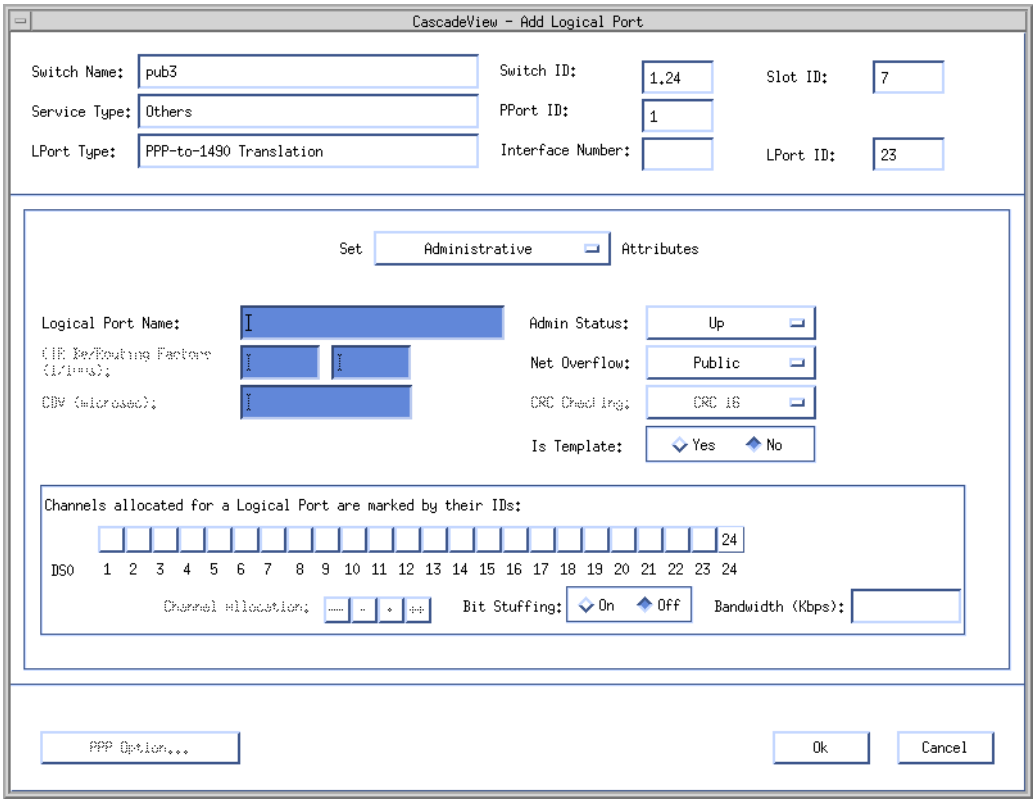

Figure 4-19. Add Logical Port — Set Administrative Attributes Dialog Box

9. Complete the Add Logical Port — Set Administrative Attributes dialog box fields described in Table 4-13.

Table 4-13. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	Select the DS0 channel that corresponds to the LPort ID you entered in Step 3 on page 4-36. To add or remove an X in a channel, click the left mouse button on the channel.

Table 4-13. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Bit Stuffing	Choose the Bit Stuffing setting that matches the bandwidth capability of the CPE connected to this B-channel: *On*: Provides 56 Kbps of bandwidth *Off*: Provides 64 Kbps of bandwidth
Is Template	(*Optional*) Choose *Yes* if you want to save these settings as a template that you can use again to quickly configure a logical port with the same options.

10. Choose OK to return to the Set All Logical Ports in PPort dialog box.
11. If you need to configure additional B-channels, return to Step 1 on page 4-34. Otherwise, proceed to "Configuring E.164 Called Addresses" on page 4-82.

Configuring the E1/ISDN I/O Module

Configuring the E1/ISDN I/O module consists of the following tasks:

- Setting the E1/ISDN I/O Module Attributes (page 4-44)
- Configuring the Module's Physical Port Attributes (page 4-49)
- Configuring the D-Channel(s) (page 4-54)
- Defining the B-Channels (page 4-63)

Setting the E1/ISDN I/O Module Attributes

Configure the E1/ISDN I/O (PRI E1) module as follows:

1. Access the Switch Back Panel dialog box with the Set Parameters command (refer to "Accessing the Switch Back Panel Dialog Box" on page 4-9).
2. Select the specific PRI E1 module you want to configure. The Set Card Attributes dialog box appears (see Figure 4-20).

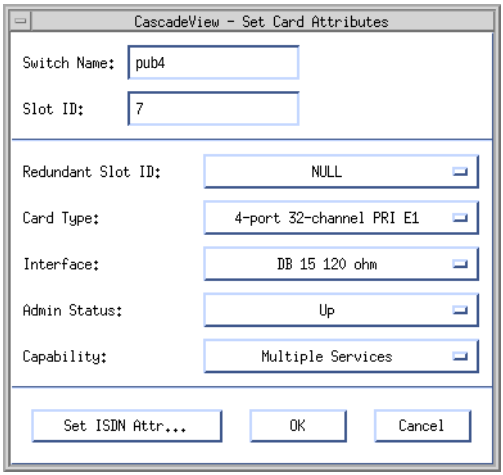

Figure 4-20. Set Card Attributes Dialog Box

3. Complete the Set Card Attributes dialog box fields described in Table 4-14.

Table 4-14. Set Card Attributes Fields

Field	Action/Description
Card Type	Select 4-port 32-channel PRI E1.
Redundant Slot ID	(*Optional*) Set if this PRI I/O module is to have a redundant standby partner installed. The default setting is NULL. You must always install and configure the redundant PRI I/O module in the next higher slot from its main partner. For a more complete description of configuring B-STDX modules and redundancy, refer to the *Network Configuration Guide for B-STDX/STDX*.
Admin Status	Set to *Up* for normal operation. *Up* — This PRI I/O module becomes fully operational when you start the switch. *Down* — This PRI I/O module does not come on-line when you start the switch. The configuration is saved in the database but is not downloaded to the switch. Use this option when you run foreground diagnostics. Maintenance — This PRI I/O module does not receive the application software when you start the switch. A module in this state only has its boot flash loaded; application code is not running. This setting enables you to reset the PRAM for a module that cannot boot due to invalid PRAM. You can also use this option to troubleshoot a hardware problem.

4. Choose the *Set ISDN Attr . . .* command.

The Set ISDN Card Attributes dialog box appears (see Figure 4-21). The ISDN Card Attributes dialog box enables you to specify the signaling to be used between the Central Office and the Ascend B-STDX switch.

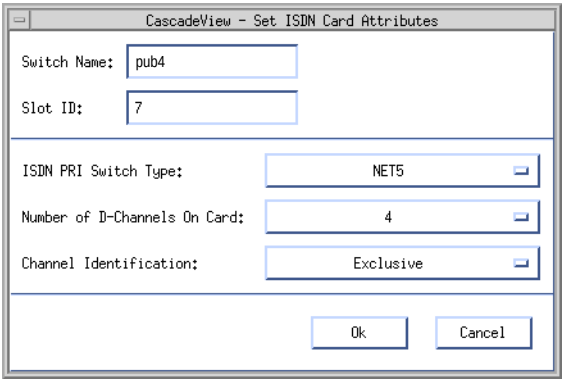

Figure 4-21. Set ISDN Card Attributes Dialog Box

5. Complete the Set ISDN Card Attributes dialog box fields described in Table 4-15.

Table 4-15. Set ISDN Card Attributes Fields

Field	Action/Description
ISDN PRI Switch Type	Select the type that corresponds to the signaling standard used by the ISDN central office switch. *TPH* (Australian ISDN) *NET5* (Euro ISDN) The AT&T 5ESS, AT&T 4ESS, and NT DMS-100 selections are gray and are not available, since they are for T1 PRIs.
Number of D-Channels On Card	Defaults to 4, which configures one D-channel for each of the four physical ports. You cannot configure a Super D-channel on the E1 card.

Table 4-15. Set ISDN Card Attributes Fields (Continued)

Field	Action/Description
Channel Identification	Select *Exclusive.* The Channel Identification method defines how the central office will handle the incoming ISDN call. *Exclusive* — Enables the central office switch to assign the B-channel as soon as the call is received. *This is the standard method of operation.* *Preferred* — Enables the Ascend switch to assign the B-channel.

6. Choose OK to return to the Set Card Attributes dialog box.
7. Choose OK to return to the Switch Back Panel dialog box.

   The PRI E1 module you configured is displayed (see Figure 4-22).

Proceed to the next section to configure the module's physical port attributes.

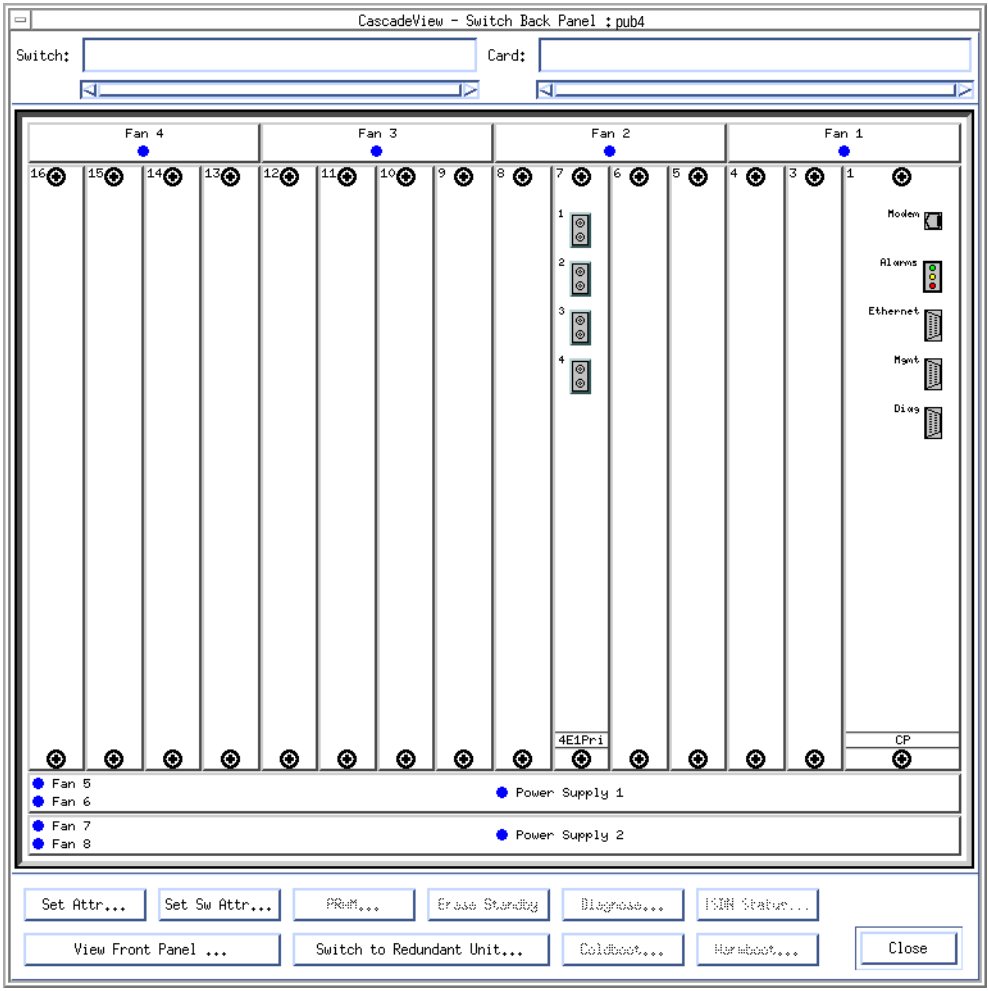

Figure 4-22. Switch Back Panel Dialog Box

Configuring the E1/ISDN/I/O Module's Physical Port Attributes

This section describes how to configure those attributes that are specific to each physical port on the PRI I/O module. Some attributes define the framing and encoding of the data passing through the module. Others are used to define the clock source, the connection type, and the length of the ISDN line used to connect the Central Office to the Ascend B-STDX switch.

To configure the physical port attributes:

1. Access the Switch Back Panel dialog box with the Set Parameters command (refer to "Accessing the Switch Back Panel Dialog Box" on page 4-9).

2. Select the physical port you want to configure by placing the cursor on the port you want to configure and double-clicking on the left mouse button.

   The Set Physical Port Attributes dialog box appears (see Figure 4-23).

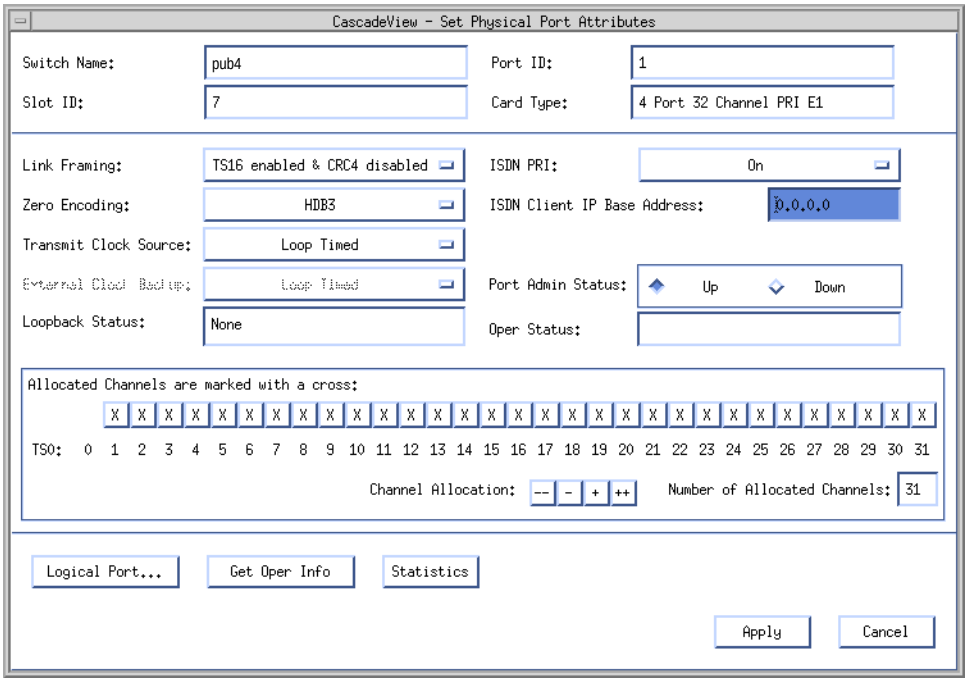

Figure 4-23. Set Physical Port Attributes Dialog Box

*If **none** is not displayed in the **loopback status** field, 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.*

3. Complete the Set Physical Port Attributes dialog box fields described in Table 4-16.

Table 4-16. Set Physical Port Attributes Fields

Field	Action/Description
Link Framing	Link Framing defines a framing specification. Framing provides a method of distinguishing between the individual channels; it is accomplished by adding one additional bit to each frame. Make sure you configure the customer premise equipment (CPE) to use the same framing specification as the Ascend physical port. Select one of the following options. TS16 enabled & CRC4 disabled. This is the default. TS16 enabled & CRC4 enabled **TS16** refers to time slot 16. By enabling TS16, the D-channel can be time slot 16. **CRC4** performs a cyclic redundancy check when it is enabled.

Table 4-16. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Zero Encoding	Zero Encoding specifies the format of the data signal encoding. HDB3 is an encoding scheme associated with European PCM-30 (E-1) format designed to provide clear channel capabilities by substituting any consecutive string of eight zeros with an established pattern. The default is HDB3. Refer to your facility service provider for more information about selecting a zero encoding method.
Transmit Clock Source	This option defines the source of the transmit clock. Select one of the following options. *Looped Time* — This is the default. The clock source is derived from the network timing received. *Internal* — The internal T1 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 *Looped Time* or *Internal* clock source. Refer to the *Network Configuration Guide for B-STDX/STDX* for more information about external clock source.

Table 4-16. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
ISDN PRI	Select *On* to enable this E1 physical port to use ISDN PRI services. If you select *Off*, the physical port behaves as a standard E1. Refer to the *Network Configuration Guide for B-STDX/STDX* if you need to configure this module for standard E1 access.
ISDN Client IP Base Address	Leave the default address of 0.0.0.0 to disable this feature. When this feature is disabled, the IP address of the remote user will be used. If you want the switch to maintain a pool of IP addresses for the physical port and dynamically assign a temporary IP address to a remote user, enter the base IP address for this physical port. This address comes from the end-user LAN administrator. The Ascend switch will maintain a pool of IP addresses for the physical port that range from the base address you enter (x.y.z.n) to (x.y.z.n + 29). This provides 30 distinct IP addresses per physical port. The subnet mask is set on the ISDN CPE.
Port Admin Status	Select *Up*. *Up* — This option enables the port. *Down* — This option saves the configuration in the database without activating the port or to take the port off-line to run diagnostics. Each time you modify the Port Admin Status, choose Apply to send the change to the switch.

