NavisCore NMS
Getting Started Guide

Ascend Communications, Inc.

Product Code: 80070
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

Appendix B The NavisCore Configuration File

Appendix C Configuring Poll Server

Glossary

Index

List of Figures

List of Tables

About This Guide

This guide describes how to use Ascend's NavisCore network management software to set up and manage a switch network. Specifically, this guide describes how to manage the Network Management Station (NMS), configure a gateway switch (the first switch in the network), and manage network maps and switches.

This guide supports the following NMS and switch software releases:

- NavisCore, Release 4.0
- B-STDX, Release 6.0
- CBX 500, Release 3.0
- GX 550, Release 1.0

What You Need to Know

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

This guide assumes you have already installed the Ascend switch hardware, using one of the following guides:

- *STDX 6000 Hardware Installation Guide*
- *B-STDX 8000/9000 Hardware Installation Guide*
- *CBX 500 Hardware Installation Guide*
- *GX 550 Hardware Installation Guide*

and you have installed the NMS software, using the *Network Management Station Installation Guide*.

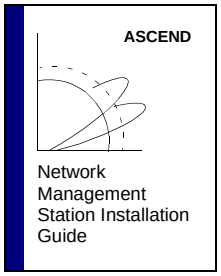
Reading Path

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

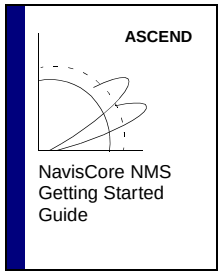
- NMS Documentation
- Switch Software Documentation

NMS Documentation

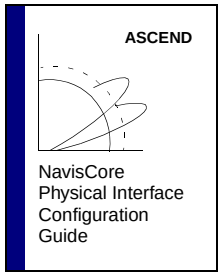
Read the following documents to install and operate NavisCore Release 4.0.



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



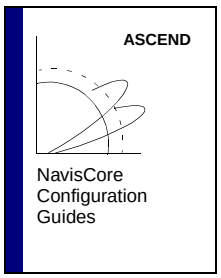
This guide describes how to configure and manage NavisCore, network maps, and Ascend switches.



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

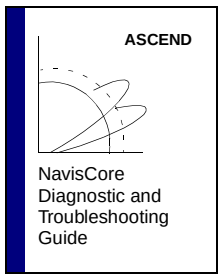
Switch Software Documentation

Read the following documents to configure switch software for B-STDX Release 6.0, CBX Release 3.0, and GX Release 1.0.

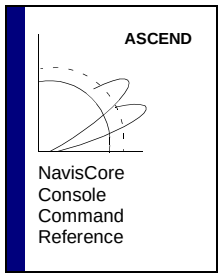


These guides describe how to configure WAN services on the STDX, B-STDX, CBX, and GX switch platforms:

- *NavisCore Frame Relay Configuration Guide*
- *NavisCore ATM Configuration Guide*
- *NavisCore IP 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

The following table highlights the chapters in this guide.

Read	To Learn About
Chapter 1	General features of the Network Management Station (NMS).
Chapter 2	The following NMS system administration tasks: • NMS startup and shutdown • NavisCore security passwords • Audit Trail utility
Chapter 3	Creating a direct trunk between two switches. This configuration example enables you to verify the software and hardware installation.
Chapter 4	Managing network maps, for example: • Create and add objects to a network map • Designate the Class-B IP-addressing scheme
Chapter 5	Configuring the NMS and gateway switch.
Appendix A	Downloading the configuration file to the switch.
Appendix B	The *cascadeview.cfg* configuration file.
Appendix C	Configuring the poll server product.
Appendix D	The NavisCore menu system.

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*]**
Boldface	User input in text.	Type **cd install** and . . .
Menu ⇒ Option	Select an option from the menu.	NavisCore ⇒ Logon
Boxes surrounding text	Notes, cautions, and warnings.	See examples below.
Italics	Book titles, new terms, filenames, 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 Physical Interface Configuration Guide* (Product Code: 80080)
- *NavisCore Frame Relay Configuration Guide* (Product Code: 80071)
- *NavisCore ATM Configuration Guide* (Product Code: 80072)
- *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

Table 1 lists and describes some of the acronyms used throughout this guide.

Table 1. Common Acronyms

Acronym	Description
ATM	Asynchronous Transfer Mode
CDE	Common Desktop Environment
CIR	committed information rate
CLP	cell loss priority
CP	control processor
DLCI	data link connection identifier
EFCI	explicit forward congestion indication
FCP	flow control processor (FCP)
HSSI	High-Speed Serial Interface
IOM	input/output module
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MIB	Management Information Base
NMS	network management station
NP	node processor
OSPF	Open Shortest Path First
PDU	protocol data unit
PRAM	parameter random access memory
PVC	permanent virtual circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Managment Protocol
SP	switch processor

Table 1. Common Acronyms (Continued)

SVC	switched virtual circuit
UDP	User Datagram Protocol
VC	virtual channel
VCI	virtual circuit identifier
VPI	virtual path identifier
VPN	virtual private network

1

NavisCore Overview

NavisCore is an integrated network management software package that runs on a Network Management Station (NMS). NavisCore enables you to:

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

Figure 1-1 illustrates the various software packages that make up the NMS:

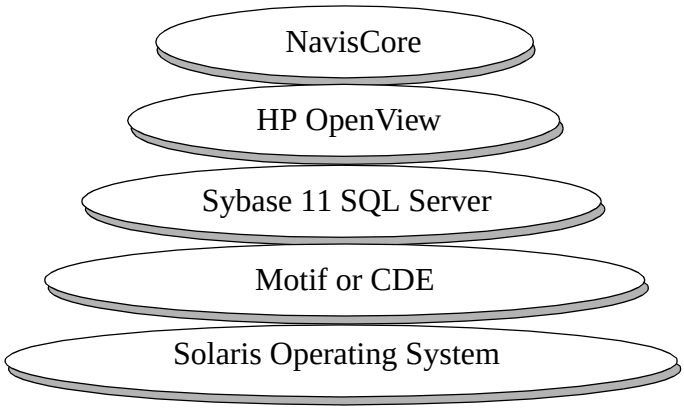


Figure 1-1. NavisCore Network Management Station (NMS)

Combined, these software programs present an easy-to-use graphical user interface that allows you to configure and maintain an Ascend network. A description of these software programs follows:

Solaris Operating System — The operating system you install on your SPARCstation. Solaris is a UNIX-based operating system used to design and develop complex networks.

MOTIF and CDE — Window managers that run client applications. MOTIF and CDE (Common Desktop Environment) enable you to customize your window's visual display.

SYBASE 11 SQL Server — SYBASE 11 SQL Server is a relational database software program used to store database information and provide backup and recovery of database files.

HP OpenView — HP OpenView provides the interface to add, modify, and delete nodes, trunks, and switch configurations from the network map and database.

NavisCore — NavisCore provides a graphical user interface for setting up a switch network.

About the Network Management Platform

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

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

You download the initial network configuration and any updates from the NMS to the switch. The switch stores this configuration in parameter random access memory (PRAM).

About Ascend Multiservice WAN Switches

Each Ascend multiservice WAN switch contains a Simple Network Management Protocol (SNMP) agent, which enables you to manage an Ascend switch from any SNMP management system that supports the Ascend Enterprise MIB extensions. When you configure an NMS with NavisCore, the NMS communicates with the switches through either the Internet Protocol (IP) for in-band management connections, or the Serial Line Internet Protocol (SLIP) for out-of-band management.

Running NavisCore, the NMS supports in-band management using an Ethernet connection to a local Ascend switch; alternately, you can configure the NMS and the switch on the same IP network.

Monitoring Features

After you create your Ascend network, you can closely monitor network activity through the NavisCore monitoring features. NavisCore provides several options for obtaining status information from the network, including:

- A pop-up menu that enables you to obtain configuration information for a physical port, logical port, and circuit on a per-card or per-port basis.
- The Monitor Ascend Objects selection enables you to obtain status information for a switch, port, trunk, and circuit.
- You can also monitor the network by running diagnostics, collecting statistical data, generating reports, and reviewing the traps log.

See the *NavisCore Diagnostic and Troubleshooting Guide* for information on these NavisCore monitoring features.

Troubleshooting Features

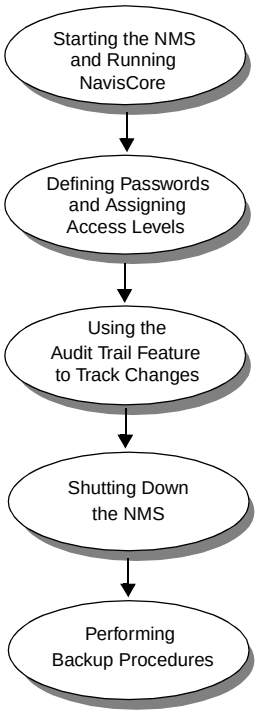
NavisCore uses a color scheme to identify network problems. When you open a network map, all nodes that are operating and communicating with the NMS appear green. Nodes that are either not operational or unable to communicate with the NMS appear red or wheat, respectively. An I/O module in a switch that is out of synch appears yellow.

NavisCore also uses a color scheme to indicate the status of a configured trunk link between two Ascend switches, the status of I/O modules, processor modules, fans, power supplies, etc. For more information, see the *NavisCore Diagnostic and Troubleshooting Guide.*

2

Administering NavisCore

This chapter describes the following administrative tasks:



This guide assumes you have already installed NavisCore and its supporting applications. If you have not installed all of these software products, refer to the *Network Management Station Installation Guide* for detailed instructions on how to perform the NMS installation.

Starting the NMS and Running NavisCore

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

To start the NMS:

1. Power on the Sparc Station.
2. At the console prompt, log in as the nms user and enter the appropriate password (the login you used when you installed Solaris).

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

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

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

    ```
    /usr/OV/bin/ovstart
    ```
11. To start HP OpenView, enter **/usr/OV/bin/ovw &** in a console window. The default HP OpenView window appears (see Figure 2-1).

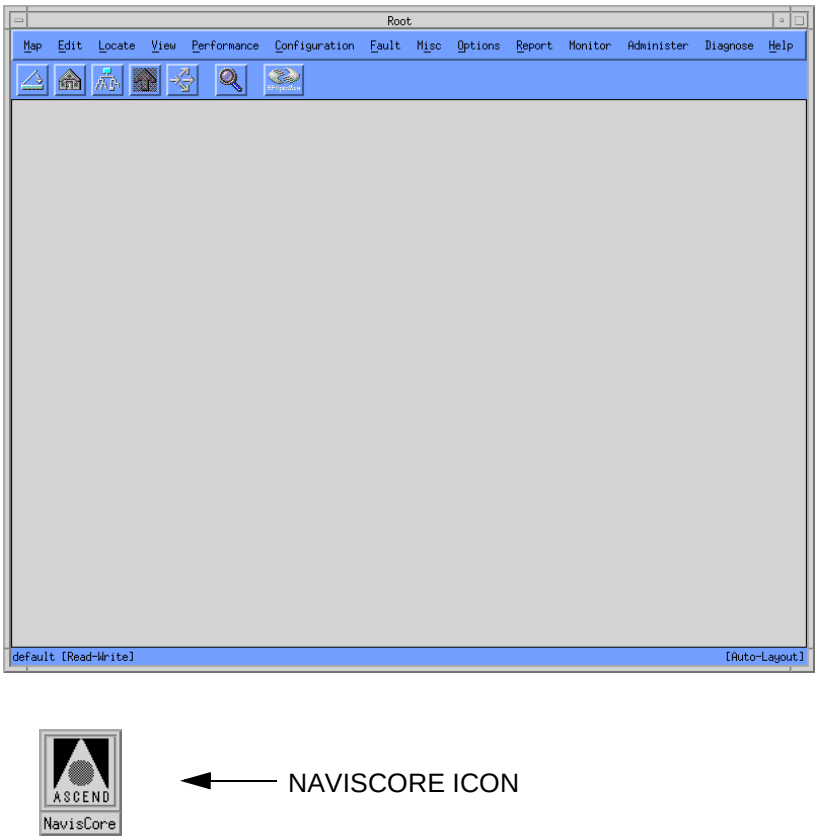


Figure 2-1. NavisCore Window

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

Defining Passwords

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

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

You can define three levels of access for NavisCore:

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

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

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

Assigning Access Levels

To define access levels and modify the default passwords:

1. From the Administer menu, select NavisCore ⇒ Set Password and select one of three access levels: Administrator, Operator, or Provisioning. The Change Provision Password dialog box appears (see Figure 2-2).

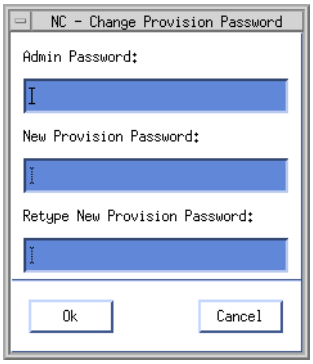


Figure 2-2. Change Provision Password [*level*] Dialog Box

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

Logging On

To log on to NavisCore:

1. From the HP OpenView Misc menu, select NavisCore ⇒ Logon. The NavisCore - Logon dialog box appears (see Figure 2-3).

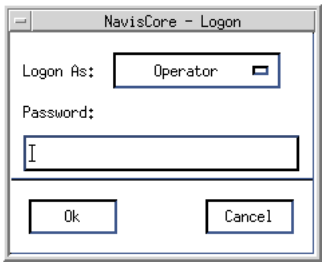


Figure 2-3. NavisCore Logon Dialog Box

2. Enter the appropriate password.

You can now perform NavisCore administrative tasks.

Using the Audit Trail Utility

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

The Audit Trail utility logs the following network activity:

- Switch status
- Invalid login attempts
- Login or logoff actions
- Add, modify, or delete functions for a switch, module, logical port, trunk, or circuit
- Reboot functions for a switch or module
- Download activity for switch software, initialization script files, or PRAM synch files
- Standby module activity when it takes over in a redundant pair
- Add, delete, or modify functions for a Management Path or NMS entry
- User session timeout

Enabling/Disabling the Audit Trail

To enable the Audit Trail:

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

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

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

   ```
   CV_AUDIT_TRAIL_ENABLE=TRUE
   export CV_AUDIT_TRAIL_ENABLE
   ```

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

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

      ```
      cd /usr/OV/bin
      ./ovstop
      ```

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

   The filename format is *cv-audit-log.[day of the week].[date]*. For example, the file *cv-audit-log.thu.5-7-98* contains information for May 7, 1998.

   The Audit Trail utility creates a different file for each day of operation (a file for Monday, a file for Tuesday, and so on).
7. To view the ASCII log file, enter:

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

Figure 2-4 shows the Audit Trail Window with an example log file, which you can display through the **more** command.

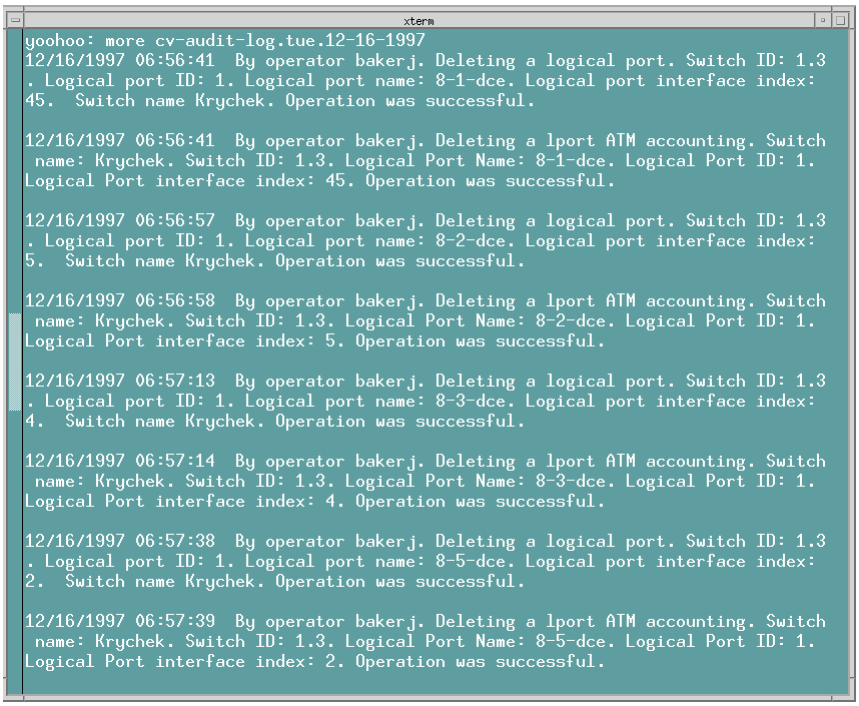


Figure 2-4. Audit Trail Window

Shutting Down the NMS

To close all NMS processes and power off the UNIX workstation:

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

   `/usr/OV/bin/ovstop`
5. Log in as the Sybase user by entering **su - sybase**.
6. At the prompt, enter the Sybase password.

7. *If you are using Sybase 11*, enter the following commands to shut down the backup server. Otherwise, proceed with Step 8.

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

8. To shut down the Sybase server, enter:

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

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

Performing Backup Procedures

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

The Ascend Technical Assistance Center (TAC) recommends that you perform daily backups of the Sybase server and the HP OpenView database.
If you need to recover switch data in the database, contact the TAC for specific instructions. **Do not** attempt to restore this database without Ascend's help. You can contact the TAC at one of the following numbers:

1-800-DIAL-WAN for the United States and Canada

1-978-952-7299 for all other areas

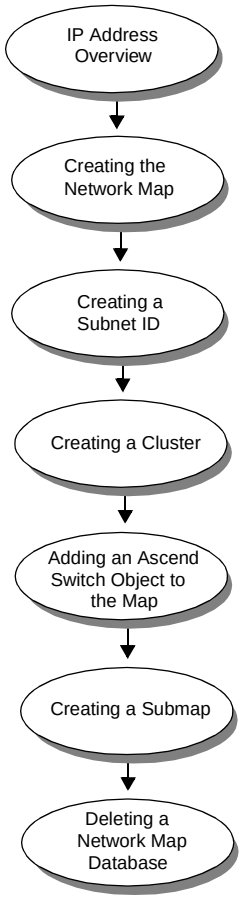
0-800-96-2229 for the United Kingdom

3

Creating and Managing Network Maps

This chapter describes IP addressing and subnet addressing concepts. It also describes how to create a network map and subnet ID and add the Ascend switch objects to the network map.

This chapter describes the following topics and tasks:



About IP Addresses

This section provides an overview of IP addresses and describes the three primary classes of IP addresses (specifically, Class B IP). See the *NavisCore IP Configuration Guide* for a detailed description of the supported IP features.

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

The position of the first zero bit in the first four bits determines the class to which an address belongs. The remaining bits specify two subfields, a *network identifier* (*netid*) and a *host identifier* (*hostid*). The netid defines what network the system belongs to, and the hostid represents the specific location on that network (see Figure 3-1).

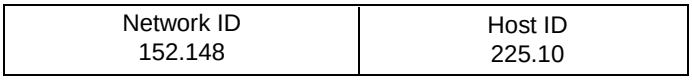


Figure 3-1. Class B IP Address

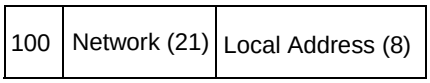
Three Primary Classes of IP Addresses

There are three primary classes of IP addresses. Each class uses a different address format to accommodate different size networks. Table 3-1 shows the network id and host id formats for each class. This guide does not discuss Class D addresses (used for multicasting).

Table 3-1. IP Address Classifications

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

Table 3-1. IP Address Classifications (Continued)

Class	Network ID	Host ID	Format
C	21 bits	8 bits	Class C addresses are used in smaller networks and allow 254 host addresses. 

Class B IP Addresses

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

If you have a mixed network (for example, switches running two versions of switch code), you must configure all switches running the same version of switch code with circuits within the same subnet.

About Subnets

A subnet divides a large network into smaller groups (subnets). Subnets support a three-level hierarchy (as opposed to a two-level hierarchy) in which the host number is divided into two parts, the subnet number and the host number on that subnet (see Figure 3-2).

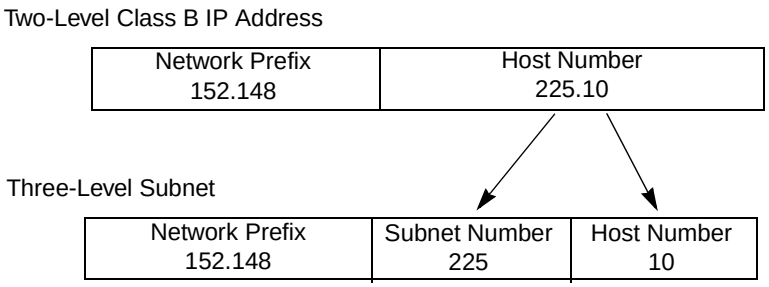


Figure 3-2. Subnet Example

You can use a subnet to:

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

Choosing a Subnet ID (Mask)

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

- Number of subnets in your network
- Number of hosts accessing each subnet

Creating the Network Map

When you create a network map, you specify a unique name for the map and you configure network-wide parameters, such as the network number. These parameters enable the NavisCore application to manage the network map from within HP OpenView.

Use the following procedure to configure a new NavisCore map. This procedure assumes you have started NavisCore.

To create the network map:

1. Access HP OpenView and start NavisCore as described in "Starting the NMS and Running NavisCore" on page 2-2.
2. To log on, select NavisCore ⇒ Logon from the Misc menu. The Logon dialog box appears (see Figure 3-3).

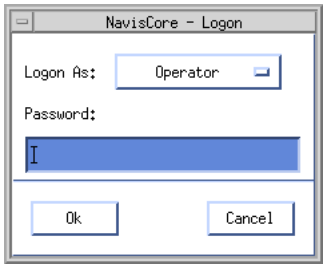


Figure 3-3. NavisCore Logon Dialog Box

3. Enter the Operator password.
4. From the Map menu, select Maps ⇒ New. The New Map dialog box appears (see Figure 3-4).

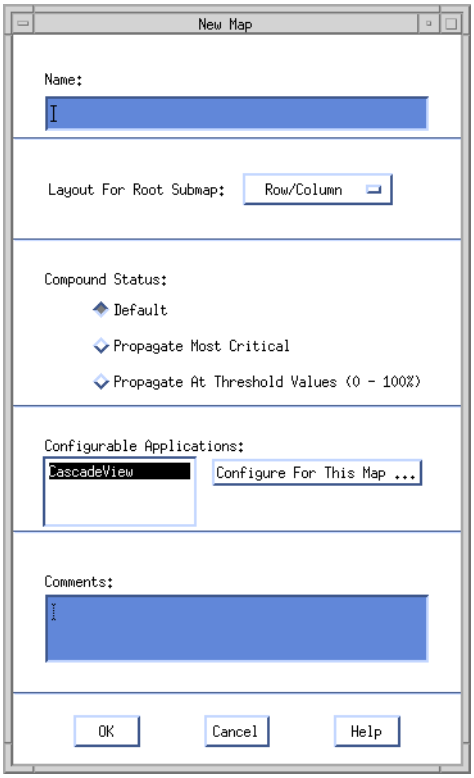


Figure 3-4. New Map Dialog Box

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

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

Table 3-2. New Map Fields

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

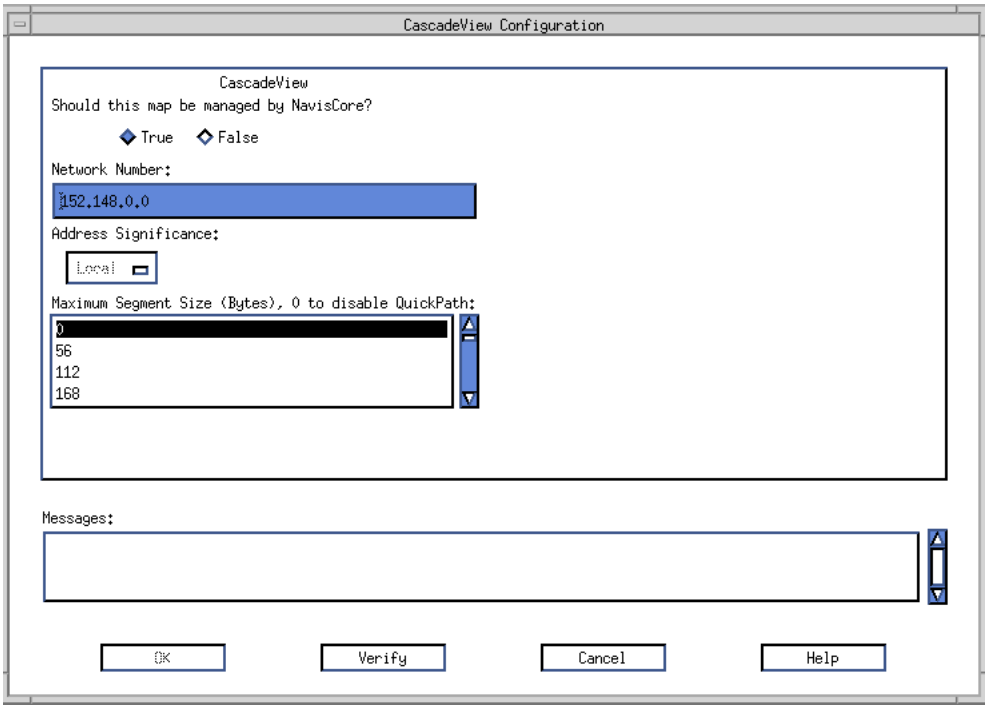


Figure 3-5. Configuration Dialog Box

6. Complete the fields described in Table 3-3.

Table 3-3. Configuration Fields

Field	Action/Description
Should this map be managed by NavisCore?	Select True.
Network Number	Displays the switch IP network number you specified when you added a static route during the NavisCore installation. Contact the Ascend Technical Assistance Center if you must change this number.
Address Significance	Defaults to Local and cannot be changed.
Maximum Segment Size (Bytes), 0 to disable Quickpath	This option is not supported.

