NavisCore SMDS Configuration Guide

Ascend Communications, Inc.

Product Code: 80073
Revision 00
September 1998

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 how to configure SMDS services on an Ascend B-STDX switch. Specifically, this guide describes how to configure B-STDX logical ports and trunks to enable SMDS services in your network.

What You Need to Know

As a reader of this guide, you should be familiar with the UNIX operating system and HP OpenView. The system administrator should be familiar with relational database software to properly maintain Sybase, the database used by NavisCore.

This guide assumes you have installed the Ascend switch hardware, using the *B-STDX Hardware Installation Guide* and installed the NMS software, using the *Network Management Station Installation Guide*.

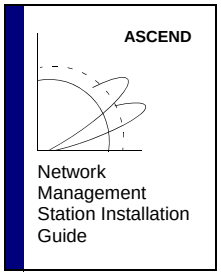
Reading Path

This section describes all of the documents that support the NavisCore NMS and switch software. The documents are grouped as follows:

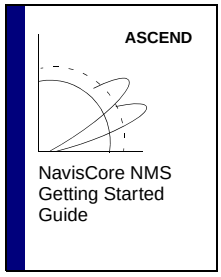
- NMS Documentation
- Switch Software Documentation

NMS Documentation

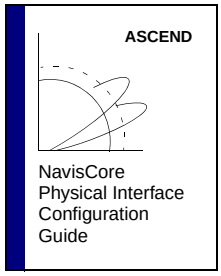
Read the following documents to install and operate NavisCore Release 4.0.



This guide describes prerequisite tasks, hardware and software requirements, and instructions for installing Solaris, HP OpenView, and NavisCore on the NMS.



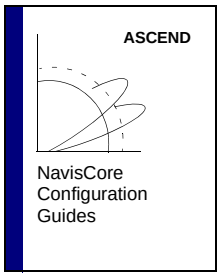
This guide describes how to configure and manage NavisCore, network maps, and Ascend switches.



This guide describes how to configure processor and I/O modules on Ascend switches.

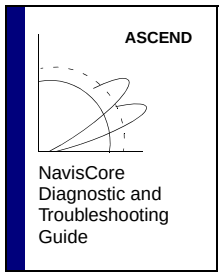
Switch Software Documentation

Read the following documents to configure switch software.

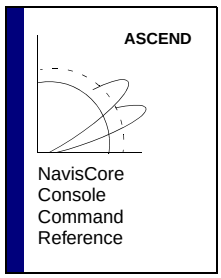


These guides describe how to configure WAN services on the STDX, B-STDX, CBX, and GX switch platforms:

- *NavisCore Frame Relay Configuration Guide*
- *NavisCore ATM Configuration Guide*
- *NavisCore IP Navigator Configuration Guide*
- *NavisCore ISDN Configuration Guide*
- *NavisCore SMDS Configuration Guide*



This guide describes how to diagnose and troubleshoot your NavisCore switch network.



This reference lists and describes the NavisCore switch console commands.

How to Use This Guide

This guide contains the following information:

Read	To Learn About
Chapter 1	SMDS services and addressing.
Chapter 2	Network parameters, such as country codes, address prefixes, and address masking.
Chapter 3	Configuring SSI-DTE and DXI/SNI logical ports and defining attributes.
Chapter 4	Configuring individual and group addresses.
Chapter 5	Configuring SMDS management addresses.
Chapter 6	Deleting logical ports.
Chapter 7	Configuring trunks.

Conventions

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

Convention	Indicates	Example
`Courier Bold`	User input on a separate line.	**`eject cdrom`**
`Courier`	Screen or system output.	`Please wait...`
[*bold italics*]	Variable parameters to enter.	**[*your IP address*]**
`<Return>`	Press Return or Enter.	`<Return>`
Boldface	User input in text.	Type **cd install** and . . .
Menu ⟹ Option	Select an option from the menu.	CascadeView ⟹ Logon
Boxes surrounding text	Notes and warnings.	See examples below.
Italics	Book titles, new terms, file names, directories, and emphasized text.	*Network Management Station Installation Guide*

Notes provide additional information or helpful suggestions that may apply to the subject text.

Cautions notify the reader to proceed carefully to avoid possible equipment damage or data loss.

Warnings notify the reader to proceed carefully to avoid possible personal injury.

Related Documents

This section lists the related Ascend documentation that may be helpful to read.

- *Network Management Station Installation Guide* (Product Code: 80014)
- *NavisCore NMS Getting Started Guide* (Product Code: 80070)
- *NavisCore Physical Interface Configuration Guide* (Product Code: 80080)
- *NavisCore Frame Relay Configuration Guide* (Product Code: 80071)
- *NavisCore ATM Configuration Guide* (Product Code: 80072)
- *NavisCore ISDN Configuration Guide* (Product Code: 80039)
- *NavisCore IP Navigator Configuration Guide* (Product Code: 80056)
- *NavisCore Diagnostic and Troubleshooting Guide* (Product Code:80074)
- *NavisCore Console Command Reference* (Product Code: 80075)
- *B-STDX Hardware Installation Guide* (Product Code: 80005)
- *CBX 500 Hardware Installation Guide* (Product Code: 80011)
- *GX 550 Hardware Installation Guide* (Product Code: 80077)

Customer Comments

Customer comments are welcome. Please respond in one of the following ways:

- Fill out the Customer Comment Form located at the back of this guide and return it to us.
- E-mail your comments to cspubs@ascend.com.
- FAX your comments to 978-692-1510, attention Technical Publications.
- Open a case in CaseView for documentation.

Customer Support

To obtain release notes, technical tips, or support, access the Ascend FTP Server or contact the Technical Assistance Center (TAC) at:

- 1-800-DIAL-WAN or 1-978-952-7299 (U.S. and Canada)
- 0-800-96-2229 (U.K.)
- 1-978-952-7299 (all other areas)

Acronyms

This guide uses the following acronyms:

Acronym	Description
ATM	asynchronous transfer mode
CIR	committed information rate
CSU	channel service unit
CPE	customer premise equipment
CRC	cyclic redundancy check
CSU	channel service unit
DCE	data communications equipment
DS0	digital signal level 0 (64 Kbps)
DSU	data service unit
DTE	data terminal equipment
DXI	Data Exchange Interface
GA	Group address
HSSI	High-Speed Serial Interface
IA	individual address
IOP	I/O processor
IP	Internet Protocol
KA	keep-alive
Kbps	kilobits per second

Acronym	Description
LTP	Link Trunk Protocol
NMS	Network Management Station
NNI	Network-to-Network Interface
OSPF	Open Shortest Path First
PDN	public data network
PDU	protocol data unit
QOS	quality of service
SMDS	Switched Multimegabit Data Service
SNI	Subscriber Network Interface
SSI	SMDS-to-Access Server Interface
UDP	User Datagram Protocol
VPN	virtual private network

1

Overview

This chapter describes Switched Multimegabit Data Services (SMDS), a public packet-switched service that provides local area network features and performance across wide geographical areas. Unlike Frame Relay and ATM services, which require established connections to transfer data packets or cells, SMDS is a connectionless service that does not require dedicated lines to transmit data.

Ascend supports SMDS services on the B-STDX 8000/9000, running switch software version 4.x and earlier. If you are running a later version of the switch software, you can continue using previously configured SMDS interfaces but cannot configure new interfaces for SMDS services. For a description of Ascend's implementation of SMDS services, see the *Networking Services Technology Overview.*

About SMDS Services

Through NavisCore network management software, you can dynamically configure and monitor an SMDS network by defining the SMDS logical ports and SMDS addresses. The following sections describe some of the SMDS addressing concepts. See Chapter 3 for more information on SMDS logical ports.

SMDS Addressing

After you configure an SMDS logical port, you must specify the individual and group addresses that the SMDS network uses to send and receive data.

Individual address — The SMDS individual address uses the E.164 address format.

Group address — The SMDS group address also uses the E.164 address format. Each group address may contain individual (member) addresses.

You define each group address on a per-network map basis. You define each individual address on a per-DXI basis. Each SSI has an individual feeder address.

SMDS Address Screening

SMDS address screens enable you to set restrictions on the exchange of SMDS data units with other CPEs. Source address screening checks the data units received from a particular source, while destination-address screening checks the data units sent to a particular destination. Table 1-1 lists the address screening capacities for both individual and group address screens.

Individual address screens — Contain a list of individual addresses and an allowed/disallowed option. You can apply the allowed/disallowed option globally to all individual addresses in the list of addresses. The B-STDX switch supports only one individual address screen per DXI/SNI.

Group address screens — Contain a list of group addresses and an allowed/disallowed option. You can apply the allowed/disallowed option globally to all group addresses in the list. The B-STDX switch supports only one group address screen per DXI/SNI logical port.

Table 1-1 lists the SMDS maximum addressing capacities for the B-STDX switch with IOP+ and Release 4.0/4.1 or Release 4.2 switch software.

Table 1-1. SMDS Address Capacity on the B-STDX

Maximum Capacity for...	Release 4.0/4.1	Release 4.2
DXI/SNI logical ports per switch	1680	1680
Individual address screens per DXI/SNI logical port	1	1
Group address screens per DXI/SNI logical port	1	1
Individual addresses that can be assigned to a DXI/SNI logical port	240	240
Individual addresses per IOP	240	240
Individual addresses per switch	3360	3360
Group addresses per switch	1024	400
Alien addresses per switch	1024	2048
Members per group	3360	3360
Members per individual address screen	4384	5408
Members per group address screen	2048	2448
Groups in which an individual address can be a member	1024	400

Table 1-1. SMDS Address Capacity on the B-STDX (Continued)

Maximum Capacity for...	Release 4.0/4.1	Release 4.2
Individual addresses that can be associated with an SSI logical port	no limit	N/A

Network Addressing Parameters

SMDS also supports network-wide address masking. *Address masking* is a feature used to identify "area numbers" for SMDS. The area number is mapped to the switch's internal IP address and is identified by applying an area mask to the E.164 SMDS address. Inter-switch traffic switching uses area numbers for routing purposes. Other network parameters include:

- country codes
- address prefixes
- SMDS address masking

See Chapter 2, "Setting SMDS Network Parameters," for descriptions and configuration instructions.

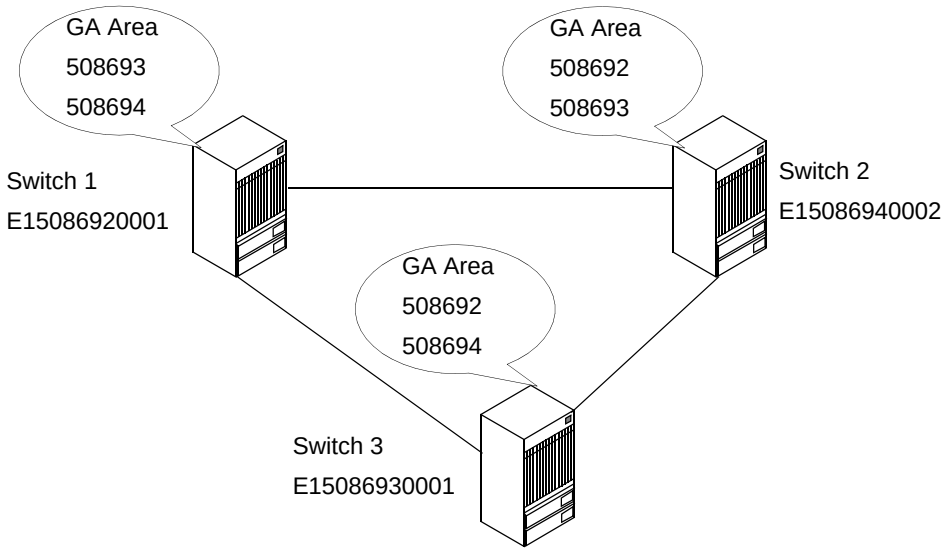
Network Group Addresses

Group addressing (GA) enables customer premise equipment (CPE) to broadcast the same data unit(s) to several recipients. When the SMDS switch receives a group-addressed packet from a DXI/SNI port, it sends a copy of the data unit to each DXI/SNI port whose address is in the same group. The SSI associated with the multiplexed DXI/SNI port receives a copy of the packet. However, DXI/SNIs that are multiplexed to other SSIs do not receive a copy of the group-address data unit. If more than one individual address within a single DXI/SNI logical port belongs to the same group, only a single copy is sent to the DXI/SNI port.

If an SSI link goes down, non-Ascend users must wait until the link is restored before the switching systems can transmit individual and group-address traffic.

Selective Group-Address Frame Processing

Group-address frames are processed based on the GA masking parameters and the defined GA area. SMDS services do not blindly broadcast frames to every member of the group; instead, frames are broadcast *only* to those members with the same defined group-address area. This method relies less on the SMDS cloud and more on SMDS trunks. Figure 1-1 shows how the switch processes SMDS group-address frames.



In this example, if Switch 1 broadcasts to area address 508694, only Switch 3 receives the broadcast. Only Switch 3 has a defined group address area of 508694.

Figure 1-1. Group-Address Processing

Group Address Frame Processing

Figure 1-2 shows how the B-STDX switch processes group-address frames. In this figure, all DXI logical ports are members of the same group address.

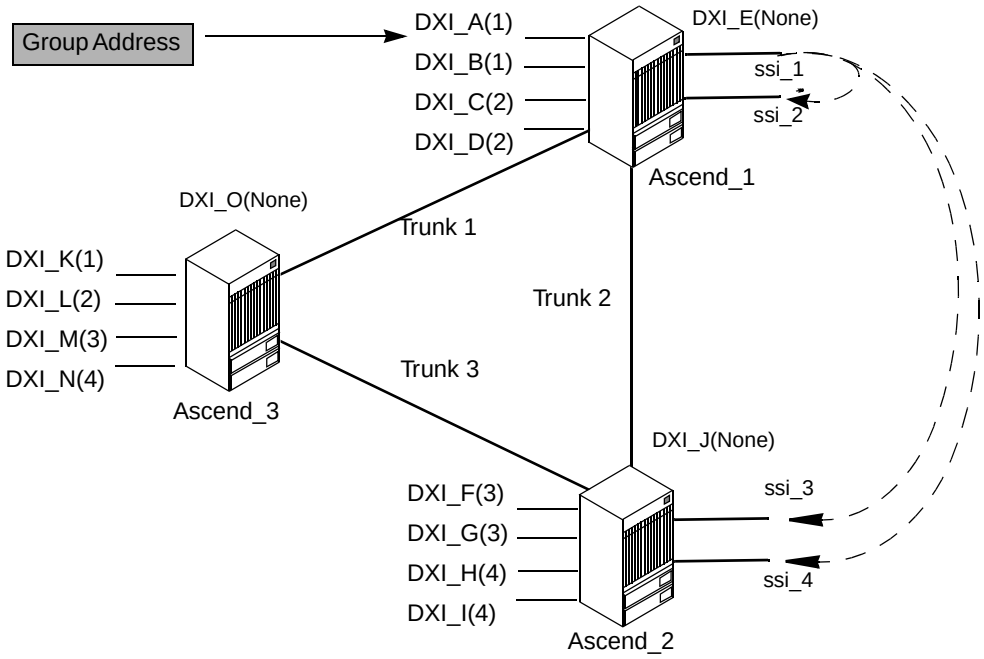


Figure 1-2. Group-Address Frame Processing

Table 1-2 describes how SMDS switching systems process group-address frames on the B-STDX.

Table 1-2. Group-Address Processing

If/When the...	Then...
GA frame enters DXI_A(1) port	Ascend_1 switch distributes the frame to DXI_B(1), DXI_C(2), DXI_D(2), and DXI_E(none). Ascend_1 sends one frame to SSI (since originating DXI (DXI_A) is multiplexed to SSI_1, and one frame to Ascend_2 and Ascend_3 (since these switches have DXIs that are members of this GA). ***Note**: SSI multiplexing is not involved when the GA frame goes to the same switch.*

Table 1-2. Group-Address Processing (Continued)

If/When the...	Then...
GA frame arrives at the trunk port on Ascend_2	The switch checks if the originating port is DXI and distributes the GA frame to DXI_F(3), DXI_G(3), DXI_H(4), DXI_I(4), and DXI_J(none). ***Note**: SSI multiplexing is not involved when the GA frame goes to the same switch.*
GA frame arrives at the trunk port on Ascend_3	The switch checks if the originating port is DXI and distributes the GA frame to DXI_F(3), DXI_G(3), DXI_H(4), DXI_I(4), and DXI_J(none). ***Note**: SSI multiplexing is not involved when the GA frame goes to the same switch.*
GA frame enters SSI_3 at Ascend_2	The switch checks if the source address and individual area addresses (also known as the NPA/NXX) exist in the routing table. In Figure 1-2, the source address of DXI_A(1) should exist in the routing tables, so frames are discarded. The same process applies to frames arriving at SSI_2 and SSI_4. Discarding these frames eliminates duplication of GA frames to DXI ports.
Non-Ascend switch sends a GA frame to the SSIs	The Ascend switch checks the source address and the NPA/NXX numbers in the received frames. In Figure 1-2, the source address and the NPA/NXX do not exist, so the GA frame is distributed according to SSI multiplexing.

Bellcore Vs. Ascend Group-Address Processing

You can set the SMDS group address processing mode to either Bellcore or Ascend as shown in Table 1-3 and Table 1-4. The advantage of the Ascend processing mode is that, because the trunks are not connected through the core, problems within the core do not effect switching. With Bellcore, if there is a problem in the core, frames cannot pass though.

Table 1-3. Group-Address Processing (Bellcore Group-Address Switching)

Source	Destination				
	Local DXI/None	**Local DXI/SSI**	**Remote DXI/SSI**	**Remote DXI/None**	**SSI**
DXI/Local SSI	Y	Y (if same SSI)	Y (if same SSI)	Y	Y
DXI/Remote SSI	Y	Y (if same SSI)	Y (if same SSI)	Y	Y
DXI/None	Y	Y	Y	Y	N
SSI	N	Y	Y	N	N

Table 1-4. Group-Address Processing (Ascend Group-Address Switching)

Source	Destination				
	Local DXI/None	**Local DXI/SSI**	**Remote DXI/SSI**	**Remote DXI/None**	**SSI**
DXI/Local SSI	Y	Y	Y	Y	Y
DXI/Remote SSI	Y	Y	Y	Y	Y
DXI/None	Y	Y	Y	Y	N
SSI (SA = Ascend)	N	Y (if same SSI)	Y (if same SSI)	N	N
SSI (SA = Ascend)	N	N	N	N	N

SMDS Services Configuration Sequence

Before configuring SMDS services, you must first configure the I/O module and physical ports. If you have not already set the card attributes and configured physical ports, see the *NavisCore Physical Interface Configuration Guide* for instructions.

Figure 1-3 shows the SMDS services configuration flowchart.

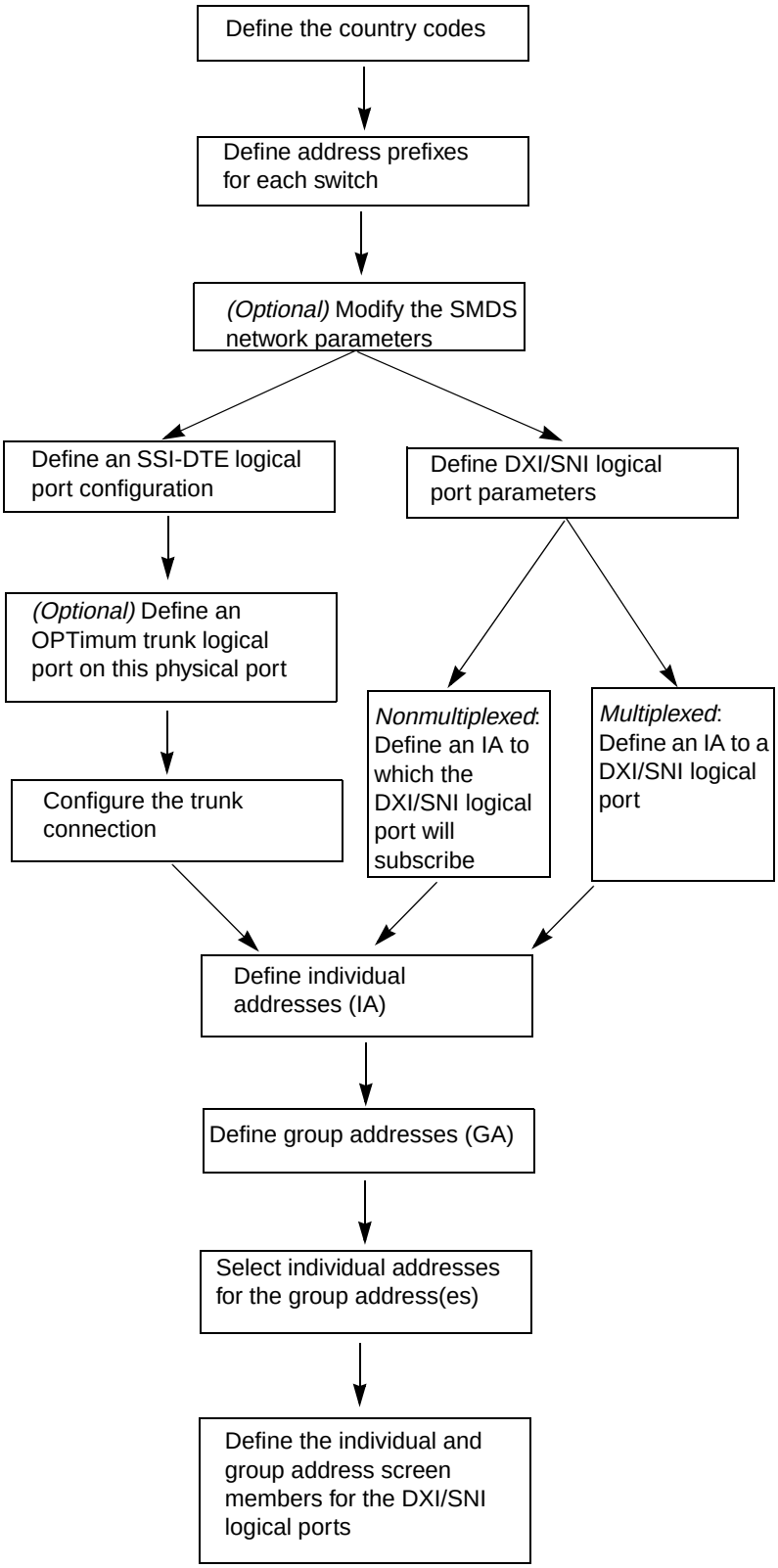


Figure 1-3. SMDS Services Configuration Flowchart

2

Setting SMDS Network Parameters

This chapter describes how to configure the following SMDS network parameters:

- Country codes
- Address prefixes
- Individual masking and group address masking

For information about individual and group addressing, see “SMDS Addressing” on page 1-1.

About SMDS Country Codes and Address Prefixes

You can define multiple *country codes* (for example, North America and United Kingdom) on one map. The country code may be up to three digits in length and is used with the SMDS address prefix.

The SMDS address prefix is a numeric string consisting of at least three digits. To define a unique individual address, you must first assign an address prefix and then add the remaining digits (address suffix).

You cannot change an address prefix once you use it to define an individual address. However, you can combine the same address prefix with different address suffixes to create a unique address. For example:

prefix 1: 508692	address suffix: 2600	result: (508692)2600
prefix 2: 508692	address suffix: 2400	result: (508692)2400

All of these components combine to form the SMDS E.164 address, as in the following example:

C15086922600

where **C** indicates an individual address and **1** represents the country code for North America. An **E** would indicate a group address. For example, **E**15086922600.