Table 4-16. Set Physical Port Attributes Fields (Continued)

Field	Action/Description
Allocated Channels are marked with a cross	Ensure that the channels you want to allocate are marked with an X, and remove the X from any channels you want to disable. By default, all TS0 channels are selected. To add or remove an X in a channel, click the left mouse button on the channel. You can also add and remove X's by using the four editing buttons: -- Deselects all channels. – Deselects the highest numbered channel that is allocated. + Selects the lowest numbered channel that is not allocated. ++ Selects all channels.

4. Notice the Number of Allocated Channels.

   This number is equal to the number of TS0 channels you enabled. TS016 is used for the D-channel, and the rest of the allocated channels can be configured as B-channels.

5. Choose Apply and then OK to save the physical port attributes.

   This sends an SNMP Set command to the switch.

6. Choose Cancel to exit the dialog box.

Configuring the D-Channel(s)

The D-channel carries common channel-signaling information to control circuit-switched calls on the associated B-channels. You use TS0 channel 16 for D-channel support.

Define one D-channel logical port on each of the physical ports that you are configuring B-channels on.

Proceed as follows to define the D-channel for ISDN services:

1. For the physical port on which you are defining the D-channel, access the Set All Logical Ports in PPort dialog box (see Figure 4-24). Refer to “Access the Set All Logical Ports in PPort Dialog Box” on page 4-3.

If the LOOPBACK field displays “loopback”, do not modify or delete the selected logical port.

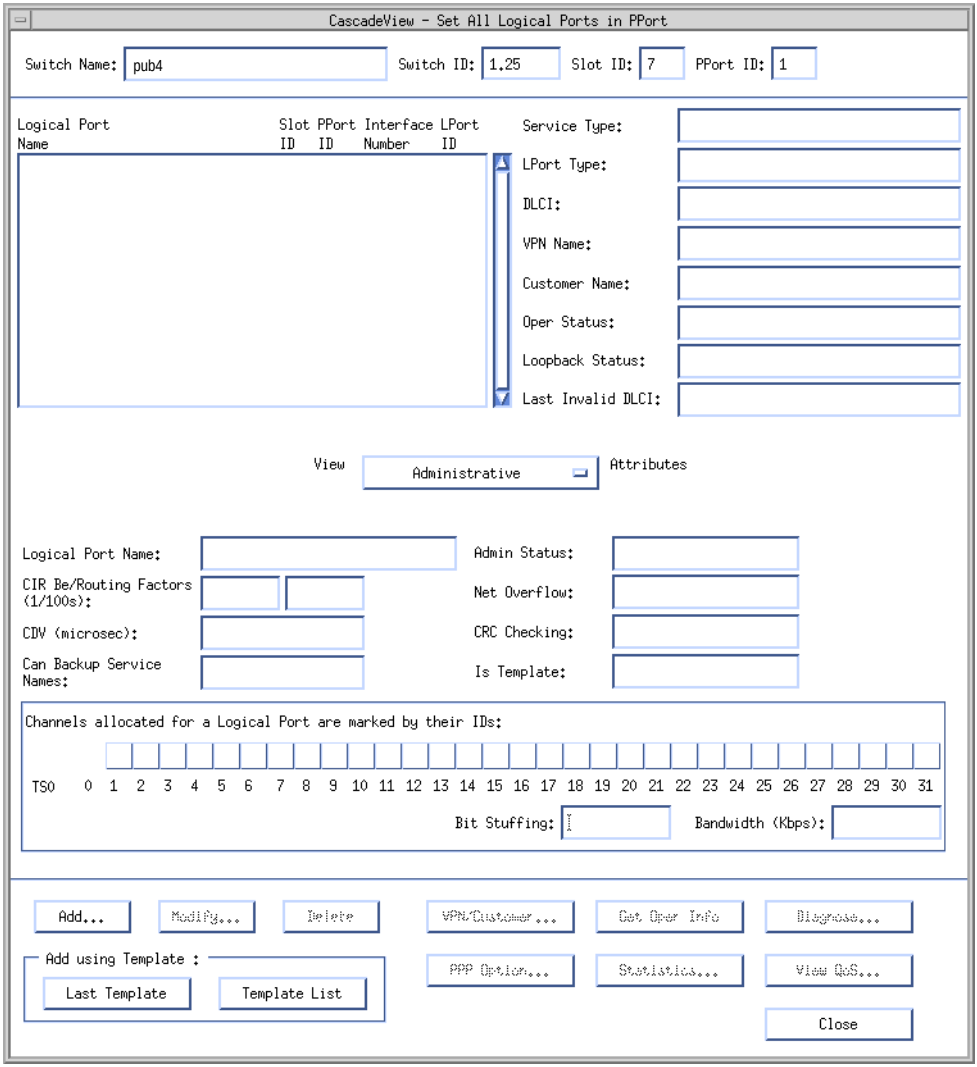

Figure 4-24. Set All Logical Ports in PPort Dialog Box

2. Choose Add if you are not using a template to enter values for the logical port. If you want to base the values for the logical port on a template, choose:

   - Last Template to use the last template you created
   - Template List to choose from a list of the templates you have created

   The Add Logical Port dialog box appears (see Figure 4-25).

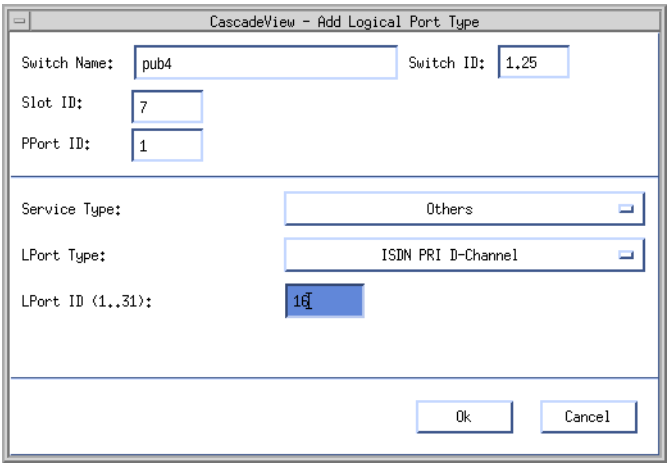

Figure 4-25. Add Logical Port Dialog Box

3. Complete the Add Logical Port dialog box fields described in Table 4-17.

Table 4-17. Add Logical Port Fields

Field	Action/Description
Service Type	Select Others.
LPort Type	Select ISDN PRI D-Channel.
LPort ID	Type 16 to reserve TS0 channel 16.

4. Choose OK. The Add Logical Port dialog box re-appears (see Figure 4-26).

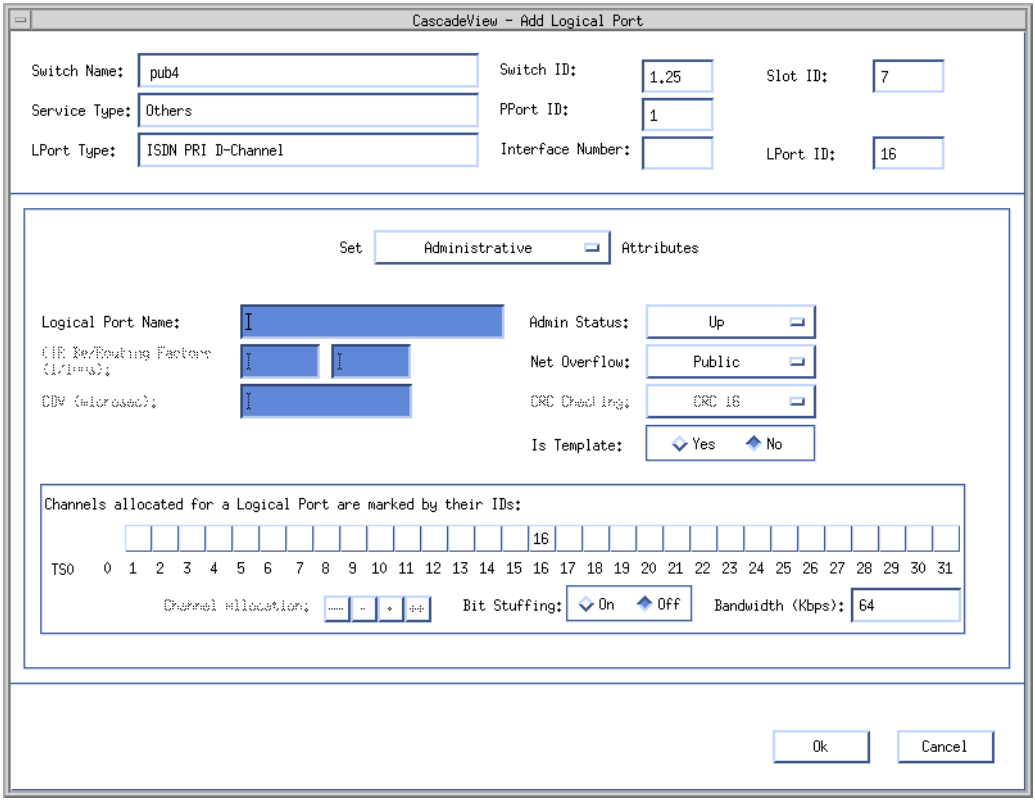

Figure 4-26. Add Logical Port Dialog Box — Set Attributes

5. Complete the Add Logical Port dialog box fields described in Table 4-18.

Table 4-18. Add Logical Port Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric name for this logical port. CascadeView/UX uses this name to reference the logical port.

Table 4-18. Add Logical Port Fields (Continued)

Field	Action/Description
Admin Status	Set the Admin Status to *Up*. *Up* — This option places the port in an active state. This is the default setting. *Down* — This option places the port in an inactive state. You can 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.

6. Select *Trap Control* from the Set Attributes menu. The Add Logical Port — Set Trap Control Attributes dialog box appears (see Figure 4-27).

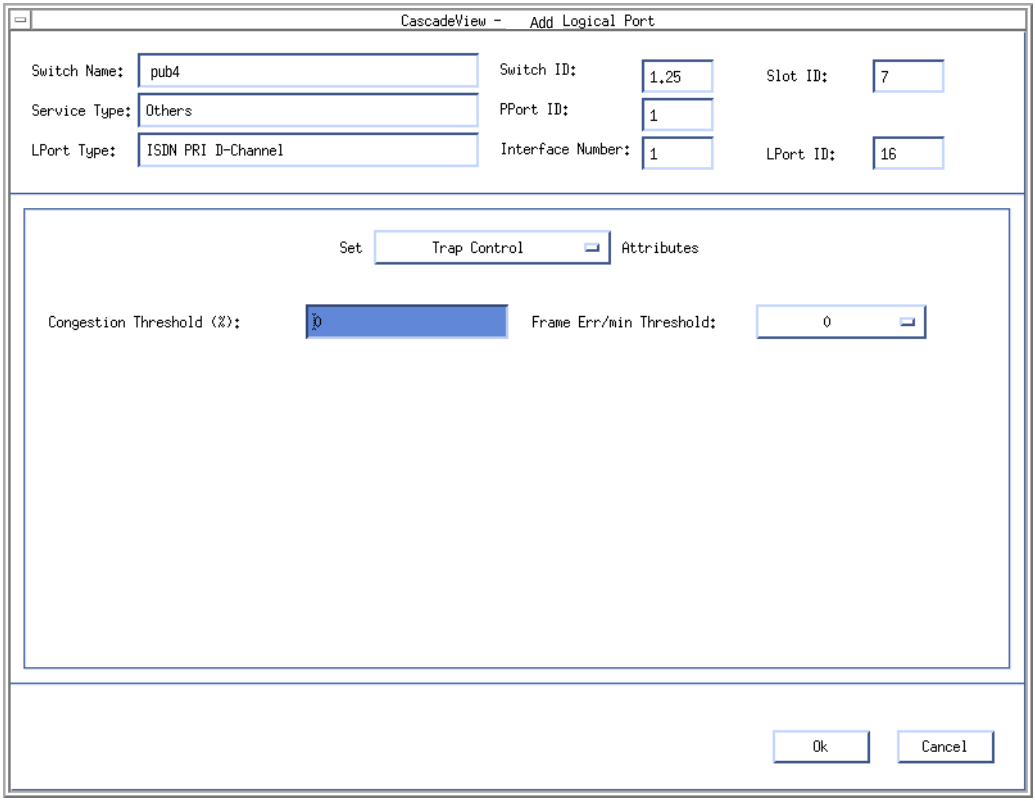

Figure 4-27. Add Logical Port — Set Trap Control Attributes Dialog Box

7. Complete the Add Logical Port — Set Trap Control Attributes dialog box fields described in Table 4-19.

Table 4-19. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold	Enter a value between 0 and 100 (%). This percentage is used 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 this value depending on how sensitive this port needs to be to network congestion. • Set this value low to generate a trap at the first sign of congestion. • Set this value high to generate traps only for serious network congestion. • Use the default of zero to disable this feature — no traps are generated for this logical port.

Table 4-19. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Frame Err/Min Threshold	Select a value between 0 and 16384. The pull-down list includes 0, 1, and powers of 2 up to 16384. The value you enter defines the threshold of frame errors on this logical port and triggers a trap to be sent to the NMS. If the number of frame errors received in one minute exceeds the number you specify, a trap is sent to the NMS. The default setting is zero. Adjust this value depending on how sensitive this port needs to be to frame errors. This logical port becomes more sensitive to frame errors if you configure a low threshold. Set this value *high* to only generate traps when a significant number of frame errors occurs within a one-minute period. Use the default of zero to disable this feature. If you enter zero, no traps are generated for this logical port.

8. Select *Administrative* from the Set Attributes menu. The Add Logical Port — Set Administrative Attributes dialog box appears (see Figure 4-28).

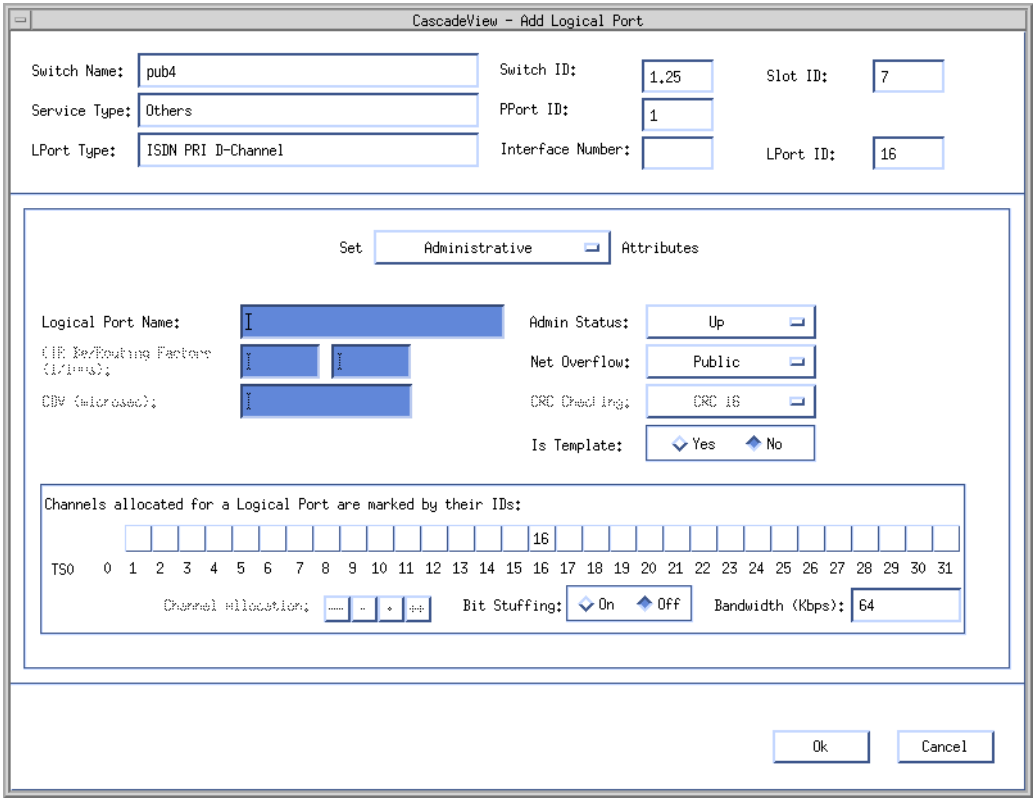

Figure 4-28. Add Logical Port — Set Administrative Attributes Dialog Box

9. Complete the Add Logical Port — Set Administrative Attributes dialog box fields described in Table 4-20.

Table 4-20. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	Verify the field displays Lport ID 16 in the box for TS0 16. When you configure a D-channel, the box for TS0 16 displays the LPort ID you entered in Step 3 on page 4-56. This channel performs all ISDN signaling.