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

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

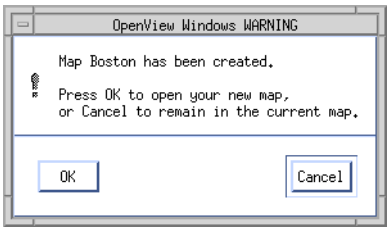


Figure 3-6. OpenView Windows WARNING Dialog Box

9. Choose OK to open the new network map.

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

10. To log on to the network map, select NavisCore ⇒ Logon from the Misc menu and enter the logon password (cascade is the default). See Figure 3-7.

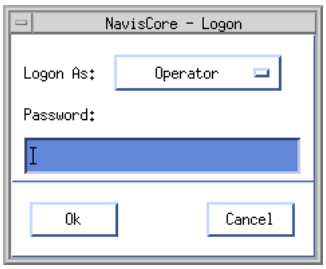


Figure 3-7. Logon Dialog Box

You are now logged on to the new map.

Creating a Subnet ID

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

To add a subnet ID:

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

   The Set All Subnets dialog box appears (see Figure 3-8).

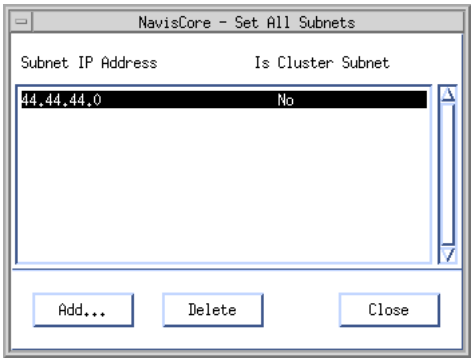


Figure 3-8. Set All Subnets Dialog Box

2. Select Add. The Add Subnet dialog box appears (see Figure 3-9).

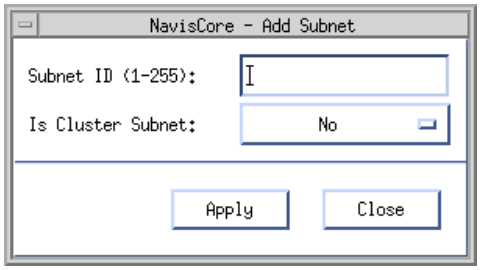


Figure 3-9. Add Subnet Dialog Box

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

Table 3-4. Add Subnet Fields

Field	Action/Description
Subnet ID (1-255)	Enter a subnet number between 1 and 255.
Is Cluster Subnet (*optional*)	Select Yes to make this subnet a cluster subnet (See "Creating a Cluster" on page 3-11 for instructions). The default is No. If you select No, proceed with "Adding an Ascend Switch Object to the Map" on page 3-13.

4. Choose Apply to add the subnet ID.
5. Choose Close to exit the Add Subnet dialog box.

Creating a Cluster

A cluster defines a group of switches that operates in a single OSPF routing domain. The switch number in the IP address increments according to the cluster ID, as shown in Table 3-5.

Table 3-5. Cluster ID and IP-Address Range

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

See the *NavisCore IP Configuration Guide* for information about configuring OSPF parameters. If you selected Yes in the Is Cluster Subnet field (see Table 3-4), you must create a cluster.

To create a cluster:

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

   The Set All Clusters dialog box appears (see Figure 3-10).

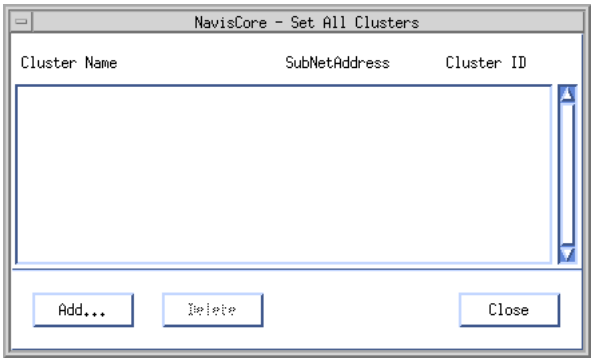


Figure 3-10. Set All Clusters Dialog Box

2. Select Add. The NavisCore - Add Cluster dialog box appears (see Figure 3-11).

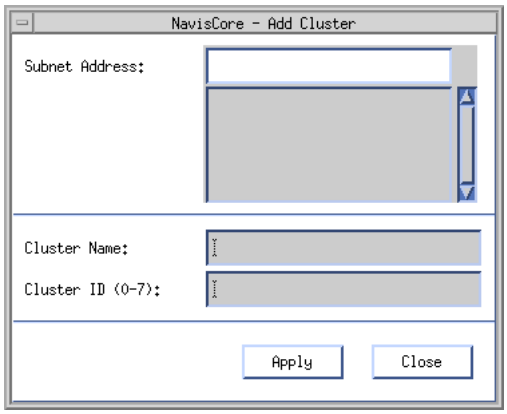


Figure 3-11. Add Cluster Dialog Box

3. Complete the fields described in Table 3-6.

Table 3-6. Add Cluster Fields

Field	Action/Description
Subnet Address	Select the subnet address to which this cluster belongs.
Cluster Name	Select a name for this cluster.
Cluster ID (0-7)	Select an ID between 0-7 for this cluster.

Adding an Ascend Switch Object to the Map

When you add an Ascend switch object to the network map, you first select and drag the switch object to the network map. You then define the object attributes that enable NavisCore to manage this switch through HP OpenView.

To add an Ascend switch object to the network map:

1. From the Edit menu, select Add Object. The Add Object : Palette dialog box appears (see Figure 3-12).

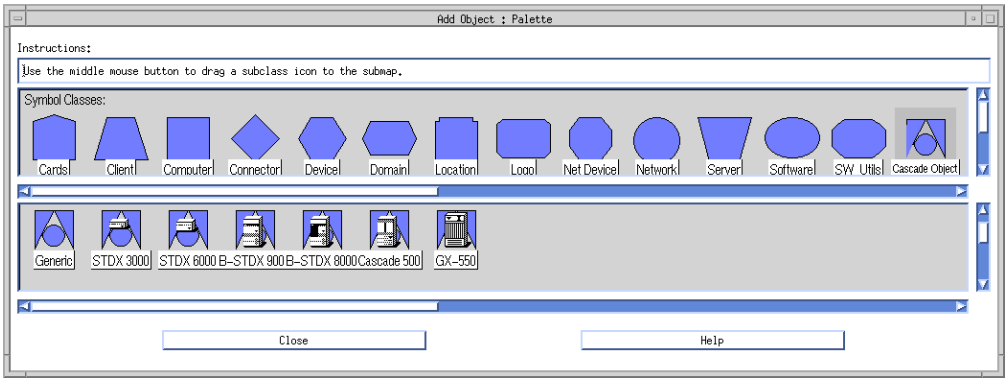


Figure 3-12. Add Object : Palette Dialog Box

2. Scroll through the Object Palette to locate the Cascade Object symbol.
3. Select Cascade Object. The symbol subclasses appear.
4. Add the desired Ascend switch(es) to the network map (STDX 3000, STDX 6000, B-STDX 8000, B-STDX 9000, CBX 500, and GX 550). To do this, position the mouse pointer on the object, hold down the *middle* mouse button, drag the object to the map, and release the mouse button. The Add Object dialog box appears (See Figure 3-13).

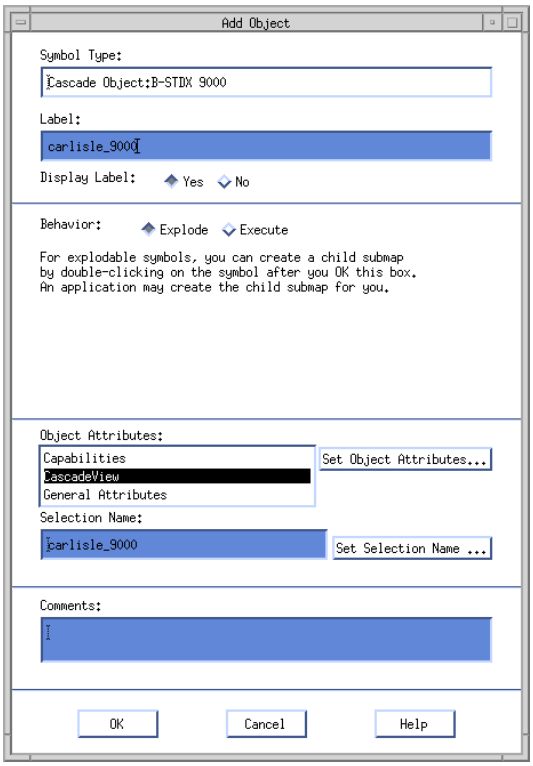


Figure 3-13. Add Object Dialog Box

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

Table 3-7. Add Object Fields

Field	Action/Description
Symbol Type	Displays the selected switch type (object) to add to the network map.
Label	Enter a name to identify the object.
Display Label	Select Yes to display the label beneath the object on the network map. Select No if you do not want the label to appear.
Behavior	Displays the default (Explode). See the *HP OpenView User's Guide* for more information about using the Execute function.
Object Attributes	Select CascadeView and then choose Set Object Attributes. The Add Object – Set Attributes dialog box appears (see Figure 3-14).

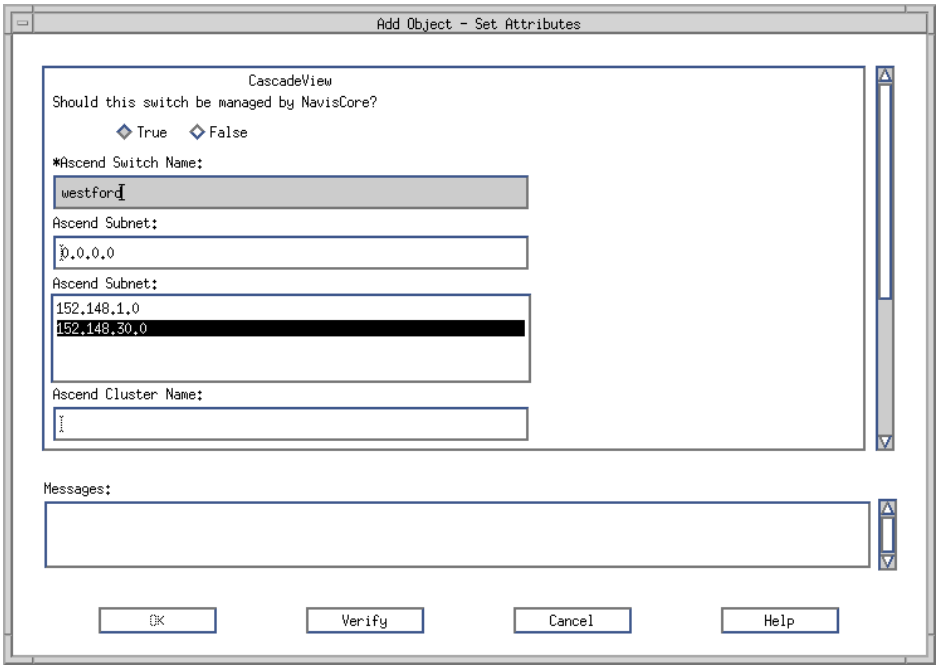


Figure 3-14. Add Object - Set Attributes Dialog Box

6. Complete the fields described in Table 3-8.

Table 3-8. Add Object-Set Attributes Fields

Field	Action/Description
Should this switch be managed by NavisCore?	Select True.
Ascend Switch Name	Enter a unique name for the switch.
Ascend Subnet	Highlight the Ascend subnet to which this switch belongs.
Ascend Cluster Name	Displays the name of the cluster to which this subnet belongs. See "Creating a Cluster" on page 3-11 for more information.
Should this switch be a gateway switch of the selected cluster?	Select True to make this a gateway switch. Select False if you do not want this switch to be a gateway switch for the selected cluster.
Ascend Switch IP Address	NavisCore displays the switch's IP address. Every time you add an object to the map, NavisCore increments the last octet (host id) by 1. If the next host ID number is already in use in the network, NavisCore selects the next available number. If you want a different IP address from the one displayed, you can manually change the last octet. If you created a cluster, the system displays the IP address range (shown in Table 3-5 on page 3-11).
Number of Power Supplies (CBX 500 only)	Select the number of power supplies that this switch supports; either two (2) or three (3).

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

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

   ```
   Verification has completed.
   ```

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

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

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

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

10. Choose OK. The network map displays an object icon representing the new switch. The object appears blue and quickly turns red, indicating that the NMS cannot access the switch.

11. Select the switch object and from the Map menu, select Unmanage Objects. The switch object turns to a wheat color, indicating that the object is in an unmanaged state.

12. Repeat Step 1 through Step 11 to add more Ascend switches to the network map.

When you finish adding switch objects to your network map, continue with Chapter 5, “Setting Switch Parameters” to configure switch parameters and define the path between the NMS and an Ascend switch.

> To turn off the automatic layout feature so you can move a switch object on the map. From the View menu, choose Automatic Layout ⇒ For All Submaps ⇒ Off for All Submaps.

About Submaps

Small to medium size WANs are easy to configure and manage from a single-level network map. As the WAN grows larger, the network often becomes difficult to manage because of its increased complexity (see Figure 3-15). A submap enables you to organize a growing network.

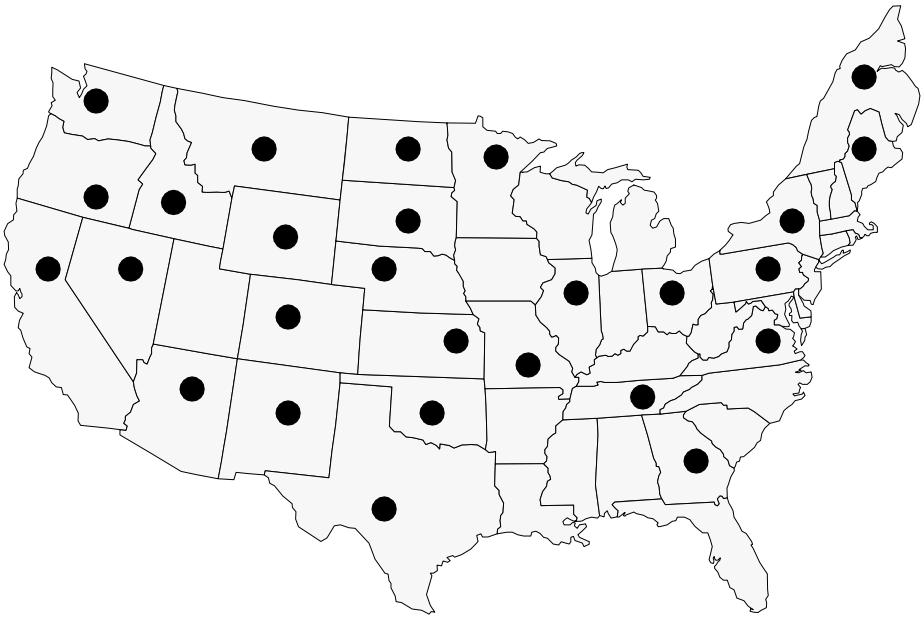


Figure 3-15. Top-level Map without Submaps

A submap is a hierarchical approach to network management. With submaps, a network administrator can divide a map into multiple submaps, then view the overall organization of the network from the top-level map. Figure 3-16 illustrates a top-level map with submaps.

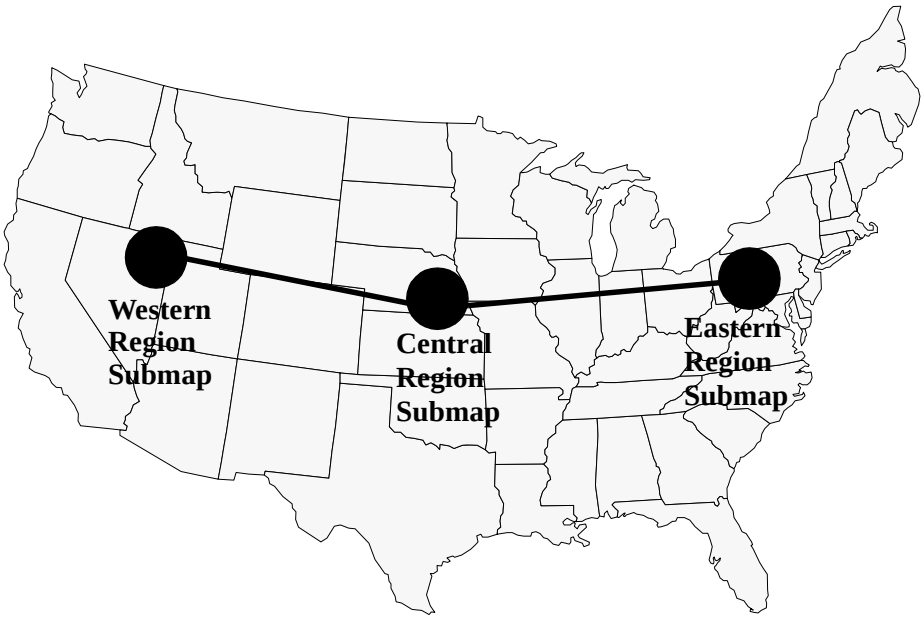


Figure 3-16. Top-Level Map with Submaps

Submaps provide the following features:

- A high-level network view
- A top-level status summary
- Ease of use
- Scalability
- Enhanced map detail

These features are described in the following paragraphs.

High-Level Network View

Submaps enable you to view the overall organization of the network by viewing the top-level map. The top-level map summarizes the logical connectivity between submaps without cluttering the map with the details of each physical connection.

Top-Level Status Summary

The status of individual network components propagates upward through the layers of submaps so that the top-layer map shows a status summary of the entire network that is easy to interpret.

Ease of Use

Well-organized submaps make it easy to locate a particular piece of information (in much the same way that directories make it easy to find the correct file).

Scalability

Submaps can be easily moved on a top-level map without the need to move multiple objects. All switches contained in the submap will automatically move with the submap with no further user interaction required.

Enhanced Map Detail

With submaps, you can size individual icons large enough so that you can recognize them on the top-level map. Without submaps, you must reduce the icons to fit onto one map, making them impossible to identify.

Creating a Map with Submaps

To create a map with submaps:

Develop a Submap Plan

The submap plan should cover the following areas:

- Number of submaps on the main map
- Submap names
- Submap division criteria (by geography, network operations center, etc.)
- List of switches in each submap
- Connectivity between switches within a submap
- Connectivity between submaps

Create a New Map

See "Creating the Network Map" on page 3-5 for information on how to create a new network map.

Add Submap Icons to the Main Map

1. Select Edit ⇒ Add Object and select the Location symbol.

   A selection of icon types appears.

2. Position the pointer over the Generic symbol, press the middle mouse button, then drag the symbol onto the map.

   The Add Object window appears.

3. Enter the submap name in the label field and choose OK.

Arrange Submap Icons

Disable automatic layout by choosing View ⇒ Automatic Layout ⇒ For All Submaps ⇒ Off for All Submaps.

Once automatic layout is disabled, you can arrange the submaps on the root map in any way you want.

It may be helpful to move all switch objects on the top-level map to the side of the map while you are positioning the submaps.

(Optional) Disable User Plane Shadow

Select View ⇒ User Plane ⇒ Off For All Submaps.

Disabling User Plane Shadow will help to eliminate any confusion as to whether or not the submap can be managed.

Create Submaps for Each Submap Icon

1. Double-click on each submap icon.
2. Choose OK to create the submap.

Create New Switches

See “Adding an Ascend Switch Object to the Map”. Be sure to drag the switch icon to the submap, instead of to the root-level map.

Create an Intra-Submap Connection

See “Configuring a Trunk Connection”.

Create an Inter-Submap Connection

1. Select Edit ⇒ Add Connection to draw a connection between Submap A and Submap B.
2. Enter an appropriate label for the inter-submap connection and choose OK.
3. Verify that the new connection is blue in color.
4. Select the blue line using the right mouse button; then select the Describe/Modify symbol.
5. Set the Status Source field to the Compound (Propagated) value; then choose OK to close this window.
6. Double-click on the blue connection line on the map and choose OK to open a submap for that line.

   Leave this connection submap open.
7. Double-click on the Submap A icon to open Submap A. Highlight all switches in Submap A that have connections into Submap B by holding down the <Ctrl> key and clicking on each switch.
8. Select Edit ⇒ Copy ⇒ From This Submap; then close Submap A.
9. Click on the connection submap and select Edit ⇒ Paste.

   A copy of the switches from Submap A will be pasted into the new object holding area of the connection submap.
10. Drag these switches to the desired location on the connection submap window.
11. Double-click on the Submap B icon (double-clicking opens).
12. Highlight any switches in Submap B that have connections into Submap A by holding down the <Ctrl> key and clicking on each switch.
13. Select Edit ⇒ Copy ⇒ From This Submap; then close Submap B.
14. Click on the connection submap and select Edit ⇒ Paste.

    A copy of the switches from Submap B is pasted into the new object holding area of the connection submap.
15. Drag these switches to the desired location on the connection submap window.

    The connected nodes from Submap A and Submap B are copied into the connection submap.
16. Select Edit ⇒ Add Connection to add the trunks that connect switches inside the connection submap. See “Configuring a Trunk Connection” for a description of how to configure the trunks.

Only add the connections that go between Submap A and Submap B in this connection submap. The intra-submap connections already exist in the submaps themselves and do not need to be added.

17. Close the connection submap.
18. Verify that the connection line on the root map is no longer blue.

    The connection line will change colors to reflect the status of the underlying trunk connections.

Create Connections from Switches on the Root Map to Switches in Submaps

1. Select Edit ⇒ Add Connection to draw a connection between Submap A and Switch B.
2. Enter an appropriate label for the inter-submap connection and choose OK.
3. Verify that the new connection is blue.
4. Select the blue line and choose the Describe/Modify Symbol.
5. Select Status Source/Compound (Propagate) from the Describe/Modify Symbol menu.
6. Select the blue connection line on the map and choose OK to open the submap for that line.

   Leave this connection submap open.
7. Double-click on Submap A.
8. Select any switches in Submap A that have connections to Switch B.

   You can do this by holding down the <CTRL> key and selecting each switch.
9. Select Edit ⇒ Copy ⇒ From This Submap; then close Submap A.
10. Select the connection submap and choose Edit ⇒ Paste.

    A copy of the switches from Submap A is pasted into the new object holding area of the connection submap.
11. Drag these switches to the desired location in the connection submap window.
12. Select Switch B on the root-level submap and choose Edit ⇒ Copy ⇒ From This Submap.
13. Select the connection submap and choose Edit ⇒ Paste.

    A copy of Switch B is pasted into the new object holding area of the connection submap.
14. Drag this switch to the desired location in the connection submap window.