Figure 2-1 shows the country code, address prefix, and address suffix which create the E.164 address, C440175662424.

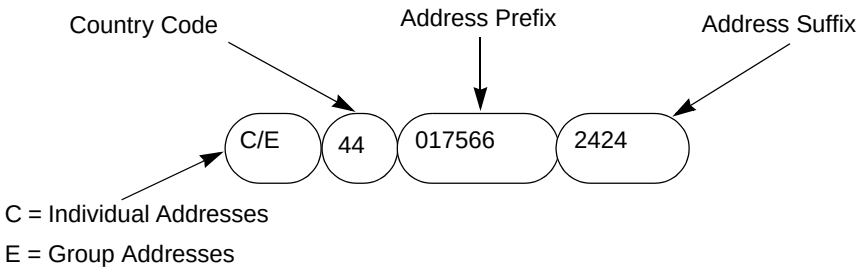


Figure 2-1. SMDS E.164 Address Example

About SMDS Network Address Masking

SMDS uses address masking to identify area numbers. The area number is mapped to the switch's internal IP address and is identified by applying an area mask to the E.164 SMDS address. Inter-switch traffic uses area numbers for routing purposes.

You can modify the mask size and mask starting position for group addresses and individual addresses in the entire network. A maximum of 16 digits is allowed for the individual group-address mask. Each switch in the network must have the same masking parameters.

The mask start position indicates the beginning of the mask. The mask size indicates the number of digits the switch uses to make a switching decision. The area definition is based on the mask position and mask size. The Open Shortest Path First (OSPF) protocol uses the area definition for routing purposes.

In Figure 2-2, a mask start position of 2 and a mask size of 9 indicates the mask starts at 5 and is 9 digits in length. To modify the mask size, see "Setting Network Parameters" on page 2-5.

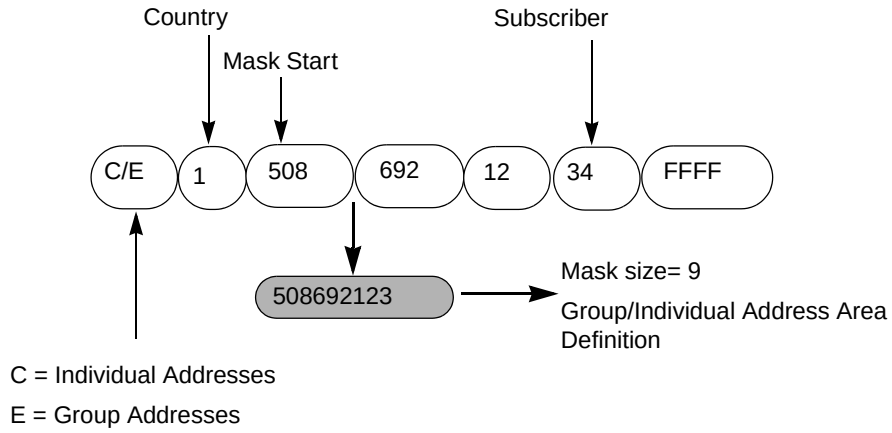


Figure 2-2. SMDS Address Masking

Defining the Country Code and Address Prefix

Country codes and address prefixes are set from the Administer menu. Be sure that you are logged on with appropriate privileges before setting these fields.

Defining Country Codes

To define the SMDS country code and address prefix:

1. From the Administer menu, select Ascend Parameters ⇒ Set All SMDS Parameters ⇒ Set All Country Codes. The Set All Country Codes dialog box appears (Figure 2-3).

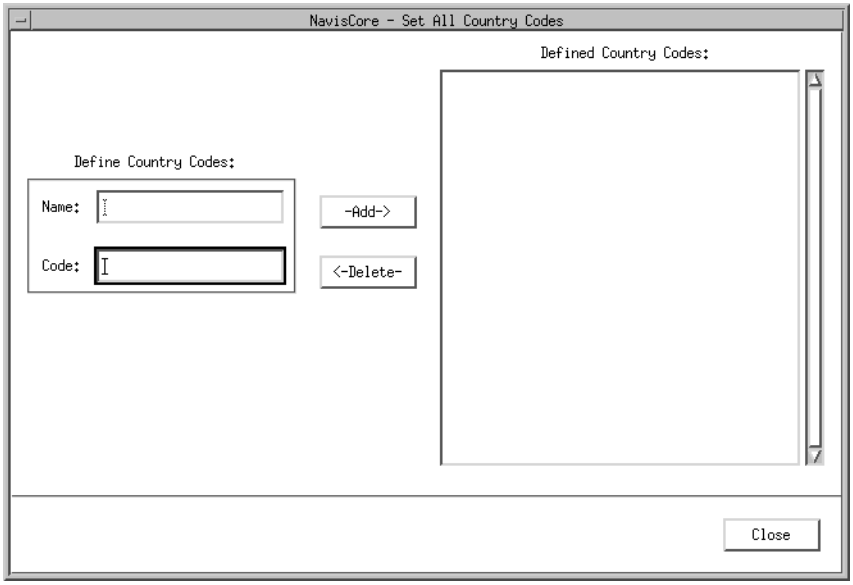


Figure 2-3. Set All Country Codes Dialog Box

2. Complete the fields as follows:

   Name — Enter a name for the country code you are defining. For example, North America or United Kingdom.

   Code — Enter the country's standard numeric telephone code. For example, 1 for North America or 44 for United Kingdom.

3. Choose Add. The system adds the country code to the Defined Country Codes list box.

4. Choose Close to exit the Set All Country Codes dialog box and return to the map.

Defining Address Prefixes

To configure the SMDS address prefix for a switch:

1. From the Administer menu, select Ascend Parameters ⇒ Set All SMDS Parameters ⇒ Set All Address Prefixes. The Set All Address Prefixes dialog box appears (Figure 2-4.)

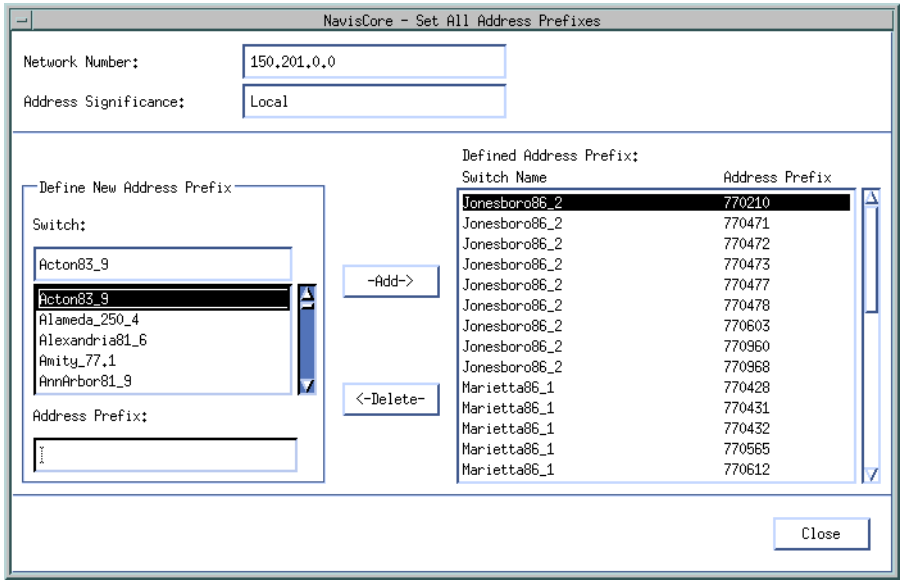


Figure 2-4. Set All Address Prefixes Dialog Box

2. On the left, select the switch for which you are defining the address prefix(es).
3. In the Address Prefix text box, enter at least three numbers.
4. Choose Add. The address prefix appears in the Defined Address Prefix list box.
5. Repeat Step 3 and Step 4 until you define all address prefixes that you require for the selected switch.
6. Choose Close to exit.

Setting Network Parameters

This section describes how to modify the individual and group address masking parameters for individual and group addresses. It also describes how to set the group address processing mode.

All switches in the network must have the same group masking parameters.

To modify the masking parameters and set the group address processing mode:

1. From the Administer menu, select Ascend Parameters ⇒ Set All SMDS Parameters ⇒ Set All Networkwide Parameters. The Set All Networkwide Parameters dialog box appears (Figure 2-5).

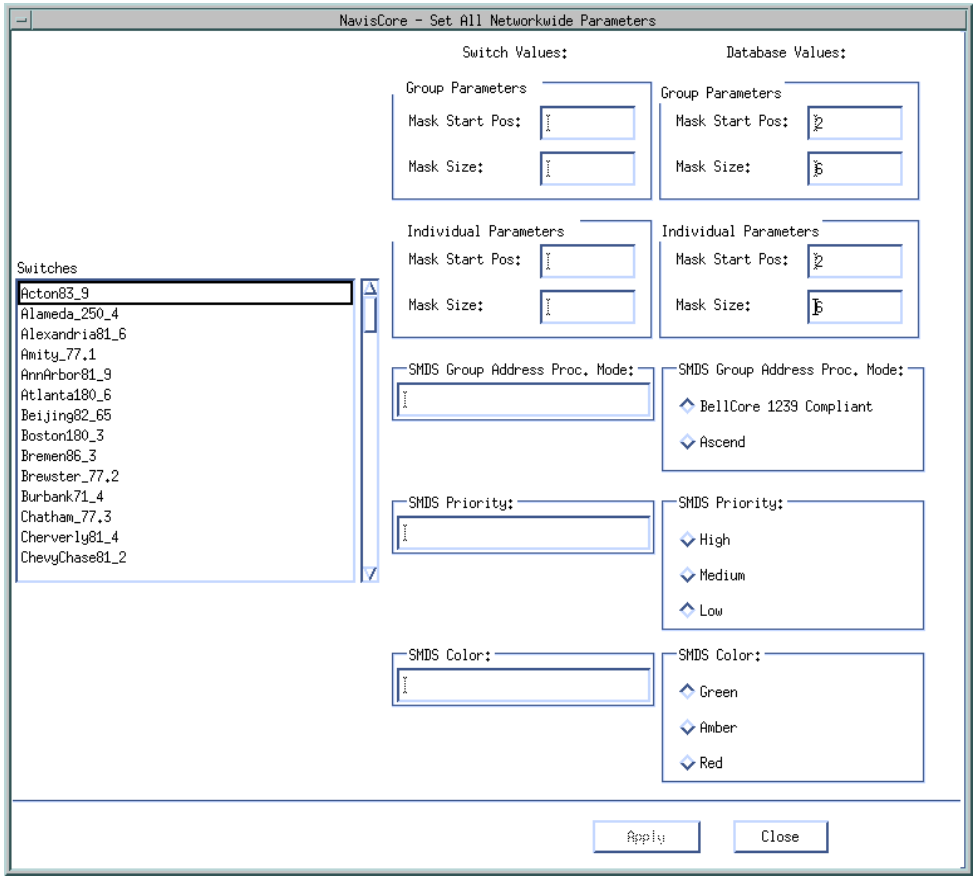


Figure 2-5. Set All Networkwide Parameters Dialog Box

2. Select a switch in the Switches field. The system displays the group and individual mask parameters for the switch and database.

3. Modify the group and individual mask parameters database values (displayed on the right side of the dialog box), by completing the fields in Table 2-1.

Table 2-1. Set SMDS Networkwide Parameters Fields

Field	Action/Description
Group Mask Parameters	
Mask Start Pos	Enter a value between 1 and 15. The default start position is 2.
Mask Size	Enter a value between 1 and 15. The default size is 6. ***Note**: If you set the Mask Size to 0, it will disable the switching system.*
Individual Mask Parameters	

Table 2-1. Set SMDS Networkwide Parameters Fields (Continued)

Field	Action/Description
Mask Start Pos	Enter a value between 1 and 16. The default start position is 2.
Mask Size	Enter a value between 1 and 16. The default size is 6.
SMDS Group Address Proc. Mode	Select an SMDS switching mode. Options include: *Bellcore 1239 Compliant (default)* – Complies with Bellcore 1239 and determines how frames are processed. *Ascend* – Uses the direct trunk connection and does not rely on the SMDS cloud. The SMDS cloud is used only to communicate with non-Ascend switches. For more information, see "Group Address Frame Processing" on page 1-5.
SMDS Priority	Select a priority level of high, medium, or low. All SMDS frames within the switch are assigned that priority. When a trunk becomes congested, the switch discards frames in order of the priority and color assignment.
SMDS Colors	Select an SMDS color of green, amber, or red. All SMDS frames within the switch are assigned that color. When a trunk becomes congested, the switch discards frames in order of the priority and color assignment. Red is discarded first, followed by amber, and then green.

4. Choose Apply to save the changes.
5. Choose Close to exit.

3

Configuring SMDS Logical Ports

This chapter describes how to create and configure the following SMDS logical ports:

- An SSI-DTE (or DCE) logical port for communicating through a third-party cloud
- An SSI-DTE (or DCE) logical port to function as an OPTimum trunk for direct communications through the network
- A DXI/SNI connection for switch-to-router communications

Logical Port Configuration Options

Table 3-1 lists the SMDS logical port types.

Table 3-1. SMDS Logical Port Types

LPort Type	Description
SSI-DTE	SMDS-to-Access Server Interface Data Terminal Equipment. Provides the interface between the network supporting SMDS services and the subscriber-owned equipment.
DXI/SNI DCE	Data Exchange Interface/Subscriber Network Interface DCE. Provides the interface to enable the customer premise equipment (CPE) to exchange Level 3 protocol data units (PDUs) with the SMDS Access Server without an SMDS DSU/CSU.
DXI/SNI DTE	Data Exchange Interface/Subscriber Network Interface DTE. The same as DXI/SNI DCE except that the CPE is connected to the Ascend switch through an SMDS DSU/CSU. ***Note:*** *The DXI/SNI DTE connection is not a typical configuration. Consult the Ascend Technical Assistance Center* ***before*** *you set up this type of configuration.*
SMDS OPTimum Trunk	Enables a single physical port to be shared among several inter-switch trunks.

About SSI-DTE Logical Ports

An SSI-DTE logical port is an SMDS switching-system interface that is used to connect an Ascend switch to another Ascend switch through a third-party network. Multiple SSI logical ports can reside on one channelized physical port, but only one SSI-DTE logical port can reside on an unchannelized physical port. The SSI-DTE is the logical port you configure to enable multiplexing between SMDS DXI/SNI logical ports. It is also the foundation logical port type for an OPTimum trunk interface.

OPTimum Trunk Configuration

You can optionally configure an SSI-DTE logical port to function as an SMDS OPTimum trunk, connecting Ascend switches across an SMDS network. This configuration allows several inter-switch trunks to share a single physical port. The Ascend OPTimum trunk feature enables private enterprise networks to purchase lower-cost, public-carrier services as the trunk between two Ascend switches, instead of using a more expensive leased line.

About DXI/SNI Logical Ports

A DXI/SNI logical port configuration can be either multiplexed or nonmultiplexed within the SMDS network.

- A multiplexed configuration multiplexes a specific SSI-DTE logical port to provide both local and remote switching capability.
- A nonmultiplexed configuration connects two routers off of a single switch.

SMDS Logical Port Configuration Flowchart

Figure 3-1 shows the configuration sequence used to:

- Add and define an SMDS SSI-DTE logical port and to optionally add an OPTimum trunk connection
- Configure a DXI/SNI logical port for multiplexed or nonmultiplexed switching

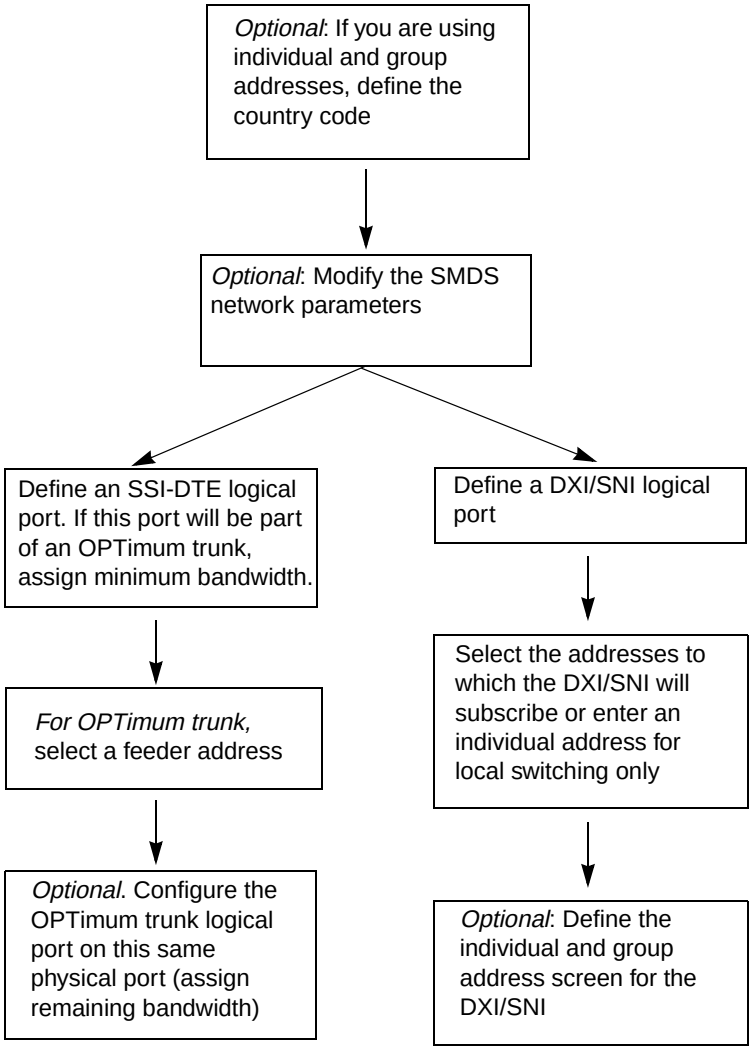


Figure 3-1. SMDS Logical-Port Configuration Sequence

Accessing Logical Port Functions

To access logical port functions, you must be logged into NavisCore with either a provisioning or operator password.

1. Select the switch to which you want to add a logical port.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the physical port on which you want to define a logical port. The Set Physical Port Attributes dialog box appears.
4. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears (Figure 3-2).

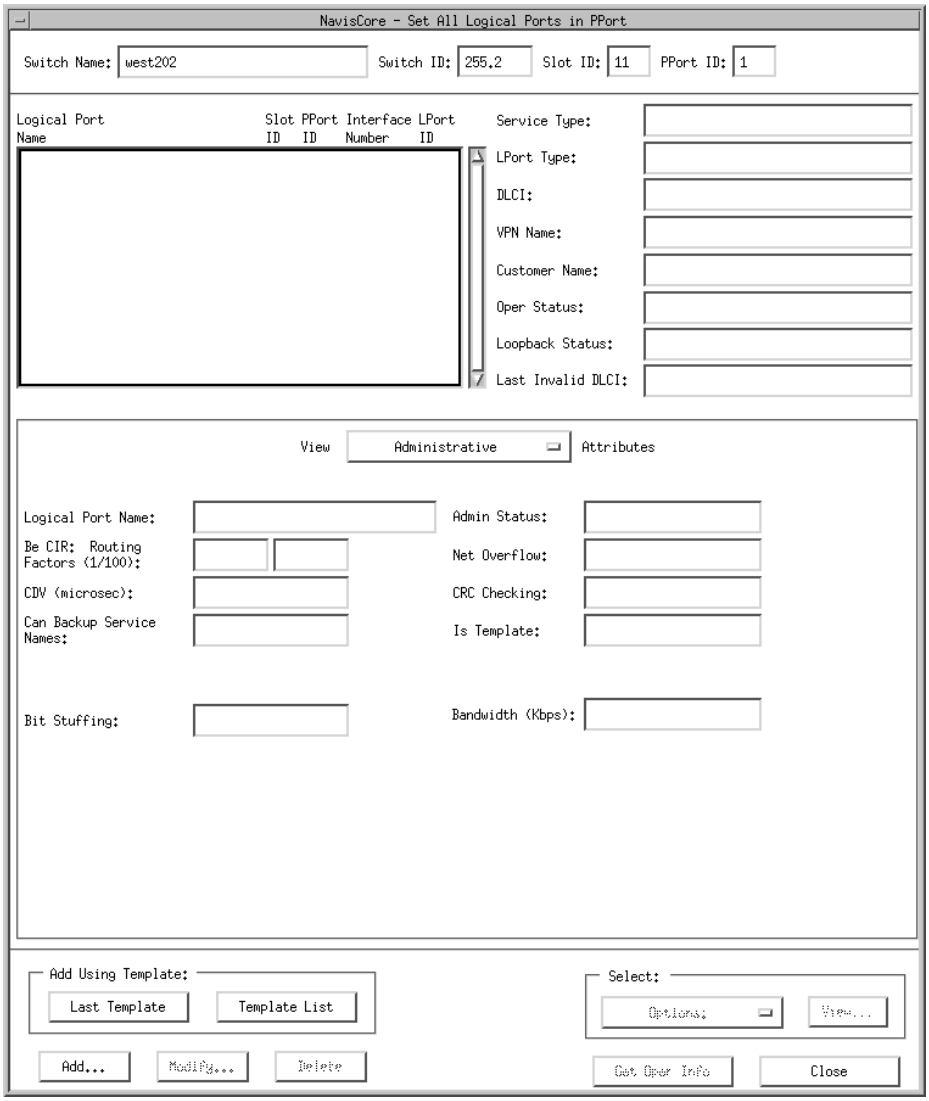


Figure 3-2. Set All Logical Ports in PPort Dialog Box

The Set All Logical Ports In PPort dialog box displays information about existing logical ports and enables you to add a new logical port. It also provides several buttons that enable you to access many NavisCore functions. Table 3-2 lists and describes the Set All Logical Ports in PPort dialog box buttons.

Table 3-2. Set All Logical Ports in PPort Dialog Box Buttons

Button	Function
Add/Modify/Delete	Enables you to add a new logical port, modify an existing logical port, or delete a logical port. For information about deleting logical ports, see Chapter 6.
Diagnose	Accesses diagnostic test functions for the selected logical port. For more information, see the *NavisCore Diagnostic and Troubleshooting Guide*.
Statistics	Displays the summary statistics for the selected logical port. For more information, see the *NavisCore Diagnostic and Troubleshooting Guide*.
Last Template/ Template List	If you defined a logical port configuration and saved it as a template, you can use this option to define a new logical port with the same parameters.
Get Oper Info	Displays a status message in the *Oper Status* field for the selected logical port.
VPN/Customer	Displays the Virtual Private Network customer's name (if a VPN exists for this logical port).
View QoS Parameters	Displays the Quality of Service parameters.

Adding an SMDS Logical Port

To add an SMDS logical port:

1. Access the logical port functions as described in "Accessing Logical Port Functions" on page 3-4.
2. Choose Add from the Set All Logical Ports in PPort dialog box. The Add Logical Port Type dialog box appears (Figure 3-3).