Table 4-20. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Bit Stuffing	Bit stuffing defaults to Off for the D-channel, and 64 Kbps of bandwidth is reserved for the D-channel.
Is Template	(*Optional*) Choose *Yes* if you want to save these settings as a template that you can use again to quickly configure a logical port with the same options.

10. Choose OK to return to the Set All Logical Ports in PPort dialog box.

    The name of the logical port you just configured appears in the list.

11. Repeat this procedure if you need to define a D-channel for any of the remaining physical ports. When you are done defining the other D-channels, the next step is to define the B-channels. Continue with the following section.

Defining the B-Channels

B-channels are referred to as *bearer* channels or *data* channels. When a D-channel receives the ISDN call setup message, a B-channel associated with this D-channel is selected to handle the call.

Select the B-channel logical port type to correspond to the network protocol of the CPE connected to this port. This chapter provides an example using a PPP-to-1490 logical port configuration.

The following example configures a B-channel for PPP over ISDN to Frame Relay. You can use similar steps to configure any service and LPort type.

To define the B-channel logical port:

1. For the physical port on which you are defining the B-channel, access the Set All Logical Ports in PPort dialog box (see Figure 4-29). Refer to “Access the Set All Logical Ports in PPort Dialog Box” on page 4-3.

If the LOOPBACK field displays “loopback”, do not modify or delete the selected logical port.

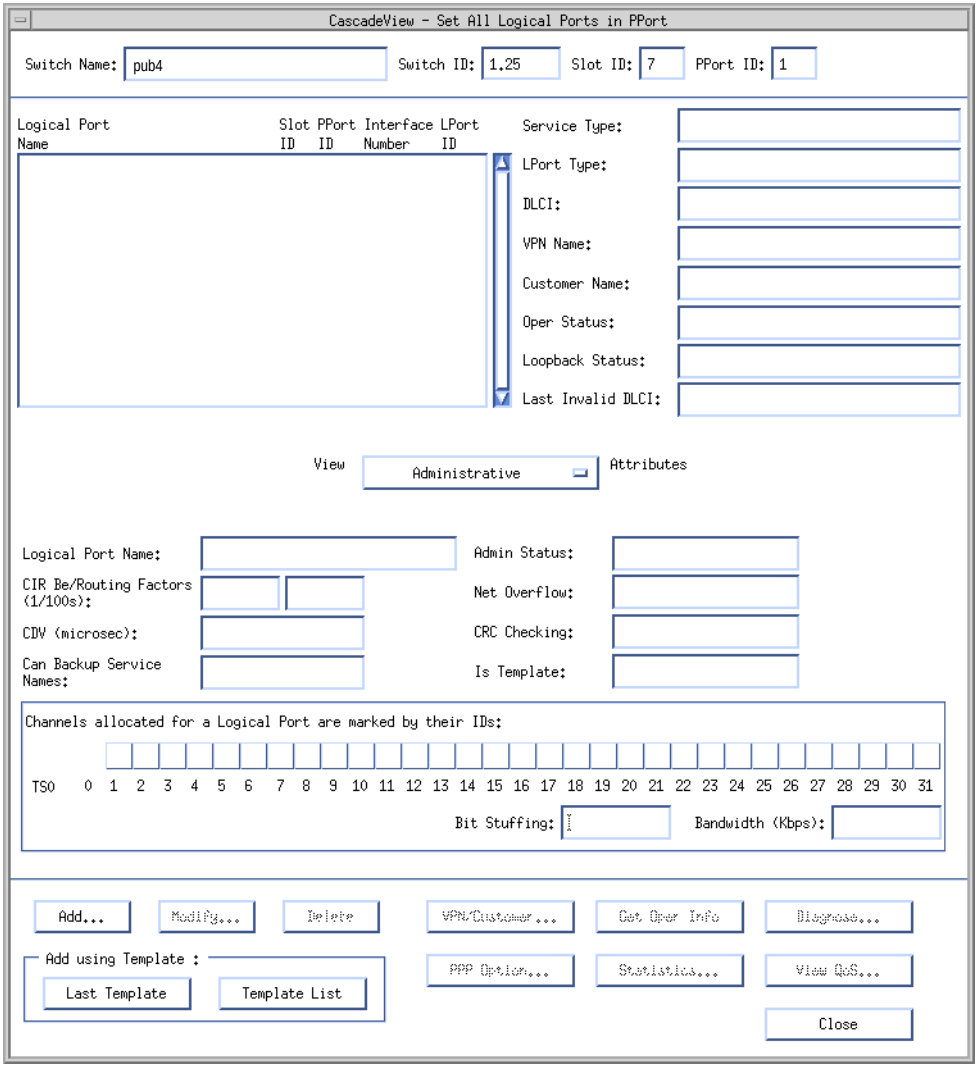

Figure 4-29. Set All Logical Ports in PPort Dialog Box

2. Choose Add if you are not using a template to enter values for the logical port.

   If you want to base the values for the logical port on a template, choose:

   - Last Template to use the last template you created
   - Template List to choose from a list of the templates you have created

   The Add Logical Port dialog box appears (see Figure 4-30).

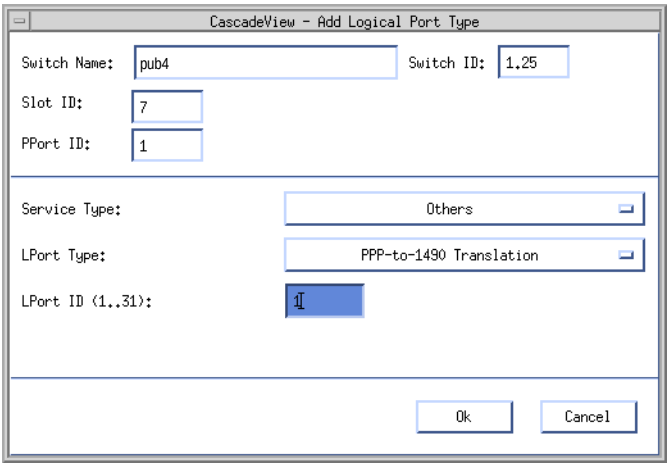

Figure 4-30. Add Logical Port Dialog Box

3. Complete the Add Logical Port dialog box fields described in Table 4-21.

Table 4-21. Add Logical Port Fields

Field	Action/Description
Service Type	Select Others to configure PPP-to-1490.
LPort Type	Select the LPort Type (PPP-to-1490).
LPort ID	Type a logical port ID between 1 and 31. This ID should correspond to the TS0 channel you are using.

4. Choose OK. The Add Logical Port dialog box reappears (see Figure 4-31).

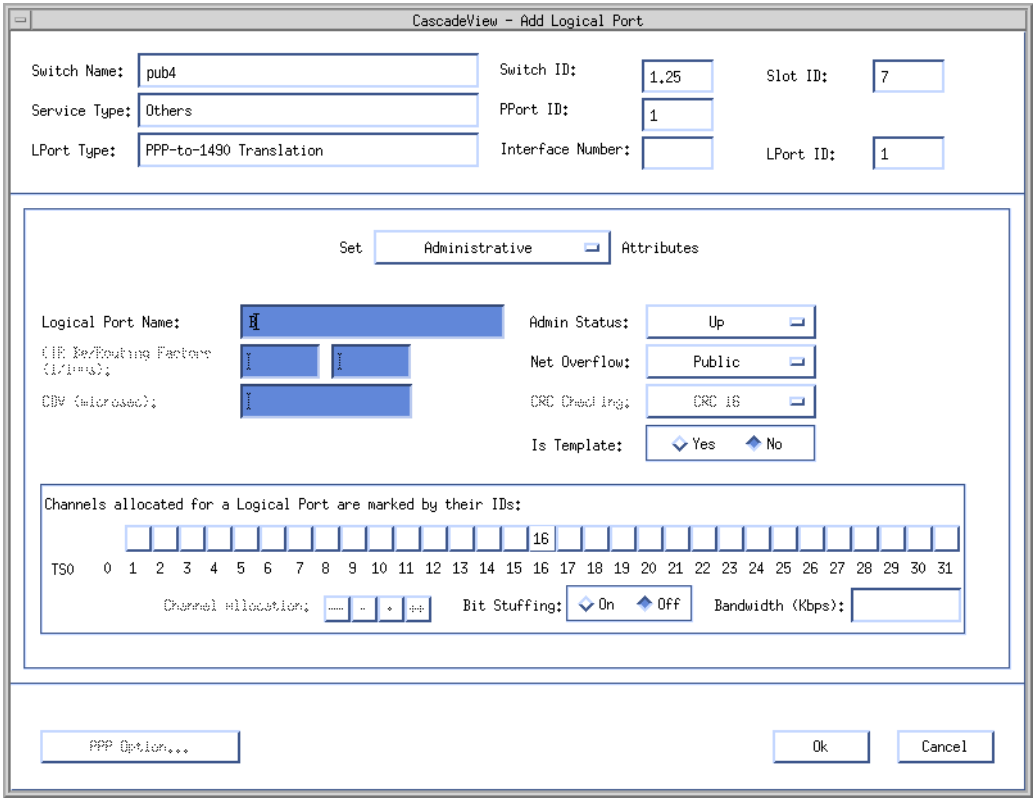

Figure 4-31. Add Logical Port Dialog Box — Set Attributes

5. Complete the Add Logical Port dialog box fields described in Table 4-22.

Table 4-22. Add Logical Port Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric name for this logical port. CascadeView/UX uses this name to reference the logical port.

Table 4-22. Add Logical Port Fields (Continued)

Field	Action/Description
Admin Status	Set the Admin Status to *Up*. *Up* — This option places the port in an active state. This is the default setting. *Down* — This option places the port in an inactive state. You can 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.

6. Select *Trap Control* from the Set Attributes menu. The Add Logical Port — Set Trap Control Attributes dialog box appears (see Figure 4-32).

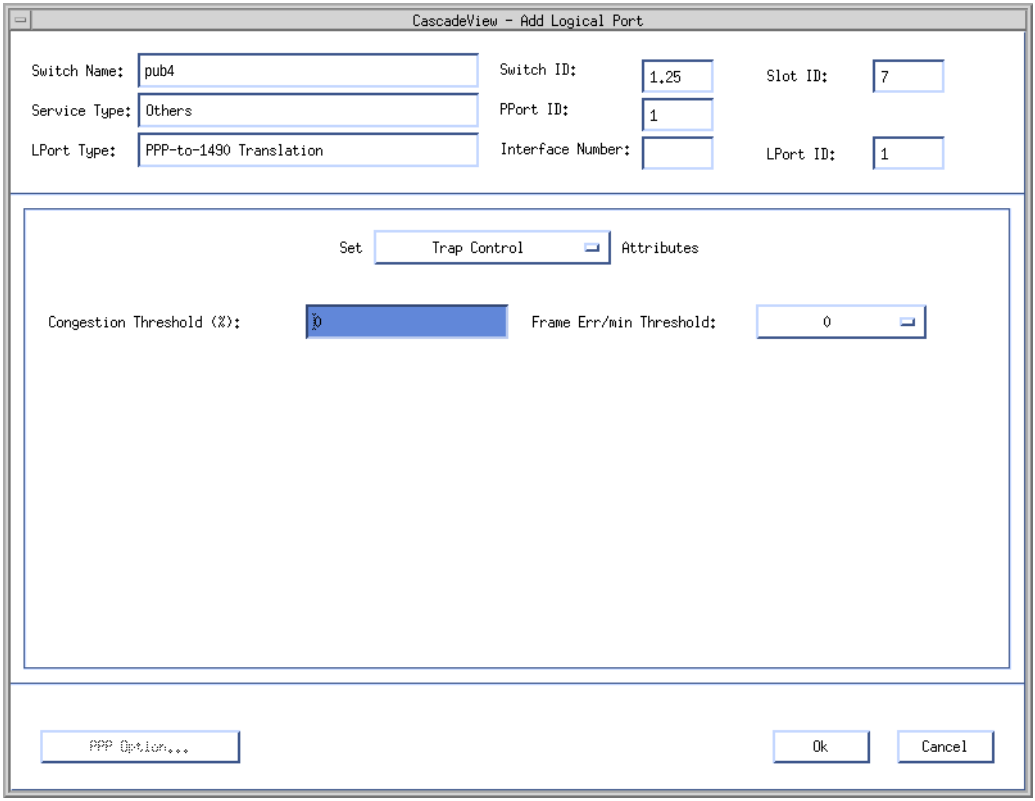

Figure 4-32. Add Logical Port — Set Trap Control Attributes Dialog Box

7. Complete the Add Logical Port — Set Trap Control Attributes dialog box fields described in Table 4-23.

Table 4-23. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold	Enter a value between 0 and 100 (%). This percentage is used 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 this value depending on how sensitive this port needs to be to network congestion. • Set this value low to generate a trap at the first sign of congestion. • Set this value high to generate traps only for serious network congestion. • Use the default of zero to disable this feature — no traps are generated for this logical port.

Table 4-23. Add Logical Port — Set Trap Control Attributes Fields

Field	Action/Description
Frame Err/Min Threshold	Select a value between 0 and 16384. The pull-down list includes 0, 1, and powers of 2 up to 16384. The value you enter defines the threshold of frame errors on this logical port and triggers a trap to be sent to the NMS. If the number of frame errors received in one minute exceeds the number you specify, a trap is sent to the NMS. The default setting is zero. Adjust this value depending on how sensitive this port needs to be to frame errors. This logical port becomes more sensitive to frame errors if you configure a low threshold. Set this value *high* to only generate traps when a significant number of frame errors occur within a one-minute period. Use the default of zero to disable this feature. If you enter zero, no traps are generated for this logical port.

8. Select *Administrative* from the Set Attributes menu. The Add Logical Port — Set Administrative Attributes dialog box appears (see Figure 4-33).

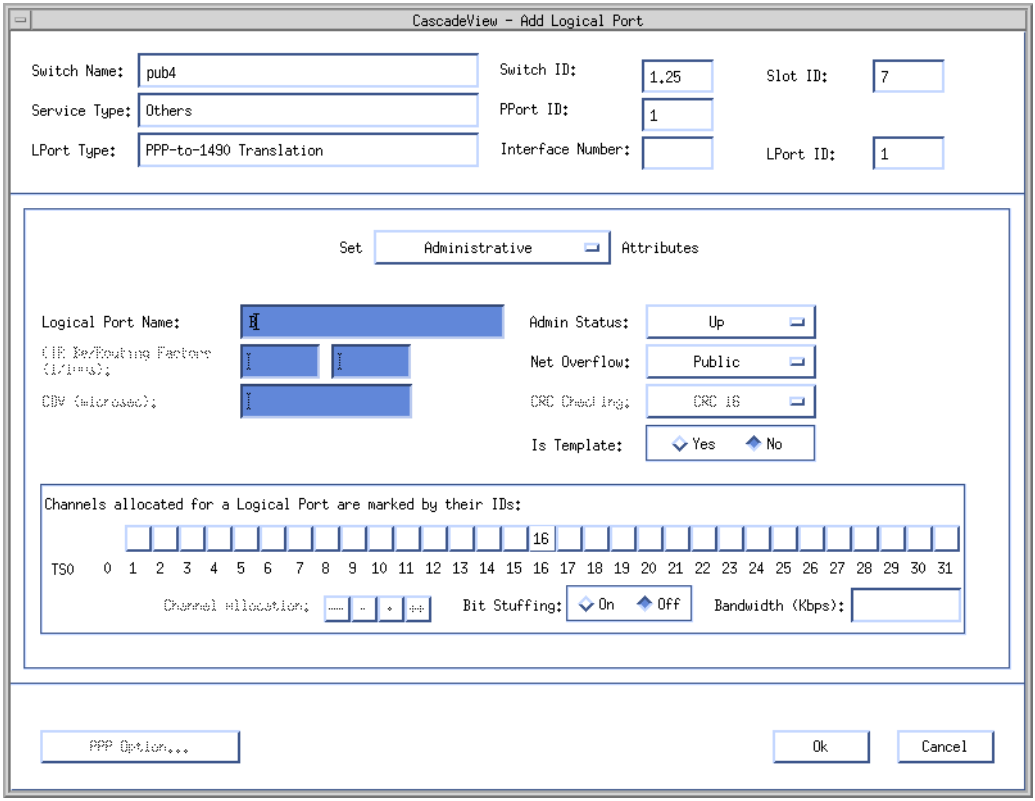

Figure 4-33. Add Logical Port — Set Administrative Attributes Dialog Box

9. Complete the Add Logical Port — Set Administrative Attributes dialog box fields described in Table 4-24.

Table 4-24. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Channels allocated for a Logical Port are marked by their IDs	Select the TS0 channel that corresponds to the LPort ID you entered in Step 3 on page 4-66. To add or remove an X in a channel, click the left mouse button on the channel.