15. Select Edit ⇒ Add Connection to add the trunks that connect Switch B and the switches from Submap A inside the connection submap. See "Configuring a Trunk Connection" for a description of how to add the trunks.

Only add the connections that go between Submap A and Switch B in this connection submap. The intra-submap connections already exist in the submaps themselves and do not need to be added to this connection submap.

16. Close the connection submap.
17. Verify that the connection line on the root map is no longer blue.

    The line will change colors to reflect the status of the underlying trunk connections.
18. Repeat Step 9 for each switch-to-submap connection on the root map.

Deleting a Network Map Database

Deleting a network map removes the map information from the HP OpenView database, enabling you to create a new map. To delete a map:

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

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

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

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

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

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

   `rm /usr/OV/log/xnmevents.[`*`username`*`]`

   `rm /usr/OV/log/trapd.log`

   `rm /usr/OV/log/trapd.log.old`

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

    `/usr/OV/bin/ovstart ovwdb`

    `/usr/OV/bin/ovw -fields`

    `/usr/OV/bin/ovstart`

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

12. Enter the following command at the # prompt:

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

    The system displays the following message:

    ```
    Verifying super user privileges...
    ```

    ```
    Would you like to view (tail -f) the install log (default=y)?
    ```

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

13. Press Return to view the Tail window.

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

14. At the NavisCore Installation menu, enter **3** to select HP OpenView Integration Only (NO DB Action).

    The system displays the message:

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

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

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

    The system displays the following message:

    ```
    Configuring NavisCore Environment.
    ```

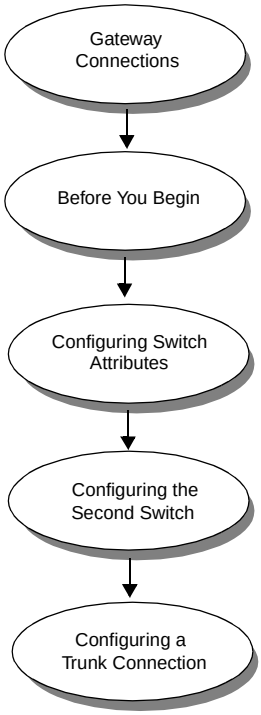
    ```
    Install NavisCore successful...
    ```

The system recreates the NavisCore environment. You now have a clean HP OpenView database.

4

Configuring the Gateway Switch

This chapter describes how to configure the *gateway switch* — the first switch in your network — and add a second switch to enable NMS communications. This chapter describes the following topics and tasks:



About Gateway Connections

The gateway switch acts as a master switch and communicates the status of all switches on the Ascend network to the NMS. Once the NMS can communicate with the gateway switch, you can configure the second switch (and subsequent switches) on the network.

Figure 4-1 illustrates an Ascend switch network with a local Ethernet or Serial Line Internet Protocol (SLIP) connection to the gateway switch.

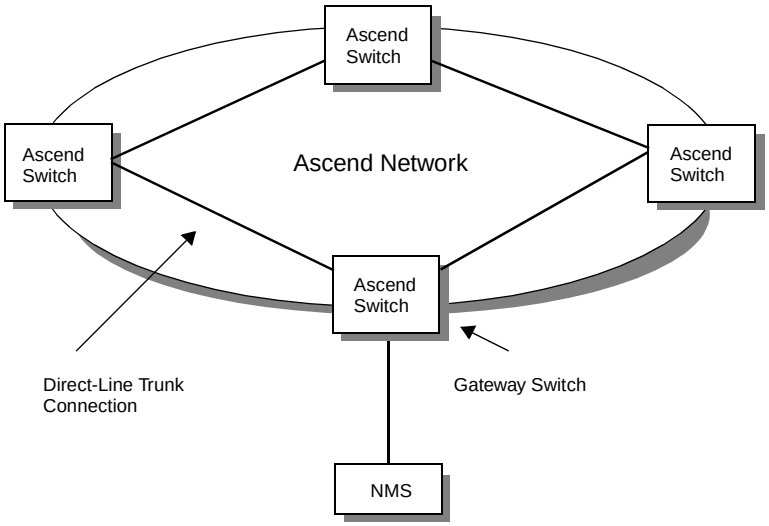


Figure 4-1. NMS with a Local Connection to the Gateway Switch

Figure 4-2 illustrates an Ascend switch network with a remote connection to the gateway switch.

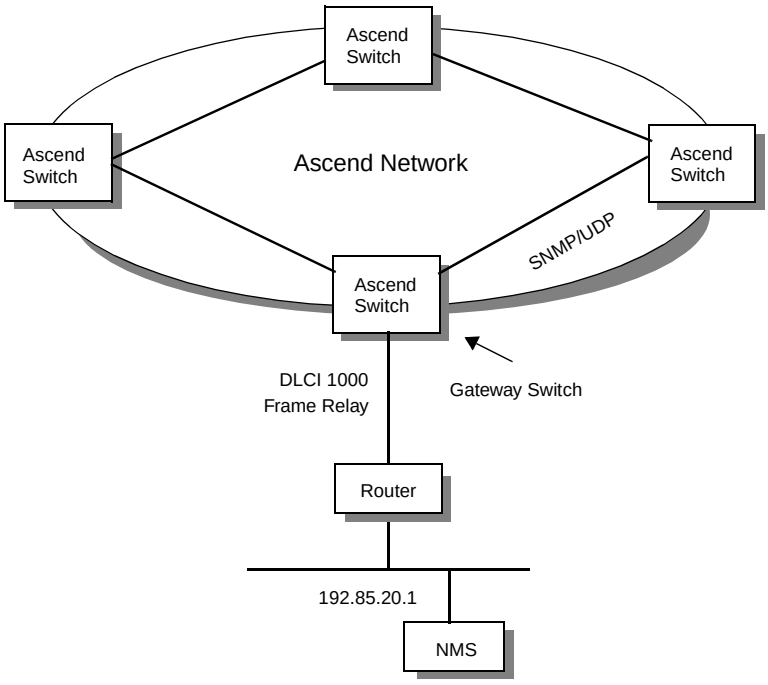


Figure 4-2. NMS with a Remote Connection to the Gateway Switch

This chapter describes a typical configuration in which the NMS uses a local Ethernet or SLIP connection to access the switch (see Figure 4-1) and the switch has never been initialized. See Chapter 5 for information about connecting if the NMS connects to the Ascend switch network via remote access (for example, the NMS and the switch are on separate LANs as in Figure 4-2) or through a management PVC.

Before You Begin

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

- ☑ Connect the NMS SPARCstation to the switch through one of the methods described in your hardware installation guide. Note whether the NMS is connected via direct Ethernet, indirect Ethernet (on a separate LAN segment), or through a SLIP connection (see "About Gateway Connections" on page 4-2).
- ☑ Connect the NMS SPARCstation (either directly or through modems) to the switch through its serial port. This enables you to download the configuration file from the NMS to the switch. (If you choose not to download the configuration file from the NMS, you can copy the configuration file to any workstation that can access the switch. You can then run any terminal emulation package to download the configuration to the switch's PRAM.)
- ☑ Clear switch PRAM if the switch has an existing configuration. See Appendix A, "Erasing PRAM" for a description.
- ☑ Create the network map and add the first switch object to it. See "Creating the Network Map" on page 3-5 for a description.

Creating the Network Map

See Chapter 3, "Creating and Managing Network Maps" for a complete description of how to create a network map and configure the first switch on the network map.

Configuring Switch Parameters

To configure switch parameters:

1. Select the switch object and from the Misc menu, select NavisCore ⇒ Logon. Enter your operator password.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for your type of switch.
3. To configure switch parameters, choose Attrs... The Set Switch Attributes dialog box appears (see Figure 4-3).

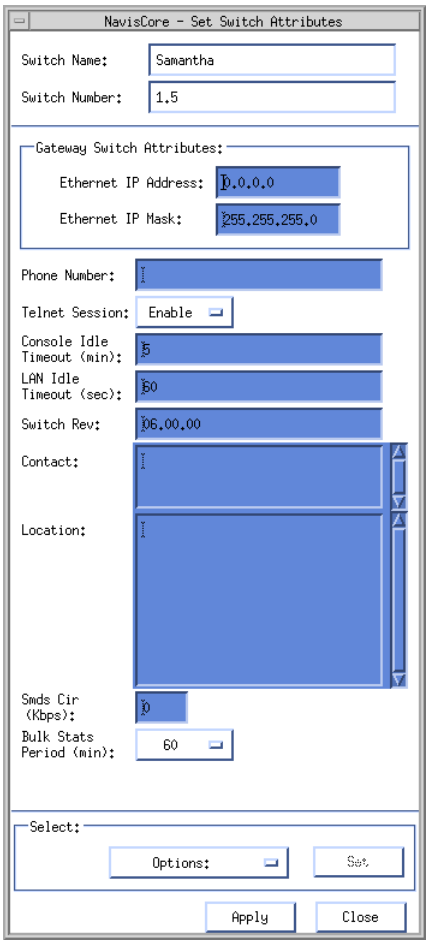


Figure 4-3. NavisCore - Set Switch Attributes Dialog Box

4. Complete the Gateway Switch Attributes fields as described in Table 4-1.

Table 4-1. Set Switch Attributes Fields (Gateway Switch)

Field	Action/Description
Ethernet IP Address	Enter the local IP address of the switch. This address is the external Ethernet address of the switch. See your network administrator if you do not know this address. ***Note**: You only need to enter the Ethernet IP address for the switch or switches that have an Ethernet connection and will communicate with the NMS via this connection.*
Ethernet IP Mask	Enter the in-band (Ethernet) IP mask for this switch. The default is 255.255.255.0.

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

Table 4-2. Set Switch Attributes Fields

Field	Action/Description
Phone Number	Enter the phone number of the contact person responsible for switch operations.
Telnet Session	Specify Enable (default) to allow the switch to connect to a remote terminal for troubleshooting purposes. Ascend recommends that you do not disable this function.
Console Idle Timeout (min)	Specify the time period (in minutes) that the console remains inactive before it is logged off. The default is 5 minutes.
LAN Idle Timeout (sec):	Specify the Idle Timeout interval, in seconds, for the Ethernet interface that connects the switch to the NMS. If the Ethernet interface receives no valid IP traffic during this period, the interface is marked as idle and will not be used for outbound traffic. Receipt of a valid IP packet restarts the Idle Timeout counter and reactivates the idle interface.
Switch Rev:	Displays the current switch-software revision level.
Contact	Enter the name of the contact person responsible for operating the switch.
Location	Enter the switch's physical location.

Table 4-2. Set Switch Attributes Fields (Continued)

Field	Action/Description
SMDS CIR (Kbps)	Enter the committed information rate (CIR), in Kbps, allocated to the SMDS virtual paths originating at the switch. See the *NavisCore SMDS Configuration Guide* for additional information.
Number of Power Supplies (CBX 500 only)	The number of power supplies located in the switch.

6. Choose Apply to set the parameters.
7. Choose Close to exit the dialog box.

Configuring the Processor Module

To configure the processor module, point to the processor-module slot on the switch back panel and double-click the left mouse button. The Set Card Attributes dialog box appears.

1. Complete the fields described in the appropriate table:
   - Table 4-3 for a control processor (B-STDX CP)
   - Table 4-4 for a switch processor (CBX 500 SP)
   - Table 4-5 for a node processor (GX 550 NP)

Table 4-3. Set Card Attributes Fields (CP Module)

Field	Action/Description
Redundant Slot ID (*Optional*)	To configure a redundant CP, select the redundant Slot ID 2. You must always configure the main CP in Slot 1. The default, NULL, indicates there is no redundant CP module installed.
Card Type	This read-only field automatically defaults to control processor.
Admin Status	Set this field as follows: *Up (default)* – This CP becomes fully operational when you start the switch. *Down* – This CP does not come online when you start the switch. This setting saves the configuration in the database but does not download it to the switch. Use this option when you run foreground diagnostics.

Table 4-3. Set Card Attributes Fields (CP Module) (Continued)

Field	Action/Description
Capability	Set this field as follows: *CP Basic* – This CP module has a black dip switch located on the front panel. It is often used in both the B-STDX 8000 and 9000 models. *CP Plus* – This CP module has a red dip switch located on the front panel. It has more memory than the CP Basic and can be used in either B-STDX model. This CP type is required for SMDS Billing. ***Note**: If you do not know the CP type and cannot physically view it, you can use the show card or show system console commands to retrieve this information. See the* NavisCore Console Command Reference *for a list of console commands.* The CP 30, 40, and 50 use a 260 or 520 MB internal disk and each CP supports a different amount of memory. For switch code versions 4.2 and higher, set this field as follows. For more information on installing these CP cards, see the *B-STDX 8000/9000 Hardware Installation Guide.* *CP 30* – This CP module replaces the CP Basic and has 16 MB IRAM. *CP 40* – This CP module replaces the CP Plus and has 64 MB memory for IP routing. *CP 50* – This CP module replaces the CP Plus and has 128 MB memory for IP routing.

Table 4-4. Set Card Attributes Fields (SP Module)

Field	Action/Description
Redundant Slot ID (*Optional*)	Select NULL if you have a non-redundant SP configuration. Select 2 if you have a redundant SP installed in the switch.
Card Type	Select one of the following: • Switch Processor 10 (Model 10) • Switch Processor 20 (Model 20) • Switch Processor 30 (Model 30) • Switch Processor 40 (Model 40)
Admin Status	Select one of the following: *Up (default)* – The SP module becomes fully operational when you start the switch. To become operational, the module gets its application code from the PCMCIA hard drive card, which resides in the SPA module. *Down* – The SP module does not come on-line when you start the switch. The configuration is saved in the switch configuration table, but is not downloaded to the switch. Use this option when running foreground diagnostics. *Maintenance* – The SP module does not receive the application code when you start the switch. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that is failing to boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.

Table 4-5. Set Card Attributes Fields (NP Module)

Field	Action/Description
Node Processor	
Redundancy	Select Stand Alone if you have a non-redundant NP configuration. Select Redundant if you have a redundant NP installed in the switch.
Admin Status	Select one of the following: *Up (Default)* – The NP module becomes fully operational when you start the switch. To become operational, the module gets its application code from the NP disk drive. *Down* – The NP module does not come on-line when you start the switch. The configuration is saved in the switch configuration table, but is not downloaded to the switch. Use this option when running foreground diagnostics. *Maintenance* – The NP module does not receive the application code when you start the switch. A module in this state runs only from boot code. This setting enables you to reset PRAM for a module that is failing to boot due to invalid PRAM. You can also use this option to troubleshoot a possible hardware problem.
Switching Fabric (SF) Module	
Redundancy	Select Stand Alone if you have a non-redundant SF configuration. Select Redundant if you have a redundant SF installed in the switch.
Oper Status	Displays the operational status of each SF module (SF1 and SF2) installed in the GX switch.
Timing Module (TM)	
Redundancy	Select Stand Alone if you have a non-redundant TM configuration. Select Redundant if you have a redundant TM installed in the switch.
Oper Status	Displays the operational status of each TM module (TM1 and TM2) installed in the GX switch.

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

- To use either of the external clock sources or the internal clock as the switch clock source, define the switch clock sources and clock source priorities as described in "Defining System Timing" on page 4-11.
- To use a BIO module's clock source as the switch clock source, you must configure one of the BIO module's physical ports as a clock source for the switch. Choose OK and see the *NavisCore Physical Interface Guide* for information regarding the physical port type you are using as the clock source.

Defining System Timing

The SP/NP system-timing function enables you to:

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

To view the configured system-timing options, see Chapter 2 in the *NavisCore Diagnostic and Troubleshooting Guide*. To define system-timing parameters:

1. From the Set Card Attributes dialog box (SP or NP module), choose the System Timing. The Set System Timing dialog box appears (see Figure 4-4).

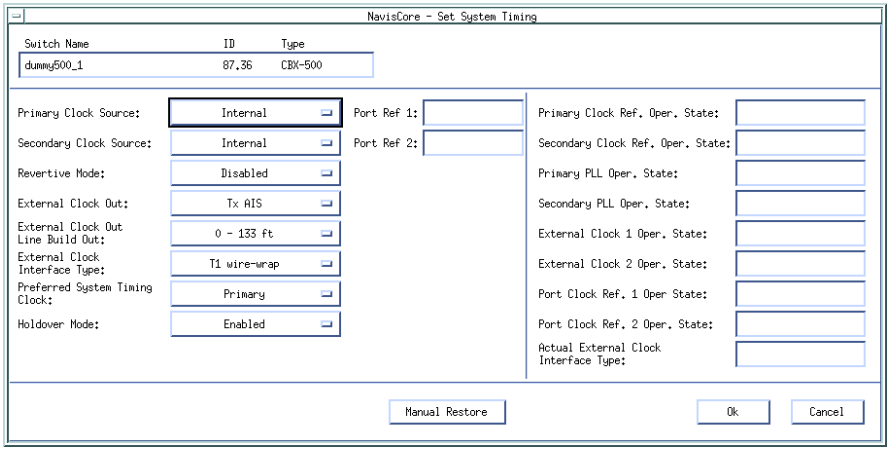


Figure 4-4. Set System Timing Dialog Box

2. Complete the fields described in Table 4-6.

Table 4-6. Set System Timing Fields

Field	Action/Description
Primary/Secondary Clock Source	Select a different option for both the Primary and Secondary clock sources. If the Primary source becomes unavailable, the Secondary source automatically takes control of system timing. Options include: *Internal* (default) – The switch uses the Stratum 3 clock on the SP/NP module as the primary (or secondary) clock source. *External Clock 1* – To use this option, you must connect an external clock source to the *primary external clock* connection on the SPA/NPA module (see your switch hardware installation guide for connection instructions). This connection is labeled "In 1." The switch uses this external clock as the primary (or secondary) system timing source. *External Clock 2* – To use this option, you must connect an external clock source to the *secondary external clock* connection on the SPA/NPA module (see your switch hardware installation guide for connection instructions). This connection is labeled "In 2." The switch uses this external clock as the primary (or secondary) system timing source. *Port Reference 1* – To use this option, first configure one of the physical ports on the switch as the Primary System Clock Source. The switch uses the incoming clock signal on the selected physical port as the primary (or secondary) system timing source. *Port Reference 2* – To use this option, first configure one of the physical ports on the switch as the Secondary System Clock Source. The switch uses the incoming clock signal on the selected physical port as the primary (or secondary) system timing source.
Revertive Mode	Select one of the following options: *Enabled* – If the switch loses the primary clock source, causing the secondary clock source to take over system timing, the system automatically reverts back to the primary clock source when it becomes available again. *Disabled* (default) – If the switch loses the primary clock source, the secondary clock source takes over system timing. However, the system will not automatically revert back to the primary clock source once it is restored. ***Note:*** *If you disable Revertive Mode, use the Manual Restore command on the Set System Timing dialog box to revert back to the primary clock source.*

Table 4-6. Set System Timing Fields (Continued)

Field	Action/Description
External Clock Out	Select one of the following options: *Tx AIS* (default) – In the event of system clock loss, the external clock output transmits an AIS signal. *Primary* – The external clock output references the clock that the switch uses as the primary source. *Secondary* – The external clock output references the clock that the switch uses as the secondary source. *Loopback ext1* – The clock that is wired to the external clock input #1 on the SPA/NPA module is fed directly to the external clock output jack.
External Clock Out Line Build Out	If the External Clock Interface Type is T1 wire-wrap, select a value for the External Clock Out Line Build Out field that matches the distance from the external clocking device. The default is 0 – 133 ft.
External Clock Interface Type	Select one of the following options: *T1 wire-wrap* (default) – The SP/NP accepts T1 timing inputs and provides T1 timing outputs. The signalling is D4 framed. *E1 BNC* – The SP/NP accepts E1 timing inputs and provides E1 timing outputs.
Preferred System Timing Clock	Select one of the following options: *Primary* – The switch uses the clock source specified in the Primary Clock Source field. *Secondary* – The switch uses the clock source specified in the Secondary Clock Source field. ***Note:*** *If the primary clock source becomes unavailable, the system automatically provides the secondary clock source to the I/O modules.*
Holdover Mode	Enables Stratum 3 system timing support. If you enable holdover mode, the system can continue to synchronize from a failed clock until a valid clock can be re-established. This feature provides an enhanced clock state controller for both primary and secondary clock recovery.

3. Choose OK to apply. The Switch Back Panel dialog box reappears.
4. To continue, configure the I/O modules in your gateway switch.

Configuring I/O Modules

Configure your I/O modules:

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

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

2. See the *NavisCore Physical Interface Configuration Guide* for instructions on how to configure each supported I/O module.
3. Configure I/O module attributes (if necessary) for your module.
4. Choose OK. When you finish configuring the necessary I/O modules, choose Close to return to the network map.

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

About Management Paths

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

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

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

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

Indirect Ethernet — This connection indicates that the NMS and the switch's Ethernet IP address are on two separate LANs and communicate via a gateway router(s). For this connection method, you enter both the NMS IP address and the associated gateway router IP address. Also, when you installed NavisCore, you entered a “static route” in the gateway router to specify how it is to reach the internal IP network address. This is the network number you specified in the Configuration dialog box in “Creating the Network Map” on page 4-4.

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

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

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

Management VPI/VCI — This connection is used when the NMS or IP host connects to the switch via an ATM router or network interface card (NIC). This is the preferred method if you only use the attached NMS or IP host to transfer information between the host and the local switch. You can use a management VPI/VCI connection to transfer information between the host and remote switch(es); however, using this method to transfer large amounts of information can negatively affect the local switch.

Setting the Management Path

To set the Management path:

1. On the network map, select the switch to connect to the NMS.
2. From the Administer menu, select Ascend Parameters ⇒ Set All Management Paths. The Set All Management Paths dialog box appears (see Figure 4-5).

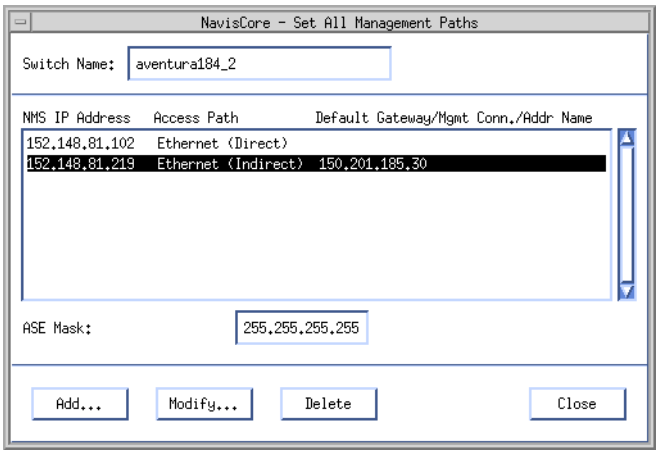


Figure 4-5. Set All Management Paths Dialog Box

3. Choose Add to create a new management path. The Add Management Path dialog box appears (see Figure 4-6).

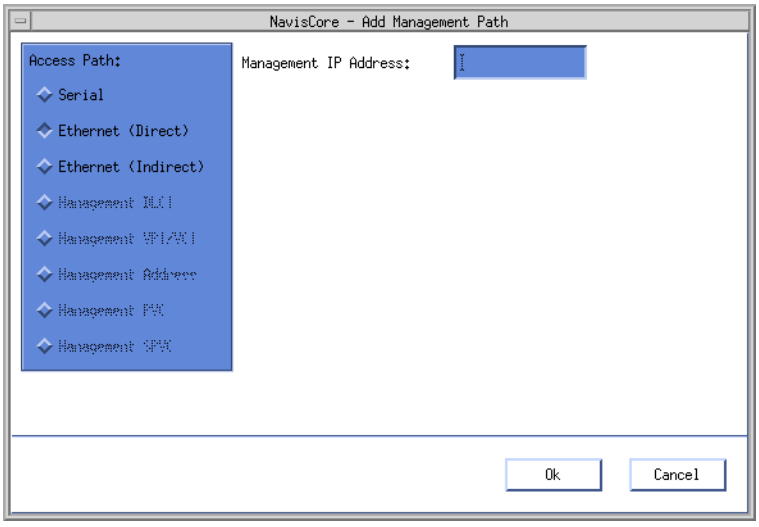


Figure 4-6. Add Management Path Dialog Box (Direct Ethernet)

4. Complete the Add Management Path dialog box fields, as follows:
   a. In the Access Path field, select the connection type you used to connect the NMS to the switch.
   b. Enter the NMS IP address. This should be the IP address of the SPARCstation.
   c. The fields that appear depend on the connection type you select.
   d. Choose OK to save your changes or Cancel to exit.
5. Choose Close to return to the network map.