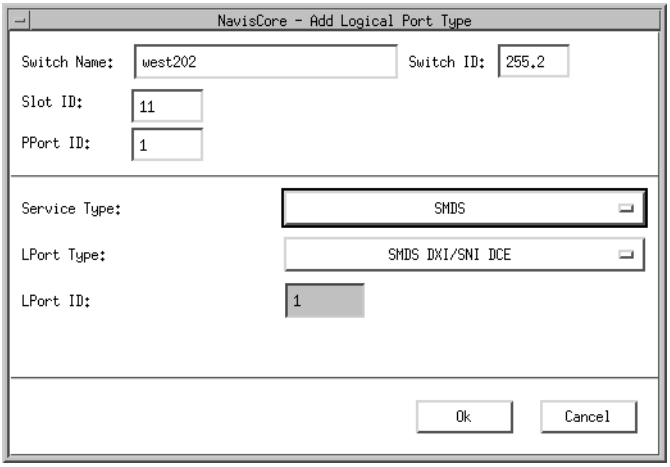


Figure 3-3. Add Logical Port Dialog Box

The settings for this dialog box vary depending on the type of logical port you are configuring. See the appropriate section for the logical port type you are configuring (see Table 3-3).

Table 3-3. SMDS Logical Port Types

Logical Port Types	See...
SMDS SSI-DTE	"Defining SSI-DTE Logical Ports" on page 3-7.
SMDS OPTimum Trunk	"Defining SMDS OPTimum Trunk Logical Ports" on page 3-19.
SMDS SNI (DTE or DCE)	"Defining DXI/SNI Logical Ports (DCE or DTE)" on page 3-20.

The Set Attributes Options Menu

When you define a new logical port, the Add Logical Port dialog box displays a Set Attributes options menu (Figure 3-4) that enables you to set different attributes for each type of logical port. Attributes include:

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

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

SMDS — Sets the polling interval and polling thresholds for each logical port.

Trap Control — Sets the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port.

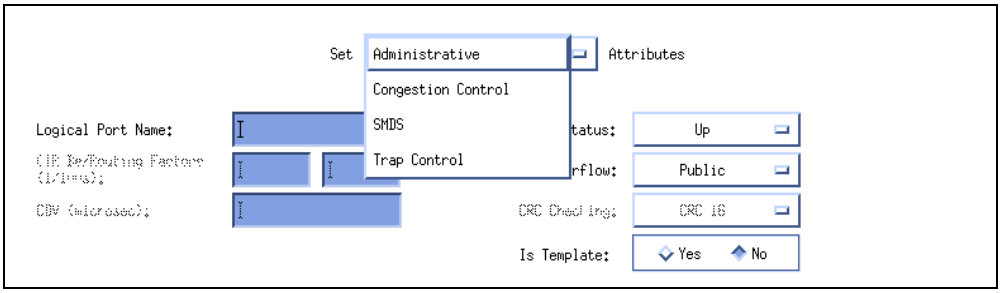


Figure 3-4. Set Attributes Options Menu

Defining SSI-DTE Logical Ports

To define an SSI-DTE logical port:

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

Table 3-4. Add Logical Port Type Fields

Field	Action/Description
Service Type	Select SMDS.
LPort Type	Select SMDS SSI DTE.
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one.

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields (Figure 3-4).

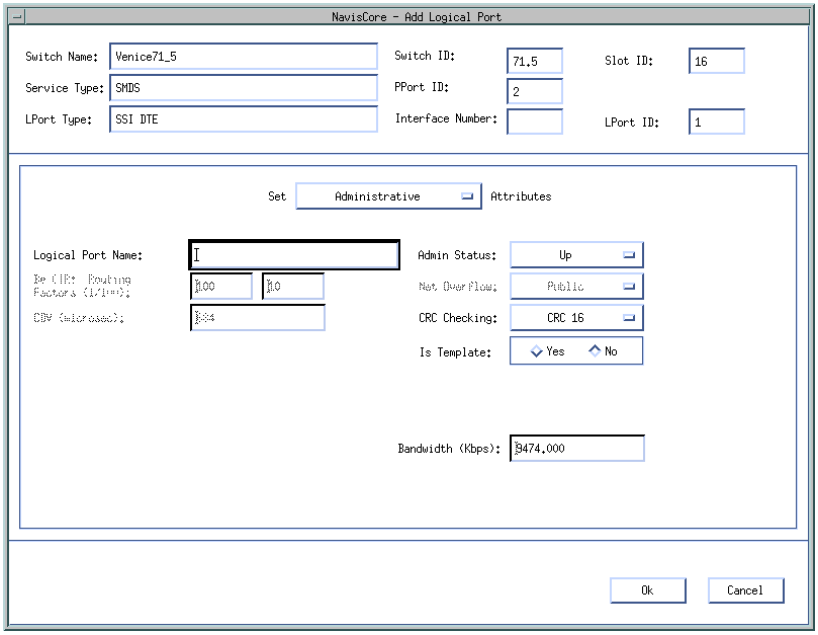


Figure 3-5. Add Logical Port (SSI-DTE)

Administrative Attributes

Complete the administrative attributes fields described in Table 3-5.

Table 3-5. Administrative Attribute Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length).
Admin Status	Set the Admin Status field to one of the following options: *Up (default)* – Activates the port. *Down* – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.
CRC Checking	Select the cyclic redundancy check (CRC) to 16- or 32-bit.
Is Template (*Optional*)	Save these settings as a template to quickly configure a new logical port with the same options. To create a template, choose Yes in the *Is Template* field.

Table 3-5. Administrative Attribute Fields (Continued)

Field	Action/Description
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth remaining from the physical clock rate, less any logical ports already configured. ***Note:*** *If you are defining an SMDS OPTimum trunk port on this same physical port, decrease the amount of bandwidth on this logical port to ensure sufficient remaining bandwidth.*
Channels allocated for a Logical Port are marked by their IDs	If you are configuring a channelized T1 or E1 module, specify the DS0 (for T1) or TS0 (for E1) channel(s) assigned to the logical port. The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, select the channel to remove the X. You can select/deselect channels by using the following Channel Allocation editing buttons. --To deselect all channels ++To select all channels -To deselect a specific channel +To select a specific channel ***Note****: The logical port bandwidth either increments or decrements depending on the number of channels you select or deselect. You can configure other logical ports with different attributes on this same physical port.*
Bit Stuffing	Select the bandwidth that matches the bandwidth capability of CPE connected to this logical port. Enables bit stuffing on T1/E1/DSX-1 ports. Bit stuffing effects the available bandwidth of each DS0/TS0 channel on this port. *On* – Provides 56 Kbps of bandwidth. *Off* – Provides 64 Kbps of bandwidth.

Congestion Control Attributes

1. Select Congestion Control from the Set Attributes option menu. The Add Logical Port dialog box displays the attributes fields (Figure 3-6).

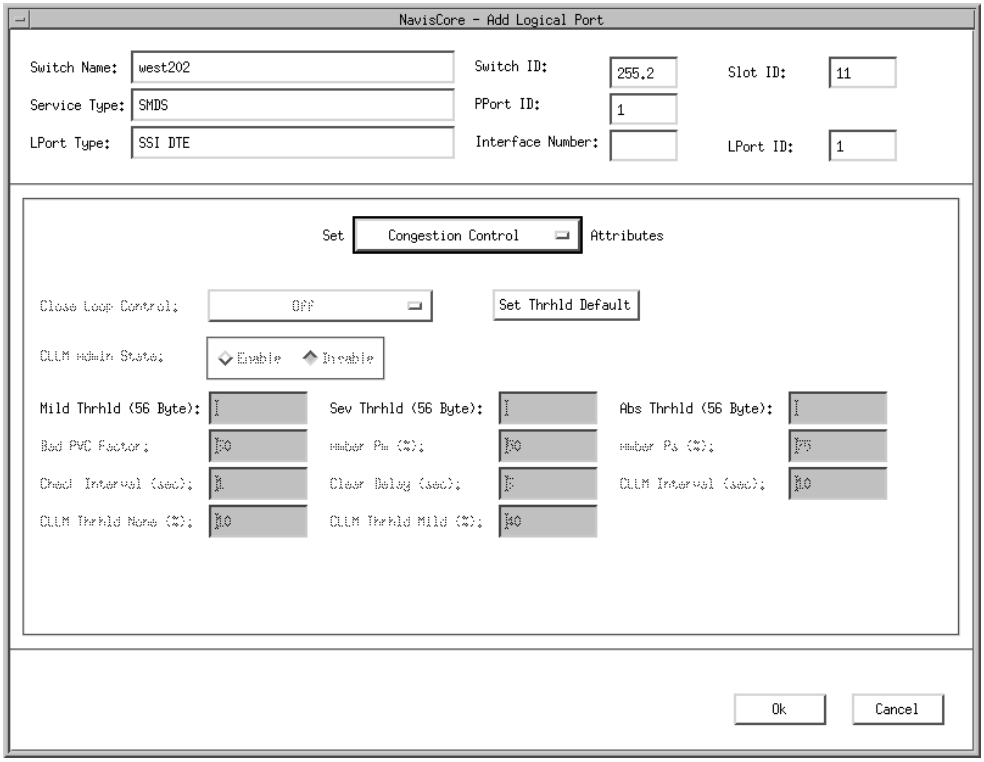


Figure 3-6. Set Congestion Control Attributes (SSI-DTE)

2. Complete the congestion control attributes fields described in Table 3-6.

Table 3-6. Set Congestion Control Attributes Fields

Field	Action/Description
Cong. Enabled	Set the congestion control parameters. This field enables/disables OSPF closed-loop congestion control for each logical port. For more information, see the *NavisCore Frame Relay Configuration Guide*. Options include: *Off (default)* – Disables closed-loop congestion. *On* – Enables closed-loop congestion.
Set Thrhld Default	Sets the Mild, Severe, and Absolute threshold settings to the default settings described in the *NavisCore Frame Relay Configuration Guide*. The default settings depend on the card type.

Table 3-6. Set Congestion Control Attributes Fields (Continued)

Field	Action/Description
Mild Thrshld (*SSI only*) Severe Thrshld (*SSI only*) Absolute Thrshld	Accept the defaults or enter values for the mild, severe, and absolute threshold fields as defined in the *NavisCore Frame Relay Configuration Guide*. ***Note**: Do not exceed the maximum threshold value for each card type. The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.* *If you are setting the threshold parameters on a T1/E1 card, the default values will not appear until you set the bit stuffing and bandwidth allocation. See Table 3-5 on page 3-8 for more information.* *For channelized T1/E1 PRI modules, if* n *DS0s are assigned per channel, the maximum number of allowed buffers is* n *x 225 (T1) and* n *x 174 (E1).*

SMDS Attributes

1. Select SMDS from the Set Attributes option menu. The Add Logical Port dialog box displays the attributes fields (Figure 3-7).

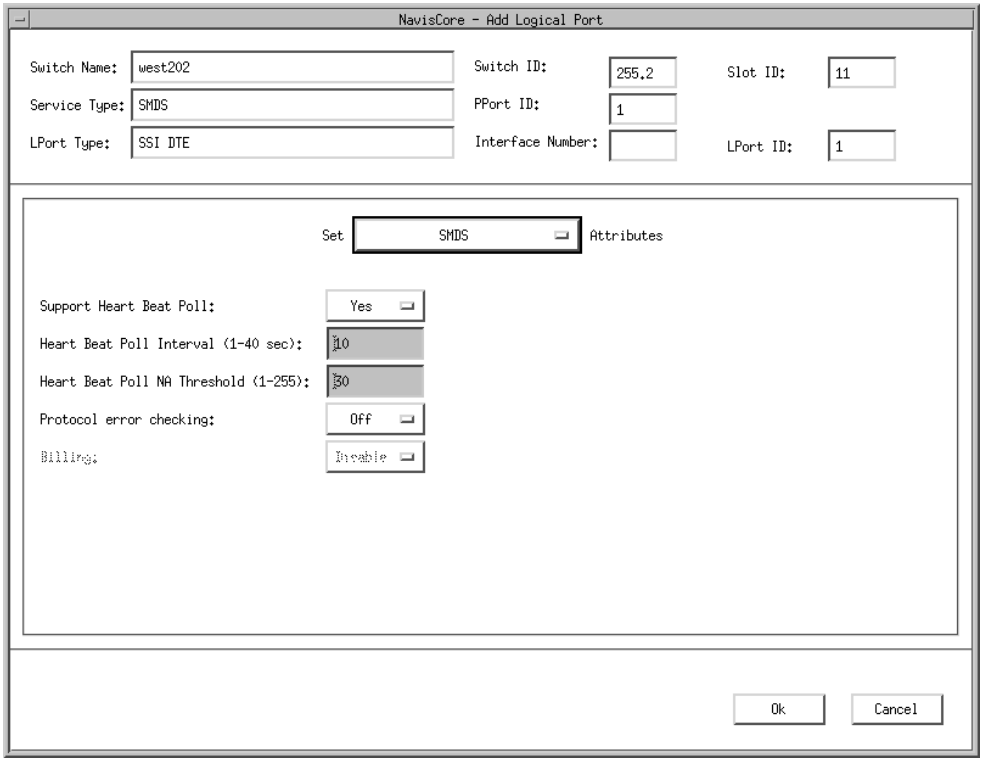


Figure 3-7. Set SMDS Attributes (SSI-DTE)

2. Complete the SMDS attributes fields described in Table 3-7.

Table 3-7. Set SMDS Attributes Fields

Field	Action/Description
Support Heart Beat Poll	Select *Yes (default)* only if the CPE connected to this port supports heart-beat poll responses; otherwise select *No*. Heart-beat polls check for a keep-alive signal coming from the CPE.
Heart Beat Poll Interval (1-40 sec)	Enter a value from 1 to 40 seconds (default is 10 seconds). This value specifies the time that occurs between heart-beat polling requests sent to the CPE.
Heart Beat Poll NA Threshold (1-255)	Enter a value from 1 to 255 (default is 30). This value represents the configured threshold of heart-beat polling requests that can go unanswered before a trap is recorded in the event log. A threshold crossing alert is sent to the NMS each time the threshold for the DXI/SNI is exceeded within a 15-minute time period. The unanswered heart-beat poll count resets every 15 minutes.
Protocol Error Checking	Set the protocol error checking parameter. This field determines the level of protocol error checking on PDUs received by this logical port. **Enable this field for debugging purposes only**. Options include: *Off (default)* – Enables minimal address checking. *On* – Enables complete Level 2 protocol error checking. This setting activates Level 2 protocol error counters for which you can view statistics. There is a slight performance cost if you enable this feature.

Trap Control Attributes

1. Select Trap Control from the Set Attributes option menu. The Add Logical Port dialog box displays the attributes fields (Figure 3-8).

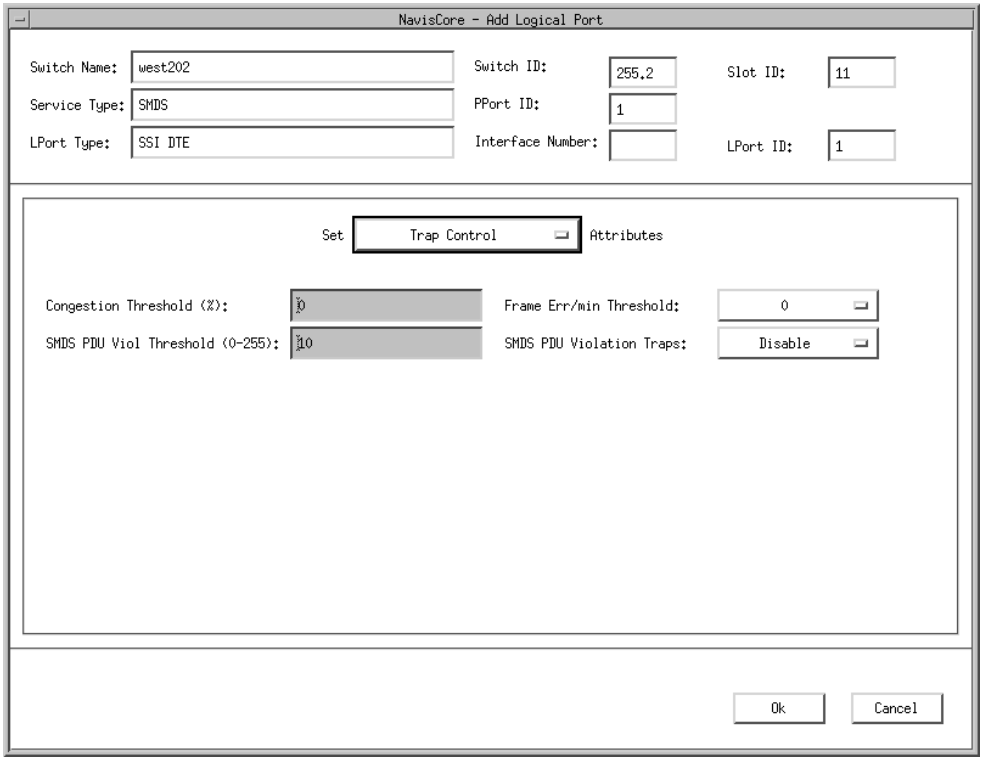


Figure 3-8. Set Trap Control Attributes (SSI-DTE)

2. Complete the trap control attributes fields described in Table 3-8.

Table 3-8. Set Trap Control Attributes Fields

Field	Action/Description
Congestion Threshold (%)	Enter a value between 0 and 100 to indicate the threshold percentage for generating and sending traps to the NMS for this logical port. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the percentage value you enter. Adjust the entered value according to how sensitive this port must be to network congestion. Options include: *Low* – Generates a trap at the first sign of congestion. *High* – Generates traps for serious network congestion. *Zero (default)* – Disables congestion threshold. If you enter zero, no traps are generated for this logical port.

Table 3-8. Set Trap Control Attributes Fields (Continued)

Field	Action/Description
SMDS PDU Viol Threshold (0-255)	Specify the number of PDU violations that can occur before a trap is sent to the NMS. The software increments a counter every time an SMDS PDU violation occurs on a logical port. The software polls these counters every 60 seconds. If a particular counter exceeds the specified SMDS PDU violation threshold for the logical port, it generates a trap corresponding to that particular violation. The default is 10 PDU violations. Options include: *Low* – Sensitive to SMDS PDU violations. *High* – Issue traps only when there is a significant number of SMDS PDU violations.
CRC Checking (*HSSI modules only*)	Set this value to match the number of error checking bits used by the CPE connected to this port. This functions performs a cyclic redundancy check (CRC) on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.
Frame Err/Min Threshold	Enter a value from 0 to 16384 to configure the threshold of frame errors on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS. Adjust this value according to how sensitive this port must be to frame errors. Options include: *Low* – Port is sensitive to frame errors. *High* – Generates traps when a significant number of frame errors occurs within a one-minute period. *Zero (default)* – Disables this feature, which prevents traps from being generated for this logical port.
SMDS PDU Violation Traps	Enable or disable this field. An SMDS PDU violation can be either an SIP3 SMDS address failure or an invalid DXI2 frame header. These errors mean incoming frames are bad and that there are problems with the CPE configuration. Options include: *Disable (default)* – Turns off traps. *Enable* – Issues traps for PDU violations.

3. When you are done setting attributes, choose OK. The Set All Logical Ports in PPort dialog box appears, displaying the configured attributes for the logical port.
4. Choose Close. The Set Physical Port Attributes dialog box appears.
5. Configure the remaining logical ports for this physical port.

6. If you are configuring an OPTimum trunk logical port on this same physical port, define the SSI feeder as described in the next section "Defining the Feeder Address for an SSI-DTE Logical Port."
7. Otherwise, you can configure the DXI/SNI logical port(s). See "Defining DXI/SNI Logical Ports (DCE or DTE)" on page 3-20 for more information.

Defining the Feeder Address for an SSI-DTE Logical Port

Before you define an OPTimum trunk (on the SSI-DTE logical port), you must define a feeder address on the logical port. The OPTimum trunk logical port inherits the subscribed address from the SSI feeder address.

If you select an individual address to use as the feeder address for an SSI-DTE logical port, a DXI/SNI cannot subscribe to it. An SSI-DTE logical port can subscribe to one feeder address only.

To define the feeder address and select the individual address to which the SSI-DTE logical port subscribes:

1. From the Set Physical Port Attributes dialog box, select Logical Port. The Set All Logical Ports in PPort dialog box appears (Figure 3-9).

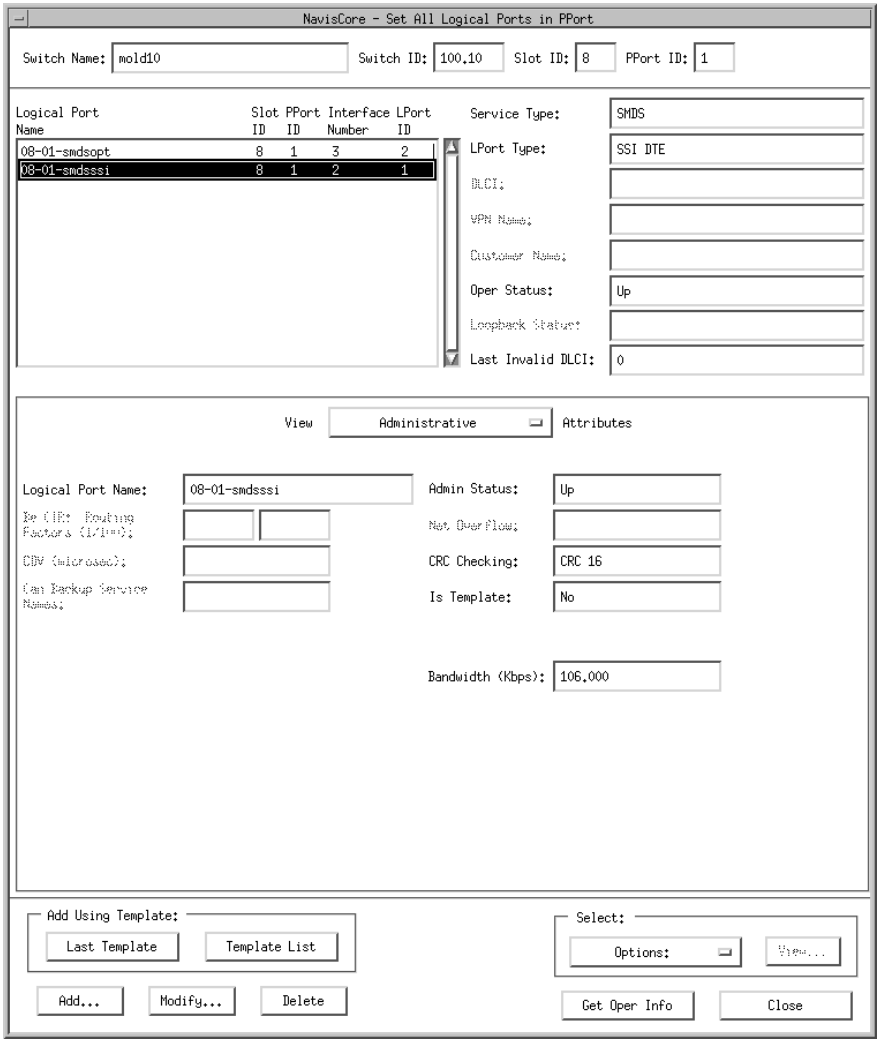


Figure 3-9. Set All Logical Ports in PPort Dialog Box

2. Select the SSI-DTE logical port from the list box and choose Modify. The Modify Logical Port Type dialog box appears.
3. Choose OK. The Modify Logical Port dialog box appears, displaying the attributes for the selected logical port (Figure 3-10).