Table 4-24. Add Logical Port — Set Administrative Attributes Fields

Field	Action/Description
Bit Stuffing	Choose the Bit Stuffing setting that matches the bandwidth capability of the CPE connected to this B-channel: *On*: Provides 56 Kbps of bandwidth *Off*: Provides 64 Kbps of bandwidth
Is Template	(*Optional*) Choose *Yes* if you want to save these settings as a template that you can use again to quickly configure a logical port with the same options.

10. Choose OK to return to the Set All Logical Ports in PPort dialog box.
11. Repeat this procedure if you need to configure additional B-channels. Otherwise, proceed to "Configuring E.164 Called Addresses" on page 4-82.

Modify a Logical Port Configuration

To modify a logical port configuration:

1. For the physical port on which the logical port is located, access the Set All Logical Ports in PPort dialog box (see Figure 4-34). Refer to "Access the Set All Logical Ports in PPort Dialog Box" on page 4-3.

If the LOOPBACK field displays "loopback", do not modify or delete the selected logical port.

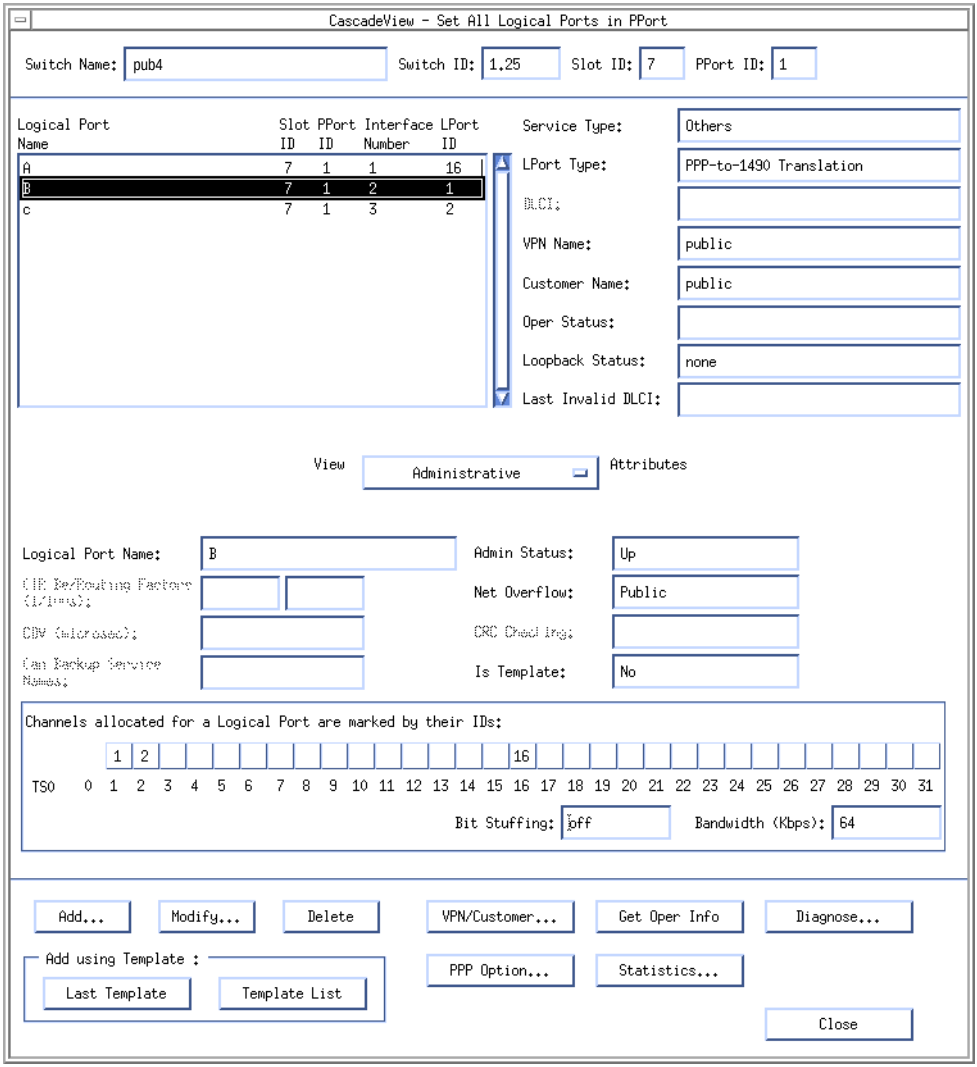

Figure 4-34. Set All Logical Ports in PPort Dialog Box

2. Select the logical port and choose Modify. The Modify Logical Port dialog box appears (see Figure 4-35).

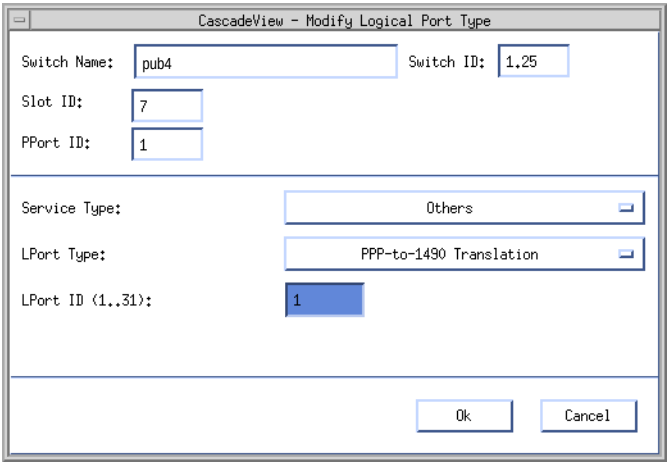

Figure 4-35. Modify Logical Port Dialog Box

3. Make desired changes, and choose OK. The Modify Logical Port dialog box reappears, displaying the rest of the attributes of the selected logical port (see Figure 4-36).

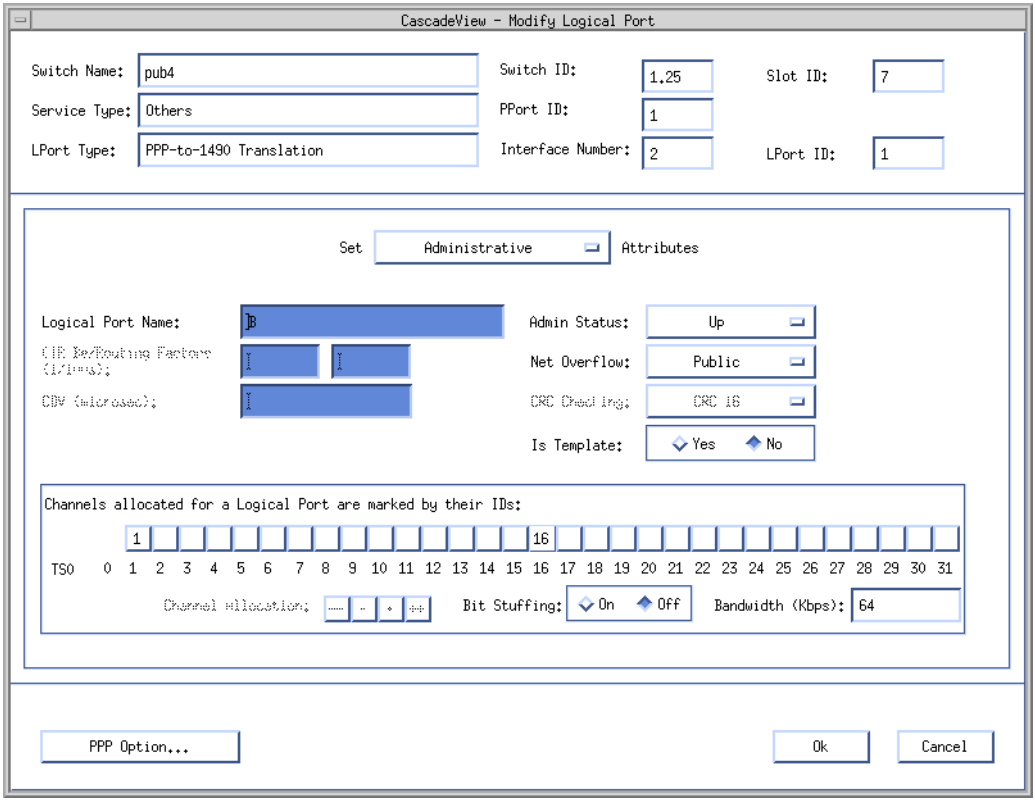

Figure 4-36. Modify Logical Port Dialog Box — Set Attributes

4. Make desired changes, and choose OK to return to the Set All Logical Port in PPort dialog box. You cannot change the logical port name in this dialog box.

Delete a Logical Port

To delete a logical port, refer to the *Network Configuration Guide for B-STDX/STDX*.

Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box

Purpose

You need to access the Modify Logical Port (Set ISDN Attributes) Dialog Box before you can perform the following procedures on a B-channel (logical port):

- Configuring E.164 Called Addresses (page 4-82)
- Configuring Caller ID Screening (page 4-86)
- Configuring the Logical Port Parameters for RADIUS (page 4-89)
- Enabling the Echo Request Function (page 4-98)
- Enabling and Configuring MP and BAP/BACP (page 4-101)

Access the Modify Logical Port (Set ISDN Attributes) Dialog Box

Perform the following steps:

1. For the physical port on which the B-channel logical port is located, access the Set All Logical Ports in PPort dialog box (see Figure 4-37). Refer to “Access the Set All Logical Ports in PPort Dialog Box” on page 4-3.

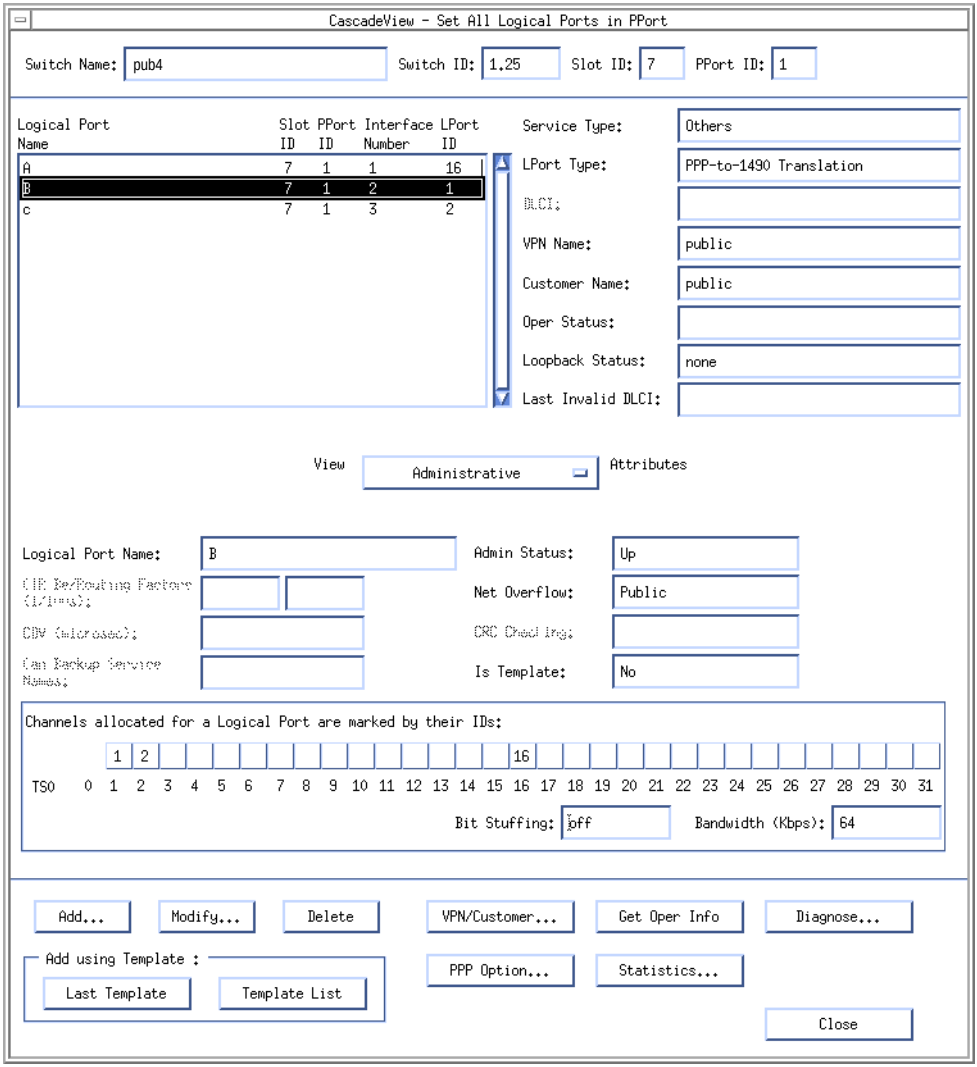

Figure 4-37. Set All Logical Ports in PPort Dialog Box

2. Select the logical port and choose Modify. The Modify Logical Port dialog box appears, displaying the service and LPort type (see Figure 4-38).

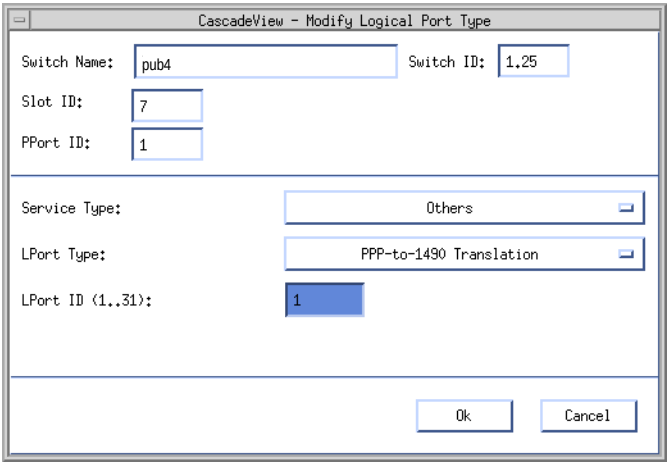

Figure 4-38. Modify Logical Port Dialog Box

3. Choose OK. The Modify Logical Port dialog box reappears, displaying the attributes for the selected logical port (see Figure 4-39).

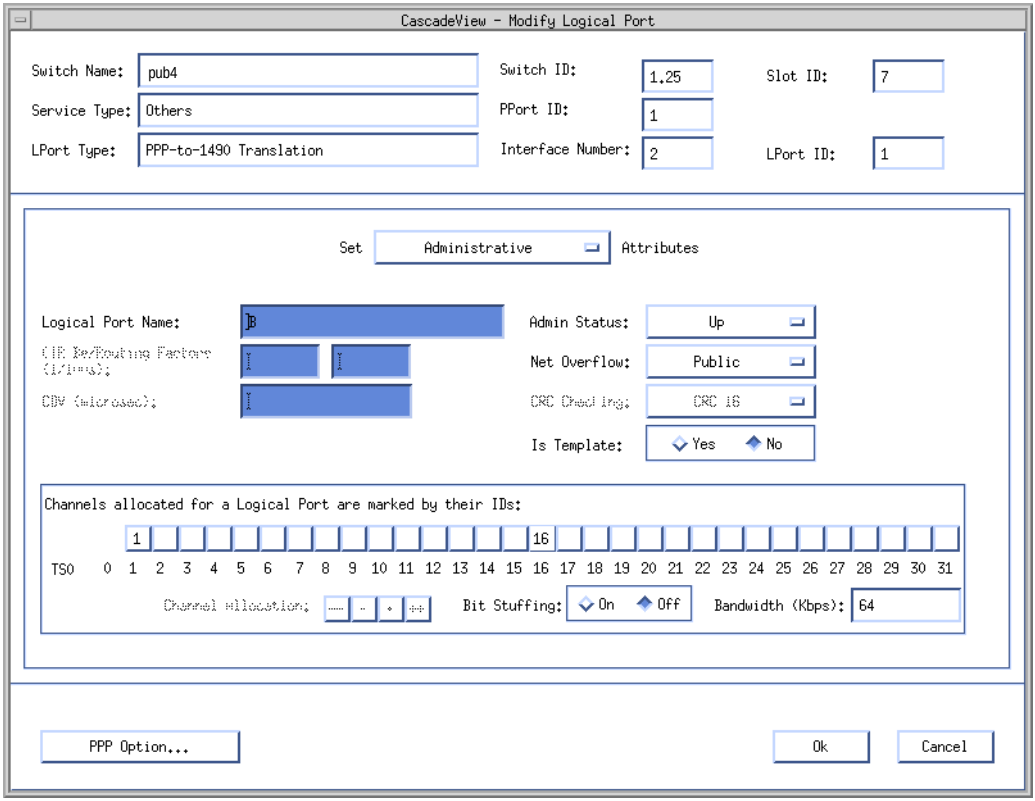

Figure 4-39. Modify Logical Port Dialog Box — Set Attributes

4. Select *ISDN* from the Set Attributes menu. The Modify Logical Port — Set ISDN Attributes dialog box appears (see Figure 4-40).