Generating and Downloading the Configuration File

You now need to initialize the switch to generate an ASCII text file. This text file contains the basic parameters needed to activate the switch. See Appendix A, "Downloading the Configuration" for instructions.

Configuring the Second Switch on the Network Map

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

- ☑ Set up the NMS SPARCstation and gateway switch as described in the "Adding an Ascend Switch Object to the Map" on page 3-13. The gateway switch object should be green on the map.
- ☑ Install the physical connection for creating a trunk line between this switch and the gateway (or any active switch you can configure as a hop between this switch and the gateway). See the appropriate switch hardware installation guide.

The following procedure describes the basic steps required to get your second switch (and any other switches) synchronized and communicating with each other and the NMS. To do this, you must add a second switch to the same map, configure the physical and logical port, and define a trunk connection between the two switches.

1. If necessary, start the NMS and access NavisCore.
2. From the Misc menu, select NavisCore ⇒ Logon.
3. From the Map menu, select Maps ⇒ Open/List Maps and select the desired map. Choose OK.
4. To add the second switch to the map, See "Adding an Ascend Switch Object to the Map" on page 3-13. When you finish, the network map should display the second switch, which is "unmanaged" (wheat color).
5. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
6. To configure the process module, double-click the left mouse button on the module slot. Verify that the Admin Status is Up and configure the module as described in Table 4-3 on page 4-7.
7. Choose OK. The Switch Back Panel dialog box reappears.
8. To configure the first I/O module, double-click on its slot. Refer to the *NavisCore Physical Interface Configuration Guide* for a detailed description of how to configure each supported I/O module.
9. Choose OK. Repeat Step 8 for each I/O module in this switch. When you finish setting the card attributes, choose Close to return to the network map.

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

Configuring a Trunk Connection

This section describes how to configure a direct-line trunk connection between the first switch (the *gateway switch*) and the second switch in a new Ascend network. To configure a direct-line trunk, you must first configure the physical port and logical port on the gateway switch and the second switch. Figure 4-7 shows an example of a direct-line trunk connection.

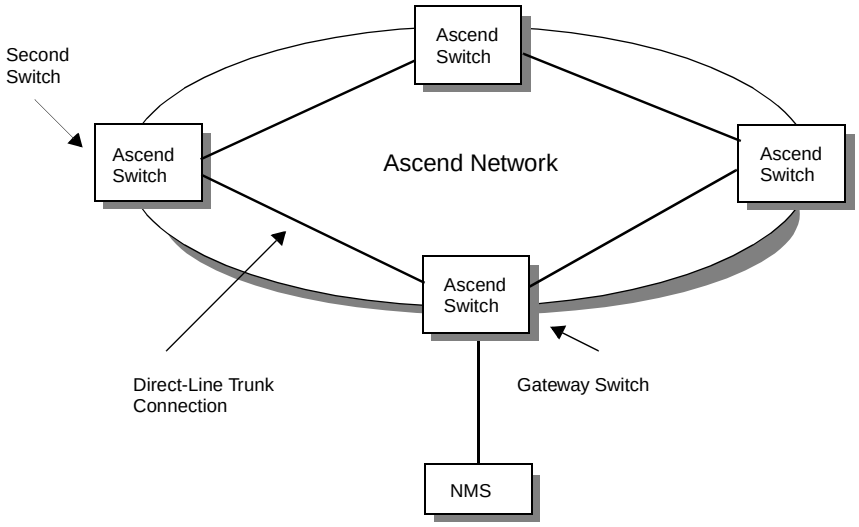


Figure 4-7. Direct-Line Trunk Connection

Configuring the Trunk's Physical Port

To configure the physical port:

1. On the network map, select the *gateway switch* and from the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. To configure a physical port, select the appropriate I/O module. Double-click on the port to use for the trunk connection. The Set Physical Port Attributes dialog box appears.
3. Specify the trunk connection's physical port attributes as described in the *NavisCore Physical Interface Configuration Guide*.
4. Choose Apply to enter your selections.

Configuring the Trunk's Logical Ports

To configure the logical port settings for the trunk:

1. Choose the Logical Port button on the Set Physical Port Attributes dialog box. The Set All Logical Ports dialog box appears.
2. Choose Add. The Add Logical Port dialog box appears.
3. Configure the logical port as described in one of the following NavisCore configuration guides:
   - *NavisCore Frame Relay Configuration Guide*
   - *NavisCore ATM Configuration Guide*
   - *NavisCore IP Configuration Guide*
   - *NavisCore ISDN Configuration Guide*
   - *NavisCore SMDS Configuration Guide*
4. Choose Close, then Cancel to return to the network map.
5. Repeat the "Configuring the Trunk's Physical Port" and "Configuring the Trunk's Logical Ports" to configure a physical and logical port for the switch (second switch) at the other end of the trunk connection.

Defining the Trunk Configuration

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

1. From the Administer menu, select Ascend Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears.
2. Choose Add. The Select End Logical Ports dialog box appears. Choose Add. The Select Logical Ports dialog box appears.
3. Complete the required dialog box fields described in Table 4-7 for both Logical Port 1 and Logical Port 2.

Table 4-7. Select Logical Port Fields

Field	Action/Description
Switch (Name, ID)	Select a switch for each endpoint. The dialog box displays the parameters for the selected switch.
LPort (Name, Slot, PPort, Inf)	Select the same trunk logical port type for each endpoint. This field also displays the physical port number and I/O slot (number) in which the module resides. **Note**: Review the LPort Bandwidth field for each endpoint to make sure the bandwidth is the same.
LPort Type	Displays the configured logical port type.
LPort BW (kbps)	Displays the bandwidth configured for the logical port. This must be the same for both endpoints.
LPort ID	Displays the logical port number.

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

5. Complete the fields described in Table 4-8.

Table 4-8. Add Trunk Fields

Field	Action/Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk. You use this same name when you create the trunk connection (see your service configuration guide for more information).
Area ID	The ID of the OSPF area to which the trunk belongs.
Subscription Factor (%) (Not for ATM services)	The trunk oversubscription factor percentage enables you to optimize the aggregate CIR you can configure on the trunk, by allowing you to oversubscribe bandwidth on 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 details on this parameter, see your service configuration guide.
Admin Cost (1-65534)	Assign an administrative cost value of 1 to 65534. The lower the admin cost of the path, the more likely that OSPF will select it for circuit traffic. The default admin cost value is 100. For details on this parameter, see your service configuration guide. ***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. See page 5-16 for information about reroute tuning. You cannot use trunk admin cost to disable a trunk.*
Keep Alive Error Threshold (3-255)	You can configure the keep-alive threshold for a value between 3 and 255 seconds. The default is 5 seconds. For details on this parameter, see your service configuration guide. ***Note**: Service is disrupted if you change this value after the trunk is online.*

Table 4-8. Add Trunk Fields (Continued)

Field	Action/Description
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – The trunk can carry network management traffic, user traffic, and OSPF address distribution. *Mgmt Only* – The trunk can carry *only* network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & User* – The trunk can carry network management traffic and user traffic. ***Note**: To calculate the most efficient route for network management traffic, OSPF uses Trunk Admin Cost. OSPF ignores trunk bandwidth when it selects a route for management traffic; management traffic can use a negative bandwidth trunk.*
Virtual Private Network	Select a virtual private network (VPN) if applicable. The default is Public.
Static Delay	Defaults to Maintain.
Trunk Type	Displays *Normal*, *Primary*, or *Backup*. Normal is a common trunk. Primary indicates that the trunk has a backup for fault tolerance. Backup indicates that it is the backup trunk (when failure occurs on the primary trunk). If you select Backup, complete Step 7.

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

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

   Switch Initializing the Call Setup – Select the name of the switch initializing the call setup.
8. Choose Close to return to the network map.

Adding a Trunk Line Connection

To add the trunk line graphic to the network map:

1. From the Edit menu, select Add Connection. The Add Connection dialog box appears (see Figure 4-8).

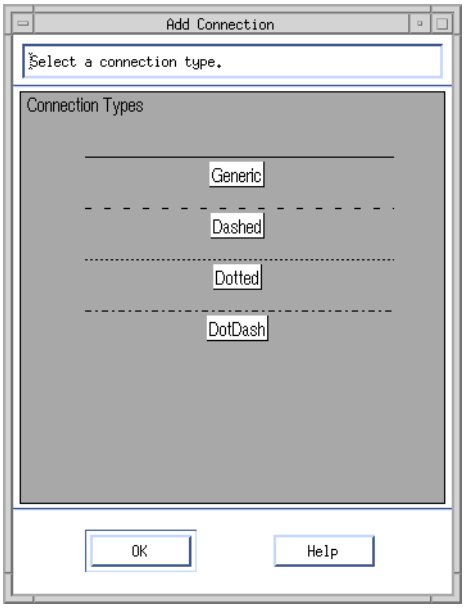


Figure 4-8. Add Connection Dialog Box

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

   The Add Object dialog box appears (see Figure 4-9).

Figure 4-9. Add Object Dialog Box

4. Complete the fields described in Table 4-9.

Table 4-9. Add Object Fields

Field	Action/Description
Symbol Type	Displays the type of connection you are adding to the map.
Label	Enter the trunk name you specified on the Add Trunk dialog box (see page 4-22).
Display Label	Select Yes to have the label appear below the object on the network map. Select No if you do not want the label displayed.
Behavior	Select Explode to create the basic 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 (see Figure 4-10).

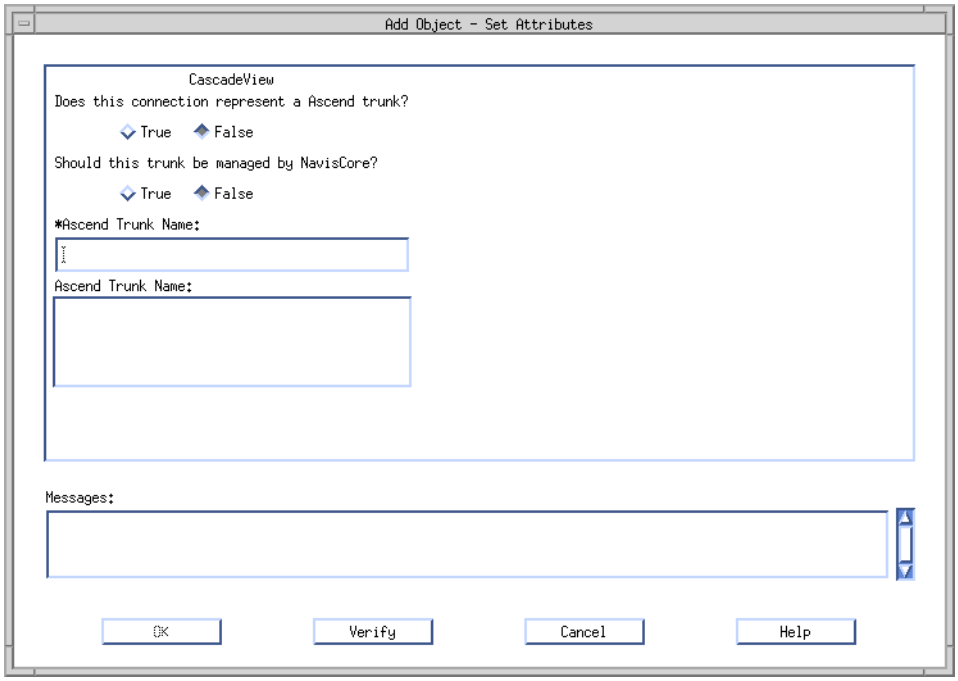


Figure 4-10. Add Object - Set Attributes Dialog Box

5. Complete the fields described in Table 4-10.

Table 4-10. 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 name you assigned to the trunk. This should be the same name you entered for the label in the Add Object dialog box on page 4-25.

6. Choose Verify to confirm your selections.
7. Choose OK to return to the Add Object dialog box.
8. Choose OK to return to the network map. The trunk line appears between the two switches on the network map.

Downloading the Configuration File to the Second Switch

Download the configuration file, and synchronize the second switch. See Appendix A, "Downloading the Configuration" for instructions.

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

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

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

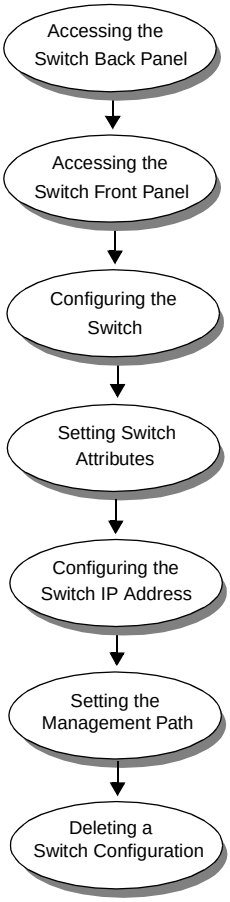
If necessary, log in as root and modify the *.profile* or *.cshrc file*. Then log out of NavisCore and log in again to restart the system.

5

Setting Switch Parameters

Once you have created a network map and defined the first switch in NavisCore, you can set the switch parameters. This chapter describes the front and back panels of a switch and how to set various switch parameters. These steps are the same for all Ascend switches.

This chapter describes the following topics and tasks:



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

- ☑ Create a network map (page 3-5)
- ☑ Create a subnet ID (page 3-10)
- ☑ Add an Ascend switch to the network map (page 3-13)

Accessing the Switch Back Panel

Figure 5-1 shows a graphical representation of a switch back panel. From the switch back panel, you can configure each I/O module in the switch. When the modules are configured, you can then select each physical port on the module to configure both physical and logical port attributes. See the *NavisCore Physical Interface Configuration Guide* for physical port configuration information. See the "Related Documents" section in the About Guide for a list of the appropriate NavisCore service configuration guides that contain logical port configuration information.

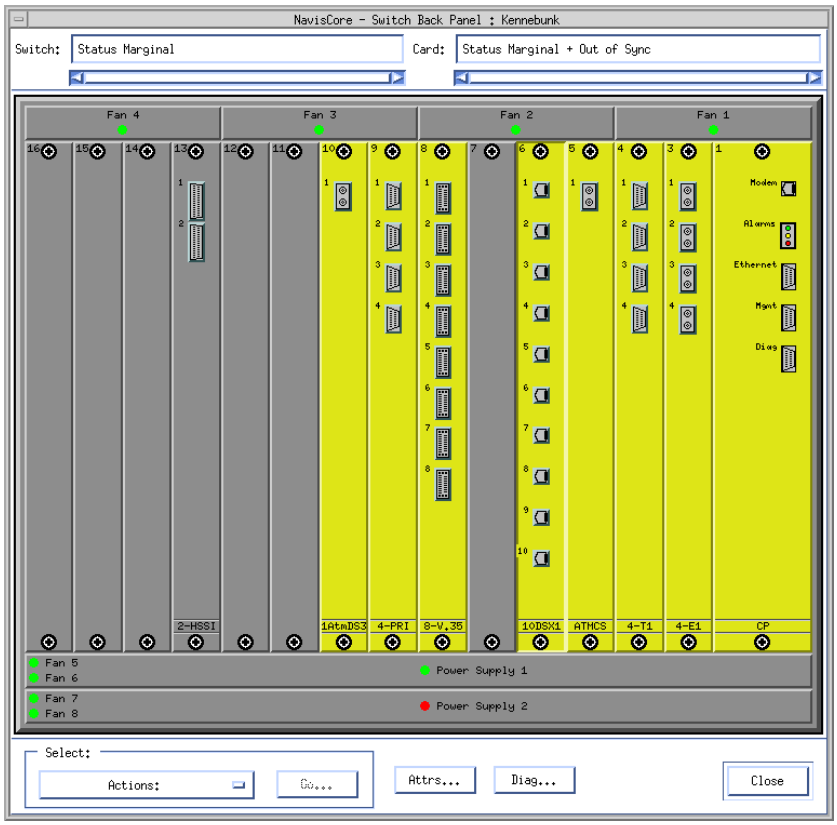


Figure 5-1. Switch Back Panel Dialog Box (B-STDX)

Table 5-1 describes the buttons on the switch back panel dialog box.

Table 5-1. Switch Back Panel Buttons

Button	Description
Actions Option Menu	Displays a list of actions you can perform (Described in detail in Table 5-2).
Go	Confirms the selected action.
Attrs	Enables you to set switch, module, physical, and logical port attributes.
Diag	Enables you to run foreground and background diagnostics.
PRAM	Ascend switches use battery backed-up PRAM to store switch configuration files. When you download a configuration file from the NMS to the switch, the NMS generates an initialization script. This file contains the SNMP SET commands that control the switch's configuration. Use the PRAM button to access one of the following functions: *Synchronize PRAM* – If the switch already contains a configuration file, sends an updated binary image of the configuration to the selected I/O module. *Erase PRAM* – Clears a configuration file from PRAM. Use Erase PRAM before you replace an existing configuration file. *Upload PRAM* – Uploads the switch configuration file stored in PRAM to the NMS. This feature is supported for Pports, Lports, and SMDS services. *Generate PRAM* – Generates SET commands to configure PRAM but does not upload the switch configuration file to the NMS. This option enables you to view the file before uploading it.

The Actions option menu button displays a list of functions that you can select in conjunction with the Go button. Although the Actions list is similar from switch type to switch type, some selections will vary.

Table 5-2. Actions Option Menu Selections

Function	Description
Set Switch Attributes	Enables you to set the switch attributes, including the local IP address of the switch. See the "Switch Back Panel Dialog Box (B-STDX)" on page 5-2.
View Front Panel	Displays the front panel of the switch. See "Switch Front Panel Dialog Box" on page 5-6 for more information.
Coldboot	Restarts the switch as if it were powered off, then on.
Warmboot	Resets the selected module. As it reboots, all physical ports, logical ports, and PVCs on the module stall for approximately 20-30 seconds.
Switch to Redundant Unit	Passes operation changes from an active I/O module to a redundant standby module. See the *NavisCore Diagnostic and Troubleshooting Guide* for more information.
View Port Redundancy	Displays physical port redundancy pairings.
ISDN Status (Not for ATM Services)	Displays the Show ISDN Status dialog box. This dialog box shows the call status and alarm status of all 4 ports on an ISDN module. This option is enabled when you select a slot containing an ISDN module.
Erase Standby	Erase a standby CP, SP, or NP module.
Enable Pop-up Help	Enables the back-panel Help/Info pop-up menu for quick module and port statistics.
Disable Pop-up Help	Disables the back-panel module and port pop-up Help.

Switch Back-Panel Status LEDs

Table 5-3 describes the operating status indicators of fans and power supply units.

Table 5-3. Back Panel Status LEDs

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

Switch Back-Panel Port Colors

Table 5-4 describes the physical port colors, which indicate port operational status.

Table 5-4. Back Panel Port Colors

Port Color	Indicates
Gray	Port is unknown. This condition usually occurs if the configuration has not been downloaded or if the NMS and PRAM configurations do not match.
Green	Port is accurately configured and operational.
Red	Port is configured but has an admin status of Down and/or an operational status of Down or no logical port has been configured.
Cyan	Port is configured but one or more (but not all) logical ports have an Admin Status or an Operational Status of Down.

Switch Back-Panel Module Colors

Table 5-5 describes the I/O module colors, which indicate operational status.

Table 5-5. Back Panel Module Colors

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

Accessing the Switch Front Panel

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

To display the NavisCore - Switch Front Panel dialog box, choose View Front Panel from the Actions Option menu and select Go. The Switch Front Panel dialog box appears (see Figure 5-2).

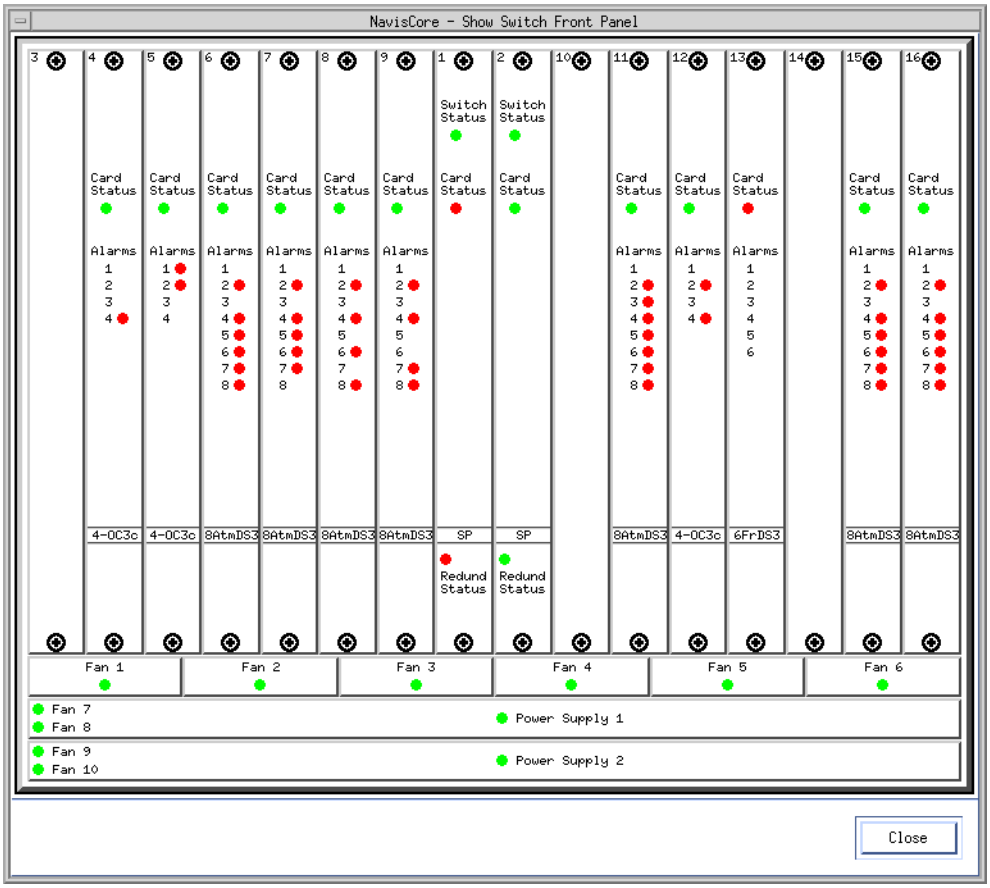


Figure 5-2. Switch Front Panel Dialog Box

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

Switch Front-Panel Status LEDs

Table 5-6 describes the front-panel status LED indicators.

Table 5-6. Switch and Module Status LEDs

LED Color	Indicates
Green	Module is operational.
Red	Module is not operational.
Blue	Blue LEDs are used on the CBX 500 switch processor, the GX 550 node processor, the STDX 3000/6000 packet processor, and the B-STDX 8000/9000 control processor. For all switches, blue LEDs are also used on the fan and power supply units. Blue indicates that the NMS cannot access the unit for status.
Yellow	Switch is “out of sync” or the switch reports a module-type mismatch or marginal state.

Switch Front-Panel Alarm Status LEDs

The number and type of alarms differ depending on the type of module. See Table 5-7 for a description of alarm LEDs.

Table 5-7. Alarm Status LEDs

LED Color	Indicates
No LED	No alarm conditions.
Red	Red alarm condition.
Yellow	Yellow alarm condition.

Before You Begin

Before you configure the switch, you need to know the following information:

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

  more /opt/CascadeView/etc/cascadeview.cfg

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

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

Step 1. (Optional) Set up an authentication domain.

Step 2. Set the switch attributes.

Step 3. Define an additional NMS, if necessary (see page 5-13).

Step 4. Define the circuit reroute tuning parameters (see page 5-16).

Step 5. Define the console authentication parameters (see page 5-17).

Step 6. Configure the IP address and access attributes for the NMS or IP host (see page 5-23).

Step 7. Configure the processor module (see the *NavisCore Physical Interfaces Configuration Guide*).

Setting Switch Attributes

To set the switch attributes:

1. Start NavisCore and access the network map.
2. Select the switch object and from the Misc menu, select NavisCore ⇒ Logon. Enter your operator password.
3. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for the selected switch (see Figure 5-1 on page 5-2).
4. To configure switch parameters, choose the Attrs button. The NavisCore - Set Switch Attributes dialog box appears (see Figure 5-3).