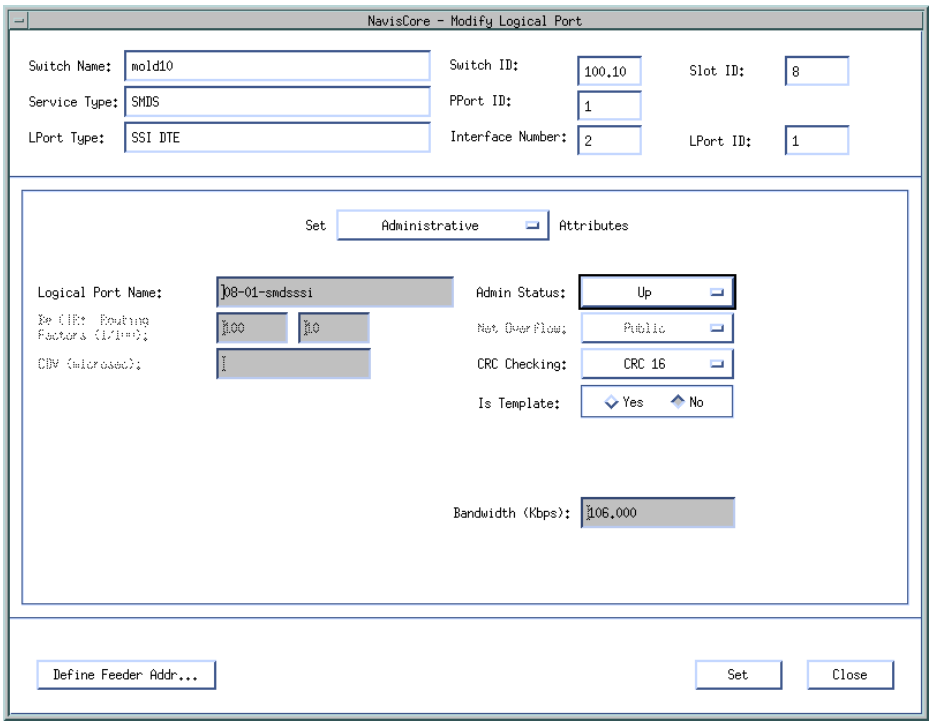


Figure 3-10. Modify Logical Port Dialog Box

4. From the Modify Logical Port dialog box, choose the Define Feeder Addr button. The Define Feeder Address for SMDS SSI LPort dialog box appears (Figure 3-11).

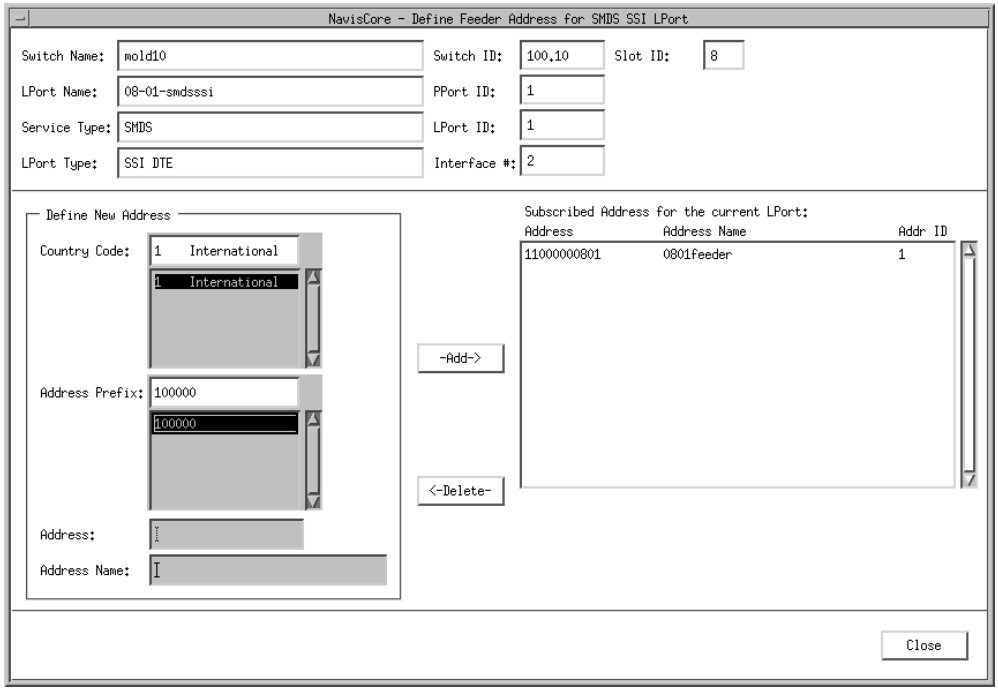


Figure 3-11. Define Feeder Address for SMDS SSI LPort Dialog Box

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

Table 3-9. Define Feeder Address for SMDS SSI LPort Fields

Field	Action/Description
Country Code	Select the country code to which the SSI-DTE logical port subscribes.
Address Prefix	Select the address prefix to which the SSI-DTE logical port subscribes.
Address	Enter the remainder of the address (address suffix) in the Address field. See "About SMDS Country Codes and Address Prefixes" on page 2-1 for more information.
Address Name (*Optional*)	Enter an alphanumeric name to further describe the address. (Do not use apostrophes.)

6. Choose Add. The address appears in the Subscribed Addresses for the current LPort list box.
7. Choose Close. The Modify Logical Ports dialog box reappears.
8. Choose Close. The Set All Logical Ports in PPort dialog box reappears.
9. Choose Close to return to the Set Physical Port Attributes dialog box.

Defining SMDS OPTimum Trunk Logical Ports

The Ascend switch architecture enables you to use Ascend OPTimum trunking for SMDS. You can configure the same physical port with one or more logical ports for an SMDS OPTimum path. This allows several inter-switch trunks to share a single physical port. All SMDS OPTimum paths are assigned one SMDS individual address, which is terminated at the logical ports. SMDS OPTimum trunk logical ports inherit their subscribed address from the SSI feeder address.

Channelized T1/E1 modules do not support OPTimum trunk logical ports.

Before you configure an SMDS OPTimum trunk, verify the following tasks are complete:

- Define an SSI-DTE logical port on the same physical port. (See “Defining SSI-DTE Logical Ports” on page 3-7.)
- Define an individual address for the SSI feeder.
- Select the individual address for the SSI feeder. (See “Defining the Feeder Address for an SSI-DTE Logical Port” on page 3-15.)

To configure an SMDS OPTimum trunk, you must first configure an SSI-DTE logical port on the same physical port. Use the following sequence:

To define an SMDS OPTimum trunk logical port:

1. Add an SSI-DTE logical port as described in “Defining SSI-DTE Logical Ports” on page 3-7.
2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields (Figure 3-12).

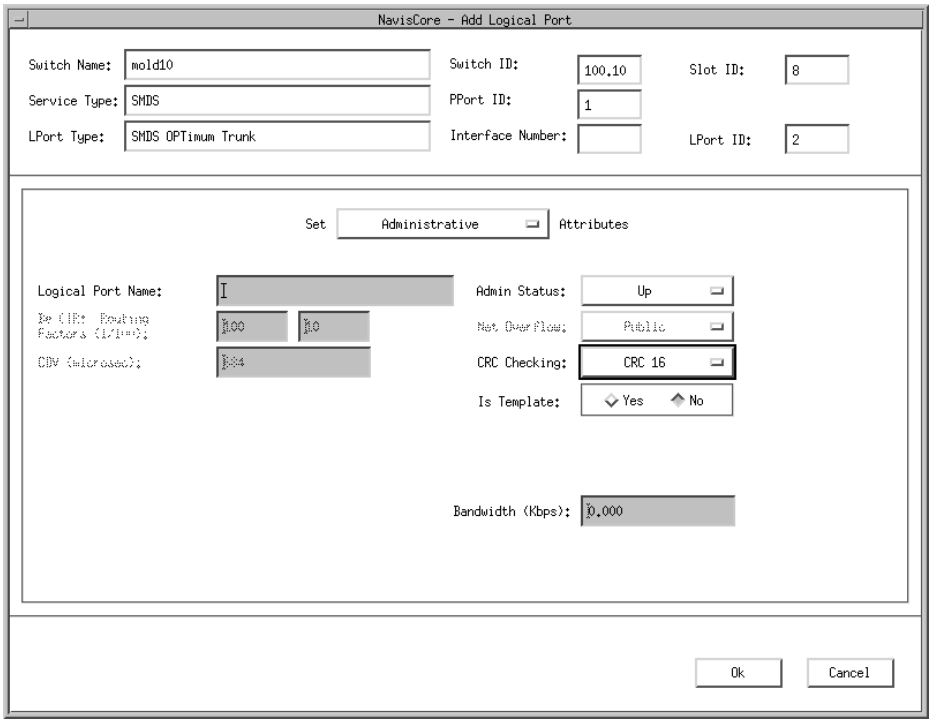


Figure 3-12. Add Logical Port (OPTimum Trunk) Dialog Box

3. Complete the administrative attributes fields described in Table 3-5 on page 3-8.
4. Complete the trap control attributes fields described in Table 3-8 on page 3-13.
5. Choose OK. The Set All Logical Ports in PPort dialog box appears and displays the name of the new logical port.
6. Choose Close. The Set Physical Port Attributes dialog box appears.

   When you finish, you can define the trunk line connection. See Chapter 7 for more information.

Defining DXI/SNI Logical Ports (DCE or DTE)

A DXI/SNI logical port performs switching within the SMDS network. If the DXI/SNI is multiplexed to a specific SSI-DTE, choose an individual address. If, however, the port performs nonmultiplexed switching only, you must select a defined address prefix and enter a unique address number to create an individual address. You can configure up to 240 DXI/SNI logical ports per IOP, up to a maximum of 3360 per switch.

The DXI/SNI-DTE connection is not a typical configuration. Contact the Ascend Technical Assistance Center before you set up this type of configuration.

Before you define an SMDS DXI/SNI logical port for either remote or local switching, verify the following tasks are complete:

- Define an SSI-DTE logical port configuration.
- Define the individual addresses.

To define a DXI/SNI logical port:

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

Table 3-10. Add Logical Port (DXI SNI) Fields

Field	Action/Description
Service Type	Select SMDS.
LPort Type	Select SMDS DXI/SNI DCE or DTE.
LPort ID	For a T1 module, enter a number between 1 and 24. For an E1 module, enter a number between 1 and 30. For all other modules, the Logical Port ID is a read-only field that automatically defaults to one (1).

2. Choose OK. The Add Logical Port dialog box displays the Set Attributes option menu and fields (Figure 3-13).

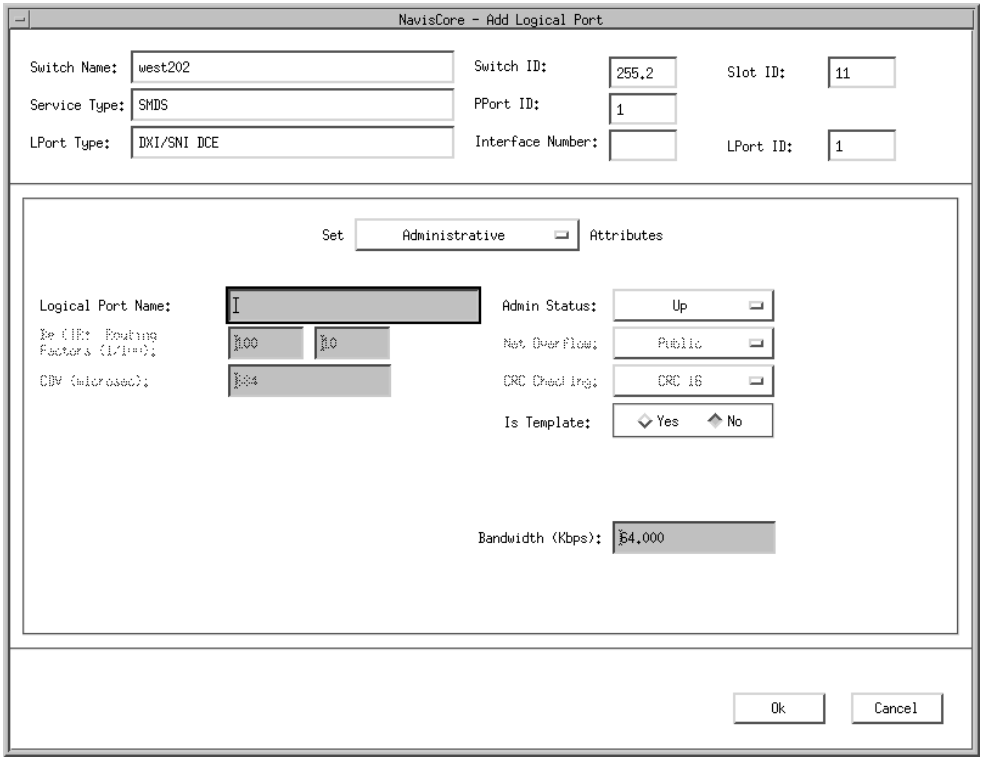


Figure 3-13. Set Administrative Attributes

3. Complete the required fields described in Table 3-5 on page 3-8.
4. Set the congestion control attributes for this DXI/SNI logical port by selecting Congestion Control from the Set Attributes option menu. Complete the fields described in Table 3-6 on page 3-10.
5. Set the SMDS attributes for this DXI/SNI logical port by selecting SMDS from the Set Attributes option menu. Complete the SMDS attributes fields described in Table 3-7 on page 3-12.
6. (*Optional*) Complete the Multiplex to this SSI field to configure the DXI/SNI logical port to multiplex to an SSI-DTE. Do one of the following:
   - If this DXI/SNI logical port is to perform local switching only, choose Select. The Select End Logical Port dialog box appears as shown in Figure 3-14. In the Switch Name field, select [None]. Choose OK. Continue with Step 8 on page 3-24.
   - If this DXI/SNI logical port is to multiplex to an SSI-DTE logical port, choose Select. The Select End Logical Port dialog box appears (Figure 3-14).

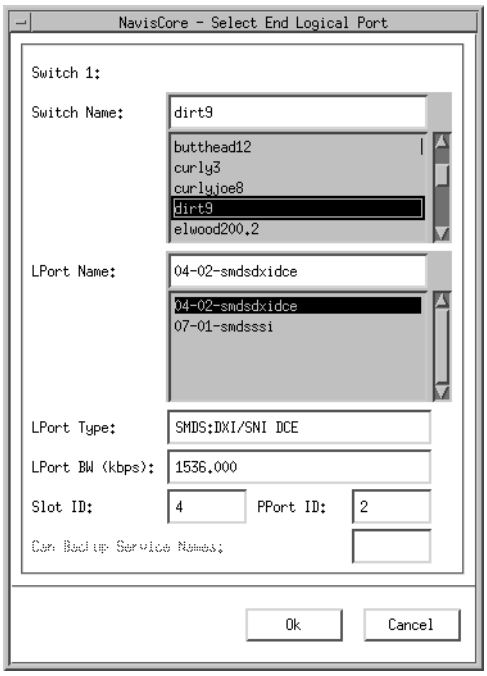


Figure 3-14. Select End Logical Port Dialog Box

7. Complete the required fields described in Table 3-11.

Table 3-11. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the switch (name) where the SSI port resides. The Switch Name field displays a list of the available SSI logical ports residing on the selected switch.
LPort Name	Select the specific SMDS to Access Server Interface (SSI) port to which this logical port will multiplex. See "Defining Individual Addresses for DXI/SNI Logical Ports" on page 4-1 for instructions.

8. Set the trap control attributes for this DXI/SNI logical port by selecting *Trap Control* from the Set Attributes option menu. Complete the fields described in Table 3-8 on page 3-13.
9. Choose OK. The Set All Logical Ports in PPort dialog box appears, displaying the name of the configured logical port.
10. Choose Close. The Set Physical Port Attributes dialog box appears.

    See Chapter 4, “Configuring Individual and Group Addresses” to set the individual addresses for the DXI/SNI logical port you configured.

4

Configuring Individual and Group Addresses

This chapter describes how to configure individual and group addresses, which SMDS uses to send and receive data. These addresses are similar to endpoint connections in connection-based networks, such as Frame Relay and ATM. You must configure these addresses after you configure an SMDS logical port.

Specifically, this chapter describes:

- Defining individual addresses for DXI/SNI locally switched and multiplexed logical ports
- Defining group addresses
- Adding individual address members to a group

Defining Individual Addresses for DXI/SNI Logical Ports

You must define individual addresses for a DXI/SNI logical port so that it can perform local switching within the map network. You must manually enter the individual addresses to which the port subscribes.

For a multiplexed DXI/SNI logical port, the SSI-DTE logical port to which a DXI/SNI logical port is multiplexed determines the available addresses. The Define Individual Address for SMDS DXI/SNI LPort dialog box lists the available addresses to which this DXI/SNI port can subscribe.

Before you define an SMDS DXI/SNI logical port for either remote or local switching, verify that you have:

- Defined the DXI/SNI logical port parameters.
- Selected the SSI associated with the multiplexed DXI/SNI logical port.

To define the individual addresses for a DXI/SNI logical port:

1. From the Set Physical Port Attributes dialog box, choose the Logical Port button. The Set All Logical Ports in PPort dialog box appears.
2. From the Set All Logical Ports in PPort dialog box, select the DXI/SNI logical port you want to configure for local switching and choose Modify. The Modify Logical Port Type dialog box appears, displaying the service type and logical port type.
3. Choose OK. The Modify Logical Port dialog box appears (Figure 4-1), displaying the logical port parameters.

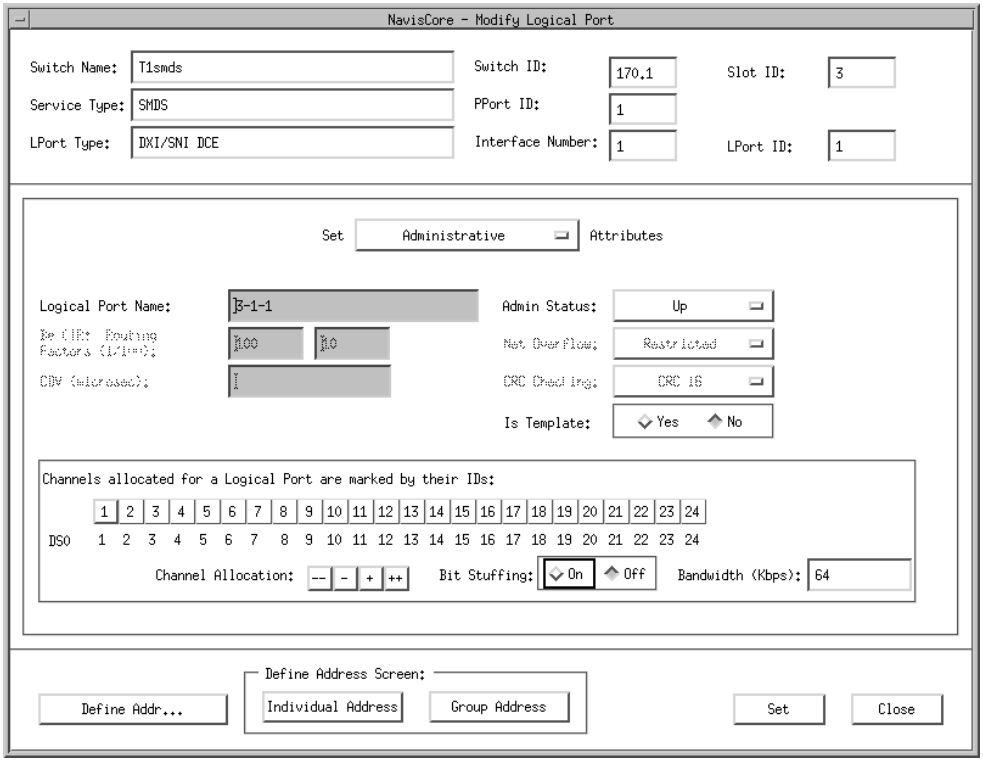


Figure 4-1. Modify Logical Port Dialog Box

4. Choose the Define Addr button. The Define Individual Address for SMDS DXI/SNI LPort dialog box appears (Figure 4-2).

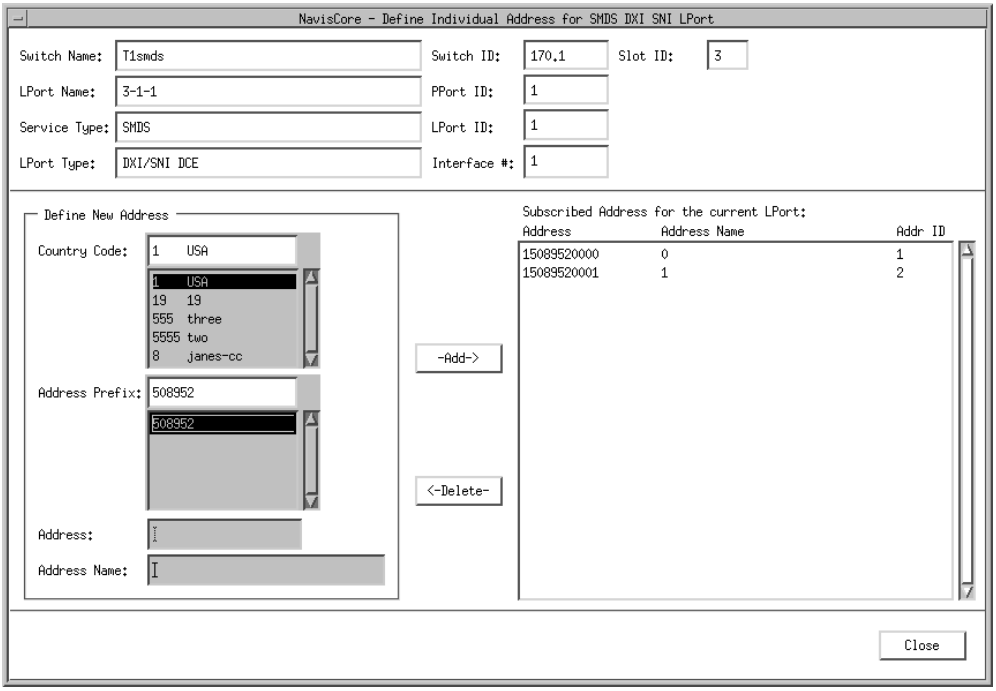


Figure 4-2. Define Individual Address for SMDS DXI SNI LPort Dialog Box

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

Table 4-1. Define Individual Address for SMDS DXI SNI LPort Fields

Field	Action/Description
Country Code	Select the country code to which the DXI SNI logical port subscribes.
Address Prefix	Select the address prefix to which the DXI SNI logical port subscribes.
Address	Enter the remainder of the address (address suffix) in the Address field.
Address Name (*Optional*)	Enter up to 16 alphanumeric characters to identify the new subscribed address (for example, westford). Do not use apostrophes.

6. Choose Add. The Subscribed Address for the current Lport list box displays the new address.

7. Repeat Step 5 and Step 6 to create additional individual addresses for the DXI/SNI logical port.

8. When you finish, choose Close. The Modify Logical Port dialog box appears.

9. Choose Close. The Set All Logical Ports in PPort dialog box appears.
10. Continue to choose Close until you return to the network map.

Defining a New Group Address

The Define Group Address dialog box displays a list of all group addresses and their members currently defined for a selected switch. From this dialog box, you can add, modify, or delete group addresses on the selected switch based on the maximum capacities described in Table 1-1 on page 1-2.