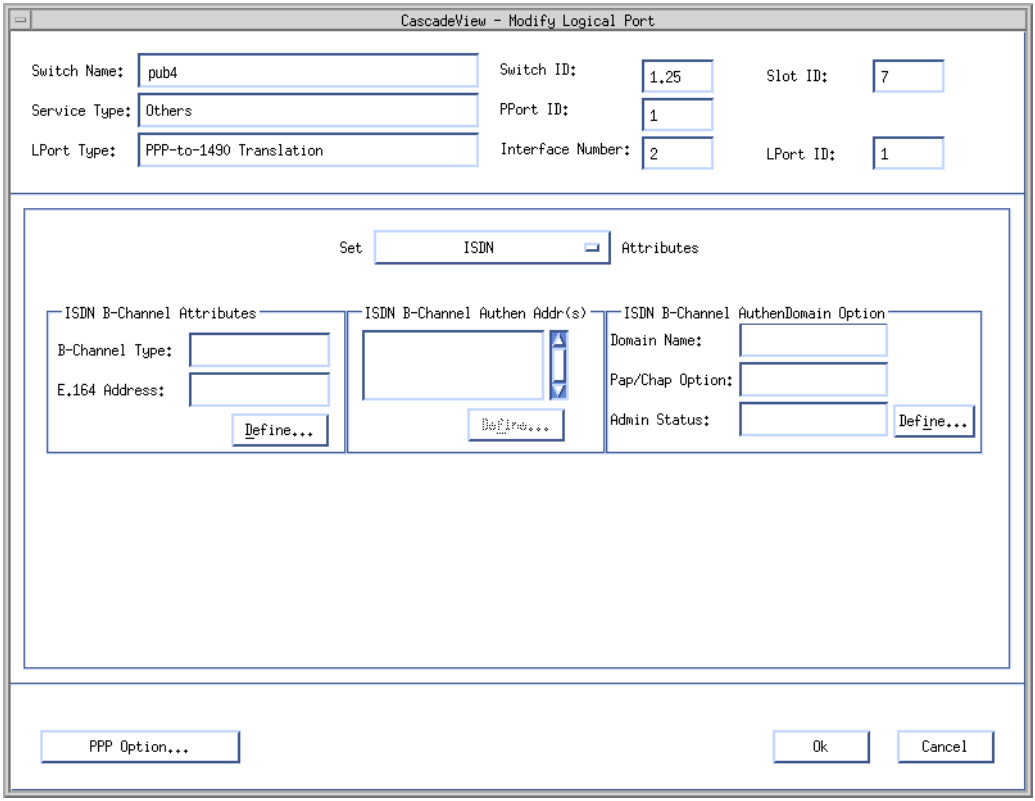

Figure 4-40. Modify Logical Port — Set ISDN Attributes Dialog Box

Configuring E.164 Called Addresses

Once you configure the B-channel logical ports, you must define the B-channel E.164 *called address*. You assign an E.164 address to each B-channel. This is the number the user device calls for dial-in access to the network.

About Hunt Groups

In addition to assigning a separate E.164 called address to each B-channel, you can also create a *hunt group.* A hunt group is a group of B-channels you can access with the same phone number. These B-channels are also connected to PVCs with the same destination. With a hunt group, you can assign the same E.164 called address to all of the available B-channels on a port.

For example, to create two hunt groups, assign the number (800) 555-1000 to B-channels 1 through 10. This phone number can accept up to 10 calls. Create a second hunt group by assigning the number (800) 555-1001 to B-channels 11 through 15 and 17 through 30. This phone number can accept up to 19 calls (see Table 4-25).

Table 4-25. Assigning Hunt Groups

Hunt Group	B-Channel	Physical Port	Phone Number (E.164 Address)
Hunt Group 1	1 - 10	1	8005551000
Hunt Group 2	11 - 15 and 17 - 30	1	8005551001

The hunt group feature simplifies setting up remote access by enabling telecommuters to use the same phone number.

Configuring the B-channel E.164 Called Addresses

> *If you are creating a hunt group, repeat the procedure to configure the same E.164 called address for each TS0 channel you want included in this group. The hunt group can have up to 120 B-channels (30 channels on each of the four physical ports).*

To define the B-channel E.164 called address:

1. Access the Modify Logical Port — Set ISDN Attributes dialog box for the B-channel (see Figure 4-41). Refer to "Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box" on page 4-77.

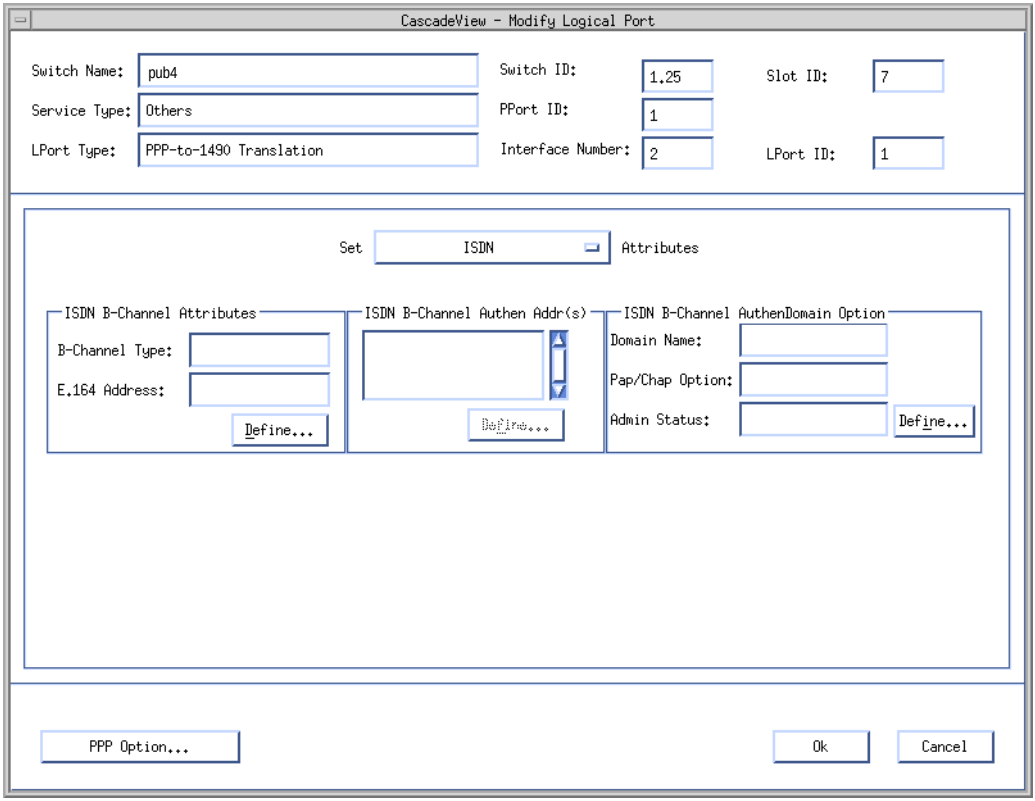

Figure 4-41. Modify Logical Port — Set ISDN Attributes Dialog Box

2. In the *ISDN B-Channel Attributes* box, choose Define to configure an E.164 called address for this B-channel.

   The Set B-Channel Attributes dialog box appears (see Figure 4-42).

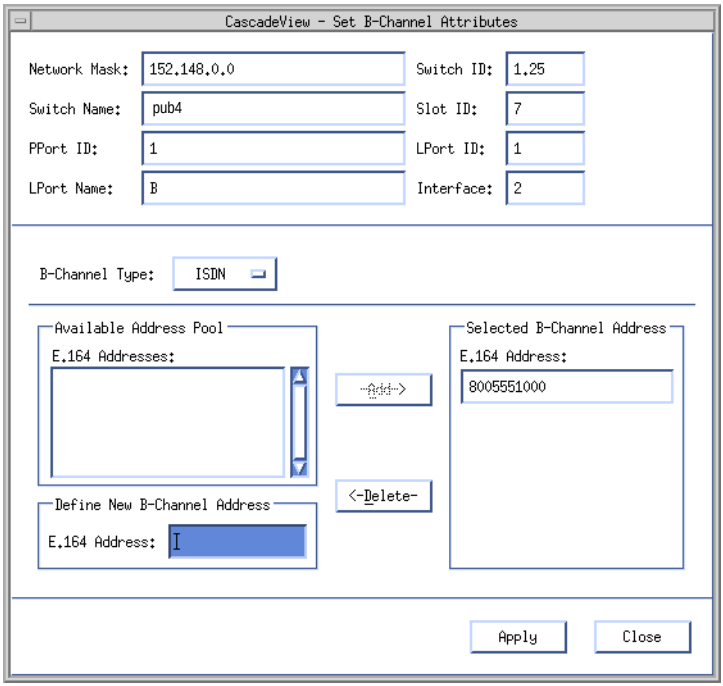

Figure 4-42. Set B-Channel Attributes Dialog Box

SW 56 enables switched digital services, which provide digital connectivity on demand. This service is typically used for temporary circuits between three or more locations.

3. Complete the Set B-Channel Attributes dialog box fields described in Table 4-26.

Table 4-26. Set B-Channel Attributes Fields

Field	Action/Description
B-Channel Type	Select either ISDN or SW 56.
Define New B-Channel Address	If you entered ISDN in the *B-Channel Type* field, either type an E.164 called address for this B-channel or select an address from the *Available Address Pool*.

4. Choose Add. The address that appears in the *Selected B-Channel Address* field represents the phone number users can call to access the network.
5. Choose Apply to return to the Modify Logical Port — Set ISDN Attributes dialog box.
6. If you need to perform further configuration on the same B-channel, go to the appropriate procedure in Step 8.
7. If you need to perform further configuration on another B-channel:
   a. Choose OK. The Set All Logical Ports in PPort dialog box re-appears.
   b. Go to the appropriate procedure in Step 8.
8. Perform the appropriate procedure:
   - Configuring E.164 Called Addresses (page 4-82)
   - Configuring Caller ID Screening (page 4-86)
   - Configuring the Logical Port Parameters for RADIUS (page 4-89)
   - Enabling the Echo Request Function (page 4-98)
   - Enabling and Configuring MP and BAP/BACP (page 4-101)

Configuring Caller ID Screening

You can restrict access to the ISDN network by creating a list of ISDN B-channel authentication addresses, which represent the only phone numbers (caller addresses) that can dial into the network.

The Ascend switch performs authentication for a hunt group by aggregating all the authentication addresses for all B-channels with the same E.164 address (called address). You can configure up to seven authentication addresses per B-channel. In this way, the total number of authentication addresses for a hunt group is 7 x N, where N is the number of B-channels in the group.

If you use B-channel authentication addresses then all calls to the associated B-channel phone number (called address) must match one of the preconfigured E.164 caller addresses.

Configure Caller ID Screening as follows:

1. If the Modify Logical Port — Set ISDN Attributes dialog box for the B-channel (see Figure 4-43) is not open, access it. Refer to "Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box" on page 4-77.

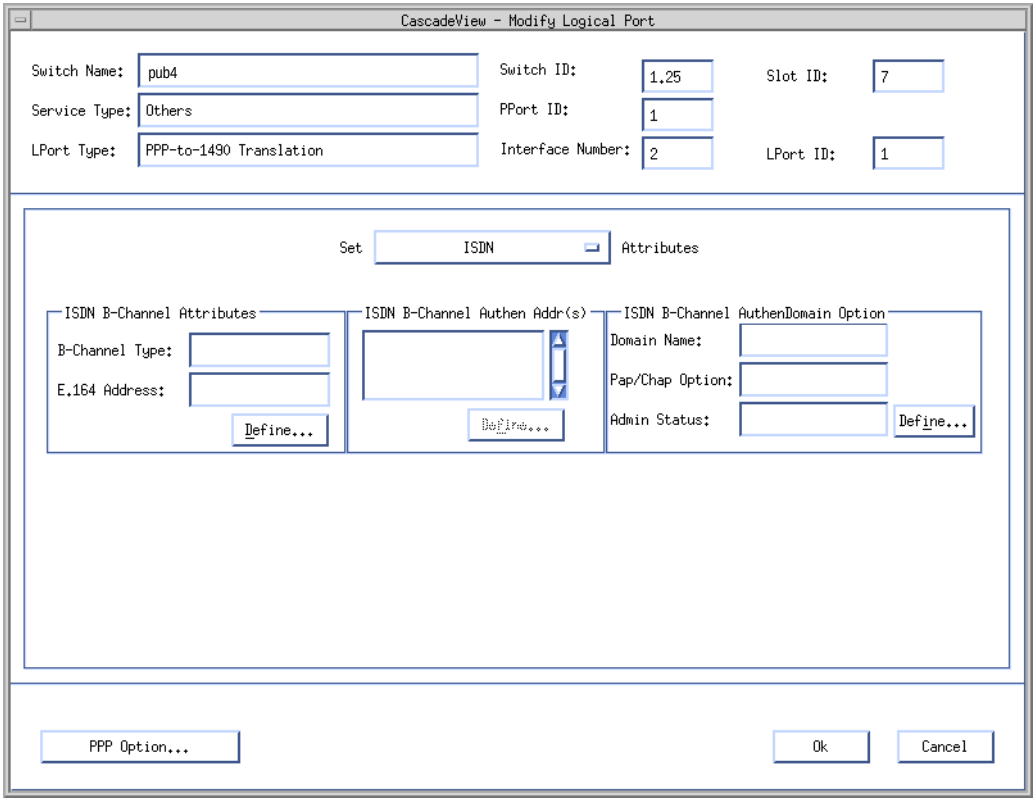

Figure 4-43. Modify Logical Port — Set ISDN Attributes Dialog Box

2. In the *ISDN B-Channel Authen Addr* box, choose the Define command to add authentication addresses. The Add Authentication Address dialog box appears (see Figure 4-44).

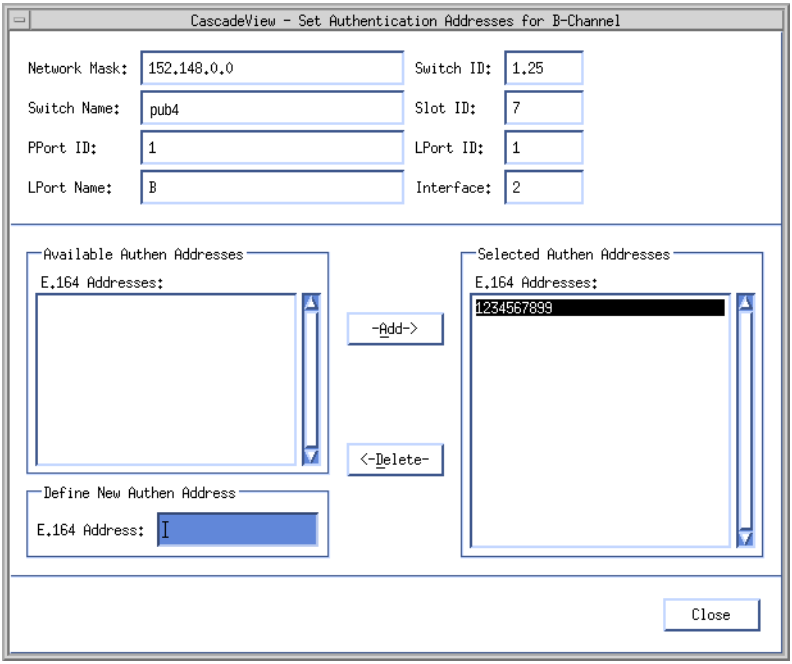

Figure 4-44. Add Authentication Address Dialog Box

3. In the Define New Authentication Address box, enter an E.164 caller address. This is the phone number (source) of the remote user device. If you already defined authentication addresses for this physical port, select an address from the Available Authentication Address list.