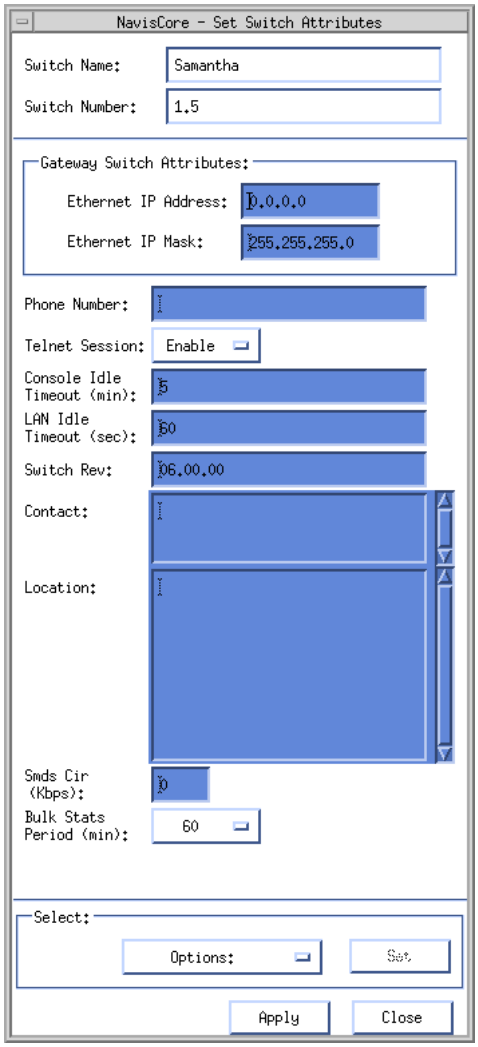


Figure 5-3. Set Switch Attributes Dialog Box

This dialog box displays the switch name (assigned to the switch when you added the object to the map) and the unique number of the switch (switch number). If this switch belongs to a cluster subnet, the switch number increments according to the Cluster ID. See "Creating a Cluster" on page 4-12 for more information.

5. Do one of the following:

- If this is a gateway switch, complete the Gateway Switch Attributes fields in the Set Switch Attributes dialog box as described in Table 5-8.
- If this is not a gateway switch, proceed to Step 6.

Table 5-8. Set (Gateway) Switch Attributes Fields

Field	Action/Description
Ethernet IP Address	Enter the local IP address of the switch. This address is the external Ethernet address of the switch. See your network administrator if you do not know this address. ***Note**: You only need to enter the Ethernet IP address for the switch or switches that have an Ethernet connection and will communicate with the NMS via this connection.*
Ethernet IP Mask	Enter the in-band (Ethernet) IP mask for this switch. The default is 255.255.255.0.

6. Complete the fields described in Table 5-9.

Table 5-9. Set Switch Attributes Fields

Field	Action/Description
Phone Number	Enter the phone number of the contact person responsible for switch operation.
Telnet Session	Specify Enable (default) to allow the switch to connect to a remote terminal connection for troubleshooting purposes. Ascend recommends that you do not disable this function.
Console Idle Timeout (min)	Specify the time period (in minutes) that the console remains inactive before it is logged off. The default is 5 minutes.
LAN Idle Timeout (min):	Specify the Idle Timeount interval, in seconds, for the Ethernet interface that connects the switch to the NMS. If the Ethernet interface receives no valid IP traffic during this period, the interface is marked as idle and will not be used for outbound traffic. Receipt of a valid IP packet restarts the Idle Timeout counter and reactivates the idle interface.
Switch Rev:	Displays the current switch-software revision level.

Table 5-9. Set Switch Attributes Fields (Continued)

Field	Action/Description
Contact	Enter the name of the contact person responsible for switch operations.
Location	Enter the switch's physical location.
SMDS Cir (Kbps) (9000 only):	Enter the committed information rate (CIR), in Kbps, allocated to the SMDS virtual paths originating at the switch. See the *NavisCore SMDS Configuration Guide* for additional information.
Number of Power Supplies? (CBX 500 only)	Enter the number of power supplies.
Options: (menu)	Lists additional attributes you can configure. See Table 5-10 for information.

Table 5-10 describes the additional switch attributes that you can set through the Options menu.

Table 5-10. Options Pull-Down Menu Features

Option	Action/Description
NMS Entries	(Optional) Select this option to define additional NMS and continue with "Defining Additional Network Management Stations" on page 5-13.
Tuning	(Optional) Select this option to define parameters that enable the NMS to balance circuits between switches. See "Defining Circuit Reroute-Tuning Parameters" on page 5-16 for more information.
Accounting	(Optional) Select this option to define parameters that enable, disable, and calculate PVC and SVC accounting. See the *NavisXtend Accounting Server Administrator's Guide* to configure this parameter.
Clock Sources	(Optional) Select this option to define the clock source on an ATM CS or ATM IWU module. You must first configure an ATM CS or ATM IWU module in the switch before you set the clock source (see the *NavisCore Physical Interface Configuration Guide* for more information).

Table 5-10. Options Pull-Down Menu Features

Option	Action/Description
Console Authen	*(Optional)* Select this option to set password protection for the switch, and continue with "About Console Authentication" on page 5-17. Console authentication allows you to assign a password (other than "cascade") to each switch.
Bulk Stats	(*Optional*) Select this option to access switch attributes for ATM bulk statistics. See the *NavisXtend Bulk Statistics Collector User's Guide*.
RIP Configuration	(*Optional*) Select this option to configure RIP parameters for a switch running IP Navigator. See the *NavisCore IP Configuration Guide* for more information.
Trap Config	(*Optional*) Select this option to clear contact alarm relays that are used to notify you of switch malfunctions. You can also use this function to disable the dry contact alarm relay function for this switch. See the *NavisCore Diagnostics and Troubleshooting Guide* for information about these alarms.
Time Server	(*Optional*) Select this option to specify a reference time server(s) to be used as a clock synchronization source for the switches in your network. See "Configuring Time Servers" on page 5-21 for more information.
Set Switch Time	(*Optional*) Select this option to configure the switch's time.
Billing	*(Optional)* Select this option if you are using the Ascend Billing feature. See the *SMDS Billing System Administrator's Guide* for more information.

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

Defining Additional Network Management Stations

Ascend switches support a maximum of 256 NMS entries and 256 NMS paths on a per node basis. Through the NMS Entries option, you can configure additional NMS workstations for read/write or read only access to the same switch. Through NMS workstations, you can communicate with switches on the network via SNMP commands.

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

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

To define an additional NMS:

1. From the Set Switch Attributes dialog box (Figure 5-3 on page 5-9), choose NMS Entries. The Set NMS Entries dialog box appears, displaying the current NMS entries as shown in Figure 5-4.

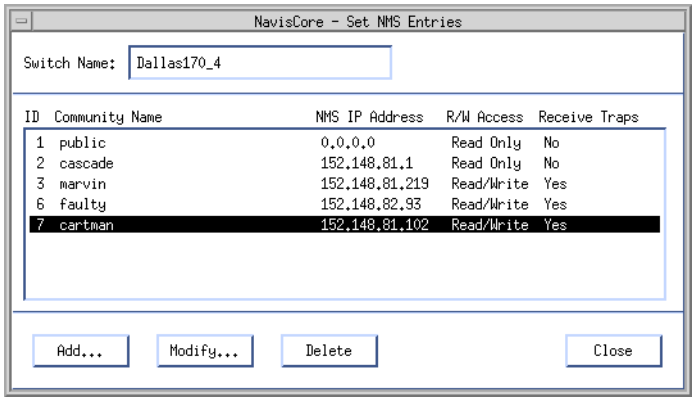


Figure 5-4. Set NMS Entries Dialog Box

2. Choose Add. The Add NMS Entry dialog box appears (see Figure 5-5).

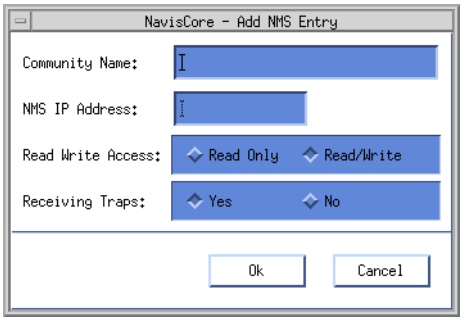


Figure 5-5. Add NMS Entry Dialog Box

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

Table 5-11. Add NMS Entry Fields

Field	Action/Description
Community Name	Enter the community name. ***Note**: If you need to modify the community name, you must first change the name from this dialog box and then edit the value* CV_SNMP_READ_WRITE_ COMMUNITY, *in the cascadeview.cfg file.*
NMS IP Address	Enter the NMS IP address for the target NMS workstation.
Read Write Access	Select the access rights for this NMS. *Read Only* – Enables you to monitor network functions from this NMS. *Read/Write* – Enables you to monitor and configure network maps from this NMS.
Receiving Traps	Select no to prevent the NMS from receiving traps. This option is on by default. Trap alarm conditions notify the operator of events taking place on the switch.

4. Choose OK to set the parameters. Repeat Step 1 through Step 3 for each NMS you want to add. The Set NMS Entries dialog box reappears with the new NMS confirmation.
5. (*Optional*) Choose Modify to modify an NMS entry or Delete to delete an NMS entry.

About Reroute Tuning

The *Reroute Tuning* feature enables the switch to rapidly redistribute permanent virtual circuits (PVCs) across trunks, based on OSPF updates and cost metrics. In large networks with thousands of PVCs, rerouting circuits while re-establishing a trunk is very time-consuming.

The Tuning option enables you to tune the rate of reroute requests per switch by defining the number of reroute requests during a single reroute batch request. You can also set the time delay (in seconds) that the switch waits between each batch request.

When you define individual circuits, you must enable the Reroute Balance parameter for circuits to benefit from the tuning parameters you define for a switch.

Load balancing enables the switch to route a circuit to a path that provides more bandwidth than the current path. You can select a load-balancing algorithm that configures the switch to aggressively search for an alternate path with greater bandwidth.

Load Balancing Example

If a switch has four modules, each with 50 PVCs, and you set the reroute count to 5 circuits and the reroute delay to 50 seconds, the switch performs a batch reroute consisting of the first five circuits on each module (for a total of 20 circuits). The switch then waits 50 seconds before it begins to reroute the next batch of 20 circuits.

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

Defining Circuit Reroute-Tuning Parameters

To set the tuning parameters:

1. From the Set Switch Attributes dialog box (Figure 5-3), choose Tuning. The Set Switch Tuning Attributes dialog box appears (see Figure 5-6).

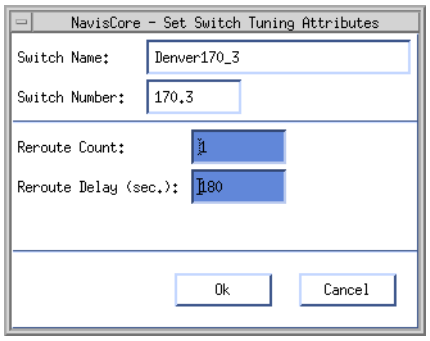


Figure 5-6. Set Switch Tuning Attributes Dialog Box

2. Complete the fields described in Table 5-12.

Table 5-12. Set Switch Tuning Attributes Fields

Field	Action/Description
Reroute Count	Enter a value between 0 and 64. The reroute count specifies the number of circuits from each module that can issue reroute requests in a single batch. The default is 1 circuit.
Reroute Delay	Enter a value between 1 and 32767. The reroute delay represents the time delay (in seconds) that each module in the switch waits between reroute batch requests. This parameter controls the rate at which each module polls the virtual circuits for a better route. The default value of 188 seconds is a very conservative setting for normal operation.

3. Choose OK to return to the Set Switch Attributes dialog box.
4. Choose Apply to set the parameters and choose Close to exit the dialog box.

About Console Authentication

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

Setting Up a RADIUS Server

To enable RADIUS authentication, you must have an active RADIUS Server that the switch can reach through the user datagram protocol (UDP) or IP. If you cannot reach the RADIUS Server when you log on to the switch console port, use the shared-secret password for the login name and login password. (You also use the shared-secret password for console debug mode.)

The RADIUS server's database must contain the following information:

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

Adding an Authentication Domain

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

To add the authentication domain and configure the RADIUS server parameters:

1. Select a switch and from the Administer menu, select Ascend Parameters ⇒ Set Authentication Domains. The Set All Authentication Domains dialog box appears (see Figure 5-7).

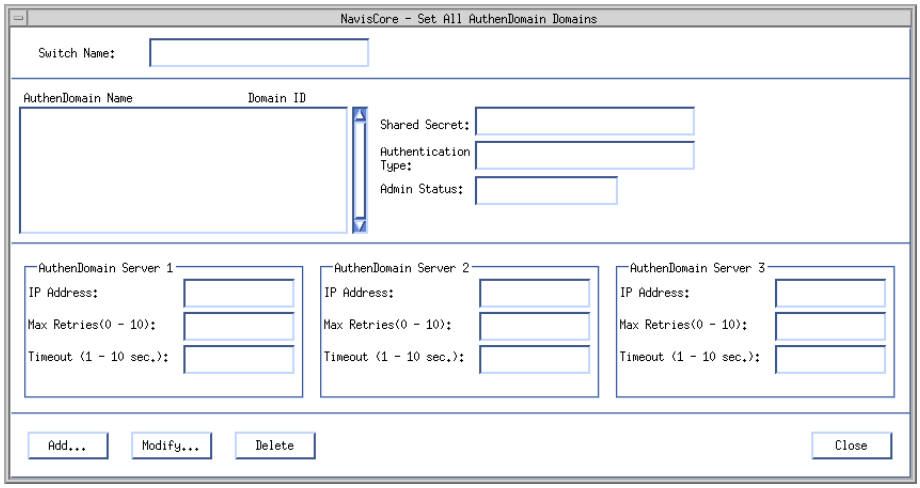


Figure 5-7. Set All Authentication Domains Dialog Box

2. Choose Add. The Add Authentication Domain dialog box appears (See Figure 5-8).

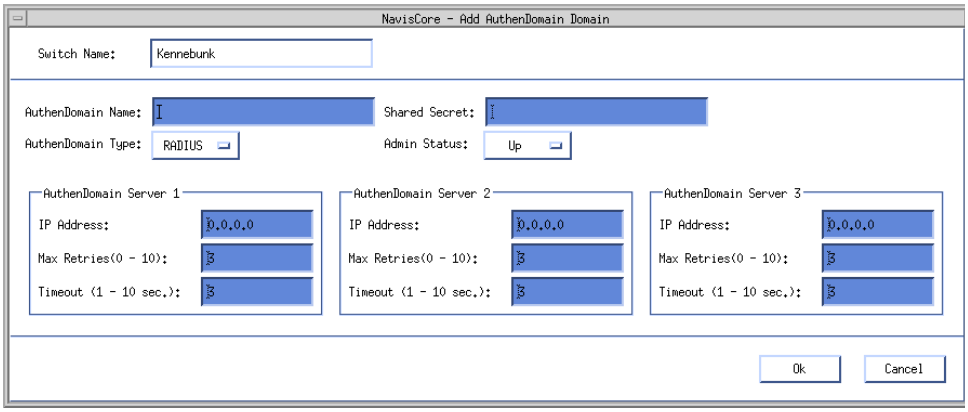


Figure 5-8. Add AuthenDomain Dialog Box

3. Complete the fields described in Table 5-13.

Table 5-13. Add AuthenDomain Fields

Field	Action/Description
AuthenDomain Name	Enter an alphanumeric name (up to 32 characters) for this domain.
AuthenDomain Type	Defaults to RADIUS and cannot be changed.
Shared Secret	Enter an alphanumeric shared secret (password) for this switch and all RADIUS Servers in this domain.

Table 5-13. Add AuthenDomain Fields (Continued)

Field	Action/Description
Admin Status	Set the Admin Status to Up to allow immediate access. Set the Admin Status to Down to disable the server. This does not disable console authentication.

4. Complete the AuthenDomain Server fields for Server 1, 2, and 3 as described in Table 5-14.

Table 5-14. AuthenDomain Server Fields

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

5. Choose OK to set the authentication parameters. The Set All AuthenDomain dialog box reappears.
6. Choose Close to return to the network map.
7. Enable the authentication parameter described in "Configuring Console Authentication" on page 5-20.

Configuring Console Authentication

On the Set Switch Attributes dialog box, you can access the Console Authentication function to enable and disable authentication on a switch.

To enable the authentication parameters:

1. From the Set Switch Attributes dialog box options menu (see Figure 5-3 on page 5-9), choose *Console Authen*. The Console Authen dialog box appears (see Figure 5-9).

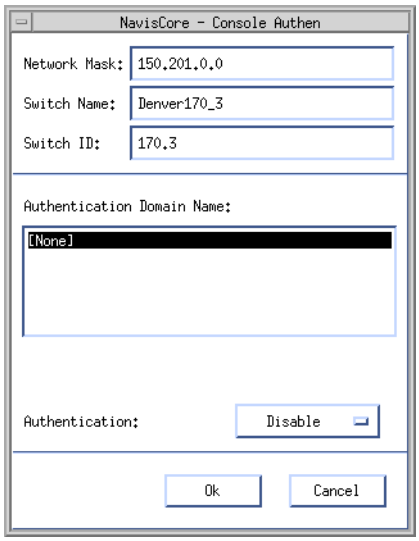


Figure 5-9. Console Authen Dialog Box

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

2. Select a domain from the list.
3. Set the Authentication parameter to Enable or Disable (default).
4. Choose OK to set the authentication parameters. The Set Switch Attributes dialog box reappears.

Configuring Time Servers

NavisCore and the Network Timing Protocol (NTP) enable you to specify from 1 to 3 reference time servers. A reference time server is used as a clock-synchronization source for the switches in your network.

Since a reference time server is not required and not all switches have configued reference time servers, you should still use a nightly **cron** job to set all the switch clocks. When modifying or adding a reference time server, the time sent to the server will be the time on the NMS workstation.

To configure reference time servers:

1. From the NavisCore - Set Switch Attributes dialog box options menu (Figure 5-3), choose Time Server. The Configure Reference Time Servers dialog box appears (see Figure 5-10).

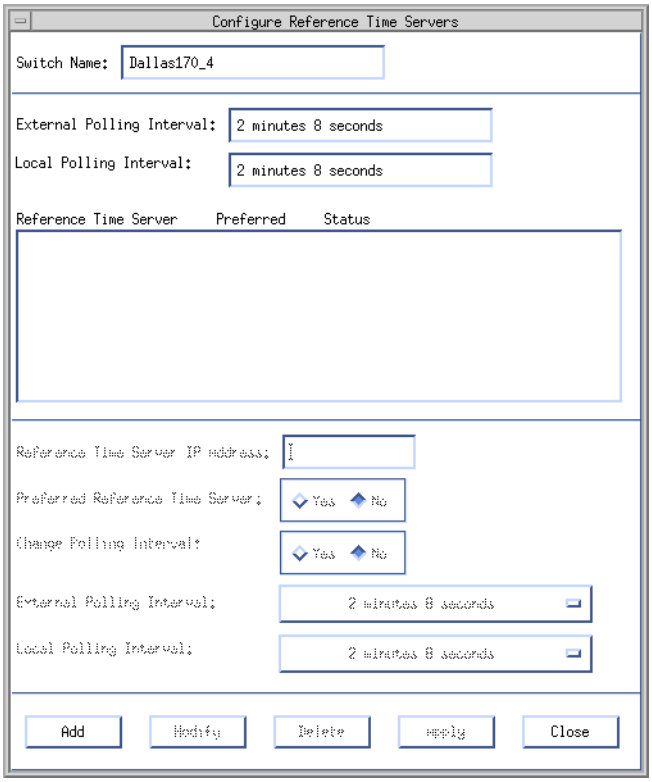


Figure 5-10. Configure Reference Time Servers Dialog Box

2. Choose Add. The Add Reference Time Server dialog box appears (see Figure 5-11).

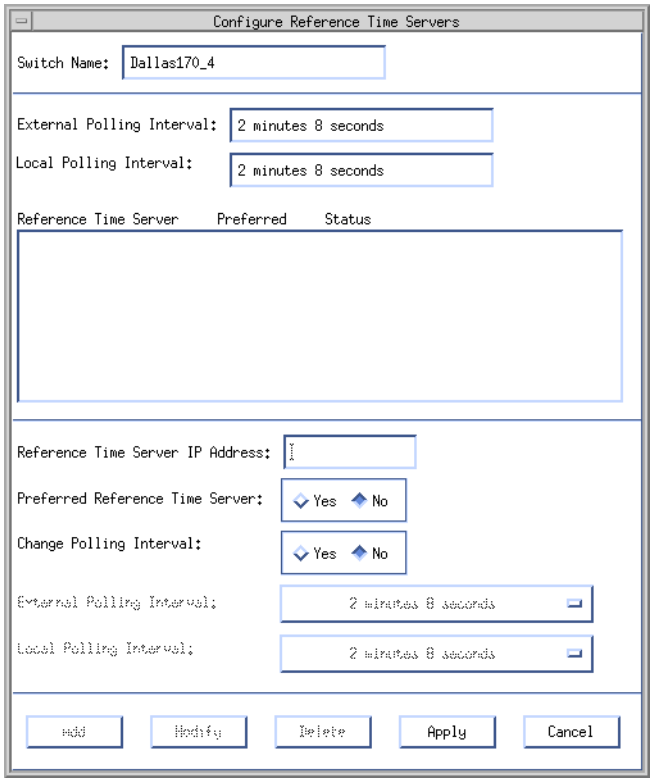


Figure 5-11. Add Reference Time Server Dialog Box

3. Complete the fields described in Table 5-15.

Table 5-15. Reference Time Server Fields

Field	Action/Description
Reference Time Server IP Address	Enter the IP address of the reference time server.
Preferred Reference Time Server	Select yes to make this server the preferred reference time server. If you do not select a preferred reference time server, the switch will select one for you.
Change Polling Interval	Select yes to change the polling interval. Doing so will enable the external and local polling intervals.
External Polling Interval	Select the rate (in seconds) at which each individual reference time server will be polled. This setting applies to all reference time servers.

Table 5-15. Reference Time Server Fields (Continued)

Field	Action/Description
Local Polling Interval	Select the rate (in seconds) at which each I/O module and redundant CP/SP module polls the active CP/SP for time. This setting applies to one switch.

4. Choose Apply. Repeat steps 1 through 4 for each reference time server.
5. (*Optional*) Choose Modify to modify a reference time server entry, or Delete to delete a reference time server entry.

Deleting a Switch Configuration from the Database

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

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

Step 1. Delete all PVCs defined for the switch.

Step 2. Delete all trunk connections for the switch.

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

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

Step 5. Delete the switch icon from the map.

Configuring Processor and I/O Modules

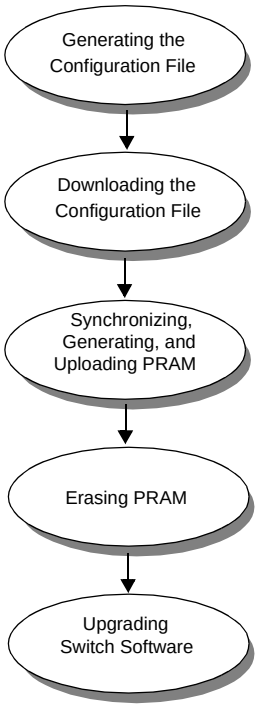
After you set the switch attributes, you must configure the processor module I/O modules in NavisCore. You can also configure a *redundant standby module*. See the *NavisCore Physical Interfaces Configuration Guide* for a detailed description of how to configure the various processor and I/O modules.

A

Downloading the Configuration

This appendix describes how to download information to the switch and establish NMS-to-switch communications. You can use these procedures to activate a new switch or to reconfigure an existing switch.

This appendix describes the following topics and tasks:



Before You Begin

After you define the switch configuration through NavisCore, you must create an initialization-script file and download it to the switch.

You download a switch configuration file as follows:

Step 1. Create the initial switch configuration by generating an initialization-script file from the NMS.

Step 2. Make a console connection to the switch.

Step 3. Start the terminal emulation software.

Step 4. Download the script file to the switch.

Step 5. Synchronize the switch from the NMS.

Generating the Initialization-Script File

The Initialize Switches function generates an initialization-script file that contains the SNMP SET commands for each configuration. The initialization-script file is then used to load the initial switch configuration or to reload the configuration if the original configuration is erased or destroyed. The initialization-script file is stored in the */var/CascadeView/initFiles* directory as *switchname.init*.