To define a network-wide group address:

1. From the Administer menu, select Ascend Parameters ⇒ Set All SMDS Parameters ⇒ Set All Network Group Addresses. The Set All Network Group Addresses dialog box appears (Figure 4-3).

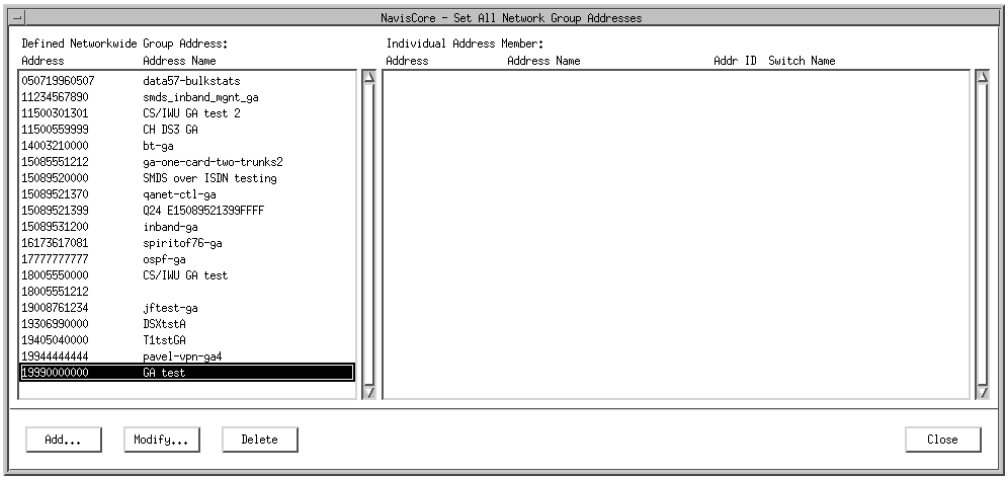


Figure 4-3. Set All Network Group Addresses Dialog Box

2. Choose Add. The Add Networkwide Group Address dialog box appears (Figure 4-4).

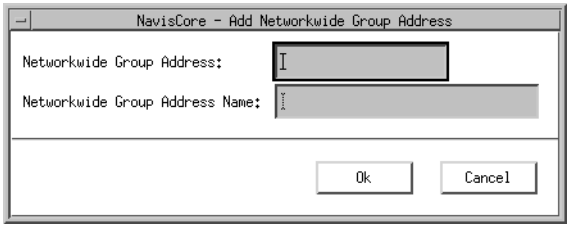


Figure 4-4. Add Networkwide Group Address Dialog Box

3. Complete the fields described in Table 4-2.

Table 4-2. Add Networkwide Group Address Fields

Field	Action/Description
Networkwide Group Address	Enter the complete group address (including the country code and address prefix).
Networkwide Group Address Name (*Optional*)	Enter up to 16 alphanumeric characters to identify the new group address (for example, massachusetts). Do not use apostrophes.

4. Choose OK. The Set All Network Group Addresses dialog box reappears, listing the new group address.
5. Repeat Step 2 through Step 4 to define additional group addresses.

Adding Individual Address Members to a Group

To add individual members to a network-wide group address:

1. From the Set All Network Group Addresses dialog box (Figure 4-3), select the group address for which you are defining members.
2. Choose Modify. The Modify Networkwide Group Address dialog box appears (Figure 4-5).

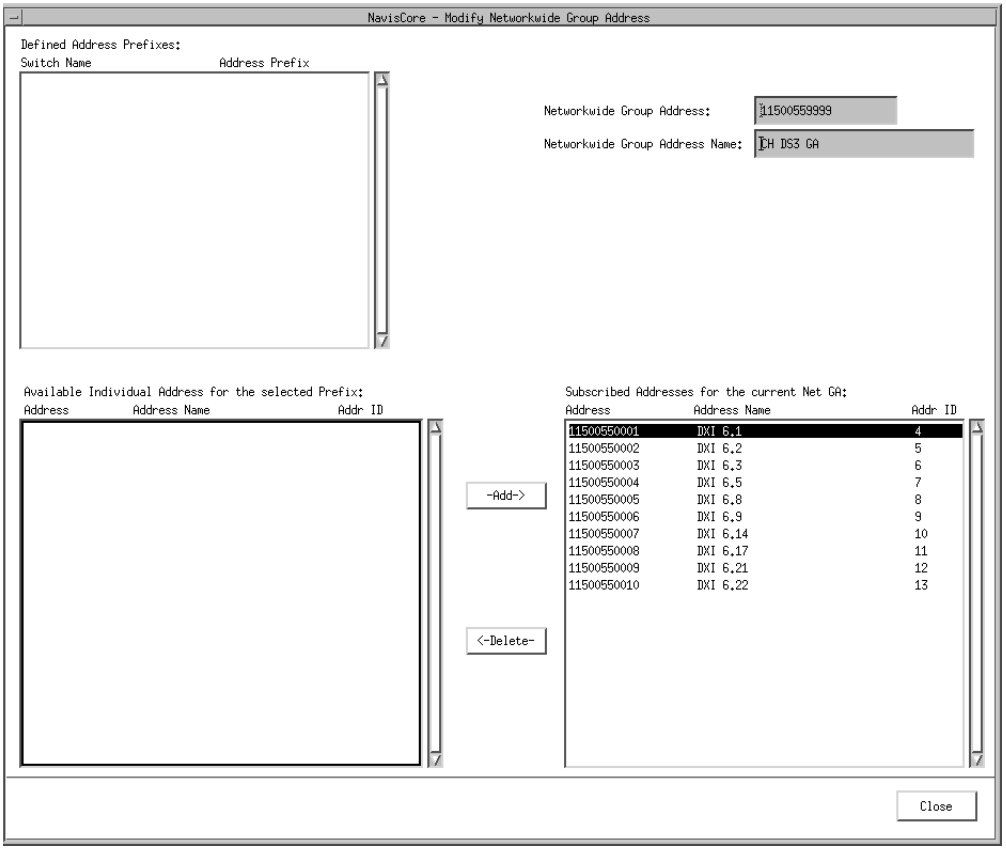


Figure 4-5. Modify Networkwide Group Address Dialog Box

3. In the Defined Address Prefixes list box, select an address prefix. The system displays available individual addresses (for the selected address prefix only) in the Available Individual Address for the selected Prefix list box. (The system does not display individual addresses from the entire network.)

4. In the Available Individual Address for the selected Prefix list box, select the individual address you want to include as a member of the group, and choose Add.

The selected individual address appears in the Subscribed Address for the current Net GA list box.

5. Repeat Step 4 until you have added all individual addresses that you want to include in the group.

6. When you finish selecting the individual address members that make up the group, choose Close. The Set All Network Group Addresses dialog box appears.

7. Choose Close to return to the network map.

5

Configuring SMDS Management Addresses

This chapter describes how to configure SMDS management addresses, which consist of the following:

- Address screens used to restrict data exchange
- In-band management addresses which enable SMDS to manage SNMP/UDP/IP protocol packets

Configuring Address Screens

This section describes how to define individual and group address screens. Screens enable you to restrict data exchange on specified DXI/SNI logical ports. For more information, see “SMDS Address Screening” on page 1-2.

Defining an Individual-Address Screen

The individual address screen enables you to restrict the data received from the CPE as well as the data transmitted to the CPE. An individual address screen consists of a set of allowed/disallowed addresses.

To define an individual address screen for a DXI/SNI logical port:

1. From the Set All Logical Ports in PPort dialog box, select the DXI/SNI logical port.
2. Choose Modify. The Modify Logical Port Type dialog box appears, displaying the service type and logical port types.
3. Choose OK. The Modify Logical Port dialog box displays the attributes for the selected logical port.

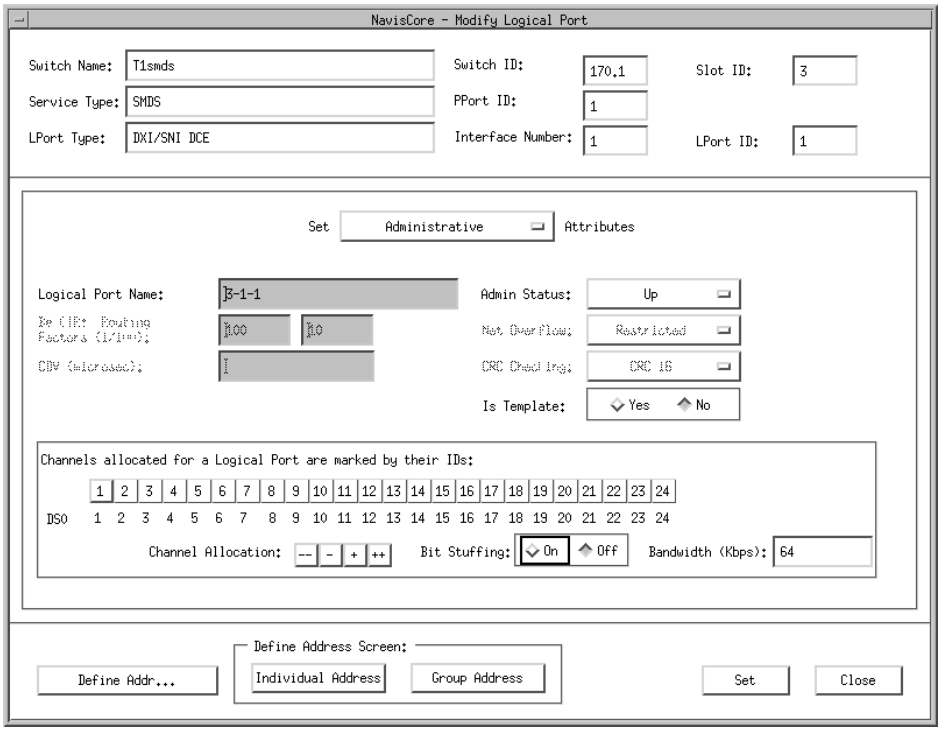


Figure 5-1. Modify Logical Port Dialog Box

4. From the Define Address Screen group, choose Individual Address. The Define Individual Address Screen dialog box appears (Figure 5-2).

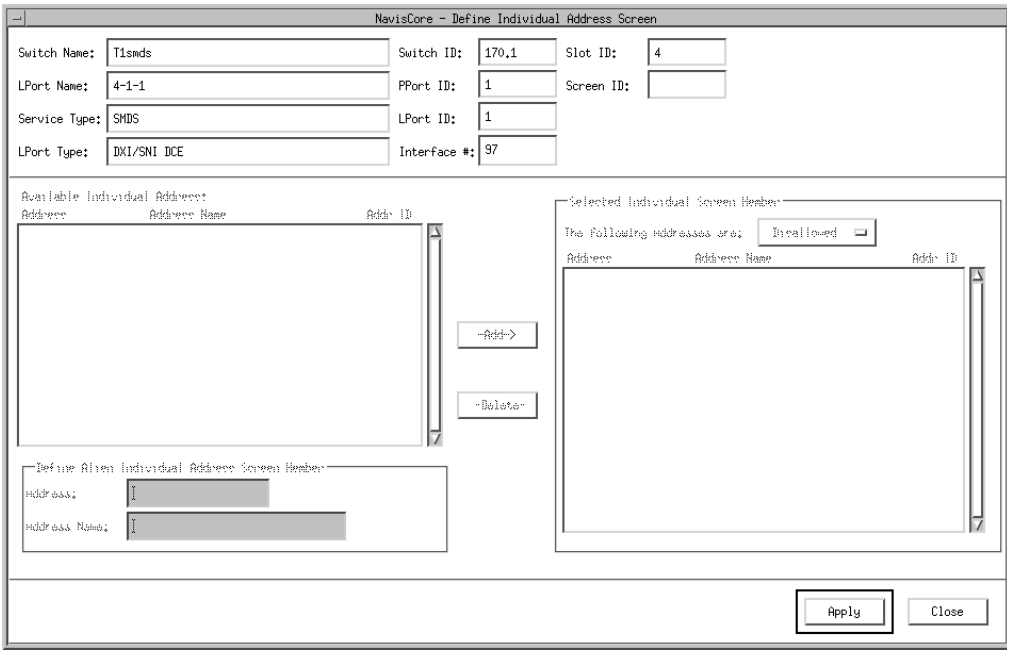


Figure 5-2. Define Individual Address Screen Dialog Box

5. Choose Apply to display the list of available individual addresses.
6. In "The following Addresses are:" field, select Allowed or Disallowed to specify the desired operation.
7. Choose Apply to enter your selection and activate the Add and Delete buttons.
8. Do one of the following:
   - Select an address from the list of available individual addresses, which includes all addresses to which the DXI/SNI ports on the selected switch subscribe.

     or

   - Enter an alien address in the Define New Alien Individual Address field. If applicable, enter the country code prefix. An alien address is any address not currently defined anywhere in the network. The alien address resides outside the switch and is used for destination screening. The Address Name field is optional.
9. Choose Add. The selected local address (or alien address) now appears in the Selected Individual Screen Member field, along with the address name and assigned address ID number (internal address).
10. Choose Close. The Modify Logical Port dialog box appears.
11. Choose Close. The Set All Logical Ports in PPort dialog box appears.

Defining a Group-Address Screen

The group address screen contains a list of group addresses and an allowed/disallowed option. The setting of the allowed/disallowed option globally applies to every group address in the list.

To define a group address screen:

1. From the Set All Logical Ports in PPort dialog box, select the DXI/SNI logical port to which you want to apply the group address screen.
2. Choose Modify. The Modify Logical Port Type dialog box appears, displaying the service and logical port types.
3. Choose OK. The Modify Logical Port dialog box displays the attributes for the selected logical port.
4. From the Define Address Screen group, choose Group Address. The Define Group Address Screen dialog box appears (Figure 5-3).

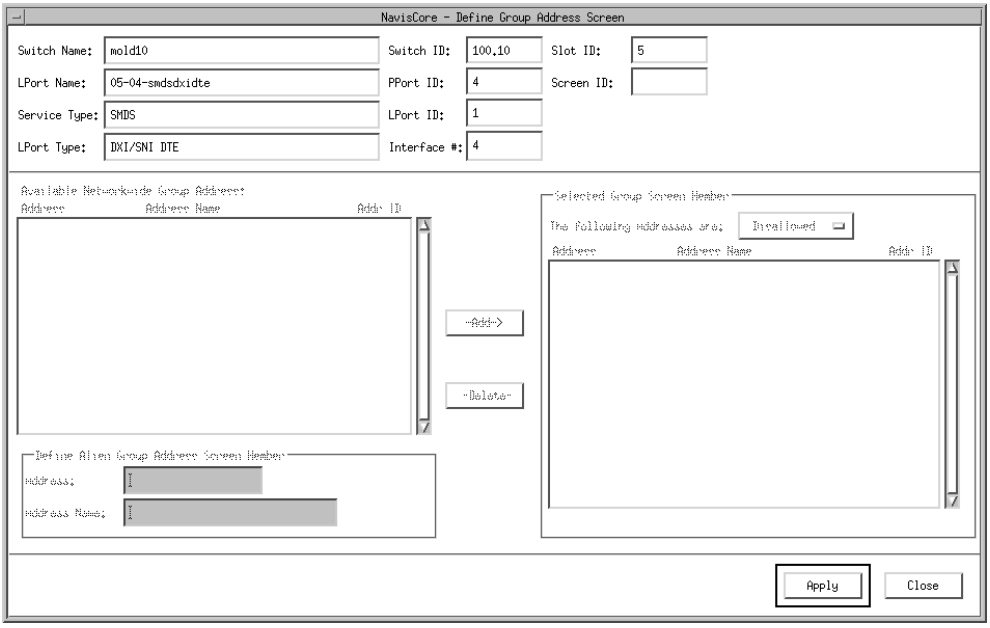


Figure 5-3. Define Group Address Screen Dialog Box

5. Choose Apply to display the list of Available Networkwide Group Addresses.
6. In “The following Addresses are” field, select Allowed or Disallowed to specify the desired operation.
7. Choose Apply to enter your selection and activate the Add and Delete buttons.

8. Do one of the following:
   - Select an address from the list of Available Networkwide Group Addresses, which includes all group addresses defined for the currently selected network.

     or
   - Enter an alien address in the Define New Alien Group Address field. If applicable, enter the country code prefix. An alien address is any address that is not currently defined for the selected switch. The Address Name is optional.
9. Choose Add. The selected group address or alien address, now appears in the Selected Group Screen Member field, along with the address name and assigned address ID number (internal address).
10. Repeat Step 8 and Step 9 to define more members.
11. Choose Close until you return to the network map.

Configuring the In-Band Management Address

An *in-band management address* enables a remote NMS that is connected to the Ascend network through SMDS to manage SNMP/UDP/IP protocol packets.

To configure the in-band management address:

1. From the Administer menu, select Ascend Parameters ⇒ Set All SMDS Parameters ⇒ Set All Management Addresses. The Set All SMDS Management Address dialog box appears (Figure 5-4).

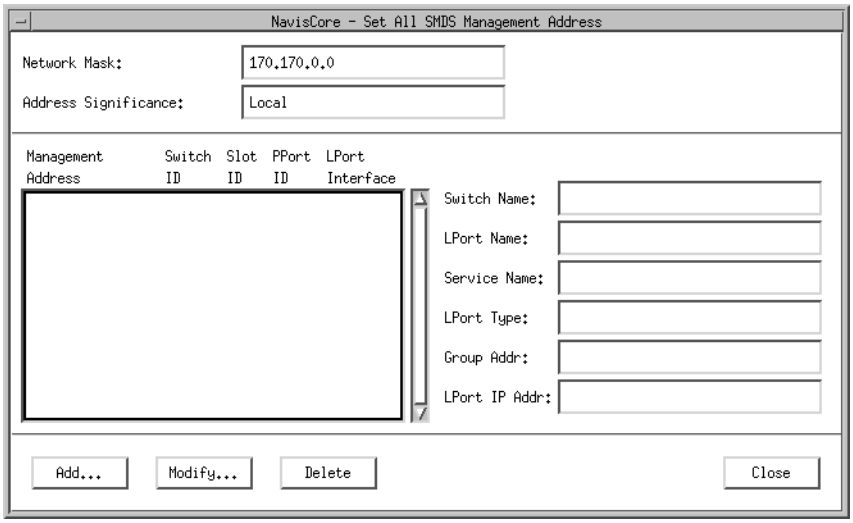


Figure 5-4. Set All SMDS Management Addresses Dialog Box

2. Choose Add to add a new address. The Select End Logical Port dialog box appears (Figure 5-5).

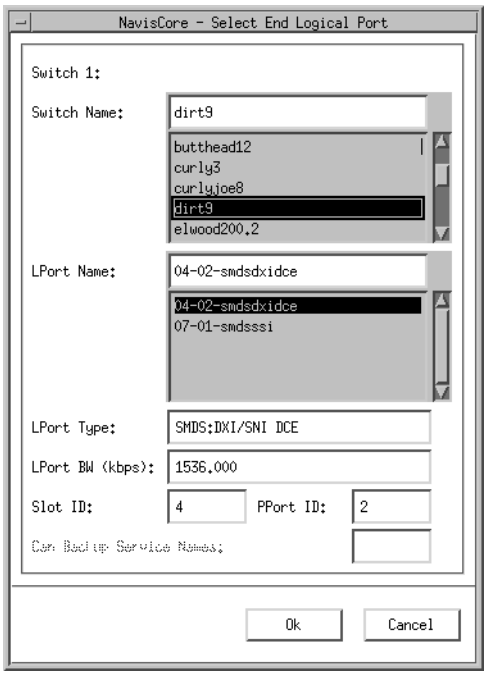


Figure 5-5. Select End Logical Port Dialog Box

3. Complete the fields described in Table 5-1.

Table 5-1. Select End Logical Port Fields

Field	Action/Description
Switch Name	Select the switch (name) that contains the address pool.
LPort Name	Select the logical port (name) for which you are defining the in-band management address.
LPort Type	Displays the logical port type.
LPort Bandwidth	Displays the logical port bandwidth.
Slot ID	Displays the I/O slot (number) in which the card resides.
PPort ID	Displays the number of the port you are configuring.

4. Choose OK. The Add SMDS Management Address dialog box appears (Figure 5-6).

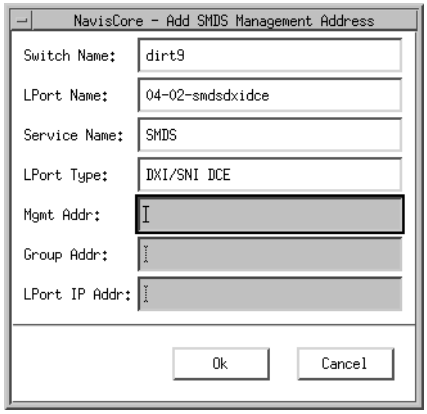


Figure 5-6. Add SMDS Management Address Dialog Box

5. Complete the fields described in Table 5-2.

Table 5-2. Add SMDS Management Address Fields

Field	Action/Description
Switch Name	Displays the name of the selected switch.
LPort Name	Displays the name of the SSI DTE logical port configuration that contains the address pool.
LPort Type	Displays the type of logical port configuration.
Mgmt Address	If the LPort Type is SSI, the management address appears. If the LPort Type is DXI/SNI, enter the individual address to which the logical port subscribes.
Group Address	If applicable, enter the group address to which the logical port subscribes.
LPort IP Address	Enter the IP address of the selected logical port.

6. Choose OK. The Set In-Band Management Addresses dialog box reappears, displaying the in-band management address.

7. Define the NMS path for in-band management as described in the *NavisCore Physical Interface Configuration Guide.*

6

Deleting SMDS Logical Ports

This chapter describes how to delete trunks, SMDS Management Addresses, and SMDS logical ports.

Before You Begin

Before deleting an SMDS logical port, verify:

- No trunks are defined on the logical port.
- No SMDS management address is configured for this logical port.
- This logical port is not defined as the feeder (SMDS SSI-DTE) for an existing SMDS OPTimum trunk logical port. You must disable the OPTimum trunk or first define another feeder before you can delete this logical port.
- This logical port is not the SMDS SSI to which other SMDS DXI logical ports can multiplex. Review the Set All Logical Ports dialog box and make sure the "Multiplex to this SSI" field displays *None*.
- The defined DXI individual address is not a member of a group address. To list members of a group address, see "Adding Individual Address Members to a Group" on page 4-5.
- No individual address is defined for this logical port. To list individual addresses, see "Defining Individual Addresses for DXI/SNI Logical Ports" on page 4-1.
- No SMDS individual/global-address screens are defined for this logical port. To list address screens, see "Configuring Address Screens" on page 5-1.

If any of these components exist and use the logical port you want to delete, you must first delete the components in the following order:

1. Trunks
2. SMDS management addresses
3. Logical port

Deleting Trunks

To delete a trunk:

1. From the Administer menu, select Ascend Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears. If necessary, select each trunk and review each logical-port endpoint.
2. Select the trunk to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting SMDS Management Addresses

1. From the Administer menu, select Ascend Parameters ⇒ Set All Management Addresses. The Set All Management Address dialog box appears.
2. Choose the Management Address you want to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting a Logical Port

If the loopback status field on the Set All Logical Ports dialog box does *not* display *None*, do not attempt to delete this logical port. If the field does not display *None*, loopback testing is in process.