4. Choose Add.

5. Repeat Step 3 and Step 4 to add up to seven caller addresses per B-channel logical port.

6. When you finish, choose Close to return to the Modify Logical Port — Set ISDN Attributes dialog box.

7. If you need to perform further configuration on the same B-channel, go to the appropriate procedure in Step 9.

8. If you need to perform further configuration on another B-channel:
   a. Choose OK. The Set All Logical Ports in PPort dialog box re-appears.
   b. Go to the appropriate procedure in Step 9.
9. Perform the appropriate procedure:
   - Configuring E.164 Called Addresses (page 4-82)
   - Configuring Caller ID Screening (page 4-86)
   - Configuring the Logical Port Parameters for RADIUS (page 4-89)
   - Enabling the Echo Request Function (page 4-98)
   - Enabling and Configuring MP and BAP/BACP (page 4-101)

Configuring RADIUS Authentication

The negotiation and execution of authentication is done through the 4-port I/O module and control processor card. In order for authentication to take place, you must configure certain authentication parameters. These tasks include:

- Configuring the Logical Port Parameters (page 4-90)
- Adding an Authentication Domain and Setting the Protocol Parameters (page 4-92)
- Fine Tuning the Configuration (page 4-96)

Before You Begin

Before you configure RADIUS authentication, make sure that you have completed the following:

- ☑ Installed the PPP software to support PPP Authentication (for example PAP and CHAP).
- ☑ Set up a RADIUS server that is running and reachable from the switch via the UDP/IP protocols.

Configuring the Logical Port Parameters

Configure the following parameters for each logical ISDN port:

- Authentication (Enabled/Disabled)
- Authentication Domain Name (RADIUS)
- PAP/CHAP Option

To configure the authentication parameters for the logical port:

1. If the Modify Logical Port — Set ISDN Attributes dialog box for the B-channel (see Figure 4-45) is not open, access it. Refer to "Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box" on page 4-77.

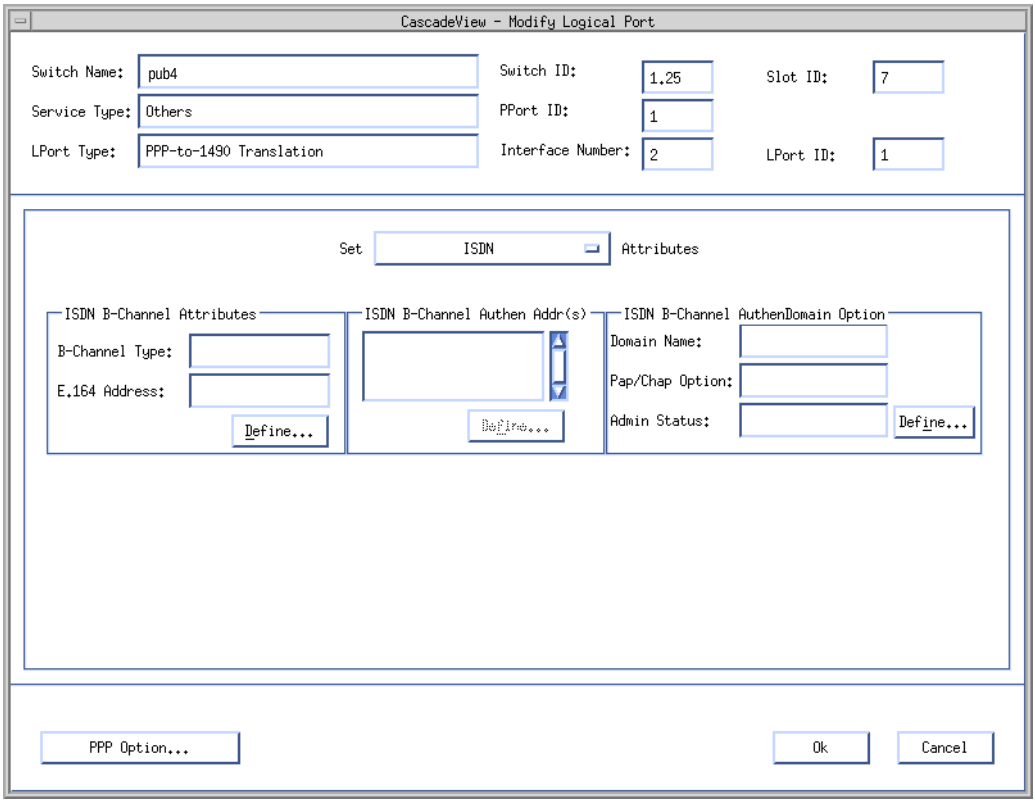

Figure 4-45. Modify Logical Port — Set ISDN Attributes Dialog Box

2. In the *ISDN B-Channel AuthenDomain Option* box, choose Define to configure authentication. The Set Authentication Info dialog box appears (see Figure 4-46).

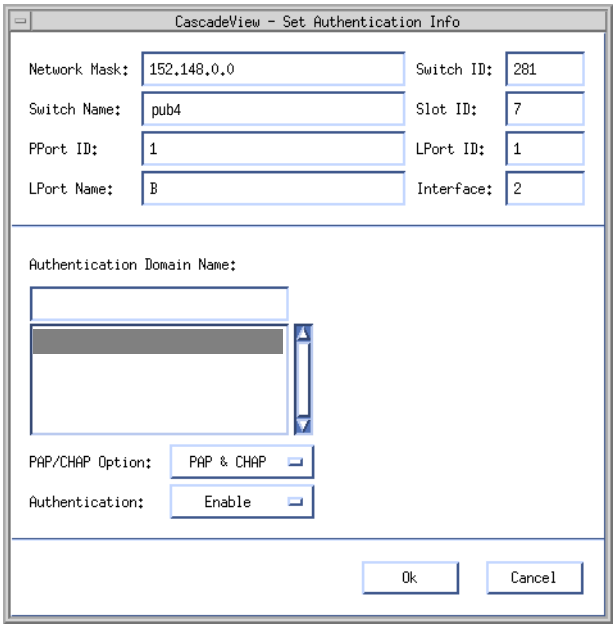

Figure 4-46. Set Authentication Info Dialog Box

3. Complete the Set Authentication Info dialog box fields described in Table 4-27.

Table 4-27. Set Authentication Info Fields

Field	Action/Description
Authentication Domain Name	Select the Authentication Domain.
PAP/CHAP Option	Select PAP only, CHAP only, or PAP & CHAP
Authentication	Select Enable or Disable.

4. Choose OK to accept the new configuration.

5. If you need to perform further configuration on the same B-channel, go to the appropriate procedure in Step 7.
6. If you need to perform further configuration on another B-channel:
   a. Choose OK. The Set All Logical Ports in PPort dialog box re-appears.
   b. Go to the appropriate procedure in Step 7.
7. Perform the appropriate procedure:
   - Configuring E.164 Called Addresses (page 4-82)
   - Configuring Caller ID Screening (page 4-86)
   - Configuring the Logical Port Parameters for RADIUS (page 4-89)
   - Enabling the Echo Request Function (page 4-98)
   - Enabling and Configuring MP and BAP/BACP (page 4-101)

Adding Authentication Domain and Setting Protocol Parameters

For each switch that will have access to a RADIUS server, you need to set up an Authentication Domain. This provides the switch with the following information:

Shared secret: Password that the switch shares with the RADIUS server.

IP Address: IP address of the RADIUS server.

No-response-timeout: The number of seconds that the switch should wait before sending another authentication request if there was no response from the previous request.

Number-of-retries: The number of times that the switch should resend unanswered authentication requests before giving up.

You can also designate backup RADIUS servers (Server 2 and Server 3) in the event that Server 1 becomes unreachable or inactive.

In a multi server Authentication Domain, you can configure each server with its own no-response-timeout and number-of-retries values. If an authentication request is sent to a server and it does not reply, the retry (number-of-retries) is sent to the next server in the domain.

To add the authentication domain and configure the server parameters:

1. On the network map, select the switch object.
2. From the Administer menu, select Cascade Parameters ⇒ Set Authentication Domains. The Set All AuthenDomains dialog box appears (see Figure 4-47).

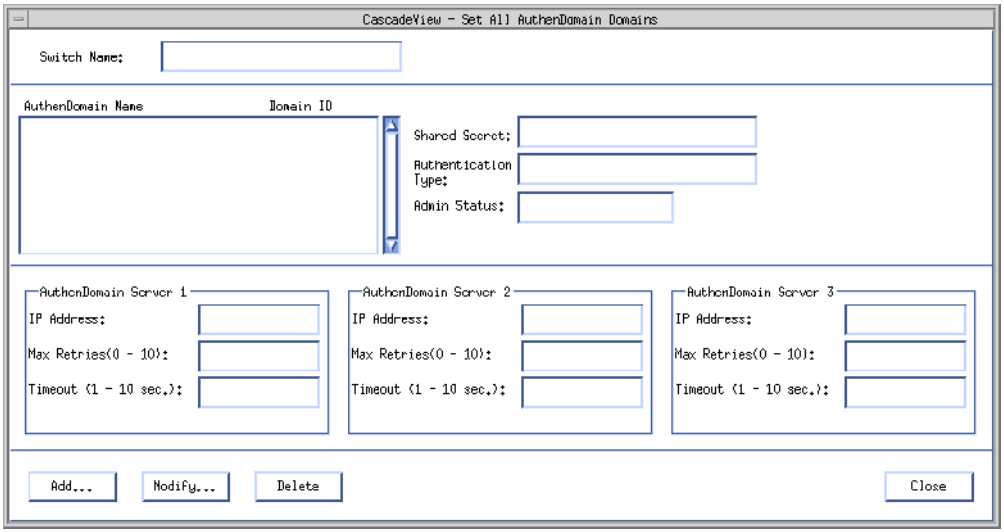

Figure 4-47. Set All AuthenDomains Dialog Box

3. Select Add. The Add AuthenDomain dialog box appears (see Figure 4-48).

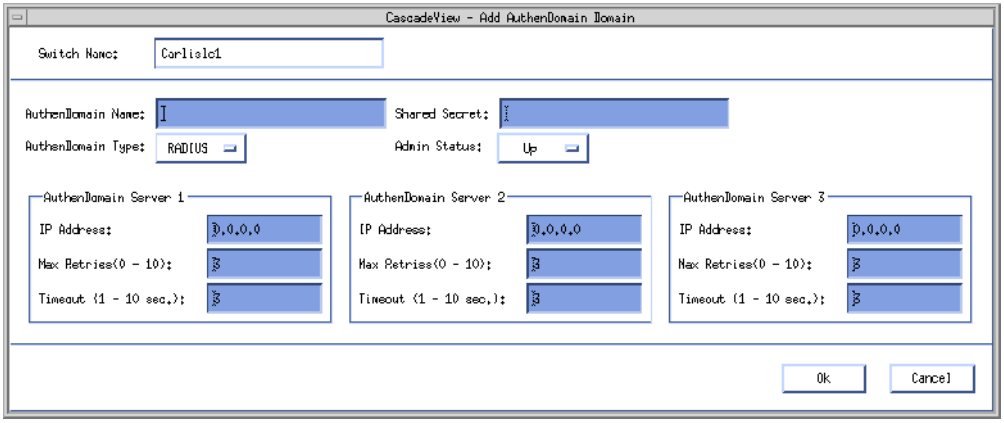

Figure 4-48. Add AuthenDomain Dialog Box

4. Complete the Add AuthenDomain dialog box fields as described in Table 4-28.

Table 4-28. Add AuthenDomain Fields

Field	Action/Description
AuthenDomain Name	Enter an alphanumeric name for this domain.
AuthenDomain Type	Defaults to RADIUS and cannot be changed.
Shared Secret	Enter an alphanumeric shared secret (hash key) for this switch and all RADIUS servers in this domain. This shared secret must be identical to the shared secret for the switch in the RADIUS Client's file, and should be at least 16 octets long.
Admin Status	Set the Admin Status to Up to allow immediate access. Set the Admin Status to Down to disable the server. This will break the connection to the RADIUS server.

5. Complete the AuthenDomain Server fields for Server 1, 2, and 3 as described in Table 4-29.

Table 4-29. 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 should make to authenticate this user. The default is 3 retries.
Timeout (1-10 sec)	Indicates the number of seconds the server should wait 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 3 seconds.

6. Choose OK to set the authentication parameters. The Set All AuthenDomain dialog box reappears.
7. Choose Close to return to the network map.
8. (*Optional*) Enable the authentication parameters as described in the next section.

Fine Tuning the Configuration

In order for authentication to work properly, you need to edit two files in the RADIUS Server database.

Users — This file contains a list of users and their authentication/authorization attributes.

Clients — This file contains a list of client IDs (switch addresses) and shared secrets (passwords).

RADIUS User's File

The RADIUS User's file contains the *Username* (login name) and *User Password* that are used to authenticate a user. For each user, edit the User's file as follows:

Username (login name) — Enter a login name.

User Password — Enter a password.

The RADIUS User's file also contains *optional* attributes that are used for authorization as follows:

Client-Id — Enter the IP address of the switch that the remote user will dial in to.

If you enter an IP address in the Client-Id field, the user must connect to that switch. If the user attempts to connect to a different switch, the authentication request fails. The user is not authorized to access the network from a switch other than the one defined in the Client-Id field. If the user desires access to the network via different switches, this field must be left blank.

Port-Id — Enter the logical port number for the port that the user will access.

In order for authentication to be successful, the user must be connected to the specified logical port. Once you specify the Port-Id, the user is unauthorized to access the switch from any other port. If the user has access to different I/O modules on the switch, this field should be left blank.

User-Service-Type — Enter Framed-User. If you use a different connection method, authentication will fail.

Framed-Protocol — Enter PPP. This attribute is an extension of the Service-Type attribute. If you use a different method, authentication will fail.

The following is an example of a User's file.

```
Peter       Password = cascade, Client-Id = 152.140.20.10
            User-Service-Type = Framed-User
            Framed-Protocol = PPP
```

The Client-Id, Username, and User Password attributes must be on the first line. If you implement the Port-Id attribute, enter it on the first line.

You can create a special user named "DEFAULT."

RADIUS Client's File

The Client's file contains a list of client IDs (switch IP addresses) and shared secrets (hash key). The Client's file shares this information with the RADIUS server. You need to edit this file for each switch that initiates authentication requests.

For each switch, type the switch IP address and the Shared Secret (password) to be shared between the switch and the RADIUS server. This secret (password) should be unique for each switch, and should be identical to the Shared Secret you entered for the switch in "Adding Authentication Domain and Setting Protocol Parameters" on page 4-92. The password is encrypted to ensure security. The secret (password) should be at least 16 octets. The following is an example of a Clients file.

```
152.140.20.10       example123
152.140.20.11       example456
```

Enabling the Echo Request Function

The Echo Request Function polls the ISDN client at a specified time interval to see if it is still active. If the client does not respond to a specified number of successive requests, CascadeView/UX issues an LCP terminate command.

Enable the Echo Request Function for a B-channel as follows:

1. If the Modify Logical Port dialog box for the B-channel (see Figure 4-49) is not open, access it. Refer to "Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box" on page 4-77.