To download a new initialization-script file to a switch that already contains a configuration, you must first clear PRAM. See either "Clearing STDX PRAM" on page A-35 or "Clearing B-STDX, CBX, and GX PRAM" on page A-36.

To generate the initialization-script file:

1. Select a switch from your network map.
2. From the Misc menu, select NavisCore ⇒ Logon. Enter your operator password.
3. From the Administer menu, select Ascend Switches ⇒ Initialize Switches. The Initialize Switches dialog box appears (see Figure A-1).

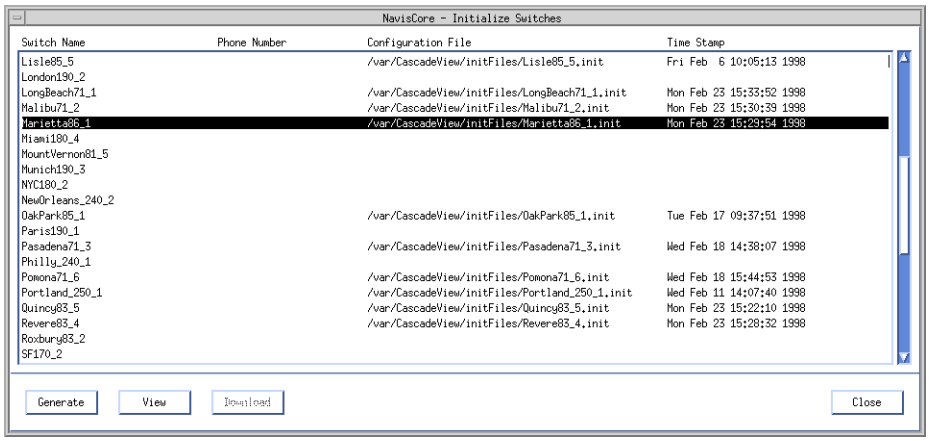


Figure A-1. Initialize Switches Dialog Box

4. From the list, select the switch you want to initialize.
5. Choose Generate to create the initialization-script file containing the SNMP SET commands. The initialization-script file will get a new date and time stamp each time the file is updated. This is the file you need to download to the switch.
6. Repeat Step 4 and Step 5 for each switch you need to initialize. Proceed to the section, “Downloading the File to the Switch” on page A-5.

Viewing the Initialization-Script File

To view the initialization-script file before downloading it to the switch:

1. From the Initialize Switches dialog box, highlight the desired switch.
2. Choose View. The system displays the file contents similar to the example in Figure A-2.

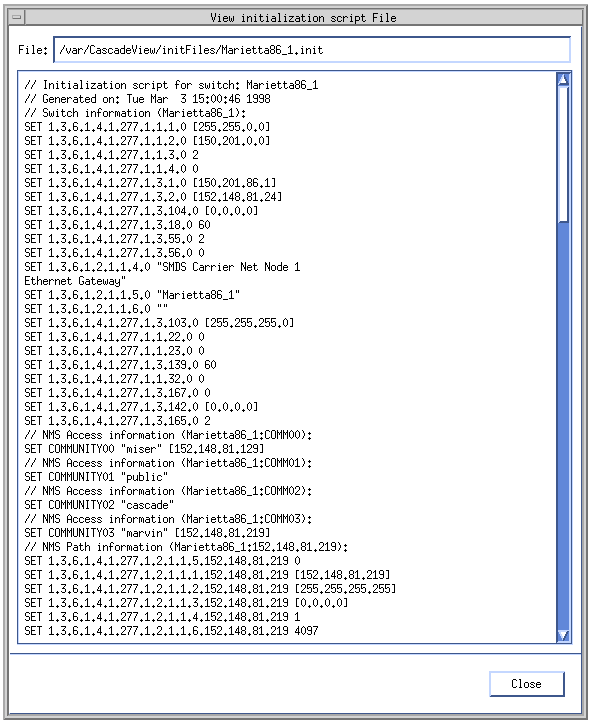


Figure A-2. View Initialization Script File Dialog Box

3. When you finish viewing the file, choose Close to return to the Initialize Switches dialog box.

Downloading the File to the Switch

After you generate and view the file, you can download it to the switch using any of the following methods:

Tip Utility — The Solaris Tip program. See "Using Tip" on page A-5.

Terminal Emulation Software — PC in terminal emulation software. See "Using Terminal Emulation Software" on page A-8 for instructions.

Kermit Utility — Console port running the kermit mode protocol. See "Using Kermit" on page A-8 for instructions.

Install Program — Connection to the console using a PC or terminal. See "Using the Console Install Program with B-STDX Switches" on page A-10 and "Using the Console Install Program with CBX and GX Switches" on page A-20 for instructions.

Ascend recommends that you configure MPVCs after you download the NMS initialization-script to initialize the switch. If you configure MPVCs before you initialize the switch, the NMS searches the entire circuit table for the presence of MPVCs; generating the initialization-script file can take ten minutes or more, depending on the size of the circuit table.

Using Tip

Before you use Tip to download a text file, verify the following:

- ☑ The console cable connects to serial port A on the back of your workstation. See your workstation hardware guide for information about locating serial port A.
- ☑ The hardwire entry device (dv) is set for */dev/cua/a*.
- ☑ The hardwire entry in the */etc/remote* file specifies 19200 bps.

  For example:

```
hardwire:\
:dv=/dev/cua/a:br#19200:el=^C^S^Q^U^D:ie=%$:oe=^D
```

In UNIX, ^D means press d while holding down the Ctrl key.

To access the switch:

1. In an xterm window, enter **su - root** and enter the root login and password.
2. Enter **tip hardwire**.

   You should get a “connected” message.
3. Enter **~#**.

   This command sends a break character to the switch. The console prompt appears.
4. Log in to the switch.
5. At the > prompt, enter the following:

   ```
   enable debug
   password: [your debug password]
   ```

   If you do not know your debug password, contact the Ascend Technical Assistance Center for help.
6. At the ## prompt, enter the following:

   ```
   ## reset pram all
   ```
7. At the “Reset PRAM on all cards? Are you sure (YES/NO)?” prompt, enter **YES**.
8. At the ## prompt, enter the following:

   ```
   ## reset system
   ```
9. At the “Are you sure (YES/NO)?” prompt, enter **YES**.

   The system displays the following message:

   ```
   resetting switch, stand by...
   ```

   When the switch comes up (approximately 1-2 minutes), the >> prompt appears. This prompt indicates you successfully erased PRAM and the switch can accept a new initialization-script file (see “Downloading the Initialization File” on page A-7). Before you download the file, verify that all I/O modules are “up” by issuing a *show card* console command.

Downloading the Initialization File

The file (executable) is located in */opt/CascadeView/bin*. If you are downloading to an STDX 3000/6000 switch, you must first convert the file to add an LF to LF-CR, using the unix2dos command. For example, enter the following:

```
unix2dos shuttle38.init shuttle38.init
```

(where *shuttle38.init* is the name of the script file.)

To download the initialization file:

1. Open a second xterm window.
2. Change directory as follows:

   ```
   cd /opt/CascadeView/bin
   ```

3. Enter the following command:

   ```
   ./script-download -in [ifn] -out [ofn] -linedelay [#in 1/10 seconds]
   ```

   where:

   [**ifn**] is the initialization filename
   (for example, */var/CascadeView/initFiles/shuttle38.init*)

   [**ofn**] is the output filename (for example, */dev/cua/a*)

   [# in 1/10 second] is the value of the line delay in 1/10th of a second (for example, use 3 to use a 3/10th-second line delay). Do not use a value less than 1.

4. When you finish, type **~^D** in the xterm window to exit the Tip session.

Observe the switch on the network map. If the switch remains yellow and does not turn green within a few minutes, see "Synchronizing STDX 3000/6000 Switches" on page A-28 or "Synchronizing B-STDX, CBX, and GX Switches" on page A-29 to synchronize the switch.

If You Have Problems

If you have problems using Tip, review the following:

- For an STDX switch, if you receive the error message "tip:unknown host term," your workstation may already have the *term* entry in the */etc/remote* file. To use the Tip program's term command, type **vi /etc/remote** and press Enter. Add the following entry to this file:

  ```
  term:\
  :dv=/dev/cua/a:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:
  ```

  Type **:wq!** and press Enter to exit vi and save your changes.

- If you receive the error "Couldn't open input file" when you ran script-download, enter the following command to change permissions on the */dev/cua/a* device (You must have root privilege to change the file permissions.):

  ```
  chmod 666 /dev/cua/a
  ```

Using Terminal Emulation Software

You can use any commercially-available terminal emulation package to download the configuration text file from a PC. Refer to the user guide that comes with this package for specific instructions for downloading text files.

Whichever emulation package you use, make sure to set the following variables:

Transfer protocol — Set this to text mode transfer.

Line delay — Set this to a minimum of 3/10 second.

Before you transfer the configuration text file to the PC, you may need to run the UNIX command, **unix2dos**, on this file.

Using Kermit

You can use the kermit function to transfer the configuration text file through the console port to your switch's CP/SP/NP module. The advantage of using kermit instead of Tip or a PC terminal emulator is that with kermit, you only have to download the PRAM files needed to establish a connection between the switch and the NMS. For gateway switches, you only need to download your switch's CP/SP/NP module PRAM file. For non-gateway nodes, you need to download the CP/SP/NP module PRAM file and the PRAM file of the module that provides the trunk connection to the gateway node.

Another advantage is that after the CP/SP/NP module reboots with the PRAM file, you do not have to PRAM Sync the Processor and module(s) that received the new configuration file.

To download the PRAM files to the switch:

1. Connect a console cable to serial port A on the back of your workstation. See your workstation hardware guide for information about serial port A.
2. Use the Generate PRAM function (refer to page A-30) to generate a configuration file for the main processor and module(s).
   - *If this is a gateway switch*, you do not have to generate PRAM for any module(s).
   - *If this is not a gateway switch*, you must generate a PRAM file for the CP/SP/NP module and the module that provides the trunk connection to the gateway node.
   - The NMS stores the generated PRAM files in the */opt/CascadeView.var/cfgSyncFiles* directory. The directory that contains the PRAM files associated with this release may look like the following:

Table A-1. PRAM Files

Switch Type	Directory Name
B-STDX 8000/9000	9000-06.xx.xx
CBX 500	500-03.xx.xx
GX 550	550-01.xx.xx

   When you look in this directory, you see a number of files that include the name of the associated switch followed by a .Pslot number. For example, for switch Westford1, the CP/SP/NP module PRAM file name would be Westford1.P01. If the PRAM file was from the module in slot 14, the PRAM file name would be Westford1.P14. These are the files you must download to the switch.
3. From either the NMS or a PC, establish a console connection to the switch (19200 bps).
4. At the console prompt, type **kermit** and press Return. This sets the console port to kermit mode for file transfer.
5. Start a kermit session with binary-file transfer mode selected.
6. Transfer the CP/SP/NP module PRAM file. Once complete, the kermit session automatically terminates and the CP/SP/NP module should automatically warm boot.
7. (*Optional*) To transfer the module PRAM file(s), repeat Step 4 through Step 6.

8. After the download is complete, the NMS should be able to access the switch. On the Switch Back Panel dialog box, if any remaining IOPs are yellow, you can PRAM Synch them. See "Using PRAM Functions" for instructions.

Using the Console Install Program with B-STDX Switches

You use the install program to enable a B-STDX 8000/9000 with no PRAM to communicate with the NMS. Once switch-to-NMS connectivity is established, you can perform the remaining configuration tasks directly from the NMS.

To access the switch using the install program, use the following steps:

1. Establish a connection to the switch console port, using the NMS workstation or a standalone PC.
2. At the [*switch name*]## prompt, enter **Reset Pram all**.
3. At the "Reset PRAM on all cards. ARE YOU SURE <Yes|No>?" prompt, enter **YES**.
4. At the [*switch name*]## prompt, enter **reset system**.
5. At the "ARE YOU SURE <Yes|No>?" prompt, enter **YES**.

   The system displays the following message:

   ```
   RESETTING SWITCH, STAND BY....
   ```

6. At the >> prompt, enter **install**.
7. The system prompts you for the following information. Enter the appropriate response and press Return after each entry.

   ```
   Enter the network number:
   ```

   ```
   Enter the network mask:
   ```

   ```
   Select the DLCI addressing scheme (Global/Local):
   ```

   ```
   Enter the address of this switch:
   ```

   Use the default internal IP address shown if this is the first switch in the network, or modify the last octet to represent the actual switch address.

   ```
   Enter the NMS IP address:
   ```

   Enter the IP address of the NMS workstation used to manage this switch.

   ```
   Enter the SNMP community name:
   ```

   Enter the community name of the NMS used to manage this switch. The default community name is cascade.

The system displays the following menu.

```
Which interface will this switch use to communicate with the
NMS?
    (1) Direct Ethernet (see "Using Direct Ethernet" on
    page A-11)
    (2) Indirect Ethernet (see "Using Indirect Ethernet
    (Through a Gateway Device)" on page A-12)
    (3) Direct Trunk (see "Using a Direct Trunk" on
    page A-13)
    (4) ATM Optimum Trunk (see "Using an ATM OPTimum Trunk
    (Through an Adjacent Switch)" on page A-15)
    (5) Frame Relay Optimum Trunk (see "Using a Frame Relay
    OPTimum Trunk (Through an Adjacent Switch)" on page A-17)
    (6) SLIP (see "Using SLIP" on page A-19)
    (7) Management DLCI (not supported)
```

8. Select your connection type, then proceed to the one of the following sections for further instructions.

Using Direct Ethernet

1. Enter the IP address of the Ethernet port.
2. Enter the IP address mask of the Ethernet port.

   The program displays your configuration information:

```
Network:150.150.156.0
Network mask:255.255.255.0
DLCI schemeLocal
Switch address:150.150.156.1
NMS address:152.148.82.11
SNMP community:Marblehead
Interface->NMS:Direct Ethernet
Ethernet IP:150.150.156.0
Ethernet IP Mask:255.255.255.0
```

3. When prompted, enter **yes** or **no** to confirm that this information is correct.

   When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

4. When prompted, enter **yes** to reboot the switch.

Using Indirect Ethernet (Through a Gateway Device)

1. Enter the IP address of the gateway device.
2. Enter the IP address of the Ethernet port.
3. Enter the IP address mask of the Ethernet port.

   The program displays your configuration information:

```
Network:150.150.156.0
Network mask:255.255.255.0
DLCI scheme:Local
Switch address:150.150.156.1
NMS address:152.148.82.11
SNMP communityMarblehead
Interface->NMS:Indirect Ethernet (through a gateway)
Gateway to NMS:152.148.80.1
Ethernet IP:152.148.80.2
Ethernet IP mask:255.255.255.0
```

4. When prompted, enter **yes** or **no** to confirm that this information is correct.

   When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

5. When prompted, enter **yes** to reboot the switch.

Using a Direct Trunk

If you are using a direct trunk to communicate with the NMS, the system displays the module type menu, as follows:

(1) 8-port UIO
(2) 4-port 24-channel fractional T1
(3) 4-port 30-channel fractional E1
(4) 10-port DSX-1
(5) 2-port HSSI
(6) Channelized DS3
(7) 1-port ATM UNI DS3
(8) 1-port ATM UNI E3
(9) 1-port ATM IWU OC3c/STM1
(10) 1-port ATM CS/DS3
(11) 12-port E1
(12) 4-port unchannelized T1
(13) 4-port unchannelized E1

1. Select the module used for the trunk and press Return.
2. When prompted, enter the following information:
   a. Enter the slot # of the module.
   b. Enter the port # of the trunk.
   c. Enter the local trunk interface # of the trunk.
   d. Enter the local trunk lport ospf area id.
   e. Enter **yes** or **no** to the “Is this ospf area 1 back compatible?”
   f. Enter the remote trunk interface # of the trunk.
   g. Enter the internal IP address of the switch at the remote end [*switch’s IP address*].

      The system displays the following clock source options:

      1 DCE
      2 Loop Timed DCE
      3 DTE
      4 Direct Trunk

3. Enter the clock source selection.
4. Enter the clock speed in Kbps.
5. Enter the IP address of the Ethernet port.

6. Enter the IP address mask of the Ethernet port.

   The program displays your configuration information:

```
Network: 150.150.156.0
Network mask:255.255.255.0
DLCI scheme:Local
Switch address:150.150.156.1
NMS address:152.148.82.11
SNMP communityMarblehead
Interface->NMS:Direct Line Trunk
IP add. of remote SWITCH:152.148.50.2
Remote trunk interface #:1
Card Type:8-port UIO
Slot number:3
Port number:1
Local trunk interface #:1
Local trunk lport ospf area ID:3
OSPF area 1 back compat:Yes
Clock source:DCE
Clock speed:64 kbps
```

You may need to configure additional parameters, depending on the card type you are configuring. Contact the Ascend Technical Assistance Center (TAC) for assistance.

7. When prompted, enter **yes** or **no** to confirm that this information is correct.

   When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

8. When prompted, enter **yes** to reboot the switch.

Using an ATM OPTimum Trunk (Through an Adjacent Switch)

If you are using an ATM OPTimum trunk to communicate with the NMS, the system displays the following module types:

(1) 1-port ATM UNI DS3
(2) 1-port ATM UNI E3
(3) 1-port ATM IWU OC3c/STM1
(4) 1-port ATM CS/DS3

1. Select the card used for the trunk and press Return.
2. When prompted, enter the following configuration information:
   - **a.** Enter the slot # of the trunk card.
   - **b.** Enter the port # of the trunk.
   - **c.** Enter the local user link (feeder) interface # of the trunk.
   - **d.** Enter the local trunk interface # of the trunk.
   - **e.** Enter the local trunk lport ospf area id.
   - **f.** Enter **yes** or **no** to the “Is this ospf area 1 back compatible?” prompt.
   - **g.** Enter the remote trunk interface # of the trunk.
   - **h.** Enter the internal IP address of the switch at the remote end.
   - **i.** Enter the Cell Payload Scrambling Mode (1 - Disabled, 2 - Enabled).
   - **j.** Enter the Cell Mapping Mode (1 - PLCP, 2 - Direct Mapping).
   - **k.** Enter the VPI for the local OPTimum-trunk endpoint.

The program displays your configuration information:

```
Network: 150.150.156.0
Network mask:255.255.255.0
DLCI scheme:Local
Switch address:150.150.156.1
NMS address:152.148.82.11
SNMP communityMarblehead
Interface->NMS:ATM Optimum Trunk (through an adjacent sw)
IP add. of remote SWITCH:152.148.50.8
Remote trunk interface #:3
Card Type:1-port ATM UNI DS3
Slot number:3
Port number:3
Local trunk interface #:3
Local trunk lport ospf area ID:0.0.0.1
OSPF area 1 back compat:YES
Local user link (feeder) int. #:3
Cell payload scrambling:Enabled
Cell mapping mode:Direct mapping
VPI:     7
```

3. When prompted, enter **yes** or **no** to confirm that this configuration is correct.

   When it receives confirmation, the system displays the following:

   ```
   Committing

   Preliminary installation completed!

   Use the NMS to complete the full installation.
   ```

4. When prompted, enter **yes** to reboot the switch.

Using a Frame Relay OPTimum Trunk (Through an Adjacent Switch)

If you are using a Frame Relay OPTimum trunk to communicate with the NMS, choose from the following module types:

(1) 8-port UIO
(2) 4-port 24-channel fractional T1
(3) 4-port 30-channel fractional E1
(4) 10-port DSX-1
(5) 2-port HSSI
(6) Channelized DS3
(7) 12-port E1

1. Select the module used for the trunk and press Return.
2. Complete the following configuration information at the prompts:
   - **a.** Enter the slot # of the trunk card.
   - **b.** Enter the port # of the trunk.
   - **c.** Enter the local user link (feeder) interface # of the trunk.
   - **d.** Enter the local trunk interface # of the trunk.
   - **e.** Enter the local trunk lport OSPF area id.
   - **f.** Enter yes or no to the “Is this ospf area 1 back compatible?” prompt.
   - **g.** Enter the remote trunk interface # of the trunk.
   - **h.** Enter the internal IP address of the switch at the remote end.
   - **i.** Enter the trunk’s local DLCI #.
   - **j.** Enter a clock speed in kbps.
   - **k.** Enter the link management interface (LMI) protocol.
   - **l.** Enter the IP address of the Ethernet port.
   - **m.** Enter the IP address mask of the Ethernet port.

The program displays your configuration information:

```
Network: 150.150.156.0
Network mask:255.255.255.0
DLCI scheme:Local
Switch address:150.150.156.1
NMS address:152.148.82.11
SNMP communityMarblehead
Interface->NMS:FR Optimum Trunk (through an adjacent sw)
IP add. of remote SWITCH:152.148.50.8
Remote trunk interface #:3
Card Type:1-port ATM UNI DS3
Slot number:3
Port number:3
Local trunk interface #:3
Local trunk lport ospf area ID:0.0.0.1
OSPF area 1 back compat:YES
Local user link (feeder) int. #:3
Clock source:Loop timed
Link framing:ESF-ANSI
Zero coding:B8ZS
```

3. When prompted, enter **yes** or **no** to confirm that this configuration is correct.

   When it receives confirmation, the system displays the following:

   ```
   Committing

   Preliminary installation completed!

   Use the NMS to complete the full installation.
   ```

4. When prompted, enter **yes** to reboot the switch.

Using SLIP

If you are using SLIP to communicate with the NMS:

1. Select interface 6 from the choices below:

   (1) Direct Ethernet

   (2) Indirect Ethernet (through a gateway device)

   (3) Direct Trunk (through an adjacent switch)

   (4) ATM Optimum Trunk (through an adjacent switch)

   (5) Frame Relay Optimum Trunk (through an adjacent switch)

   (6) SLIP

   (7) Management DLCI

   The program displays your configuration information:

   ```
   Network:150.150.156.0
   Network mask:255.255.255.0
   DLCI scheme:Local
   Switch address:150.150.156.0
   NMS address:152.148.82.11
   SNMP communitymarblehead
   Interface->NMS:SLIP
   ```

2. When prompted, enter **yes** or **no** to confirm that this configuration is correct.

   When it receives confirmation, the system displays the following:

   ```
   Committing

   Preliminary installation completed!

   Use the NMS to complete the full installation.
   ```

3. When prompted, enter **yes** to reboot the switch.

Using the Console Install Program with CBX and GX Switches

You use the install program to enable CBX and GX switches with no PRAM to communicate with the NMS. Once switch-to-NMS connectivity is established, you can perform the remaining configuration tasks directly from the NMS.

To access the switch using the install program, use the following steps:

1. Establish a connection to the switch console port, using the NMS workstation or a standalone PC.
2. At the [*switch name*]## prompt, enter **Reset Pram all**.
3. At the "Reset PRAM on all cards. ARE YOU SURE <Yes|No>?" prompt, enter **YES**.
4. At the [*switch name*]## prompt, enter **reset system**.
5. At the "ARE YOU SURE <Yes|No>?" prompt, enter **YES**.

   The system displays the following message:

   ```
   RESETTING SWITCH, STAND BY....
   ```

6. At the >> prompt, enter **install**.
7. The system prompts you for the following information. Enter the appropriate response and press Return after each entry.

   ```
   Enter the network number:
   ```

   ```
   Enter the IP address of the switch's network.
   ```

   ```
   Enter the network mask:
   ```

   ```
   Use the default, Class B, or enter 255.255.255.0 for Class C.
   ```

   ```
   Enter the address of this switch:
   ```

   Use the default internal IP address shown if this is the first switch in the network, or modify the last octet to represent the actual switch address.

   ```
   Enter the NMS IP address:
   ```

   Enter the IP address of the NMS workstation used to manage this switch.

   ```
   Enter the SNMP community name:
   ```

   Enter the community name of the NMS used to manage this switch. The default community name is cascade.