To delete the logical port:

1. Select the switch on which to delete a logical port.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the port. The Set Physical Port Attributes dialog box appears.
4. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears.

5. Select the logical port you want to delete. Verify the Loopback Status field displays None.

Make sure this logical port is not the SSI DTE logical port used as the feeder for an SMDS OPTimum trunk. You must take the OPTimum trunk out of service or first define another feeder address before you can delete this logical port.

6. Choose Delete.
7. Choose Close.

7

Configuring Trunks

This chapter describes how to configure a trunk in an Ascend switch network. The trunk is the communications circuit between two switches. It enables two Ascend switches to pass data to each other and exchange internal control messages.

About Trunks

The trunk oversubscription factor and the OSPF trunk administrative cost parameters enable you to manage trunk traffic. The oversubscription enables you to configure more circuits on a trunk than can be supported at one time. Oversubscription assumes that due to the bursty nature of network traffic, not all circuits on the trunk are operating at the committed information rate (CIR) at the same time. Therefore, trunk bandwidth should remain sufficient.

The trunk administrative cost enables you to assign a cost value for the trunk. When multiple trunks are available, a circuit will use the trunk with the lowest administrative cost.

Trunk Oversubscription Factor

The trunk oversubscription factor percentage enables you to optimize the aggregate committed information rate (CIR) allowed over the trunk. The oversubscription factor represents the “V” value for this trunk. The bandwidth on trunks is reserved at runtime based on the CIR value of the PVCs that traverse the trunk.

The Open Shortest Path First (OSPF) protocol uses the following two formulas to determine the available virtual bandwidth value:

Formula 1

This formula determines the initial value of the available virtual bandwidth:

Initial Value = 0.95 (configured bandwidth) x V(%)

Note: V = trunk oversubscription factor

Formula 2

Available Virtual Bandwidth = Initial Value – (Sum of PVC CIR)

It is important to note that the available virtual bandwidth can become negative in extreme situations. If a number of trunks fail, PVC rerouting may cause the available virtual bandwidth value to become negative. Existing PVCs can be rerouted over a negative virtual bandwidth trunk. However, *new* PVCs cannot traverse trunks that have a negative virtual bandwidth.

If you configure the trunk oversubscription factor at a higher percentage, you increase the available virtual bandwidth (more PVC CIR) over the trunk. An oversubscription value of 200% effectively doubles the available virtual bandwidth. Ascend switches reserve 5% bandwidth for network management, routing updates, and other management traffic.

If all network traffic attempts to use the network resources at the same time (for example, during multiple file-transfer sessions over the same trunk), the overhead will degrade network performance.

OSPF Trunk Administrative Cost

OSPF trunk administrative cost is a function of OSPF that gives you more control over the specific path a virtual circuit will take through the network. Through OSPF, a circuit can choose the shorter hop path (most direct route across network), regardless of the available bandwidth.

OSPF trunk administrative cost only works in networks where all switches are running switch software Release 4.1 or higher. If some switches are running an earlier release, OSPF only selects the path with the greatest amount of available bandwidth. This is not necessarily the most direct route (minimum number of hops) through the network.

When you first define a circuit, the circuit looks for a path that has enough virtual bandwidth available to handle its committed information rate (CIR). If the circuit finds more than one path with the available bandwidth, the circuit chooses the path with the lowest administrative cost. If there is more than one path with the same administrative cost, the circuit chooses the path that has the most available bandwidth.

Circuits are automatically rerouted around a trunk or switch failure. If the circuit cannot find a path with sufficient bandwidth, it chooses the path with the lowest administrative cost, even if this trunk has a negative bandwidth value. (Negative bandwidth indicates that the trunk is oversubscribed.) Circuits use a path with a negative-bandwidth only when a trunk fails.

Configuring Minimum-Hop Paths

If you use the default administrative cost value of 100, OSPF selects minimum-hop paths that meet the circuit's Quality of Services values. You can also use the following guidelines to configure this value:

- To minimize end-to-end delay, configure an administrative cost that is proportional to the propagation delay of the trunk. Set the cost of each trunk to the length of the trunk's physical media (in miles or kilometers).
- Set the administrative cost relative to the speed of the physical port. For example, a single T1 trunk hop may be equal to four HSSI trunk hops. You would set the HSSI trunk's cost to 25 and the T1 cost to 100. Keep in mind that since OSPF routing considers available bandwidth, administrative cost is not necessarily a function of bandwidth.

Link Trunk Protocol

Using Link Trunk Protocol (LTP), switches communicate by exchanging keep-alive (KA) control frames. Switches send KA requests at regular time intervals (one per second). After a switch receives a KA request, it returns a KA reply. A completed transaction consists of a KA request and a KA reply. The request and reply frame formats are identical.

Trunk Delay

Figure 7-1 illustrates the process of keep-alive frames used to measure trunk delay. When Switch A sends a KA request to Switch B, a time stamp is put into the KA request frame. When Switch B receives the KA request, it sends a KA reply to Switch A. Switch A receives the KA reply and calculates the round-trip delay from Switch A to Switch B.

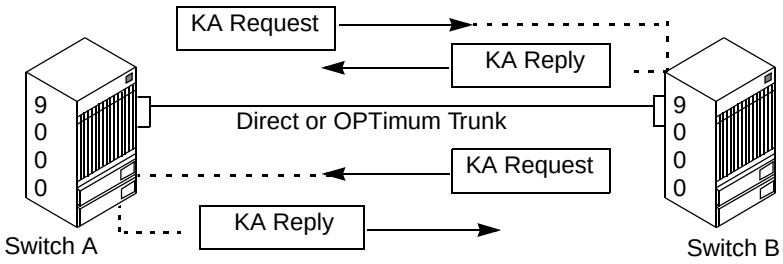


Figure 7-1. Trunk Delay - OSPF Metric and Keep-Alive Messaging

Keep-Alive Threshold

The Keep Alive Threshold field in the Set All Trunks dialog box represents the number of retries that the trunk protocol attempts, before bringing the trunk down. The retry interval is represented in seconds. You can set the keep-alive threshold value between 3 and 255 seconds. The default is 5 seconds.

SMDS CIR

To better utilize network trunking and allow for co-existence of other services (FR/ATM), SMDS circuits must be tagged with a certain amount of bandwidth. The SMDS CIR feature allocates a CIR value to SMDS circuits between switches. This feature enables you to achieve load sharing between parallel trunks. You can now 'load' a particular trunk until it is necessary to switch to another trunk to set up the remainder of the circuits. (OSPF, in conjunction with VC Manager, fulfills this role.) When trunk bandwidth is completely utilized, additional circuits are set up on the parallel or alternate trunks if bandwidth is available. This enables you to utilize *all* trunks in the network. To configure SMDS CIR, see page 7-6.

Unlike Frame Relay, SMDS traffic outside the configured CIR is not marked as green, amber, or red. (SMDS traffic does not go through the Rate Enforcement logic.) Excessive traffic results in over-usage of the trunks.

Trunk Backup

The B-STDX switch supports a trunk backup option. Trunk backup enables you to set up one or more backup trunks to replace a primary trunk. If a switch trunk line fails or requires maintenance, you can reroute PVCs from the primary trunk to the backup trunk. You can define primary and backup trunks on any I/O module.

You define a backup trunk in the Add Trunk dialog box (see Figure 7-5 on page 7-13). A backup trunk can have a total bandwidth that is less than that of the primary trunk. To avoid congestion, you can configure multiple backup trunks to back up a single primary trunk. On the B-STDX, you can define up to eight backup trunks for a single primary trunk.

Once you configure the primary and backup trunk(s), you can configure the primary trunk for automatic backup upon failure. If a trunk line requires maintenance, you can manually initiate and terminate a trunk backup.

Configuring SMDS CIR

To configure CIR, perform the following steps:

1. Select a switch icon from the network map.
2. From the Administer menu, select Ascend parameters ⇒ Set Parameters. The switch back panel appears.
3. Select Actions ⇒ Set Switch Attributes.
4. Choose Go. The Set Switch Attributes dialog box appears.

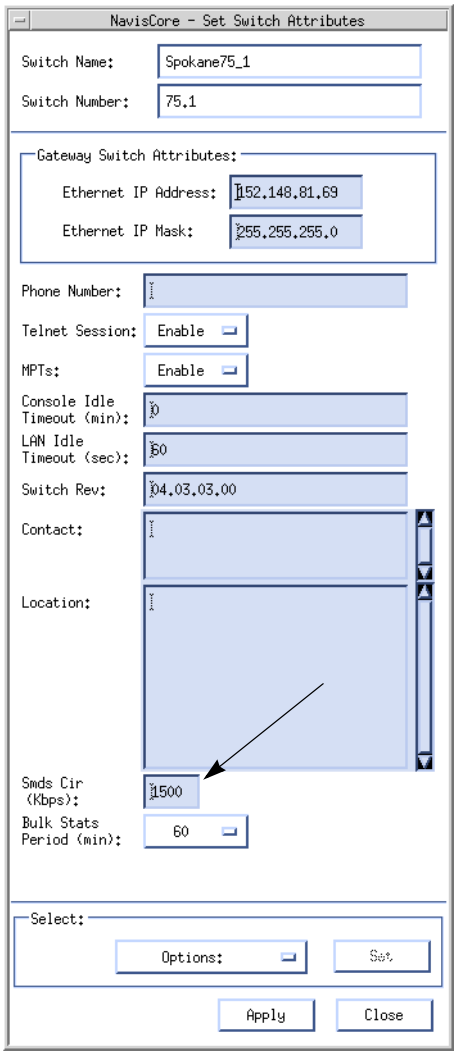


Figure 7-2. Set Switch Attributes Dialog Box

5. In the Smds Cir (Kbps) field, enter the CIR value to apply to this node. The default is zero (no deduction of trunk bandwidth).
6. Choose Apply to send the SNMP SET to the switch.

7. Choose Close to exit the dialog box.
8. Warmboot the CP card. From this point, *all* SMDS circuits will assume this CIR value for circuit setup.

The CIR value is *not* a per-circuit based entity. Each node in the network could potentially have different CIR values for the circuit setup. The CIR value depends largely on the *estimated* traffic levels to and from the switch.

Changing the SMDS CIR Value

The SMDS CIR configuration is applied to the CP card PRAM and is used for all subsequent SMDS circuits. If you want to change the value, perform the steps on page 7-6. After you change the CIR value you must warm boot the CP card in order for the new value to take effect and rebuild the SMDS circuits originating/terminating at that node.

Before You Begin

Before you define the trunk connections, verify that you have configured the trunk logical port(s) (see Chapter 3).

When you define a trunk, you must perform these steps:

Step 1. Define a trunk configuration between the two switches. See "Adding a Trunk" on page 7-12.

Step 2. Create the map line connection that corresponds to the trunk configuration. See "Creating a Trunk-Line Connection" on page 7-18.

Accessing Trunk Functions

The Set All Trunks function specifies the two endpoints for an Ascend-to-Ascend switch trunk. When you configure a trunk, you select endpoints that use the same type of logical port (such as Direct Line Trunk) and the same bandwidth.

To access the trunk functions, from the Administer menu,
select Ascend Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears (Figure 7-3.)

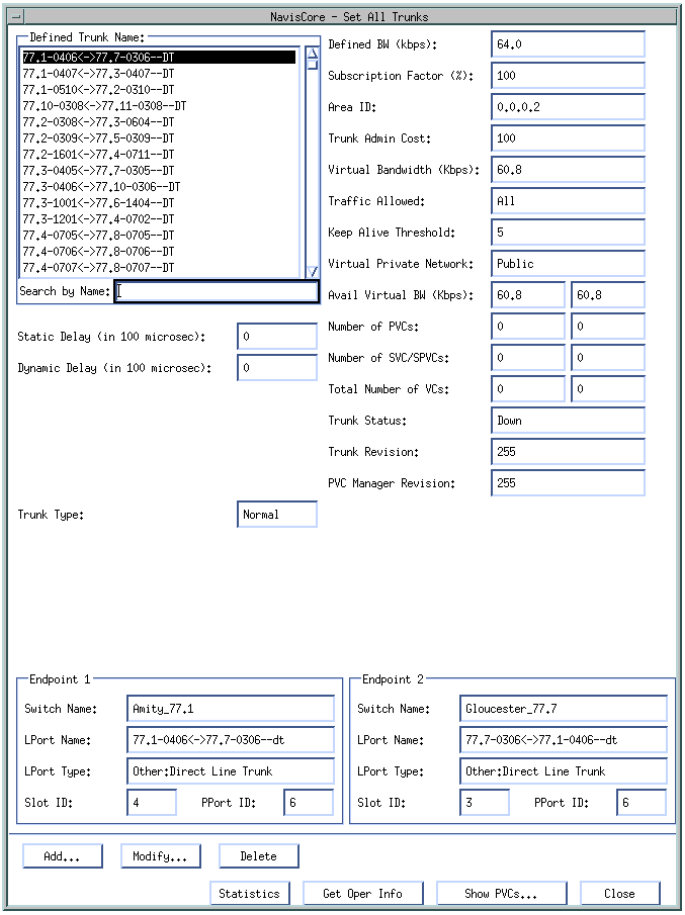


Figure 7-3. Set All Trunks Dialog Box

Set All Trunks Dialog Box

The Set All Trunks dialog box (shown in Figure 7-3) displays information about the trunk you select from the Defined Trunk Names list. It also provides several buttons that enable you to access additional trunk functions.

Table 7-1 describes the Set All Trunks dialog box fields and buttons.

Table 7-1. Set All Trunks Fields and Buttons

Field/Button	Description
Defined Trunk Name	Displays the names of the configured trunks.
Defined Bandwidth (Kbps)	Displays the amount of bandwidth, in Kbps, for the selected trunk.
Subscription Factor (%)	Displays the percentage used to calculate the available virtual bandwidth for the selected trunk.
Area ID	Displays the area ID (x.x.x.x) for the area in which you want to locate this OSPF interface. The range of available values is from 0.0.0.0 to 255.255.255.255. Area 0.0.0.0 is the network backbone area. Area 0.0.0.1 is Area 1. Areas are collections of networks, hosts, and routers used for IP routing. The area ID identifies the area. If a trunk is in Area 1 and the OSPF Backwards Compatibility option (which is set through IP services) is set to Yes, external routes are not advertised across that link. ***Note**: Area 1is reserved for Ascend switches. For a detailed description of OSPF areas, and how to use IP Services to configure multiple OSPF areas, see the NavisCore IP Navigator Configuration Guide.*
Trunk Admin Cost	Displays the cost of using this trunk for a virtual circuit when a virtual circuit is dynamically created on the switch.
Virtual Bandwidth (Kbps)	Displays the amount of virtual bandwidth in Kbps. The value *.95* is used because *.05%* of the bandwidth is reserved for network management, routing updates, and other management traffic.
Traffic Allowed	Displays the type of management traffic allowed on this trunk.

Table 7-1. Set All Trunks Fields and Buttons (Continued)

Field/Button	Description
Keep Alive Threshold	Displays the number of seconds that the trunk protocol will exchange keep alive (KA) control frames without getting a response from the remote node. ***Note**: Service is disrupted if you change this value after the trunk is online.*
Avail Virtual BW (Kbps)	Displays the amount of bandwidth, in Kbps, available for circuit configuration and allotment on the selected trunk.
Number of PVCs	Displays the total number of PVCs traversing the trunk logical port.
Number of SVC/SPVCs	Displays the total number of SVCs and SPVCs traversing the trunk logical port endpoint.
Number of VCs	Displays the number of virtual channels.
Trunk Status	Displays the current status of the selected trunk.
Trunk Revision	Displays the trunk revision.
PVC Manager Revision	Displays the PVC manager software revision.
Trunk Type	Displays the trunk type. *Normal* – Indicates a common trunk. *Primary* – Indicates that the trunk has a backup for fault tolerance. *Backup* – Indicates that it is the backup trunk (when failure occurs on the primary trunk).
Add/Modify/Delete	Enables you to add, modify, or delete any current trunk configurations.
Statistics	Displays summary statistics for the selected trunk configuration. See the *NavisCore Diagnostic and Troubleshooting Guide* for more information.
Get Oper Info	Displays a brief status for the selected trunk connection and a status message appears in the Oper Status field.
Show PVCs	Displays a dialog box that contains a list of the PVCs that traverse the selected trunk. This dialog box also provides logical port descriptions for each PVC endpoint.

Adding a Trunk

To add a trunk:

1. Access the Set All Trunks dialog box (Figure 7-3), as described in "Accessing Trunk Functions" on page 7-8.
2. Choose Add. The Select Logical Ports dialog box appears (Figure 7-4).

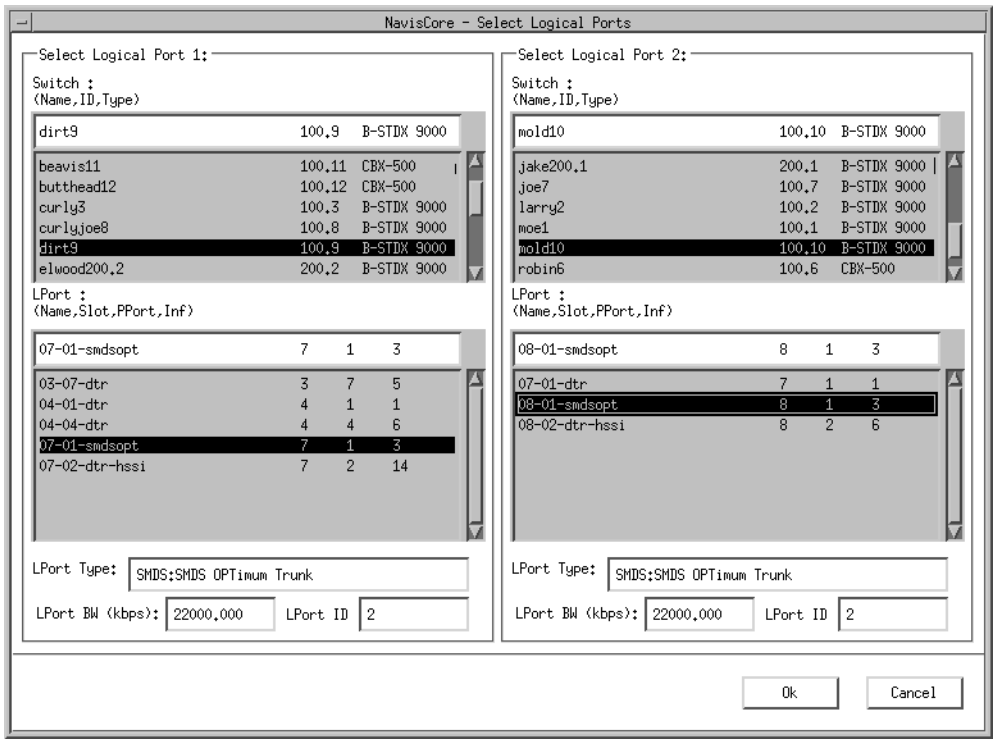


Figure 7-4. Select Logical Ports Dialog Box

3. Complete the fields described in Table 7-2.

Table 7-2. Select Logical Ports Fields

Field	Action/Description
Switch (Name, ID, Type)	Select a switch for each endpoint. The dialog box displays the parameters for the selected switch.
LPort (Name, Slot, PPort, Inf)	Select the SMDS OPTimum Trunk logical port type for each endpoint. This field also displays the ifnum, physical port number, I/O slot (number) in which the module resides. ***Note**: Check the LPort Bandwidth field for each endpoint to make sure the bandwidth is identical.*

Table 7-2. Select Logical Ports Fields (Continued)

Field	Action/Description
LPort Type	Displays the configured logical port type.
LPort BW (Kbps)	Displays the bandwidth configured for the logical port. This must be the same for both endpoints.
LPort ID	Displays the logical port number.

4. Choose OK. The Add Trunk dialog box appears, displaying the parameters for both switches (endpoints) in the trunk configuration.

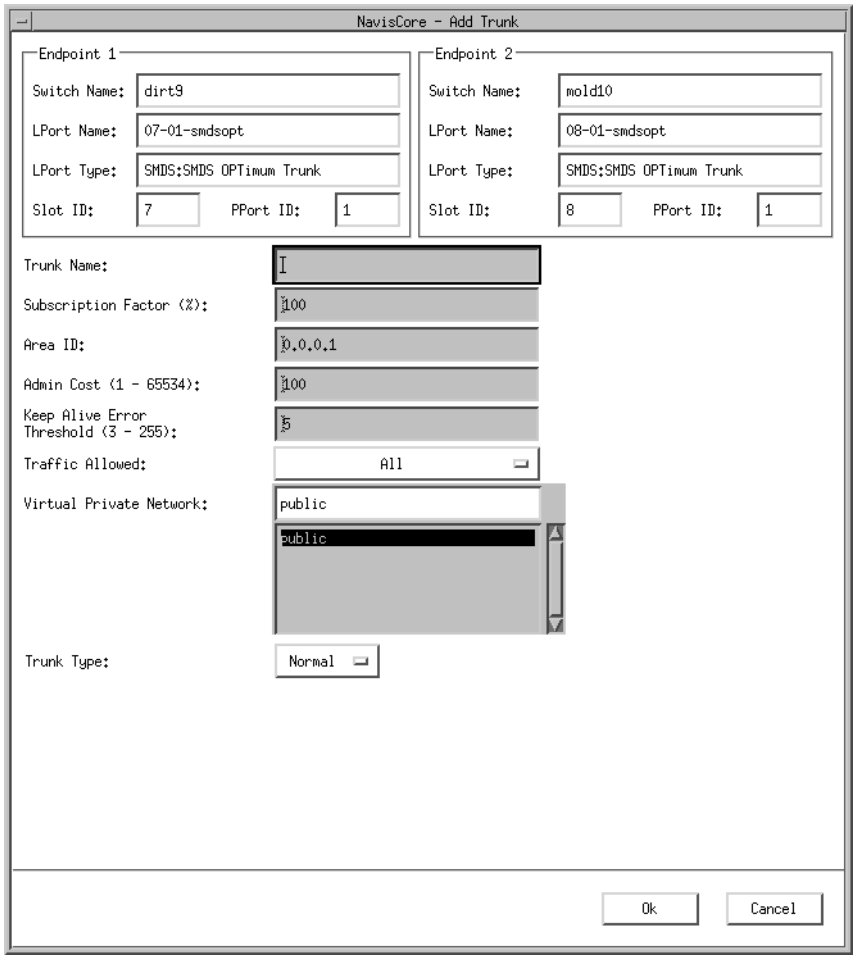


Figure 7-5. Add Trunk Dialog Box

5. Complete the fields described in Table 7-3.

Table 7-3. Add Trunk Fields

Field	Action/Description
Trunk Name	Enter a unique, alphanumeric name for the trunk. You use this same name when you create the trunk connection (see page 7-18).
Subscription Factor (%)	Enter the percentage for bandwidth. The trunk oversubscription factor percentage enables you to optimize the aggregate CIR you can configure on the trunk, by allowing you to oversubscribe the trunk. The oversubscription factor represents the V value for this trunk. The bandwidth on a trunk is reserved at runtime, based on the configured CIR value of the PVCs that traverse that trunk. For example, you can set this factor to 200% to produce a virtual bandwidth that is two times greater than the defined bandwidth. For a detailed explanation of this parameter, see "Trunk Oversubscription Factor" on page 7-1.
Area ID	Enter the area ID (x.x.x.x) for the area in which you want to locate this OSPF interface. Area 0.0.0.0 is the network backbone area. Areas are collections of networks, hosts, and routers used for IP routing. The area ID identifies the area.
Admin Cost (1-65534)	Assign an admin cost value of 1 to 65534. The lower the admin cost of the path, the more likely OSPF will select it for circuit traffic. *The default admin cost value is 100.* For a detailed explanation of this parameter, see "OSPF Trunk Administrative Cost" on page 7-2. ***Note:*** *When you increase or decrease the administrative cost of a trunk, the reroute tuning parameters control the rate at which the switch adds or removes circuits from the trunk. You cannot use trunk admin cost to force a trunk down.*

Table 7-3. Add Trunk Fields (Continued)

Field	Action/Description
Keep Alive Error Threshold (%)	Set the keep-alive threshold for a value between 3 and 255 seconds. *The default is 5 seconds.* For a detailed explanation of this parameter, see "Keep-Alive Threshold" on page 7-4. ***Note**: If you are running different switch code versions in your network, for example Version 4.1 and Version 4.2, you must accept the default value of five (5) seconds.* *Service is disrupted if you change this value after the trunk is online.*
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – The trunk can carry network management traffic, user traffic, and OSPF address distribution. *Mgt Only* – The trunk can carry *only* network management traffic, such as SNMP communication between a switch and the NMS. *Mgt & User* – The trunk can carry network management traffic and user traffic. ***Note**: To calculate the most efficient route for network management traffic, OSPF uses trunk admin cost. OSPF ignores trunk bandwidth when it selects the best path or a route for management traffic. Management traffic can use a negative bandwidth trunk.*
Trunk Type	Select one of the following: *Normal* — is a common trunk. *Primary* — indicates that the trunk has a backup for fault tolerance. See Step 6. *Backup* — indicates that it is a backup trunk (when failure occurs on the primary trunk). See "Using the Automatic Trunk Backup Feature" on page 7-17 to configure a backup trunk. ***Note**: This parameter is not supported on trunks between CBX and B-STDX switches.*

6. (*Optional*) If you selected *Primary* as the Trunk Type, the system displays the fields shown in Figure 7-6.