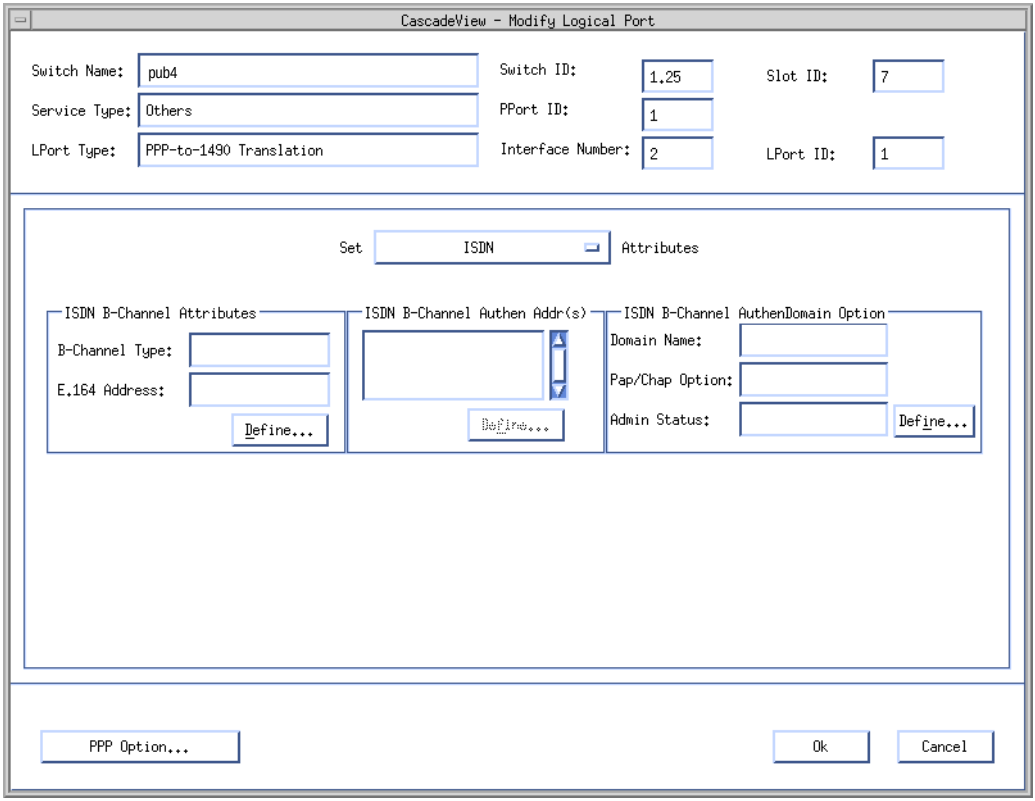

Figure 4-49. Modify Logical Port — Set ISDN Attributes Dialog Box

2. Choose the PPP Option ... button. The Set PPP Options dialog box appears, displaying the attributes for the selected logical port (see Figure 4-50).

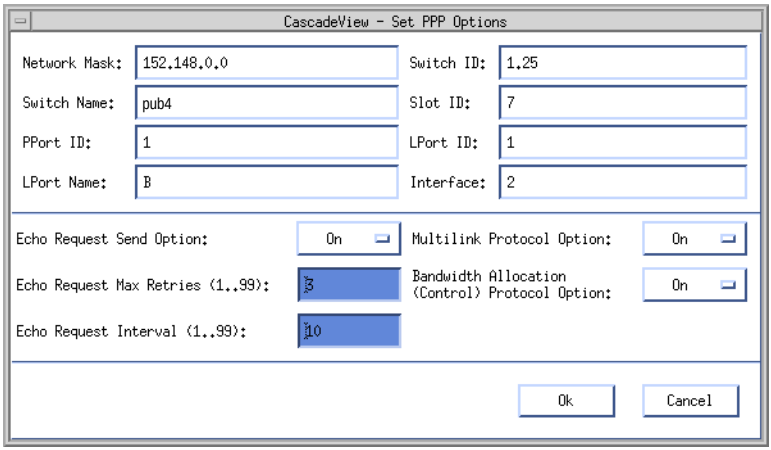

Figure 4-50. Set PPP Options Dialog Box

3. Complete the Set PPP Options dialog box fields described in Table 4-30.

Table 4-30. Set PPP Options Fields

Field	Action/Description
Echo Request Send Option	Select On to send keep-alive packets to the remote user.
Echo Request Max Retries	Enter a number from 1 to 99 that represents the maximum number of keep alive packets sent to the remote user.
Echo Request Interval	Enter a number from 1 to 99 that represents the time interval between each keep-alive packet.

4. If you need to configure MP and BAP/BACP for this B-channel, go to Step 3 on page 4-103.

5. Choose OK to return to the Modify Logical Port dialog box.

6. If you need to perform further configuration on the same B-channel, go to the appropriate procedure in Step 8.

7. If you need to perform further configuration on another B-channel:

   a. Choose OK. The Set All Logical Ports in PPort dialog box re-appears.

   b. Go to the appropriate procedure in Step 8.

8. Perform the appropriate procedure:

   - Configuring E.164 Called Addresses (page 4-82)
   - Configuring Caller ID Screening (page 4-86)
   - Configuring the Logical Port Parameters for RADIUS (page 4-89)
   - Enabling the Echo Request Function (page 4-98)
   - Enabling and Configuring MP and BAP/BACP (page 4-101)

Enabling and Configuring MP and BAP/BACP

MP and BAP/BACP Protocols

The ISDN remote access dynamic bandwidth allocation feature is implemented through the use of three protocols:

- Multilink Protocol (MP)
- Bandwidth Allocation Protocol (BAP)
- Bandwidth Allocation Control Protocol (BACP)

When MP is enabled through the NMS, multiple physical links can be combined into one logical link to increase the bandwidth of the connection. The logical link is referred to as an *MP Bundle*. Refer to the following sources for a detailed description of MP:

- RFC 1717
- MP Internet Draft

When BAC/BACP is enabled through the NMS, a more formalized method for controlling and managing bandwidth is established. Refer to the BAC/BACP Internet Draft for a detailed description of these protocols.

Interaction with RADIUS Authentication

The RADIUS database attribute *Port-Limit* specifies the maximum number of links a user can combine into an MP bundle. Set this attribute to the number you desire.

Configure MP and BAC/BACP

To configure MP and BAC/BACP for dynamic bandwidth allocation for each desired B-channel:

1. If the Modify Logical Port dialog box for the B-channel (see Figure 4-51) is not open, access it. Refer to “Accessing the Modify Logical Port (Set ISDN Attributes) Dialog Box” on page 4-77.

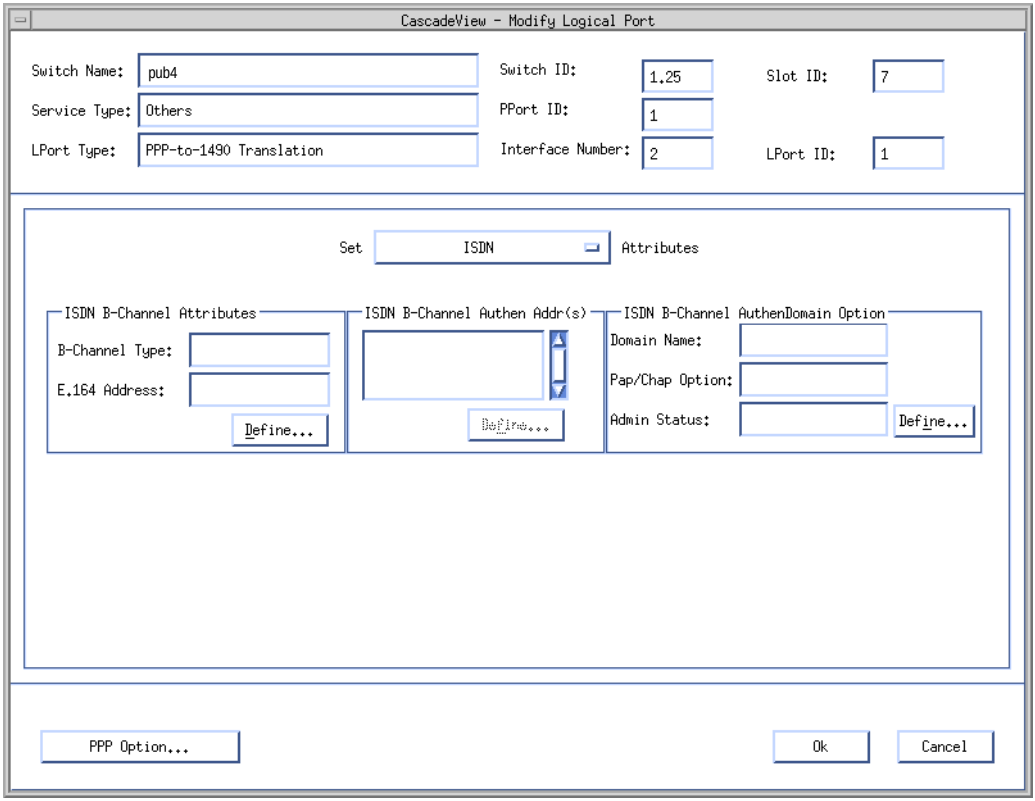

Figure 4-51. Modify Logical Port — Set ISDN Attributes Dialog Box

2. Choose the PPP Option ... button. The Set PPP Options dialog box appears, displaying the attributes for the selected logical port (see Figure 4-52).

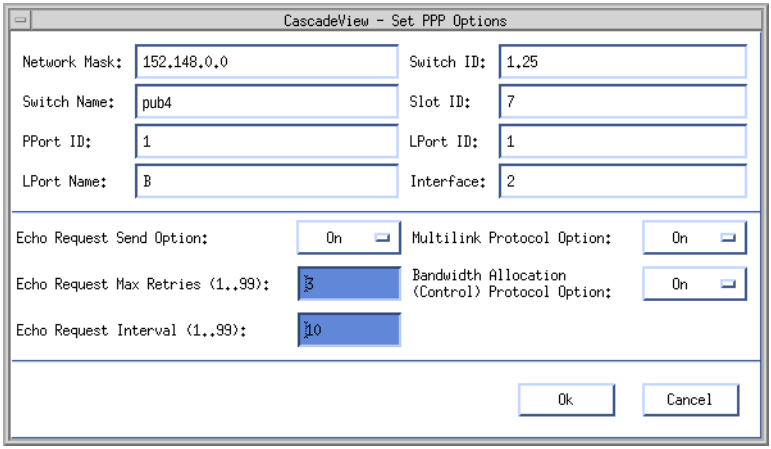

Figure 4-52. Set PPP Options Dialog Box

3. Complete the Set PPP Options dialog box fields described in Table 4-31.

Table 4-31. Set PPP Options Fields

Field	Action/Description
Multilink Protocol Option	Select On to enable dynamic bandwidth allocation.
Balance Allocation (Control) Protocol Option	Select On to enable BAP/BACP.

4. If you need to enable the echo request function for this B-channel, go to Step 3 on page 4-99.
5. Choose OK to return to the Modify Logical Port dialog box.
6. If you need to perform further configuration on the same B-channel, go to the appropriate procedure in Step 8.

7. If you need to perform further configuration on another B-channel:
   a. Choose OK. The Set All Logical Ports in PPort dialog box re-appears.
   b. Go to the appropriate procedure in Step 8.
8. Perform the appropriate procedure:
   - Configuring E.164 Called Addresses (page 4-82)
   - Configuring Caller ID Screening (page 4-86)
   - Configuring the Logical Port Parameters for RADIUS (page 4-89)
   - Enabling the Echo Request Function (page 4-98)
   - Enabling and Configuring MP and BAP/BACP (page 4-101)

Configuring a Circuit for ISDN Remote Access

Once you have configured ISDN remote access to the B-STDX 8000/9000 switch, configure circuits with the logical ports on the PRI module in the same way you configure other circuits. Refer to the *Network Configuration Guide for B-STDX/STDX*.

5

ISDN Trunk Backup

This chapter describes ISDN Trunk Backup and gives instructions for setting up an ISDN backup trunk.

ISDN Trunk Backup Description

General Description

The ISDN Trunk Backup feature allows the Ascend switches to set up one or more backup trunks over an ISDN network to replace a primary trunk. When an ISDN trunk backup is initiated, a call is made over an ISDN network to connect the switches and form a trunk over the ISDN connection.

ISDN trunk backup is distinct from the HyperPATH remote access ISDN Primary Rate Interface (PRI) support available in the Ascend switch. ISDN trunk backup is performed via connections on a Universal IOP card and is simply a vehicle for two ISDN Terminal Adapters (TAs) to establish a connection across an ISDN network. In contrast, the HyperPATH ISDN PRI support enables the Ascend switch to receive ISDN call requests and establish ISDN connections on the ISDN PRI card (refer to Chapter 4, “Configuring ISDN Remote Access”).

Features

The basic features of an ISDN backup trunk are the same as any backup trunk. These include:

- Automatic, scheduled, and manual trunk backup
- PVC rerouting
- Multiple backup trunks
- Automatic or manual primary trunk restoration

Refer to the *Network Configuration Guide for B-STDX/STDX* for details on these features.

Transmission Speed Limitations

The highest transmission rate of one PVC is limited by the circuit speed of the ISDN backup trunk.

For example, if a primary trunk contains a PVC with a CIR of 512 Kbps, and an ISDN trunk with a line speed of 64 Kbps is being used as a backup trunk, the highest transmission speed is limited to 64 Kbps for PVCs on that trunk. However, the network operator can define up to eight backup trunks to backup a single primary trunk.

Types of Traffic that Can be Backed Up by ISDN

The ISDN Trunk Backup function can be used to back up any type of primary trunk supported by the Ascend switch. However, because of the relatively low speed of an ISDN backup trunk, ATM Virtual Channels/Circuits (VCCs) are not supported on the ISDN backup trunk. ATM VCCs can be rerouted on alternate ATM trunks.

ISDN Call Setup Process

The process of activating an ISDN backup trunk is as follows:

1. To start the backup trunk, the Ascend switch raises DTR and RTS for the backup port on the Universal Input Output (UIO) card. This is the port that was defined as the Caller Node when you configured the backup trunk on the NMS.
2. The ISDN-TA port that is connected to the Caller Node detects ER and RS up.
3. The ISDN-TA ports raise CS, DR, and CD.
4. The Ascend switch port that is the endpoint of the backup trunk detects CTS, DSR, and DCD up.
5. The Ascend switch invokes a link-down routine to bring down the primary trunk. This prevents the trunk from being used as a route for any PVCs.
6. The ISDN backup trunk becomes operational.
7. Each PVC carried by the primary trunk is rerouted by the Open Shortest Path First (OSPF) routing algorithms.

ISDN Call Release Procedure

For ISDN trunk backup, release of the backup trunk occurs by the ISDN call release procedure. The procedure is as follows:

1. The Ascend switch lowers DTR and RTS for the backup port on the UIO card. This is the port that was defined as the Caller Node when you configured the backup trunk on the NMS.
2. The ISDN-TA port that is connected to the Caller Node detects ER and RS down.
3. The ISDN-TA ports lower CS, DR, and CD.
4. The Ascend switch port that is the endpoint of the backup trunk detects CTS, DSR, and DCD down.
5. The ISDN-TA releases the ISDN circuit.

6. The Ascend switch sends a trunk status SNMP trap to the NMS indicating that the backup trunk is no longer available, and sends a second SNMP trap indicating that the backup trunk has been released, to allow its status to be changed to “defined.”

Configuring an ISDN Backup Trunk

To provide sufficient backup bandwidth, the network operator can define up to eight backup trunks to back up a single primary trunk.

When defining trunks, any given backup trunk can only back up a single primary trunk, and at least one backup trunk is needed for every primary trunk requiring backup.

To add an ISDN backup trunk:

1. At each switch that will be an endpoint for the backup trunk, install an 8-port universal IOP (UIO) module with a V.35 or X.21 interface.
2. Configure a logical port on each UIO module for a backup trunk (refer to the *Network Configuration Guide for B-STDX/STDX*).
3. Connect the DTE logical port on each UIO to an ISDN terminal adapter. Figure 5-1 shows the backup trunk configuration.

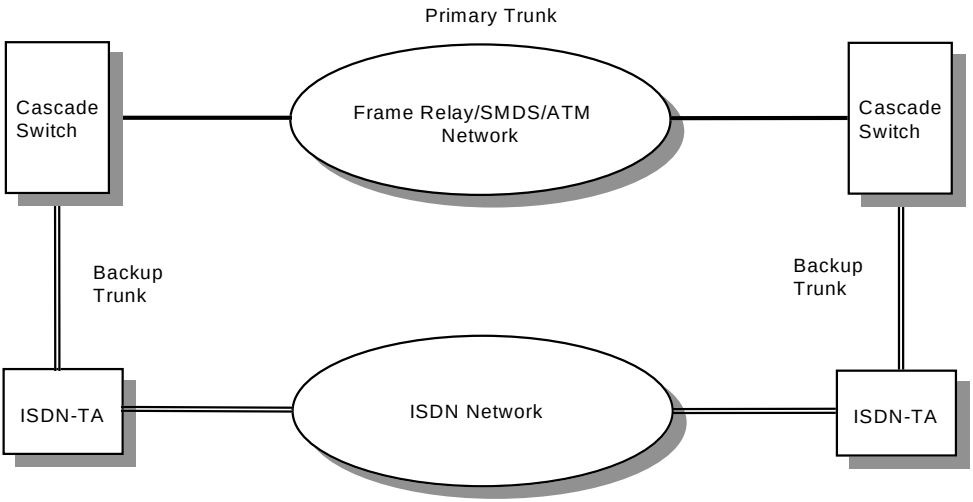

Figure 5-1. ISDN Backup Trunk Configuration

4. Determine which end of the backup trunk will perform the call setup for the backup trunk.

5. Configure the ISDN logical terminal adapter that is connected to the call setup endpoint as follows: upon detecting that ER and RS are up, this ISDN logical terminal adapter should call the ISDN logical terminal adapter that is connected to the other endpoint of the backup trunk.