The system displays the following menu.

```
Which interface will this switch use to communicate with the
NMS?

    (1) Direct Ethernet (see “Using Direct Ethernet” on
    page A-21)

    (2) Indirect Ethernet (through a gateway device)(see
    “Using Indirect Ethernet (Through a Gateway Device)” on
    page A-22)

    (3) Direct Trunk (through an adjacent switch) (see “Using
    a Direct Trunk” on page A-23)

    (4) ATM OPTimum Trunk (through an adjacent switch)
    (see“Using an ATM Optimum Cell Trunk” on page A-24)
```

8. Select your connection type, then proceed to the appropriate section for further instructions.

Using Direct Ethernet

1. Select 1 for Direct Ethernet and enter the external IP address assigned to the switch and press Return. The system then provides the entered values as shown in the following example.

```
Network: 201.201.250.0
Network mask: 255.255.0.0
Switch Address: 201.201.250.1
NMS address:152.148.81.20
SNMP community:cascade
Interface: NMSDirect Ethernet
Ethernet IP: 152.148.81.69
```

2. When prompted, enter **yes** or **no** to confirm that this information is correct.
3. When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

4. When prompted, enter **yes** to reboot the switch.

Using Indirect Ethernet (Through a Gateway Device)

1. Select 2 for Indirect Ethernet and enter the IP address of the gateway device and Ethernet port assigned to the switch and press Return. The system then provides the entered values as shown in the following example.

```
Network     201.201.250.0
Network mask255.255.0.0
Switch Address201.201.250.1
NMS address:150.124.100.1
SNMP community:cascade
Interface -> NMSIndirect Ethernet (through a gateway device)
Gateway to NMS150.124.100.2

Ethernet IP 152.148.81.69
```

2. When prompted, enter **yes** or **no** to confirm that this information is correct.
3. When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

4. When prompted, enter **yes** to reboot the switch.

Using a Direct Trunk

1. Select 3 for Direct Trunk. At the following prompts, enter the appropriate response and press Return after each entry.

```
What card type is used for the trunk?
   1       8 port DS3
   2       8 port E3
   3       4 port OC3/STM1
   4       1 port OC12/STM4
   5       8 port T1
   6       8 port E1
Enter choice: 1

Enter the slot # of the trunk card: 3

Enter the port number of the trunk: 1

Enter the local trunk interface # of the trunk: 10

Enter the remote trunk interface # of the trunk: 100

Enter the IP address of the switch at the remote end:
201.201.201.14

Enter the Cell Payload Scrambling Mode:
      1      Disabled
      2      Enabled

Enter Choice: 1

Enter Cell Mapping Mode:
      1      PLCP
      2      Direct Mapping
Enter Choice: 1

Configuration selected:
      Network: 201.201.201.0
      Network mask: 255.255.0.0
      Switch address: 201.201.201.1
      NMS address: 152.148.21.20
      SNMP community: cascade
      Interface->NMS:Direct Trunk(adjacent switch)
      IP address of SWITCH at the remote end: 201.201.201.14
      Remote trunk interface #:               100
      Card type:                              8 port DS3
      Slot number:                            3
      Port number:                            1
      Local trunk interface #:                10
      Cell payload scrambling:                Disabled
      Cell mapping mode: PLCP
```

2. When prompted, enter **yes** or **no** to confirm that this information is correct.
3. When it receives confirmation, the system displays the following:

```
Committing

Preliminary installation completed!

Use the NMS to complete the full installation.
```

4. When prompted, enter **yes** to reboot the switch.

Using an ATM Optimum Cell Trunk

1. Select 4 for ATM OPTimum Trunk. At the following prompts, enter the appropriate response and press Return after each entry.

```
What card type is used for the trunk?
         1  8 port DS3
         2  8 port E3
         3  4 port OC3/STM1
         4  1 port OC12/STM4
         5  8 port T1
         6  8 port E1
Enter choice: 1

Enter the slot # of the trunk card: 3

Enter the port number of the trunk: 1

Enter the local user link (feeder) interface # of the trunk: 9

Enter the local trunk interface # of the trunk: 10

Enter the remote trunk interface # of the trunk: 100

Enter the IP address of the switch at the remote end:
201.201.201.14

Enter the Cell Payload Scrambling Mode:
         1  Disabled
         2  Enabled

Enter Choice: 1

Enter Cell Mapping Mode:
         1  PLCP
         2  Direct Mapping

Enter Choice: 1

Enter VPI for local OPTimum trunk endpoint: 5
```

```
Configuration selected:
      Network: 201.201.201.0
      Network mask: 255.255.0.0
      Switch address: 201.201.201.1
      NMS address: 152.148.21.20
      SNMP community: cascade
      Interface->NMS: ATM Optimum Trunk (adjacent switch)
      IP address of SWITCH at the remote end: 201.201.201.14
      Remote trunk interface #:               100
      Card type:                              8 port DS3
      Slot number:                            3
      Port number:                            1
      Local trunk interface #:                10
      Local user link (feeder) interface #    9
      Cell payload scrambling:                Disabled
      Cell mapping mode:                      PLCP
      VPI   5
```

2. When prompted, enter **yes** or **no** to confirm that this information is correct.
3. When it receives confirmation, the system displays the following:

   ```
   Committing

   Preliminary installation completed!

   Use the NMS to complete the full installation.
   ```

4. When prompted, enter **yes** to reboot the switch.

Using PRAM Functions

This section describes the various PRAM functions and their use.

Synchronizing PRAM

Whenever you download an initialization-script file from the NMS to the switch for the *first time*, you must synchronize PRAM (*PRAM Sync*) for the switch to receive complete configuration information. Occasionally you may also need to synchronize a switch to correct a mismatch between the NMS database and the configuration that resides in switch PRAM. This situation occurs when you use the NMS to make modifications to a switch that is unmanaged or not actively communicating with the NMS (unreachable) or if changes are made to the switch using console commands.

The Synchronize PRAM function enables you to correct inconsistencies between the NMS database and switch PRAM. Table A-2 describes the object status indicators that identify these inconsistencies.

Table A-2. Object Status Indicators

Object Color	Description
Yellow	An I/O module in the switch may be out of sync. Display the Switch Back Panel dialog box and review the status of each module. If necessary, synchronize PRAM (see "Using PRAM Functions" on page A-26). If the switch does not turn green, see the *NavisCore Diagnostic and Troubleshooting Guide* to review background diagnostic statistics.
Wheat	The switch object is not managed. You *unmanage* an object to prevent the NMS from polling the object while you configure it. To manage an object, select Manage Object from the Map menu.
Red	The indicated object is in a failed state and cannot actively communicate with the NMS.
Green	The indicated objects/switches are actively communicating with the NMS.

For more information about monitoring the network, see the *NavisCore Diagnostic and Troubleshooting Guide*.

Before you synchronize a switch, verify that you have defined the following, as described in Chapter 5:

- ☑ NMS IP Address
- ☑ Community Name
- ☑ Read/Write privileges

CPU-intensive operations such as PRAM synchronization can cause NavisCore to drop node polls. To avoid this problem, increase the amount of time between SNMP retries. Edit the **/opt/CascadeView/etc/ cascadeview.cfg** file and increase the CV_SNMP_RETRY_INTERVAL value from 30. This value is in tenths of a second.

Ascend recommends a value of 1.5 seconds for a configuration with 10 to 15 simultaneous instances of NavisCore and more than 15 switches in the network. This change takes effect when you restart HP OpenWindows.

See the following sections to PRAM-synch a switch:

- "Synchronizing STDX 3000/6000 Switches" on page A-28
- "Synchronizing B-STDX, CBX, and GX Switches" on page A-29

Synchronizing STDX 3000/6000 Switches

To synchronize an STDX 3000/6000 switch:

1. Select the switch to synchronize and from the Misc menu, select NavisCore ⇒ Logon and enter the operator password. (You can only synchronize one switch at a time.)
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Choose the PRAM command. The Pram Sync dialog box appears.

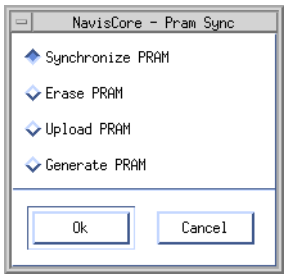


Figure A-3. Pram Sync Dialog Box

4. Select Synchronize PRAM and choose OK. This sends the binary image of the configuration to the switch, causing it to warm boot. When the switch reboots, all physical ports, logical ports, PVCs, and active sessions stall. If you have a heavily configured switch, it may take several minutes to reboot.

If you made only minimal changes to the switch configuration, you can synchronize PRAM at a later time to avoid interrupting network operation.

Synchronizing B-STDX, CBX, and GX Switches

To synchronize a B-STDX, CBX, or GX switch:

1. Select the switch to synchronize and from the Misc menu, select NavisCore ⇒ Logon and enter the operator password. (You can only synchronize one switch at a time.)
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Set Switch Back Panel dialog box appears.
3. Select the I/O module to synchronize.

> If you changed some switch attributes, such as the management path, you must synchronize the processor module before you synchronize any I/O modules. If you need to synchronize more than one module, always synchronize from the processor module first. Then work your way toward the module with the highest slot ID.

4. Choose the PRAM button. The Pram Sync dialog box appears (see Figure A-3 on page A-28).
5. Select Synchronize PRAM and choose OK. This sends the binary image of the configuration to the selected module, causing it to perform a warm boot. When the module reboots, all physical ports, logical ports, PVCs, and active sessions stall for approximately 0-30 seconds. If you have a heavily configured module, it may take several minutes or more to reboot.

> If you made only minimal changes to the configuration, you can synchronize PRAM at a later time to avoid interrupting network traffic.

Generating PRAM

The Generate PRAM function generates SNMP set commands to configure PRAM but does not upload the switch configuration file to the NMS. This feature enables you to view the configuration file before uploading it to the switch.

To generate PRAM:

1. Select the switch and from the Misc menu, select NavisCore ⇒ Logon and enter the operator password.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Choose the PRAM command. The Pram Sync dialog box appears (Figure A-3 on page A-28).
4. Select Generate PRAM and choose OK. This sends the SNMP set commands to a configuration file. See "Uploading PRAM" section for information on how to upload the configuration file to the switch.

Uploading PRAM

Occasionally the switch configuration file for a specific I/O module and the configuration in the NMS database do not match. A mismatch can occur when you upgrade your switch software, make a change through network management software (NavisCore), or change a switch configuration through SNMP commands or the MIB.

The Upload PRAM function requires the following software:

- NavisCore 4.0
- STDX switch software, Release 2.4
- B-STDX switch software Release 6.0
- CBX 500 switch software, Release 3.0
- GX 550 switch software, Release 1.0

Supported PRAM Objects

Upload PRAM currently supports the following objects:

- Physical ports
- Logical ports (except trunk ports)
- IP objects excluding Multipoint-to-Point Tunneling (MPT) Point-to-Point connections

Guidelines for Using Upload PRAM

Before you use the Upload PRAM function, review the following points:

- Use the Upload PRAM function to resolve PRAM conflicts by viewing the switch configuration file stored in PRAM. This enables you to compare the configuration file in the switch (PRAM) to the configuration file in the NMS database.
- Use the Upload PRAM function to replace the configuration file in the NMS database with the switch configuration file.
- Use Upload PRAM to add objects from switch PRAM to the NMS database, as long as the objects being added do not conflict with existing objects in the database; for example, the NMS database already contains a switch with that name.
- Use Upload PRAM to delete objects from the database. Due to the interdependency of objects in the database, *be careful* when you use Upload PRAM to delete objects from the database. In general, make sure there are no dangling objects (i.e., objects without a parent) in the switch before applying Upload PRAM. For example, deleting a logical port without first deleting all associated individual addresses or address screens, creates dangling objects and causes a problem during the Upload PRAM process.

Uploading a Switch Configuration File

To upload the switch configuration file stored in PRAM:

1. On the network map, select the switch object.
2. From the Administer menu, select Ascend Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears, displaying the back panel of the selected switch.
3. Select either the I/O module or the processor module and choose the PRAM button. The PRAM Sync dialog box appears (see Figure A-3 on page A-28).
4. Select Upload PRAM and choose OK. The Card PRAM Upload and NMS Synchronization dialog box appears (see Figure A-4).

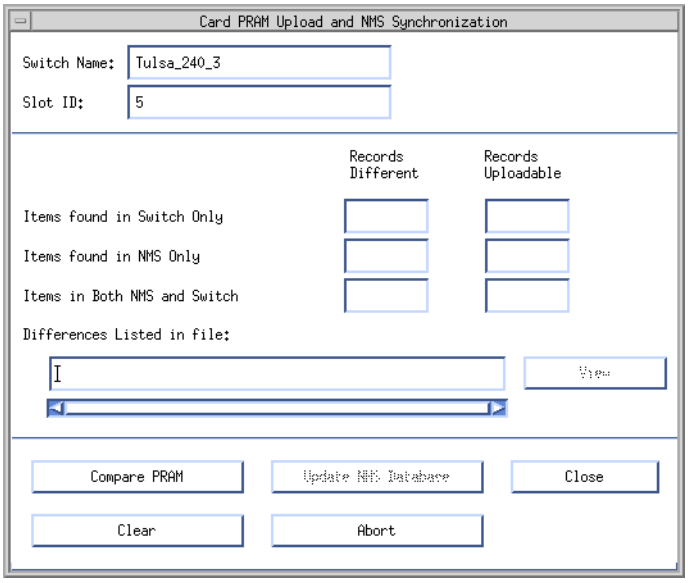


Figure A-4. Card PRAM Upload and NMS Synchronization Dialog Box

5. Choose Compare PRAM.

   The dialog box displays information about the number of inconsistencies between the PRAM configuration file and the NMS database. If the field displays a zero, there are no differences between the PRAM and NMS configuration files.

   An *item* can be a single physical port or logical port definition. Item fields include:

   Items in the NMS only — The item exists in the NMS database, but not in the switch PRAM. This discrepancy occurs when you make configuration changes to an unmanaged switch.

   Items found in Switch only — The item exists in switch PRAM but not in the NMS database. This situation occurs when you configure a switch, using a third-party network management station or use the MIB to change configuration information.

Items found in both NMS and Switch — This item exists in both places but there are discrepancies in the configuration. This can happen if you modified the configuration directly from the console. For example, if you used console commands to change the admin status of a logical port, the logical port definition in switch PRAM indicates that the logical port is Down; the NMS database records indicate the logical port is Up. These discrepancies can also occur if a PRAM synchronization or SET fails.

The dialog box displays the name and location of the file that contains the inconsistencies.

6. Choose View to compare the files. (See the example in Figure A-5.)

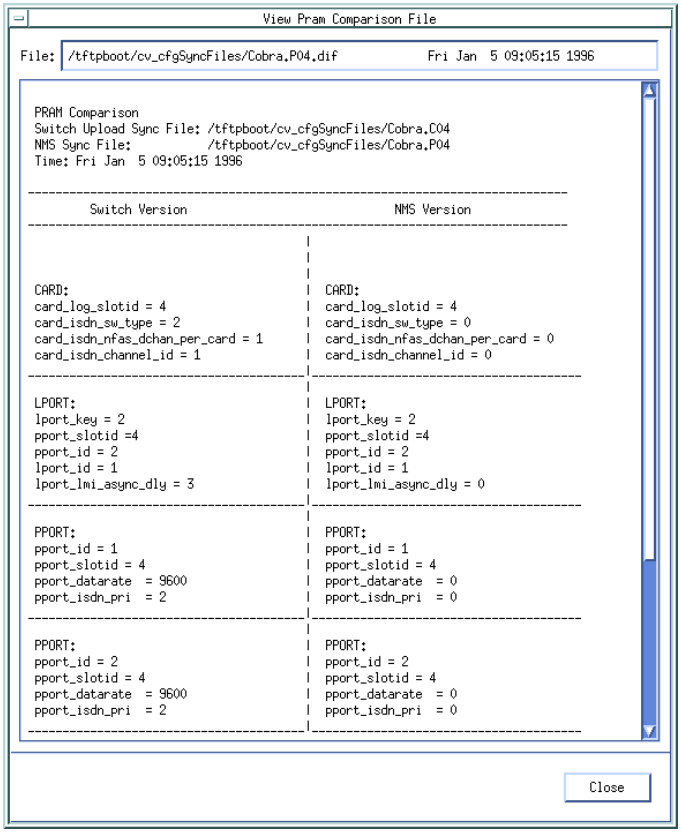


Figure A-5. View PRAM Comparison File Dialog Box

7. Choose Close to return to the Card PRAM Upload and NMS Synchronization dialog box.

8. To synchronize the configuration information between switch PRAM and the NMS database, do one of the following:
   - Choose the Update NMS Database command to use the configuration stored in switch PRAM.
   - Choose close to use the configuration stored in the NMS database and update PRAM using the Synchronize PRAM command (refer to page A-26).
9. Repeat Step 3 through Step 8 for each I/O module to complete the configuration upload process.

If an error occurs during the upload process, a message dialog appears. After closing this dialog box, you can choose Update NMS Database to continue the upload process for the remaining physical port and logical port definition.
If there are problems with the PRAM configuration file, refer to page A-26 for instructions to download the configuration file stored in the NMS database.

Erasing PRAM

Occasionally you must download the initialization-script file to switch PRAM if you suspect the switch PRAM configuration file is incorrect. If you experience problems with a new release of switch software, you might also have to download the file as part of a switch downgrade or upgrade procedure. Before you download the file, you must first clear the existing switch configuration file from PRAM using the Erase PRAM function.

See the following sections to erase PRAM on a switch:

- “Clearing STDX PRAM” on page A-35
- “Clearing B-STDX, CBX, and GX PRAM” on page A-36

Clearing STDX PRAM

To remove an existing configuration from the STDX 3000/6000:

1. Install a console terminal to the serial management port on the Packet Processor (PP).
2. Force a line break condition to the switch to display the > prompt.
3. At the > prompt, enter the following:

   ```
   login debug
   ```

   ```
   password: [your debug password]
   ```

   If you do not know your debug password, contact the Ascend Technical Assistance Center.
4. At the ## prompt, enter the following:

   ```
   ## reset pram
   ```
5. At the "Are you sure (YES/NO)?" prompt, enter **YES** (uppercase).
6. At the ## prompt, enter the following:

   ```
   ## reset system
   ```
7. At the "Are you sure (YES/NO)?" prompt, enter **YES** (uppercase).

   The system displays the following message:

   ```
   resetting switch, stand by...
   ```

   Once the switch comes up (approximately 1-2 minutes), a >> prompt appears, indicating you have successfully erased PRAM and the switch can accept a new initialization-script file download. Verify that all I/O modules are up and active.

Clearing B-STDX, CBX, and GX PRAM

You can clear the existing PRAM configuration in the following ways:

Method 1 — Use the NMS software to clear PRAM (recommended method).

Method 2 — Connect a console terminal and clear the PRAM on each I/O module. Use this second method as a backup.

Method 3 — Use as a last resort and only *after consulting an Ascend TAC representative.*

Method 1

1. On the network map, select the switch for which you want to clear PRAM.
2. From the Administer Menu, select Ascend Parameters ⇒ Set Parameters.
3. Select each I/O module (one at a time) and choose the PRAM button. The PRAM Sync dialog box appears (see Figure A-3 on page A-28).
4. Select Erase PRAM.
5. Choose OK.
6. Repeat Step 3 through Step 5 until you erase the PRAM for each module.

Method 2

1. Install a console terminal to the network management port on the main processor module. (See the section “Connecting a Console” in your hardware guide for details.)
2. Force a line break condition to the switch.
3. Enter a minimum of three characters for the login name and enter a valid community name as the password (cascade is the default community name).

If you are using console authentication, call the Ascend Technical Assistance Center for additional information. See also “Configuring Console Authentication” on page 5-20.

4. At the switchname> prompt, enter the following:

```
enable debug
Debug password: [your debug password]
```

If you are erasing PRAM on all I/O modules in the switch (including the processor module) clear the PRAM on the highest numbered slot first and continue to the lowest numbered slot (i.e., CP/SP/NP last).

5. At the switchname ## prompt, enter the following:

   ```
   reset pram [#]
   ```

   where [#] is the module or slot number. [All] will reset all cards.

6. At the "Reset PRAM. Are you sure (YES/NO)?" prompt, enter **YES** (uppercase).

Method 3

You should only use the following method as a last resort and only as instructed by an Ascend TAC representative.

1. Latch down all the cards.
2. Install a connection from the NMS SPARCstation to your switch's network management port. (See your hardware installation guide for details.)
3. Set both of the two-position dip switches (located on the front of the CP/SP/NP) to the Off position (left).
4. Latch up all the cards.
5. Establish a terminal emulation session. Set the line parameters as follows: 19,200 baud, 8 bits, no parity.
6. Press Return.
7. At the % prompt, enter the following:

   ```
   erase_pram
   ```

   Wait for the prompt to appear.

8. Latch down all of the cards.
9. Set one or both of the main processor module's two-position dip switches to the On position, pointing to the right, away from the position numbers on the switch.
10. Latch up all of the cards.

    Once the switch comes up (approximately 1-2 minutes), a >> prompt appears. This prompt indicates that PRAM is erased on the CP/SP/NP only, and the switch is ready for a new configuration file download.

Upgrading Switch Software

This section describes how to install software on your switch, using the NavisCore dual-software image feature (see Figure A-6).

1. Verify that copies of the software images (.rom files) are located in the */tftpboot/cv_switchSoftware* directory before you start the installation.
2. Verify that the TFTP daemon is running.
3. From the NavisCore map, highlight the switch.
4. From the Administer menu, select Ascend Switches ⇒ Download Switch Software. The Download Switch Software dialog box appears (see Figure A-6).

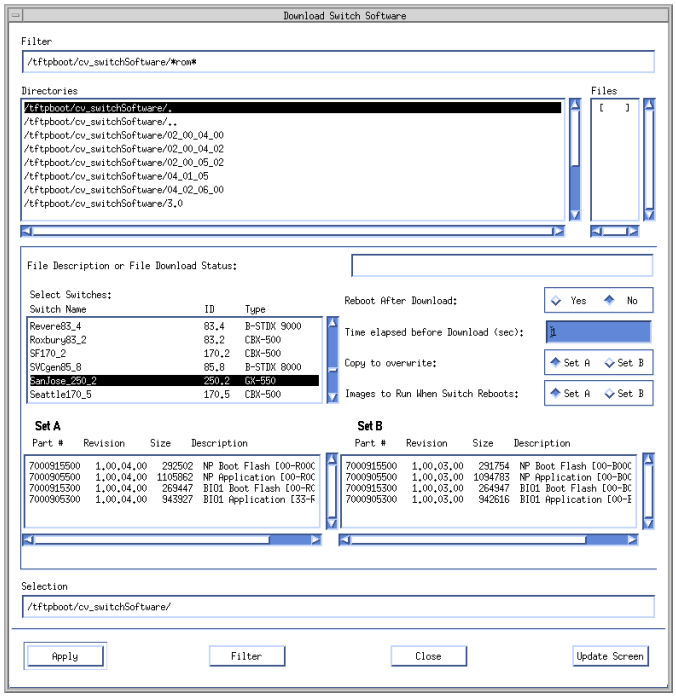


Figure A-6. Download Switch Software Dialog Box

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

Table A-3. Download Switch Software Dialog Box Fields

Field	Description
Filter	Specify the files that you want to list in the Directories list box. Specify the following path to list all of the available switch code software: **/tftpboot/switchSoftware/*rom*** and then press Enter or the Filter button to list the available files.
Directories	Lists the directories that match the criteria specified in the Filter field.
File Description or File Download Status	Lists a description of a selected file or if a file is currently being installed, displays the status of the download process.
Select Switches	Select a switch for switch code download. Lists the available switches on the map.
Reboot After Download	Select Yes to indicate that you want to reboot the switch after the download operation is complete. Select No to indicate that you do not want to reboot the switch after download.
Time Elapsed Before Download	Specify the number of seconds before the download operation will occur. One (1) second is the default value.
Copy to Overwrite	Specify Set A or B to indicate the software image set that the new files will overwrite.
Images to Run When Switch Reboots	Specify the image set that you will be using after the switch reboots.
Set A	Lists all of the switch code files for Set A.
Set B	Lists all of the switch code files for Set B.
Selection	Lists the selected directory path.

Using the Set Default Switch Software Function

The Set Default Switch Software function enables you to specify the default software image that the switch will use following a reboot. The Download Switch Software dialog box enables you to specify this information when you download the software. You can modify this information on the Set Default Switch Software dialog box.

To set switch software defaults:

1. From the NavisCore map, highlight the switch.
2. From the Administer menu, choose Ascend Switches ⇒ Set Default Switch Software. The Set Default Switch Software dialog box appears (Figure A-7) .