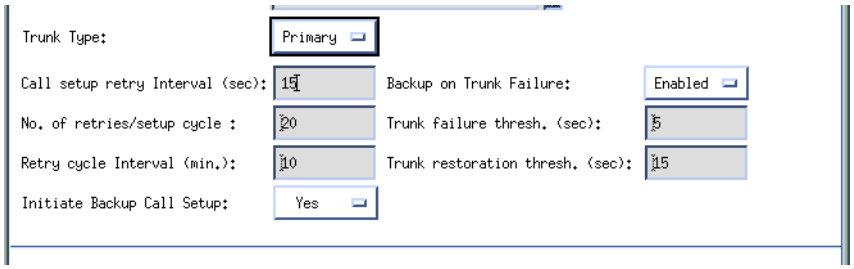


Figure 7-6. Add Trunk Dialog Box (Primary Trunk)

7. Complete the fields described in Table 7-4, or accept the default parameters.

Table 7-4. Add Primary Trunk Fields

Field	Action/Description
Call setup retry Interval (sec)	Specify the number of seconds between initiating a call. The default is 15 seconds.
No. of retries/setup cycle	Specify the number of retries per interval. The default is 20 retries.
Retry cycle Interval (min)	Specify a retry interval in minutes. The default is 10 minutes.
Initiate Backup Call Setup	Choose Yes (*default*) to initiate a backup call.
Backup on Trunk Failure	Enable (default) or disable trunk backup. If you enable trunk backup, the system automatically uses the backup trunk if the primary trunk fails. If you choose Disabled, the automatic trunk backup option is not used.
Trunk Failure thresh. (sec)	Specify the number of seconds (the default is 5). If you enabled trunk backup, this field specifies the number of seconds the system will wait before switching over to the backup trunk.
Trunk Restoration thresh. (sec)	Specify the number of seconds that the system will wait for the primary trunk to become functional before resuming use of the primary trunk. The default is 15 seconds. If the primary trunk is out of service and the backup trunk is in use, the system will not resume use of the primary trunk until it has been restored for the period of time you specify. The purpose of this field is to prevent a switch-over to a primary trunk that has only been temporarily restored.

8. When you complete the add trunk dialog box fields, choose OK.

9. Choose Close to return to the network map.

   The next step is to create a trunk-line connection. Proceed to "Creating a Trunk-Line Connection" on page 7-18.

Using the Automatic Trunk Backup Feature

To use the automatic trunk backup feature:

1. Access the Add trunk dialog box (see Figure 7-5 on page 7-13).
2. Define a trunk that has a Trunk Type of *Primary.*
3. Specify all of the primary trunk field values shown in Table 7-4 on page 7-16. Specify a value of *Yes* in the Initiate Backup Call Setup field on the Add Trunk dialog box.
4. Specify a value of *Enabled* in the Backup on Trunk Failure field on the Add Trunk dialog box.
5. Define from one to eight trunks that have a Trunk Type of *Backup*.
6. For each trunk with a Trunk Type of Backup, in the *Primary Trunk of the backup* field, select the name of the primary trunk specified in Step 2.

Process for Switching Over to a Backup Trunk

In the event of trunk failure, the system uses the following process to automatically switch over to a defined backup trunk if you have used the steps in the previous procedure to enable Automatic Trunk Backup.

1. The system switches over to the backup trunk after the trunk is out of service for the amount of time specified for the primary trunk in the Trunk Failure Threshold field (see Table 7-4 on page 7-16).
2. The system resumes use of the primary trunk after it is in service for the period of time specified in the Trunk Restoration Threshold field (see Table 7-4 on page 7-16).

Defining the Manual Trunk Backup Feature

You can override the values for automatic trunk backup by using the manual trunk backup feature. To do this, use the Start Trunk Backup and Stop Trunk Backup options on the Modify Trunk dialog box.

Creating a Trunk-Line Connection

You must define the trunk configuration between two switches before you create the trunk-line connection on the network map (see "Adding a Trunk" on page 7-12). The Add Connection function enables you to draw a line to connect the two switches on the network map.

To add a trunk-line connection:

1. From the Edit menu, select Add Connection. The Add Connection dialog box appears (Figure 7-7).

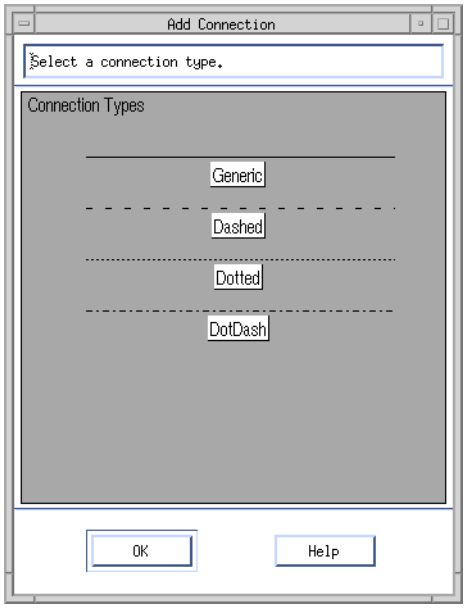


Figure 7-7. Add Connection Dialog Box

2. Select a Connection Type from the palette.
3. To create a trunk-line connection between the two switches on the network map, select the first switch object (source symbol) and then the second switch object (destination symbol).
4. The Add Object dialog box appears (Figure 7-8).

Figure 7-8. Add Object Dialog Box

5. Complete the fields described in Table 7-5.

Table 7-5. Add Object Fields

Field	Action/Description
Symbol Type	Displays the type of connection you are adding to the map.
Label	Enter the trunk name.
Display Label	Select Yes to have the label name appear beneath the trunk line object on the network map. Select No if you do not want the label name displayed.
Behavior	Select Explode to create the basic NavisCore network configuration. See the *HP OpenView User's Guide* for more information about the Execute function.
Object Attributes	Select NavisCore. Then choose Set Object Attributes. The Add Object – Set Attributes dialog box appears (Figure 7-9).

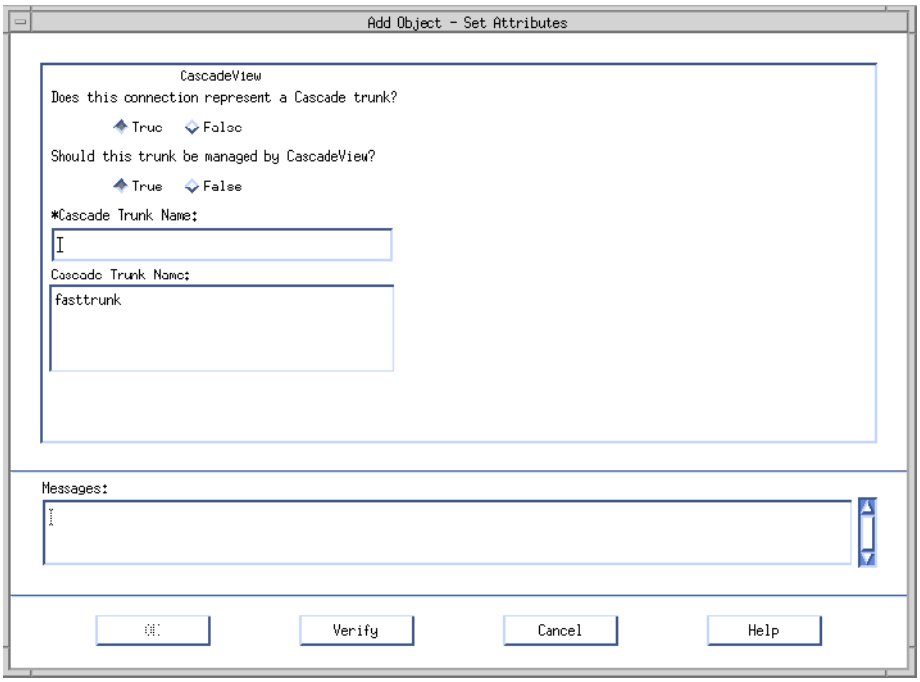


Figure 7-9. Add Object - Set Attributes Dialog Box

6. Complete the required dialog box fields described in Table 7-6.

Table 7-6. Add Object - Set Attributes Fields

Field	Action/Description
Does this connection represent a Ascend Trunk?	Select True.
Should this trunk be managed by NavisCore?	Select True.
Ascend Trunk Name	Enter the trunk name. This should be the same name you entered for the label in the Add Object dialog box on page 7-19.

7. Choose Verify to confirm your selections.

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

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

Displaying Multiple Trunks Between Switches

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

To display all trunk connections between two switches:

1. Double-click the left mouse button on the solid line between the switches. A trunk submap window appears similar to Figure 7-10.

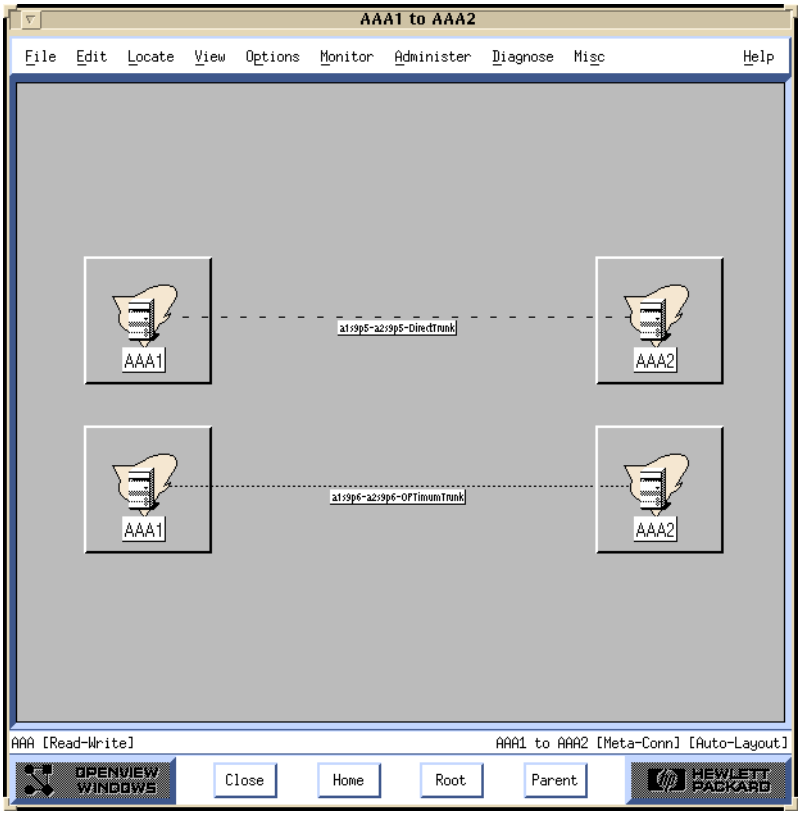


Figure 7-10. Displaying Multiple Trunks-Trunk Submap Dialog Box

2. Choose Close to return to the network map.

Trunk Coloring

All associated trunks are polled for status according to the trunk poll timer. The trunk lines on the network map change color. These colors indicate trunk status based on the polled status and the traps received by the Ascend Event Log. Table 7-7 describes the color scheme that identifies the status of a trunk connection.

Table 7-7. Trunk Color Status Indicators

Color	Status
Black	Either the line connection has not been defined as a trunk or the environment variable $XUSERFILESEARCHPATH does not point to `/opt/NavisCore/app-defaults. 1`
Red	Trunk is down.
Blue	Trunk status is unknown or unmanaged.
Yellow	More than half the trunk connections are down.
Green	Trunk connection is up.
Orange	Only one trunk connection, out of many connections, is up.
Cyan	More than half the trunk connections are up.

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

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

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

If you define more than one trunk connection between the same two switches, HP OpenView combines the status to display an orange, yellow, or cyan trunk-line. To display the individual connections, double-click on the trunk line and see Table 7-7 to interpret trunk status.

Glossary

A

absolute congestion

A congested condition in the network that occurs when the queue length reaches a third threshold (64 buffers full), and there is no more room on the queue for any packets, regardless of the type of packet.

active hub

A device that amplifies LAN transmission signals in a network, enabling signals to be sent over a much greater distance than is possible with a passive hub. Compare with *passive hub*.

address

The logical location or identifier of a network node, terminal, pc, peripheral device, or location in memory where information is stored. See also *NavisCore*.

address mask

A bit combination used to describe which portion of an SMDS address refers to the network (or subnet) and which part refers to the host. Sometimes referred to as mask. See also *subnet mask*.

administration tool

A system administration utility, such as Solaris, that allows system administrators to maintain and monitor system database files, printers, user accounts, and hosts through a graphical user interface (GUI).

AIS

See *Alarm Indication Signal*.

alarm

Message notifying an operator or administrator of a network problem.

Alarm Indication Signal

An error or alarm signal transmitted in lieu of the normal signal to maintain transmission continuity to the receiving node indicating that there is a transmission fault located either at the sending node or upstream of the sending node.

Alterable Mark Inversion

A signaling format used in T1 lines that provides for the “one” pulses to have an alternating priority. Thus, if the nth-one bit is represented by a positive pulse, the nth T1 line would be a negative pulse.

alternate path

An optional automatic feature of OSPF (Open Shortest Path First) that reroutes the PVC should a trunk fail within a manually defined path.

American National Standards Institute

A private, non-governmental, non-profit organization, which develops US standards required for commerce.

American Standard Code for Information Interchange

A code representing characters in binary form.

AMI

See *Alterable Mark Inversion*.

analog

A method that transmits electrical signals at varying amplitudes. Analog often refers to transmission methods developed to transmit voice signals rather than high speed digital signals. Compare with *digital*.

ANSI

See *American National Standards Institute*.

area id

See *area number*.

area number

One of two portions of the SMDS address, which can start at any digit and the length can be up to eight digits (4 bytes long for BCD encoding).

ASCII

See *American Standard Code for Information Interchange*.

ASCII text file

A file that contains only text characters from the ASCII character set. An ASCII file can include letters, numbers, and punctuation symbols, but does not contain any hidden text-formatting codes.

AT command set

A set of standard instructions used to activate features on a modem. Originally developed by Hayes Microcomputer Products, most modem manufacturers now use the AT command set.

attenuation

The decrease in power of a signal over distance, measured in decibels (dB).

auto-ranging

The ability for a power supply to detect the correct voltage that is being received from the power source.

B

B8ZS

See *Bipolar with 8 Zero Substitution*.

backbone

The part of a network that carries the bulk of the network traffic, e.g. over Ethernet cabling, fiber-optic cabling.

background diagnostics

Programs that run continuously in the background of the NMS to provide current operating status for all active switches. These programs do not interfere with switch operations.

balun

A small device used to connect a balanced line (such as a twisted-pair cable) to an unbalanced line (such as a coaxial cable).

bandwidth

The transmission capacity of a computer or a communications channel.

bandwidth-on-demand

A WAN feature that enables users to dial up additional bandwidth as their applications demand.

baud rate

The number of bits per second (bps) on a serial link.

Bc

See *Committed Burst Size*.

Be

See *Excess Burst*.

best-effort packets

Packets delivered to the best of the network's ability, after the requirements for delivering the guaranteed packets are met. See also *guaranteed packets*.

Bipolar with 8 Zero Substitution

A T1 encoding scheme where eight consecutive zeros are replaced with the sequence 000-+0+-if the preceding pulse was+, and with the sequence 000-+0+-if the preceding value was-, where+ represents a positive pulse, -represents a negative pulse, and 0 represents no pulse.

bit

A binary unit of measurement, which may be either a one or a zero.

bits per second

The number of bits transmitted every second during a data transfer.

blue alarm

An alarm signal, both on the NMS and switch, indicating that all one pulses are being received.

BNC connector

A small connector with a half-turn locking shell for coaxial cable. Normally used with thin Ethernet cabling.

Boot Programmable Read-Only Memory

A chip mounted on a printed circuit board used to provide executable boot instructions to a computer device.

Boot PROM

See *Boot Programmable Read-Only Memory*.

bps

See *bits per second*.

broadband network

A type of network that allows for the transmitting of large amounts of information, including voice, data, and video over long distances using the same cable.

broadcast

A message that is sent to all users currently logged into the network.

burst mode

A method of data transmission in which information is collected and then sent in a single high-speed transmission, rather than one character at a time.

byte

A series of consecutive binary digits that are operated upon as a unit (for example, an eight-bit byte).

C

Carrier Sense Multiple Access Collision Detect

Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all transmitting devices. This collision subsequently delays retransmissions from those devices for some random length of time. CMSA/CD access is used by Ethernet and IEEE 802.3.

channel

Any connecting path that carries information from a sending device to a receiving device. May refer to a physical medium (e.g., coaxial cable) or a specific frequency within a larger channel.

channel bank

Equipment that converts multiple voice signals to time division multiplexed (TDM) signals for transmission over a T1 or E1 line.

Channel Service Unit

A device that functions as a certified safe electrical circuit, acting as a buffer between the customer's equipment and a public carrier's WAN.

circuit

A communications channel or path between two devices.

circuit switching

A temporary communications connection that is established as needed between a sending node and a receiving node.

Clear To Send

A hardware signal defined by the RS-232-C standard, indicating that the transmission can proceed.

client

A device that makes use of the services provided by a server.

coldboot

A reboot enabling the user to restart the switch as if it were powered off, then on. Compare with *warmboot*.

collision detection

See *Carrier Sense Multiple Access Collision Detect*.

Committed Burst Size

The maximum amount of data, in bits, that the network agrees to transfer under normal conditions, during a time interval Tc. Committed Burst Size is defined for each PVC.

Committed Information Rate

The rate at which the network agrees to transfer information under normal conditions. The rate is averaged over a minimum increment of time, Tc. See also *bandwidth*.

Committed Rate Measurement Interval

The time interval during which the user is allowed to send only Bc committed amount of data and Be excess amount of data. In general, the duration of Tc is proportional to the burstiness of the traffic. Tc is computed from CIR and Bc as Tc=Bc/CIR.

communications protocol

A standard way of communicating between computers, or computers and terminals; also a hardware interface standard, such as RS-232C for communication between DTE and DCE devices.

community names

The name given to an SNMP community for purposes of identification. A member has associated access rights: read-only or read/write. The Ascend switch has the following default community names: public (read-only) and cascade (read/write).

concentrator

A repeater or hub that joins communications channels from several different network nodes. Concentrator devices provide bridging, routing, and other management functions.

congestion

The point at which devices in the network are operating at their highest utilization. Congestion is handled by employing a congestion avoidance mechanism. See also *mild congestion*, *absolute congestion*, and *severe congestion*.

connectivity

The degree to which any given computer or application can cooperate with other network components in a shared-resource network environment.

console commands

SNMP protocol supports three important commands: Get, Set, and Next. Get enables an NMS to query one or more objects or variables in an agent MIB. Set enables an NMS to modify a value of a MIB object or variable and may be used to boot or reboot devices. Next enables an NMS to query agent MIB tables and lists.

Control Processor

A module that makes up the hardware architecture of a B-STDX 9000 switch. A CP provides network and system management and routing functions in support of the real-time switching functions provided by the multiple, IO Processor modules (IOPs).

CP

See *Control Processor*.

CSMA/CD

See *Carrier Sense Multiple Access Collision Detect*.

CSU

See *Channel Service Unit.*

CTS

See *Clear To Send.*

D

D4-format

In T1 transmission, 24 channels per T1 line, where channels are assigned sequentially.

daemon

A special type of program that, once activated, starts itself and carries out a specific task without user intervention. Daemons typically handle tasks that run repeatedly, such as printing, mail, and communications.

Data Bus (DB) connector

A cable connector used to connect devices to parallel or serial ports. The number following DB indicates the number of pins in the connector (e.g., DB-25 connectors have 25 pins).

Data Carrier Detect

A hardware signal, defined by the RS-232-C standard, that indicates the device is on-line and ready for transmission.

Data Communications Equipment

Any device that connects a computer or terminal to a communications channel or public network.

Data Exchange Interface

A specification, described in RFC 1483, that defines how a network device can be used to convert data for interworking between different network services (i.e., Frame Relay to ATM).

data-link layer

The second of seven layers of the ISO/OSI model for computer-to-computer communications. This layer ensures data flow and timing from one node to another by synchronizing blocks of data and controlling the flow of data.

data packet

One unit of information transmitted as a discrete entity from one network node to another. In packet-switched networks, a data packet is a transmission unit of a fixed maximum length that contains a header, a set of data, and error control information.

Data Service Unit

A device that connects DTE to digital communications lines. A DSU formats the data for transmission on the public carrier WAN, and ensures that the carrier's requirements for data formats are met.

Data Set Ready

A hardware signal, defined by the RS-232-C standard, that indicates the device is ready to operate.

Data Terminal Equipment

Any device, such as a terminal or computer, that is connected to a communications device, channel, or public network.

Data Terminal Ready

A hardware signal, defined by the RS-232 standard, exchanged between devices. For example, an RS-232-C circuit that alerts a DCE device that the DTE device is ready to send and receive data.

data transfer rate

The speed at which data is transferred, usually measured in megabits per second (Mbps) or megabytes (MB) per second.

datagram

A message unit that contains source- and destination-address information, as well as the data itself, which is routed through a packet-switched network.

DCD

See *Data Carrier Detect*.