6. Using the DTE logical ports you defined on the UIO cards, use the NMS to add the trunk definition for the backup trunk. Refer to the *Network Configuration Guide for B-STDX/STDX*.

6

Monitoring and Troubleshooting

This chapter provides you with information about how to monitor and troubleshoot HyperPATH ISDN remote access activities and events on your Cascade network. This chapter describes the following:

- Monitoring the ISDN Call Status
- Diagnostic Traps for ISDN Remote Access
- Console-Based Call Lookup of Port Statistics

Monitoring ISDN Call Status

The switch software and CascadeView/UX provide call monitoring support for ISDN PRI dial-in connections through the Show ISDN Status dialog box. This section describes:

- How to open the Show ISDN Status dialog box
- The information in the Show ISDN Status dialog box

Open the Show ISDN Status Dialog Box

To open the Show ISDN Status dialog box:

1. On the network map, select the switch from which you want to obtain physical and logical port information.
2. Select Cascade Parameters ⇒ Set Parameters from the Administer menu.

   The Switch Back Panel dialog box appears as shown in Figure 6-1.

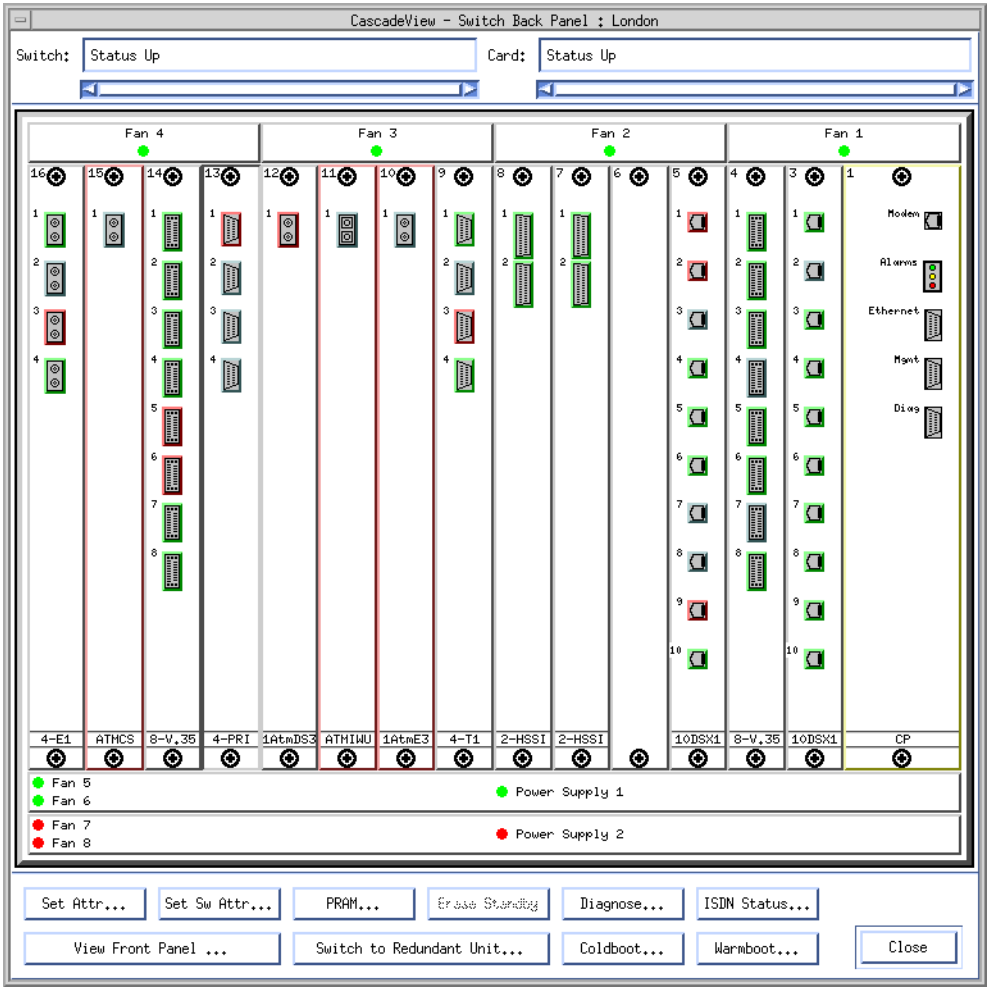

Figure 6-1. Switch Back Panel Dialog Box

3. Select the PRI I/O module that you want to monitor and choose ISDN Status.

   The Show ISDN Status dialog box appears as shown in Figure 6-2.

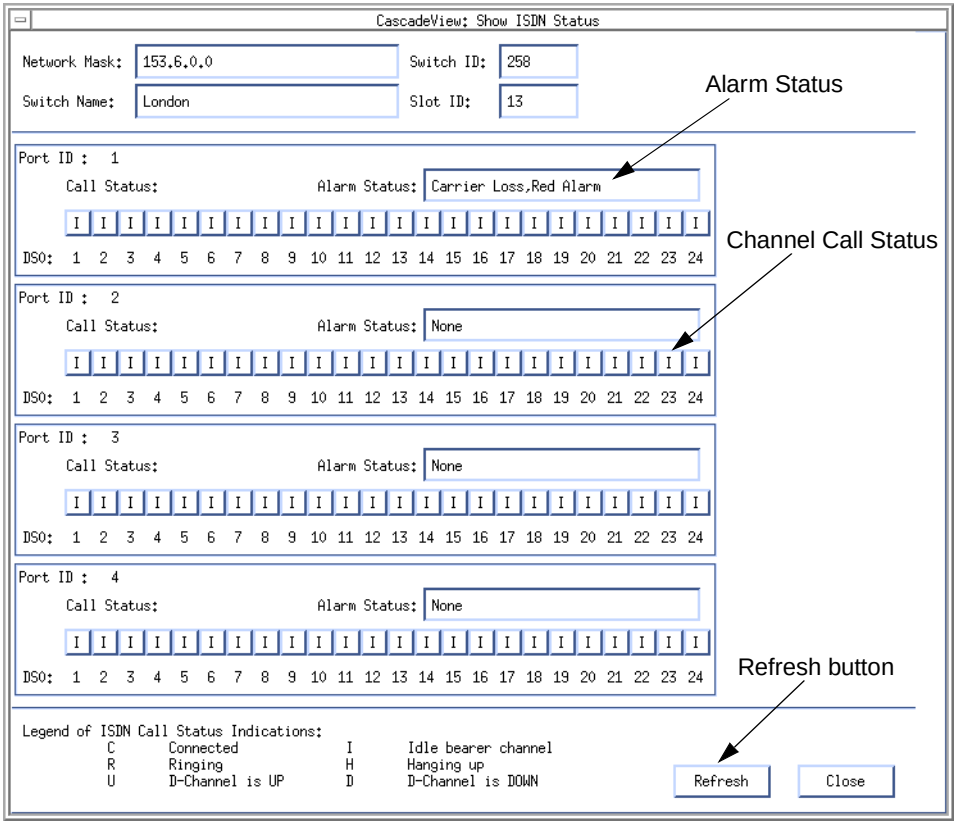

Figure 6-2. Show ISDN Status Dialog Box

Show ISDN Status Dialog Box Contents

The Show ISDN Status dialog box includes the call status of each channel and describes any alarms on the physical ports.

Alarm Status

The Show ISDN Status dialog box describes any alarms that are present on each PRI port (refer to Figure 6-2 on page 6-4). Table 6-1 describes those alarms.

Table 6-1. PRI Port Alarm Status Summary

Alarm Status	Description
Red	Loss of signal or out-of-frame error. This is due to two or more framing-bit errors within a three millisecond period or two or more errors within five or less consecutive framing bits.
Yellow	A remote channel service unit (CSU) is transmitting a Red Alarm. The remote CSU is not receiving any transmission signals from your circuit and the circuit is acting as a one-way link.
None	No alarm condition.

Channel Call Status

The Show ISDN Status dialog box presents a graphical representation of B- and D-channels for each PRI port on the I/O module. Each of the B- and D-channels can contain a single-character code representing the channel's call status (refer to Figure 6-2 on page 6-4). You can display the most current status information by choosing Refresh at the bottom of the dialog box. Table 6-2 describes each of the ISDN Call Status codes.

Table 6-2. ISDN Call Status Codes

Code	Description
C	The B-channel is connected (active).
D	The D-channel is down.
H	The B-channel is releasing the call (hanging up).
I	The B-channel is idle.
R	The B-channel is dialing (ringing).
U	The D-channel is up.

Diagnostic Traps for ISDN Remote Access

Diagnostic traps notify the operator of events taking place on the switches that are configured to report to the NMS. You can display a list of currently logged trap alarm conditions at any time by selecting the Cascade Events option from the Event Categories window. Refer to the *Diagnostic and Troubleshooting Guide for B-STDX/STDX* for more information about accessing these traps.

Three types of traps for ISDN remote access are discussed in this section:

- Failed Authentication Attempt Traps
- ISDN Call Rejected Traps
- PPP Negotiation Failed Traps

Failed Authentication Attempt Traps

A trap is generated for all failed authentication attempts. Table 6-3 contains a description of each of these traps.

Table 6-3. Failed Authentication Attempt Traps

Trap	Condition
No Response from Server	RADIUS server is unreachable.
Protocol Error	Invalid response packet received from RADIUS server.
Invalid Service-Type attribute	The Service-Type in the RADIUS Users file is not set to “Framed”.
Invalid Framed-Protocol attribute	The Framed-Protocol in the RADIUS Users file is not set to “PPP”.
Server Authentication failed	Invalid username, password, slot ID, or IP address.

ISDN Call Rejected Diagnostic Traps

The ISDN call rejected diagnostic trap has the format:

```
An ISDN call has been rejected on logical port number due to
trap name.
```

Table 6-4 contains a description of each of the possible traps.

Table 6-4. Descriptions for Rejected ISDN Calls

Trap Name	Description
Unassigned number	The destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.
No route to specified transit network	The equipment sending this cause code has received a request to route the call through a particular transit network that it does not recognize. The equipment sending this code does not recognize the transit network either because the transit network does not exist or because that particular network, while it does exist, does not serve the equipment that is sending this error.

Table 6-4. Descriptions for Rejected ISDN Calls (Continued)

Trap Name	Description
Channel unacceptable	Indicates the channel most recently identified is not acceptable to the sending entity for use in this call.
Normal call clearing	Indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.
User busy	Sent when the called user has indicated the inability to accept another call. The user equipment is compatible with the call.
No user responding	Sent when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (defined in Recommendation Q.931 by the expiring of either timer T303 or T310).
Call rejected	Indicates that the equipment sending this code does not wish to accept this call, although it could have accepted the call because the equipment sending this cause code is neither busy nor incompatible.
Number changed	Returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this capability, cause code #1 “Unassigned number” shall be used.
Destination out of order	Indicates that the destination indicated by the user cannot be reached because the interface to the destination is not allowing a signaling message to be delivered to the remote user; for example, a physical layer or data link layer failure exists at the remote user, or user equipment is off-line.
Invalid number format	Indicates that the called user cannot be reached because the called party number is not a valid format or is not complete.
Facility rejected	Returned when a facility requested by the user cannot be provided by the network.

Table 6-4. Descriptions for Rejected ISDN Calls (Continued)

Trap Name	Description
Response to STATUS ENQUIRY	Included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.
Unspecified cause	Used to report a normal event only when no other cause in the normal class applies.
No circuit available	Indicates an appropriate circuit is not presently available to handle the call.
Network out of order	Indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; for example, immediately reattempting the call is not likely to be successful.
Temporary failure	Indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; for example, the user may wish to try another call attempt almost immediately.
Network congestion	Indicates that the switching equipment generating this cause is experiencing a period of high traffic.
Access information discarded	Indicates that the network could not deliver access information to the remote user as requested, that is, user-to-user information, low layer compatibility, high layer compatibility, or sub-address as indicated in the diagnostic.
Requested circuit not available	Returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
Requested facility not subscribed	Indicates that the requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.

Table 6-4. Descriptions for Rejected ISDN Calls (Continued)

Trap Name	Description
Bearer capability not available	Indicates that the user has requested a bearer capability that is implemented by the equipment that generated this cause but that is not available at this time.
Service not available	Used to report a service not available event only when no other cause in the *service not available* class applies.
Capability not implemented	Indicates that the equipment sending this cause does not support the bearer capability requested.
Channel type not implemented	Indicates that the equipment sending this cause does not support the channel type requested.
Requested facility not implemented	Indicates that the equipment sending this cause does not support the requested supplementary service.
Invalid call reference value	Indicates that the equipment sending this cause has received a message with a call reference that is not currently in use on the user-network interface.
Identified channel does not exist	Indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment on the network attempts to use channels 13 through 23, this cause is generated.
Incompatible destination	Indicates that the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (e.g., data rate) that cannot be accommodated.
Invalid message	Used to report an invalid message event only when no other cause in the *invalid message* class applies.

Table 6-4. Descriptions for Rejected ISDN Calls (Continued)

Trap Name	Description
Mandatory information element is missing	Indicates that the equipment sending this cause has received a message that is missing an information element that must be present in the message before that message can be processed.
Message type non-existent	Indicates that the equipment sending this cause has received a message with a message type it does not recognize. The message type either is not defined or is defined but not implemented by the equipment sending this cause.
Message not compatible	Indicates that the equipment sending this cause has either received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or has received a STATUS message indicating an incompatible call state.
Information element non-existent	Indicates that the equipment sending this cause has received a message that includes information elements not recognized for the following reasons: the information element identifier is not present, is not defined, or is defined but not implemented by the equipment sending the cause.
Invalid information element contents	Indicates that the equipment sending this cause has received an information element that it has implemented; however, one or more of the fields in the information element are coded in a way that has not been implemented by the equipment sending this cause.
Message not compatible	Indicates that a message has been received that is incompatible with the call state.
Timer expired	Indicates that a procedure has been initiated by the expiration of a timer in association with Q.931 error handling procedures.
Protocol error	Used to report a protocol error event only when no other cause in the *protocol error* class applies.

Table 6-4. Descriptions for Rejected ISDN Calls (Continued)

Trap Name	Description
Interworking unspecified	Indicates that there has been interworking with a network that does not provide causes for actions it takes, and the precise cause for a message that is being sent cannot be ascertained.

PPP Negotiation Failed Diagnostic Traps

The following PPP negotiation failed diagnostic traps may appear:

```
PPP negotiation has failed on logical port number due to IP
Control Protocol failure.

PPP negotiation has failed on logical port number due to Link
Control Protocol failure.

PPP negotiation has failed on logical port number due to PVC
down.
```

Console-Based Call Lookup of Port Statistics

Console-based call lookup provides a way to diagnose a problem with an ISDN remote access connection to the B-STDX 8000/9000 switch. Call lookup displays the port statistics on the console.

Displaying Port Statistics

To display port statistics:

1. Access the Console port on the switch either directly or through a telnet session.
2. Issue the following command:

   `show isdn call [`*`telephone number of caller`*`]`

   Example:

   `show isdn call 5089521234`

   The console displays the port statistics for the remote access session.

Description of Port Statistics

Table 6-5 describes the port statistics displayed on the console.

Table 6-5. Remote Access Session Port Statistics

Statistic	Description
Calling #	The telephone number of the remote access user making the call.
Slot #	The slot number of the 4-port T1 or E1 ISDN I/O module receiving the call.
Pport #	The number of the physical port located on the ISDN I/O module.
Lport #	The number of the logical port (or ISDN channel) handling the call.

Table 6-5. Remote Access Session Port Statistics (Continued)

Statistic	Description
lfnum	The interface number of the Lport where the call is attached.
Called #	The telephone number assigned to the Lport.
IP address	The IP address of the B-STDX remote access switch.

Index

W