DCE

See *Data Communications Equipment*.

dedicated line

A communications circuit used for one specific purpose, and not used by or shared between other users.

dedicated server

A computer on the network that functions only as a server performing specific network tasks.

define path

A function that allows a manual path to be defined for the PVC, thereby bypassing the OSPF (Open Shortest Path First) algorithm to make PVC routing decisions.

delay

In communications, a pause in activity, representing the time that a message must wait for transmission-related resources to become available.

destination address

The address portion of a packet or datagram that identifies the destination node.

digital

A method of storing, processing, and transmitting information through use of distinct electronic or optical pulses that represent the binary digits (bits) 0 and 1. Digital transmission/switching technologies employ a sequence of discrete, individually distinct pulses to represent information, as opposed to the continuously variable signal of analog technologies. Compare with *analog*.

Digital Signal (Digital Service)

A classification of digital circuits. The DS defines the level of common carrier digital transmission service. DS-0 = 64 Kbps (Fractional T1), DS-1 = 1.544 Mbps (T1), DS-2 = 6.312 Mbps (T2), DS-3 = 44.736 Mbps (T3), and DS-4 =274-176 Mbps (T4).

DIP switch

See *Dual In-line Position switch*.

direct Ethernet

A connection method used by the NMS to the network. The NMS communicates directly to the gateway switch through the Ethernet port on the NMS to the Ethernet port on the switch.

disk partitions

A portion of a disk that is configured during software installations on a system or workstation.

domain

A network community of users sharing the same database information.

DS

See *Digital Signal (Digital Service)*.

DS0

A 64-Kbps channel used in T1 transmission. There are 24 DS0 channels in a T1 line.

DS1

A standard digital transmission facility, operating at 1.544 Mbps.

DSR

See *Data Set Ready*.

DSU

See *Data Service Unit*.

DSX-1

A T1 specification that indicates the physical and electrical characteristics of the standard T1 cross-connection.

DTE

See *Data Terminal Equipment*.

DTR

See *Data Terminal Ready*.

Dual In-line Position switch

A small switch used to select the operating mode of a device.

duplex channel

The ability to transmit and receive on the same channel at the same time. Also known as full duplex.

DXI

See *Data Exchange Interface*.

dynamic routing

A routing technique that allows a message's route to change "en route" through the network.

E

E1

The European counterpart to the North American T1 transmission speed. Adopted by the Conference of European Posts and Telecommunications Administrations, the E1 standard carries data at the rate of 2.048 Mbps.

EDAC

See *error detection and correction*.

encapsulation

The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before being transmitted. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

environment variable

A system- or user-defined variable that provides information to the UNIX shell about the operating environment.

error detection and correction

A feature used to determine whether transmission errors have occurred, and if so, to correct those errors. See also *Carrier Sense Multiple Access Collision Detect*.

error rate

In communications, the ratio between the number of bits received incorrectly and the total number of bits in the transmission.

Ethernet

A popular LAN protocol and cabling scheme with a transfer rate of 10 Mbps.

Ethernet address

A 48-bit number physical address. Each Ethernet address is unique to a specific network card or PC on a LAN, which forms the basis of a network-addressing scheme. Compare with *Internet Protocol address*.

Ethernet packet

A variable-length unit of data transmitted on an Ethernet LAN.

Excess Burst

The maximum allowed amount of uncommitted data (in bits) in excess of Bc that the network attempts to deliver during time interval Tc. In general, this data (Be) is delivered with a lower probability than Bc.

external testing

A loopback test that tests the ability of the port to send and receive data. This test requires an external loopback connector installed on the physical port.

F

fail count

A statistic that displays the number of tests that produced an error condition.

failed LED

A red status indicator that indicates a fatal system fault (such as a system crash).

FDDI

See *Fiber Distributed Data Interface*.

FDM

See *Frequency-Division Multiplexing*.

Fiber Distributed Data Interface

An ANSI standard for fiber-optic links with a data transmission rate up to 100 Mbps.

File Transfer Protocol

A method of transferring information from one computer to another, either over a modem and telephone line, or over a network. FTP is a TCP/IP application utility.

foreground diagnostics

A set of tests used to check for non-fatal errors indicated by background diagnostics or statistics. Foreground tests may also run at start up to test new equipment functions.

fractional T1

One channel of a T1 circuit. T1 circuits consist of 24, 64-Kbps channels. Customers can lease as many of these channels as needed; they are not required to lease all 24 channels in one circuit.

Frequency-Division Multiplexing

A method of sharing a transmission channel by dividing the total bandwidth of the circuit into several smaller channels. This is accomplished by allocating specific frequency ranges to each channel. All signals are carried simultaneously. Compare with *Time Division Multiplexing*.

FTP

See *File Transfer Protocol*.

full-duplex (FDX)

See *duplex channel*.

G

gateway

A shared connection between a LAN and a larger system (such as a mainframe computer), or a large packet-switched network whose communication protocols differ.

good LED

A green status indicator on an Ascend switch that indicates normal system status and operation during the system-boot process.

graceful discard

When enabled, this function turns red frames into best-effort frames. When disabled, this function discards frames.

green frames

Ascend's own class of packet frames used to identify packets as they travel through the network. Green frames are never discarded by the network except under extreme circumstances, such as node or link failure.

group addressing

The ability to send a single datagram/packet to multiple locations.

guaranteed packets

Data delivered according to some time constraint with high reliability.

H

Hayes-compatible modem

Any modem that recognizes commands in the industry-standard AT command set.

HDLC

See *High-level Data Link Control*.

header

The initial part of a data block, packet, or frame, which provides basic information about the handling of the rest of the block, packet or frame.

heartbeat polling process

An exchange of sequence numbers between the network and a user device to ensure that both are operational and communicating.

HELLO

A routing protocol used principally by NSFnet nodes (nodes in the National Science Foundation Network). Hello allows trusting packet switches to discover minimal delay routes.

Hello protocol

Protocol used by OSPF systems for establishing and maintaining neighbor relationships.

heterogeneous network

A network that consists of workstations, servers, network interface cards, operating systems, and applications from many different vendors, all operating together as a single unit. Compare with *homogeneous network*.

High-level Data Link Control

An international protocol defined by ISO. In HDLC, messages are transmitted in variable-length units known as frames.

High-Speed Serial Interface

A high-speed interface (up to 52 Mbps full duplex) between a DTE and a DCE. The DCE provides the timing for the interface. HSSI can operate over a 50 ft- (15m) shielded twisted-pair cable.

homogeneous network

A network that consists of one type of workstation, server, network interface card, and operating system, with a limited number of applications, all purchased from a single vendor. All nodes use the same protocol and the same control procedures. Compare with *heterogeneous network*.

hop (count)

The number of links that must be “jumped” to get from a source node to a destination node.

host name

A unique name identifying a host system.

hot swappable

A feature that allows the user to add, replace, or remove interface processors in an Ascend switch without interrupting switch operations.

HP OpenView

The UNIX-based network management application used with NavisCore on an NMS to manage an Ascend switch network.

HSSI

See *High-Speed Serial Interface*.

hub

A wiring device that contains multiple connections of network and internetworking modules. Active hubs amplify or repeat signals to extend a LAN (in terms of distance). Passive hubs do not repeat, but split the transmission signal, allowing the administrator to add users to a LAN.

I

ICMP

See *Internet Control Message Protocol*.

IEEE

See *Institute of Electrical and Electronic Engineers*.

IEEE standards

Various specifications defined by the Institute of Electrical and Electronic Engineers (such as Token Ring, Ethernet) to establish common networking standards among vendors.

indirect Ethernet

A LAN topology or an extended LAN where the NMS and the switch reside on different LANs and must use a router for access.

Input/Output Adapter

A module that connects the various IOP and IOP Plus modules in a switch. IOA configurations vary according to the specific IOP module they support.

Input/Output Processor

A module in a switch that manages the lowest level of a node's trunk or user interfaces. An IOP performs physical data link and multiplexing operations on external trunks and user links.

Institute of Electrical and Electronic Engineers

Professional organization that defines network standards.

Integrated Services Digital Network

A CCITT standard for a worldwide digital communications network, intended to replace all current systems with a completely digital transmission system.

internal clocking

A hardware function of the Ascend switch that provides the transmit and receive clocks to the user equipment.

internal testing

A hardware diagnostic that performs an internal loopback test on the I/O card and other cards.

International Standards Organization

An international standards group based in Geneva, Switzerland that establishes global standards for communications and information exchange.

International Telecommunication Union Telecommunication Standard Sector

An advisory committee established under the United Nations to recommend worldwide standards for voice and data. One of the four main organizations of the International Telecommunications Union.

Internet Control Message Protocol

The IP portion of TCP that provides the functions used for network layer management and control.

Internet Protocol

The TCP/IP session-layer protocol that regulates packet forwarding. See also *Internet Control Message Protocol*.

Internet Protocol address

A 32-bit address assigned to hosts using TCP/IP. The address is written as four octets separated with periods (dotted decimal format), which are made up of a network section, an optional subnet section, and a host section.

IOA

See *Input/Output Adapter*.

IOP

See *Input/Output Processor*.

IP

See *Internet Protocol*.

IP address

See *Internet Protocol address*.

ISDN

See *Integrated Services Digital Network*.

ISO

See *International Standards Organization*.

ITU-T

See *International Telecommunication Union Telecommunication Standard Sector*.

J

jitter

A type of distortion found on analog communications lines, resulting in data transmission errors.

K

Kbps

Kilobits per second.

L

LAN

See *Local Area Network*.

LAP

See *Link Access Protocol*.

LAP-B

A bit-oriented data-link protocol used to link terminals and computers to packet-switched networks.

LED

See *Light Emitting Diode*.

Light Emitting Diode

A semiconductor light source that emits light in the optical frequency band (visible light) or the infrared frequency band. A major light source for optical fiber transmission, LEDs are used with multimode optical fiber in applications that require a low-cost light source. See also *good LED*, *marginal LED*, *and failed LED*.

Link Access Protocol

The link-level protocol used for communications between DCE and DTE devices.

link-state routing protocol

A sophisticated method of determining the shortest paths through the network. See also *Open Shortest Path First*.

load balancing

A technique that distributes network traffic along parallel paths to maximize the available bandwidth while providing redundancy at the same time.

Local Area Network

Any physical network technology that connects a number of devices and operates at high speeds (10 Mbps through several gigabits per second) over short distances. Compare with *Wide Area Network*.

logical port

A configured circuit that defines protocol interaction.

loopback test

A diagnostic that directs signals back toward the transmitting source to test a communications path.

loss of signal

A T1 error condition when j175+_75 consecutive zeros are received.

low level debugger

A state whereby the CP switch is powered on. If both positions on the CP switch are in the OFF position (pointing left), power up diagnostics are bypassed and the system debugger is enabled.

M

Management Information Base

The set of variables forming a database contained in a CMIP or SNMP-managed node on a network. Network management stations can fetch/store information from/to this database.

marginal LED

An amber status indicator on a switch module that indicates a non-fatal system fault (such as low memory).

Mbps

Megabits per second.

MIB

See *Management Information Base*.

mild congestion

The state of a link when the threshold (more than 16 buffers by default) is exceeded.

mount point

A directory in a file hierarchy at which a mounted file system is added to the machine making the mount.

multicast

A type of broadcast transmission that sends copies of the message to multiple stations, but not to all possible stations.

multiplexer (mux)

A device that merges several lower-speed transmission channels into one high-speed channel at one end of the link. Another mux reverses this process at the opposite end.

multiplexing

A technique that transmits several signals over a single communications channel.

N

name server

A server connected to a network that converts network names into network addresses.

name service

A distributed database service that allows a single set of system configuration files to be maintained for multiple systems on a network.

NavisCore

The UNIX-based graphical user interface used to configure and monitor an Ascend switch network.

network address

A network layer address refers to a logical, rather than a physical network device; also called protocol address.

Network Interface Card

A card, usually installed in a pc, that enables you to communicate with other users on a LAN; also called adapter.

Network-to-Network Interface

The standard that defines the interface between ATM switches and between Frame Relay switches. In an SMDS network, an NNI is referred to as Inter-Switching System Interface (ISSI).

NIC

See *Network Interface Card*.

NNI

See *Network-to-Network Interface*.

node

Any device such as a pc, terminal, workstation, etc., connected to a network and capable of communicating with other devices.

node number

A unique number that identifies a device on the network.

noise

Extraneous signals on a transmission channel that degrade the quality or performance of the channel.

O

Open Shortest Path First

A routing protocol that takes into account network loading and bandwidth when routing information over the network. Incorporates least-cost routing, equal-cost routing, and load balancing.

Open Systems Interconnection

An international standard program created by ISO and ITU-T to develop standards for data networking, such as the OSI model, to facilitate multi-vendor operating environments.

OPTimum PVC trunk

A logical port configuration that optimizes interoperability in performance and throughput in networks where both ends are connected by Ascend switches.

OPTimum trunking

A software function that allows public data networks based on Frame Relay, SMDS, or ATM to be used as trunk connections between Ascend switches.

OSI

See *Open Systems Interconnection*.

OSPF

See *Open Shortest Path First*.

P

packet

Any block of data sent over a network. Each packet contains sender, receiver, and error-control information in addition to the actual message; sometimes called payload or data bits.

Packet Assembler/Disassembler

A device connected to a packet-switched network that converts a serial data stream from a character-oriented device (e.g., a bridge or router) into packets suitable for transmission. It also disassembles packets into character format for transmission to a character device.

packet processor

The Ascend switch module that performs the frame format validation, routing, queuing and protocol conversion for the STDX switch. This module is not hot swappable.

packet-switched network

A network that consists of a series of interconnected circuits that route individual packets of data over one of several routes and services.

packet switching

Type of networking in which nodes share bandwidth with each other by intermittently sending logical information units (packets). In contrast, a circuit-switching network dedicates one circuit at a time to data transmission.

PAD

See *Packet Assembler/Disassembler*.

Parameter Random Access Memory

The PRAM on a switch that contains the module's downloaded configuration file, and which is stored in battery backup.

pass count

A statistic that displays the number of background diagnostic tests that have passed without error.

passive hub

A wiring device used in some networks to split a transmission signal, allowing additional workstations to be added to the network. Compare with *active hub.*

path

The complete location of a directory or file in the file system. See *define path* and *alternate path*.

payload

The portion of a frame that contains the actual data.

PDN

See *Public Data Network.*

Point-to-Point Protocol

A protocol that provides router-to-router and host-to-network connections.

polling

An access control method in which one master device, such as the NMS, polls or queries other network devices, requesting them to transmit one at a time.

PPP

See *Point-to-Point Protocol*.

PRAM

See *Parameter Random Access Memory*.

PRI

See *Primary Rate Interface*.

primary group

The main group to which associated users belong. The system identifies the primary group by the group field in the user account (stored in the /etc/password file) and by the group ID associated with a new file.

Primary Rate Interface

An ISDN interface to primary rate access, which consists of a single 64-Kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.

protocol

A set of rules governing communication between two entities or systems to provide interoperability between services and vendors. Protocols operate at different layers of the network, e.g., data link, network, and session.

proxy service

A management service provided for one or more devices by another. For example, the Ascend SMDS Access Servers/switches are proxy-managed through the SMDS network.

Public Data Network

Any government-owned or controlled commercial packet-switched network, offering WAN services to data processing users.

Q

QoS

See *Quality of Service*.

Quality of Service

A statistical report that specifies certain characteristics of network services, sessions, connections, or links. For example, a NavisCore statistics report describes the lost packets and round-trip delay measurements.

R

RAM

See *RAM*.

Random Access Memory

The main system memory in a computer used for the operating system, applications, and data.

rate enforcement

A process used to measure the actual traffic flow across a given connection and compare it to the total admissible traffic flow for that connection. Traffic outside of the acceptable level can be tagged and discarded en route if congestion develops. ATM, Frame Relay, and other types of networks use rate enforcement.

reboot

To restart the computer and reload the operating system, usually after a crash.

Receive Data

A hardware signal, defined by the RS-232-C standard, that carries data from one device to another. Compare with *Transmit Data*.

red alarm

A T1 alarm condition indicating a loss of signal or loss of frame at the device's local termination point.

red frames

A type of frame to be discarded. Color designators green, amber, and red identify packets as they travel through the network.

redundancy

The duplication of hardware or software within a network to ensure fault-tolerant or back-up operation.

remote connection

A workstation-to-network connection made using a modem and telephone line or other WAN services equipment. Remote connections enable you to send and receive data over greater distances than you can with conventional cabling methods.

repeater

A device that receives data on one communication link and transmits it, bit by bit, on another link as fast as it is received without buffering.

Request For Comment

A series of notes and documents available on-line that describe surveys, measurements, ideas, techniques, and observations, as well as proposed and accepted Internet protocol standards, such as Telnet and FTP.

Request To Send

A hardware signal, defined by the RS-232-C standard, that a device sends to request permission to transmit.

RFC

See *Request For Comment*.

RIP

See *Routing Information Protocol*.

router

An intelligent LAN-connection device that routes packets to the correct LAN segment destination address(es). The extended LAN segments may or may not use the same protocols. Routers link LAN segments at the ISO/OSI network layer.

routing

The process of directing data from a source node to a destination node.

Routing Information Protocol

A routing protocol that maintains a list of accessible networks and calculates the lowest hop count from a particular location to a specific network.

routing protocol

A protocol that implements routing using a specific routing algorithm. Routing protocols include IGRP, OSPF, and RIP.

RTS

See *Request To Send*.

RXD

See *Receive Data*.

S

SEAL

See *Simple Network Management Protocol*.

Serial Line over Internet Protocol

A protocol that enables point-to-point serial communication over IP using serial lines or telephone connections and modems.

serial management port

A management port on the Packet Processor card in an Ascend switch.

severe congestion

A state or condition that occurs when the queue size is greater than a second predetermined threshold (32 buffers full). In this state, the continued forwarding of amber and red packets jeopardize the successful delivery of green packets.

shielded cable

Cable protected against electromagnetic and radio frequency interference.

shortest path routing

A routing algorithm that calculates the path distances to all network destinations. The shortest path is then determined by a cost assigned to each link. See also *OSPF.*

SIG

See *SMDS Interest Group*.

Simple Network Management Protocol

A standard network management protocol used to manage and monitor nodes and devices on a network.

SIP

See *SMDS Interface Protocol*.

SLIP

See *Serial Line over Internet Protocol*.

smart hub

A concentrator with certain network management features built into the firmware. This capability enables the user to manage LAN configurations.

SMDS

See *Switched Multimegabit Data Services*.

SMDS In-Band Network Management

The NMS manages the SMDS network traffic using SMDS In-Band Network Management. To be managed from this NMS, all SMDS Access Servers/Switches must be in the same IP subnet.

SMDS Interest Group

A consortium of vendors and consultants committed to advancing worldwide SMDS as an open, interoperable solution for high-performance data connectivity.

SMDS Interface Protocol

The protocol defined at the network and end-user interface connection.

SNMP

See *Simple Network Management Protocol*.

static route

A route or path that is manually entered into the routing table. Static routes take precedence over routes or paths specified by dynamic routing protocols.

subnet address

An extension of the Internet addressing scheme that allows a site to use a single Internet address for multiple physical networks.

subnet mask

A 32-bit address mask used in IP to specify a particular subnet. See also *address mask.*

superuser (root)

In UNIX, a user (also known as root) with special privileges. Only the superuser, for example, can change the password file and edit major system administration files in the /etc directory.

Switched Multimegabit Data Services

A high-speed WAN service based on the 802.6 standard for use over T1 or T3 circuits.

synchronization

The timing of separate elements or events to occur simultaneously. In communications, hardware and software must be synchronized so that file transfers can occur.

synchronous transmission

A data transmission method that uses a clock signal to regulate data flow.

T

T1

A long-distance, point-to-point circuit that provides 24 channels at 64 Kbps each (for a total of 1.544 Mbps). See also *E1*.

T3

A long-distance, point-to-point circuit that provides up to 28 T1 channels. T3 can carry 672 channels of 64 Kbps (for a total of 44.736 Mbps).

Tc

See *Committed Rate Measurement Interval*.

TCP

See *Transmission Control Protocol*.

TDM

See *Time Division Multiplexing*.

telnet

The Internet standard protocol for remote terminal-connection services.

throughput

The actual speed of the network.

Time Division Multiplexing

A timing mechanism that allocates bandwidth for multiple channels onto one channel based on preassigned time slots.

time interval "T"

The time interval over which the number of bits used to average the number of bits transmitted, is averaged. To calculate **T,** use the following formula: Bc/CIR=T.

topology

The map or configuration design of a network. Physical topology refers to the location of hardware. Logical topology refers to the paths that messages take to get from one node to another.

transceiver

A device that connects a host interface to a LAN. A transceiver transmits and receives data.

Transmission Control Protocol

The Internet standard, transport-level protocol that provides the reliable, full duplex, stream service on which many application protocols depend.

Transmit Data

A hardware signal, defined by the RS-232-C standard, used by the DTE to transmit data to the DCE. Compare with *Receive Data*.

trap

An unsolicited message generated by an SNMP agent on a network device (e.g. switch) due to a predefined event occurring or alarm threshold being exceeded, which triggers an alarm at the NMS.

trunk

The communications circuit between two switches.

trunk backup

A configuration setting specified by a network operator via the NMS. The network operator can initiate or terminate primary trunk backups at any time via the NMS. Trunk backups take over a connection should the primary trunk fail.

trunk failure

A condition (alarm) that occurs when the Ascend switch status indicates that a trunk is no longer available.

trunk restoration

A process that reroutes the PVCs carried on the backup trunk, and frees up the circuit on the backup trunk.

TXD

See *Transmit Data*.

twisted-pair cable

Cable that consists of two or more pairs of insulated wires twisted together. One wire carries the signal, and the other is grounded.

U

UIO module

See *Universal Input Output Module*.

UDP

See *User Datagram Protocol*.

unshielded cable

Any cable not protected from electromagnetic or radio frequency interference.

UNI

See *User-to-Network Interface*.

UNI DCE

See *User Network Interface Data Communications Equipment*.

UNI DTE

See *User Network Interface Data Terminal Equipment*.

Universal Input Output Module

In the Ascend switch, a module that has three 80-pin connectors and is used for redundancy, and also as an I/O module for X.21, RS449, V.35, EIA530, and EIA530A interfaces.

User Datagram Protocol

An unreliable transport-layer protocol from the TCP/IP protocol suite. It simply acts as an interface to various applications through the use of different ports.

User Network Interface Data Communications Equipment

A device that performs the Frame Relay DCE functions for link management and expects a Frame Relay DTE device (e.g., Ascend switch) to be attached to it.

User Network Interface Data Terminal Equipment

A device that performs the Frame Relay DTE functions for link management. The user specifies this option on the NMS to connect to a Frame Relay DCE, where the Ascend switch acts as the DTE.

User-to-Network Interface

A standard defined by the ATM Forum for public and private ATM network access. UNI connects an ATM end system (such as a router) and an ATM switch, and is also used in Frame Relay. UNI is called SNI (Subscriber Network Interface) in SMDS.

V

V.35

A standard module used for communication between a network access device and a packet network. It provides clocking from 19.2 Kbps to 4.0966 Mbps.

virtual bandwidth

Channel capacity calculated to allow for oversubscription of channel usage.

W

WAN

See *Wide Area Network*.

warmboot

A reboot performed after the operating system has been running for a period of time. Compare with *coldboot*.

Wide Area Network

A network that usually consists of packet-switching nodes over a large geographical area.

Y

yellow alarm

A T1 alarm that is generated when the interface receives a red alarm signal from the remote end.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

V