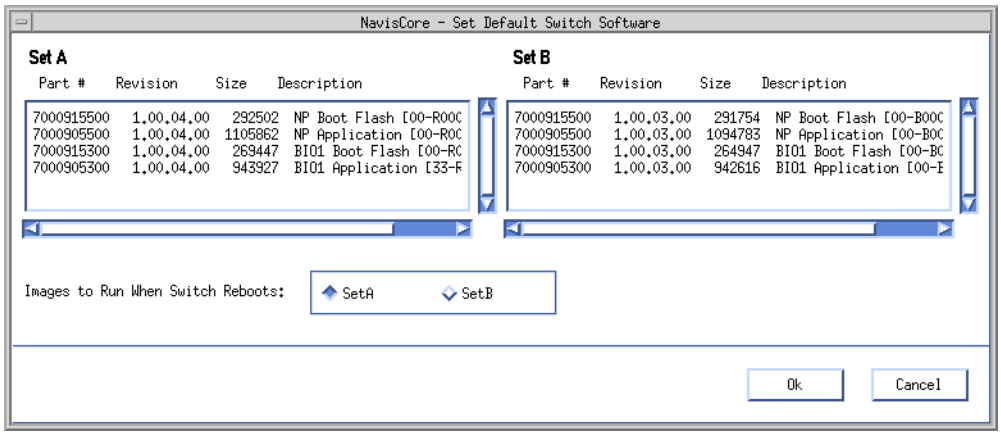


Figure A-7. Set Default Switch Software Dialog Box

The dialog box displays two software image sets called Set A and Set B.

3. Select Set A or B as the software image set that the switch will use when it reboots.
4. Choose OK.

B

The NavisCore Configuration File

This appendix describes the NavisCore defaults configuration file, *cascadeview.cfg*. This file is located in */opt/CascadeView/etc/* and contains the default variables for many Ascend switch software features.

Whenever you modify this file, you must restart NavisCore for the changes to take effect. See Chapter 2, “Administering NavisCore” for instructions on stopping and starting NavisCore.

cascadeview.cfg Contents

To view the contents of *cascadeview.cfg*, enter:

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

```
#!/bin/sh
#  @(#)cascadeview.cfg  (version: $Revision:   1.22  $Date$)
#  CascadeView configuration file.
#  Copyright 1994 Cascade Communications Corp.
#  All rights reserved.
#
#  Config for tracing:
CV_TRACE_ENABLED=0
CV_TRACEFILE=
export CV_TRACE_ENABLED CV_TRACEFILE
#
#  Config for message catalogs:
CV_ERROR_MSG_CAT_PATH=/opt/CascadeView/nls/C/cascadeview-errors.cat
export CV_ERROR_MSG_CAT_PATH
#
#  Config for database:
CVDB_TRACE_FILE_NAME=
export CVDB_TRACE_FILE_NAME
#
#  Config for map application:
CV_DEF_ADDRESS_SIGNIFICANCE=2       #local
CV_DEF_NETWORK_NUMBER=152.148.0.0
export CV_DEF_ADDRESS_SIGNIFICANCE CV_DEF_NETWORK_NUMBER
#
#  Config for switch initialization:
CV_SWITCH_INIT_FILE_DIR=/var/CascadeView/initFiles
export CV_SWITCH_INIT_FILE_DIR
#
```

```
#  Config for configuration sync.:
CV_SYNC_FILE_DIR=/tftpboot/cv_cfgSyncFiles
CV_SYNC_CHECK_DELAY=8
CV_SYNC_CHECK_INTERVAL=3
CV_SYNC_CHECK_COUNT=10
export CV_SYNC_FILE_DIR
export CV_SYNC_CHECK_DELAY CV_SYNC_CHECK_INTERVAL CV_SYNC_CHECK_COUNT
#
# Config for offline pram sync file name
CV_SYNC_FILE_OFFLINE_LIST=/tftpboot/cv_cfgSyncFiles/offline.lst
export CV_SYNC_FILE_OFFLINE_LIST
#
#  Config for SNMP management
CV_SNMP_IS_ENABLED=1
CV_SNMP_REQUEST_TIMEOUT=256
CV_SNMP_MAX_RETRIES=4
CV_SNMP_RETRY_INTERVAL=30
CV_SNMP_PUBLIC_COMMUNITY=public
CV_SNMP_READ_WRITE_COMMUNITY=constitution
export CV_SNMP_IS_ENABLED CV_SNMP_REQUEST_TIMEOUT CV_SNMP_MAX_RETRIES
export CV_SNMP_RETRY_INTERVAL CV_SNMP_PUBLIC_COMMUNITY
export CV_SNMP_READ_WRITE_COMMUNITY
#
# Hostname of NMS IP address used in building SNMP requests.
# Only necessary if NMS workstation has more than 1 IP interface.
# Default is hostname of workstation having only 1 IP interface.
#
CV_SNMP_NMS_HOSTNAME=
export CV_SNMP_NMS_HOSTNAME
#
#  Config for diagnostics (all time periods are in seconds):
#
CV_BG_DIAG_POLL_INTERVAL=3
CV_FG_DIAG_CHECK_DELAY=5
CV_FG_DIAG_CHECK_INTERVAL=1
CV_FG_DIAG_CHECK_COUNT=3
CV_DIAG_REASON_CATALOG=/opt/CascadeView/nls/C/cvDiagReasons.cat
export CV_BG_DIAG_POLL_INTERVAL CV_FG_DIAG_CHECK_DELAY
export CV_FG_DIAG_CHECK_INTERVAL CV_FG_DIAG_CHECK_COUNT
export CV_DIAG_REASON_CATALOG
#
```

```
#  Config for switch configuration:
CV_NODE_QOS_POLL_TIMER=300
export CV_NODE_QOS_POLL_TIMER
#
#  Config for status monitoring (time periods are in seconds):
CV_STATUS_POLL_INTERVAL=90
export CV_STATUS_POLL_INTERVAL
#
#  Config for physical port performance tuning:
#
CV_PPORT_DEF_DISCARD_HIGH=32
CV_PPORT_DEF_DISCARD_LOW=10
CV_PPORT_DEF_AQL_THRESHOLD=16

export CV_ENV_PPORT_DEF_DISCARD_HIGH
export CV_ENV_PPORT_DEF_DISCARD_LOW
export CV_ENV_PPORT_DEF_AQL_THRESHOLD
#
#  Config for SMDS Prefix Length: (temporary)
#
CV_SMDS_MASK_SIZE=6
export CV_SMDS_MASK_SIZE
#
#  Disable SMDS Switching System
#  0 to enable and 1 to disable
CV_DISABLE_SMDS_SS=0
export CV_DISABLE_SMDS_SS
#
#  Enable audit trail
#
CV_AUDIT_TRAIL_ENABLE=TRUE
export CV_AUDIT_TRAIL_ENABLE
#
```

```
#  Determine how frequent to refresh the out-of-sync flag from the database.
#  0 will be used to disable this feature and
#  N implies out-of-sync flag will be refreshed for every N node poll intervals
#
CV_OUT_OF_SYNC_REFRESH_CNT=5
export CV_OUT_OF_SYNC_REFRESH_CNT
#
#  Enable HSSI PPort over clocking
#  Warning: User is not recommended to enable this feature because overclocking
#  the HSSI pport may cause instability to the HSSI card.
#
CV_ENABLE_HSSI_PPORT_OVERCLOCKING=FALSE
export CV_ENABLE_HSSI_PPORT_OVERCLOCKING
#
#  Enable ATM OPTimum Trunk Bandwidth over subscribing.
#
CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE=FALSE
export CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE
#
#  Override default max LPorts per STDX 3000/6000.
#  <= 0 or missing - use default (currently 150). > 0 - use this value.
CV_MAX_INTERFACES_PER_STDX=150
export CV_MAX_INTERFACES_PER_STDX
CV_POLL_SERVER_PORT=10888
CV_POLL_SERVER_ADDRESS=localhost
export CV_POLL_SERVER_PORT CV_POLL_SERVER_ADDRESS
#
```

```
#  ATM UNI logical port defaults.
#
#    o  "UNI Type" defaults can be "PUBLIC" or "PRIVATE"
#    o  "Connection Type" defaults can be "NET_ENDSYS" or "NET_NET"
#
CV_ATMUNI_UNI_TYPE_DEFAULT=PUBLIC
CV_ATMUNIDCE_CONN_TYPE_DEFAULT=NET_ENDSYS
export CV_ATMUNI_UNI_TYPE_DEFAULT
export CV_ATMUNIDCE_CONN_TYPE_DEFAULT
#
#  Enable Move All Circuit
CV_ENABLE_MOVE_ALL_CIRCUIT=TRUE
export CV_ENABLE_MOVE_ALL_CIRCUIT
#
#  Checking the card type for Move All Circuit
CV_MV_CKT_CARD_TYPE_CHECKING=TRUE
export CV_MV_CKT_CARD_TYPE_CHECKING
#
# VPN/Customer configuration
#
# CV_CUR_VPNCUST =[VPN | CUSTOMER ]
CV_CUR_VPNCUST=
CV_CUR_VPN_NAME=
CV_CUR_CUST_NAME=
export CV_CUR_VPNCUST
export CV_CUR_VPN_NAME
export CV_CUR_CUST_NAME
#
#  Default Login settings
# CV_LOGON_TYPE =[OPERATOR | PROVISIONING]
#
#CV_LOGON_TYPE=OPERATOR
#export CV_LOGON_TYPE
```

```
#
# 4 or 16 levels of circuit priorities
#
# CV_CKT_PRIORITY_LEVELS = [FOUR | SIXTEEN]
CV_CKT_PRIORITY_LEVELS=FOUR
export CV_CKT_PRIORITY_LEVELS
#
# Time interval to refresh QoS metrics (time periods are in seconds):
# Range is (300 to 1799)
#
#CV_OSPF_LSA_REFRESH_INTERVAL=0
export CV_OSPF_LSA_REFRESH_INTERVAL

#
# SNMP Trace FILE
#
CV_SNMP_TRACE_FILE=
export CV_SNMP_TRACE_FILE

#
# Cell Circuits defined as interworking
#
# CV_CELLCKT_TYPE = [NORMAL | INTERWORKING]
# CV_CELLCKT_TYPE = INTERWORKING
# export CV_CELLCKT_TYPE

#
# enable Config for PRAM Upload Abort button; 1 to enable;
#                                          otherwise to disable
#
CV_PRAM_UPLOAD_ABORT_ENABLED=1
export CV_PRAM_UPLOAD_ABORT_ENABLED
#
# enable 310 bulk lport creation
# CV_310_BULK_LPORT= [TRUE | FALSE] default is disabled
CV_310_BULK_LPORT=TRUE
export CV_310_BULK_LPORT
```

```
#  Network distribution evaluation interval.
#
#    o  CV_NET_DIST_EVAL_INTERVAL is the number of seconds to pause
#       between evaluations when determining the network distribution
#       of a distributed Cascade object.  To be used when defining an
#       evaluation threshold for a Cascade distributed object.  Allowable
#       values are "1" to "60".
#
CV_NET_DIST_EVAL_INTERVAL=2
export CV_NET_DIST_EVAL_INTERVAL
#
#  SVC Closed User Groups network distribution evaluation threshold.
#
#    o  CV_SVC_CUG_NODE_EVAL_THRESH is the number of nodes (out of all of
#       the nodes in the network to be evaluated) on which to match configured
#       SVC addresses against a member rule regular expression at one time
#       before pausing for CV_NET_DIST_EVAL_INTERVAL seconds.  A value of
#       zero ("0") results in all nodes in the network being evaluated at
#       once with no pause.
#    o  CV_SVC_CUG_LOGFILE is the path and filename to log the results of
#       matching configured SVC addresses against a member rule regular
#       expression when determining whether or not a node belongs in a member
#       rule's network distribution.  A valid value enables logging.  A null
#       or invalid value disables logging.  The CascadeView PID will be
#       appended to the filename.
#
CV_SVC_CUG_NODE_EVAL_THRESH=0
CV_SVC_CUG_LOGFILE=
export CV_SVC_CUG_NODE_EVAL_THRESH
export CV_SVC_CUG_LOGFILE
#
```

```
#  CBX 500 shared switching fabric thread bandwidth limit enforcement
#
#    When this variable is set to "TRUE" CascadeView will restrict the sum
#    of the logical port bandwidth on two IOMs sharing a common switching
#    fabric thread to the thread's maximum supported bandwidth.  Setting this
#    variable to "FALSE" will disable this restriction and permit logical
#    ports to oversubscribe the thread.
#
CV_ENFORCE_CBX500_THREAD_BW_LIMIT=TRUE
export CV_ENFORCE_CBX500_THREAD_BW_LIMIT
#
#  Config for Loading Profile Rate Tables
#
CV_PROFILE_DISCARD_FILE=/opt/CascadeView/etc/cvDiscard.dat
CV_PROFILE_CONGESTION_FILE=/opt/CascadeView/etc/cvCongestion.dat
CV_PROFILE_RIF_FILE=/opt/CascadeView/etc/cvRif.dat
CV_PROFILE_RDF_FILE=/opt/CascadeView/etc/cvRdf.dat

export CV_PROFILE_DISCARD_FILE
export CV_PROFILE_CONGESTION_FILE
export CV_PROFILE_RIF_FILE
export CV_PROFILE_RDF_FILE
#
# Env variable to DISABLE Get Card Status action before an
# ADD or DELETE or MODIFY is performed on a Circuit object
#CV_CARD_STATS=DISABLE
#export CV_CARD_STATS
#
# Config for saving statistics directory
# Note: directory must be writable by others
#
CV_SAVE_STATS_DIR=
export CV_SAVE_STATS_DIR

#
# Default trunk OSPF area
#
CV_DEFAULT_TRUNK_OSPF_AREA=0.0.0.1
export CV_DEFAULT_TRUNK_OSPF_AREA

#
```

```
# Caching Dialogs
# To cache a dialog, and therefore only create one instance of it,
# set the CV_CACHE_SET_ALL_LPORTS_DIALOG environment variable to TRUE.
#
# Caching LPort screens
CV_CACHE_SET_ALL_LPORTS_DIALOG=
export CV_CACHE_SET_ALL_LPORTS_DIALOG


#
#
# The following environment variable allows the user to enable
# Drag and Drop. To do this, uncomment out the “export XENVIRONMENT”
# line and restart ovw.
#
XENVIRONMENT=/opt/CascadeView/app-defaults/CVEnableDragDrop
# export XENVIRONMENT
#  end cascadeview.cfg
#
```

cascadeview.cfg Variables

The *cascadeview.cfg* file contains the following variable descriptions:

CV_TRACE_ENABLED=0 — This trace tool variable is for Ascend Customer Support diagnostic purposes only. Set to 1 to enable tracing.

CV_TRACEFILE — Specifies the location of the trace file.

CV_ERROR_MSG_CAT_PATH=/opt/CascadeView/nls/C/cascadeview-errors.cat — Sets the location of the error file that NavisCore uses. **Do not modify** this path and filename.

CVDB_TRACE_FILE_NAME — Displays the trace filename for database trace. This file is used by Ascend Customer Support in conjunction with the previous trace variable.

CV_DEF_ADDRESS_SIGNIFICANCE=2 # local — Indicates that the addressing scheme used for DLCIs is of local significance only. A DLCI must only be unique to a logical port. **Do not modify** this value.

CV_DEF_NETWORK_NUMBER — Displays the internal IP address for the Ascend network. The NMS uses this number to contact and communicate with the gateway switch. This number must be a unique number within the LAN environment and must not be the same as any external Ethernet address. See Chapter 3, “Creating and Managing Network Maps” for more information about configuring the network number for the NMS.

CV_SWITCH_INIT_FILEDIR=/var/CascadeView/initFiles — Sets the location of the switch initialization files. **Do not modify** this path and filename.

CV_SYNC — These variables provide specific PRAM sync information:

CV_SYNC_FILE_DIR=/tftpboot/cv_cfgSyncFiles – Sets the location of the following PRAM synchronization files. **Do not modify** this path and filename.

CV_SYNC_CHECK_DELAY=8

CV_SYNC_CHECK_INTERVAL=3

CV_SYNC_CHECK_COUNT=10

CV_SYNC_FILE_OFFLINE_LIST=/tftpboot/cv_cfgSyncFiles/offline.lst (*B-STDX only*) — Sets the location of the offline PRAM synchronization files. **Do not modify** this path and filename.

CV_SNMP_IS_ENABLED=1 — This setting enables SNMP. **Do not modify**.

CV_SNMP_REQUEST_TIMEOUT =256 — This variable is not used.

CV_SNMP_MAX_RETRIES=4 — Specifies the number of retries the SNMP client attempts before it declares a timeout. The default is 4. In larger networks where the NMS is on a very busy LAN segment or is multiple hops away from the switch that contains the Ethernet module, you may need to increase this value to 5.

CV_SNMP_RETRY_INTERVAL=30 — Specifies the amount of time (in tenths of a second) between SNMP retries. CPU-intensive operations, such as PRAM synchronization, can cause NavisCore to drop node polls. Increase the amount of time between SNMP retries to avoid this problem. Restart OpenWindows if you modify this value.

Ascend recommends a value of 30 seconds for a configuration with 10 to 15 simultaneous instances of NavisCore and more than 15 switches in the network.

CV_PUBLIC_COMMUNITY=public — Specifies the SNMP public community name.

CV_SNMP_READ_WRITE_COMMUNITY=cascade — Specifies the default master community name of the NMS. Each NMS you define must use this name.

CV_SNMP_NMS_HOSTNAME — Specifies an alternate SNMP hostname. Use this variable if your NMS has more than one IP interface. The default for this variable is the NMS with one IP interface.

CV_BG_DIAG_POLL_INTERVAL=3 — This variable has no effect since background diagnostics do not poll the background diagnostic result.

CV_FG_DIAG_CHECK_DELAY=5 — Sets the time delay (in seconds) that the NMS waits before it sends the first PDU to check that foreground diagnostics are complete.

CV_FG_DIAG_CHECK_INTERVAL=1 — The NMS sends a “check PDU” multiple times until the diagnostics are complete. The CHECK_INTERVAL is the interval (in seconds) between the check PDUs.

CV_FG_DIAG_CHECK_COUNT=3 — The CHECK_COUNT is the maximum number of check PDUs that the NMS will send.

The value of CHECK_COUNT is used as the interval and the value of CHECK_INTERVAL is used as the count. **Do not modify** these values.

CV_DIAG_REASON_CATALOG=/opt/CascadeView/nls/C/cvDiagReasons.cat — This variable points to the catalog file that contains the diagnostics result strings. **Do not modify** this path and filename.

CV_NODE_QOS_POLL_TIMER=300 — Sets the default value for the Quality of Service (QoS) statistics for retrieving circuit data from the switches.

CV_STATUS_POLL_INTERVAL=90 — The NMS node poll status interval variable sets the time interval that NavisCore uses to poll the nodes in the network. The default value is in seconds and the default is 5 minutes (300 seconds).

You can change the interval based on the number of users running NavisCore. A system with 30 users polls approximately once every 10 seconds. This change takes effect when you restart HP OpenView. In a configuration with 10-15 simultaneous instances of NavisCore, 60 seconds is an acceptable value for this variable.

The following "CV_PPORT_DEF" values are used for physical port performance tuning. **Do not modify** these values.

- CV_PPORT_DEF_DISCARD_HIGH=32
- CV_PPORT_DEF_DISCARD_LOW=10
- CV_PPORT_DEF_AQL_THRESHOLD=16

CV_SMDS_MASK_SIZE=6 (*B-STDX only*) — Use this variable to modify the size of the SMDS address mask for the entire network map. The mask size indicates the number of address digits a switch uses to make a switching decision. Valid values are 1 through 15. A mask size of 0 will disable the SMDS switching system. For more information, see the *NavisCore SMDS Configuration Guide*.

CV_DISABLE_SMDS_SS=0 (*B-STDX only*) — Use this variable to enable (0) or disable (1) the SMDS switching system for the entire NavisCore network. If you modify this value, you must PRAM Sync each CP card in the network.

CV_AUDIT_TRAIL_ENABLE=TRUE — Use this variable to enable (TRUE) or disable (FALSE) the Audit Trail utility. If you modify this variable, you must shut down and then restart NavisCore. For more information about the Audit Trail utility, refer to page 2-6.

CV_OUT_OF_SYNC_REFRESH_CNT=5 — The map you display in each session of NavisCore refreshes every N node polls, where N is the number of specified node polls. To refresh, NavisCore checks the database for any out-of-sync conditions. Edit this variable to modify the refresh rate. To disable this feature, set this variable to 0.

CV_ENABLE_HSSI_PPORT_OVERCLOCKING=FALSE (*B-STDX only*) — Use this variable if you must exceed the maximum HSSI module capacity. The total bandwidth of all physical ports on the HSSI module can exceed the maximum module capacity of 44.212 Mbps. However, this setting can cause frame errors if all physical ports are running at full speed. To resolve this problem, set this variable to True.

CV_ENABLE_ATM_TRK_BW_OVERSUBSCRIBE=FALSE — If you set this value to True, the total bandwidth of all ATM OPTimum trunk logical ports on a single physical port can exceed maximum physical port bandwidth.

CV_MAX_INTERFACES_PER_STDX=150 — This value specifies the maximum number of logical ports that can be defined on an STDX switch. You can set this value between 0 and 254.

CV_ATMUNI_UNI_TYPE_DEFAULT=PUBLIC — This value is set to Public if at least one end of this connection attaches to a public network. It is set to Private if this connection resides completely within a private network. See the *NavisCore Frame Relay Configuration Guide* for more information about ATM UNI logical ports.

CV_ATMUNIDCE_CONN_TYPE_DEFAULT=NET_ENDSYS — This value is set to Net_Endsys if this port connects to a router or host. It is set to Net_Net if this port connects to another ATM switch. See the *NavisCore Frame Relay Configuration Guide* for more information about connection types.

CV_POLL_SERVER_PORT=10888 — This variable represents the port NavisCore polls when using the Poll Server function. The default value is 10888. The value must match the POLL_SRV_SRV_PORT. See Appendix C, “Configuring Poll Server” for more information.

CV_POLL_SERVER_ADDRESS=localhost — This variable is required and provides the IP address (in dot notation) of the node used to run the Poll Server. If the Poll Server runs on the same node as NavisCore, this variable is set to a value of “localhost.” Setting this variable and the CV_POLL_SERVER_PORT variable enables Poll Server. See Appendix C, “Configuring Poll Server” for more information.

CV_ENABLE_MOVE_ALL_CIRCUIT=TRUE — If this variable is set to True, the Move Circuit function is enabled for this network; if set to False, it is disabled. See your switch configuration guide for information about the Move Circuit function.

CV_MV_CKT_CARD_TYPE_CHECKING=TRUE — The Move Circuit function fails if the number of circuits moved exceeds the maximum allowed for the IOM. If this variable is set to True, the NMS notifies you that this problem exists before you move the circuit. If you set this variable to False, notification is not sent.

CV_CUR_VPNCUST — Indicates the current view (binding) for this map, either VPN or Customer.

CV_CUR_VPN_NAME — If CV_CUR_VPNCUST indicates a VPN binding, this variable displays the VPN name the map is using.

CV_CUR_CUST_NAME — If CV_CUR_VPNCUST indicates a customer binding, this variable displays the customer name the map is using.

CV_LOGON_TYPE — This variable displays the logon privilege you enabled for this map, either Operator or Provisioning.

CV_CKT_PRIORITY_LEVELS=FOUR — This variable represents the time interval (in seconds) to refresh QoS metrics. Valid values are FOUR and SIXTEEN. The range is 300 to 1799.

CV_310_BULK_LPORT=FALSE — This variable adds the Bulk LPort Create button to the Set All Lobical Ports dialog box. This feature is disabled by default.

CV_NET_DIST_EVAL_INTERVAL=2 — This variable represents the number of seconds to pause between evaluations when determining the network distribution of a distributed Ascend object. It is used when defining an evaluation threshold for an Ascend distributed object. Valid values range from 1 to 60.

CV_SVC_CUG_NODE_EVAL_THRESH=0 — This variable represents the number of nodes (out of all the nodes in the network to be evaluated) on which to match configured SVC addresses before pausing for the number of seconds identified by the variable CV_NET_DIST_EVAL_INTERVAL. A value of zero (0) results in all nodes in the network being evaluated at once with no pause.

CV_SVC_CUG_LOGFILE — This variable represents the path and filename used to log the results of matching configured SVC addresses when determining if a node belongs in a member rule's network distribution. A valid value enables logging. A null or invalid value disables logging. The NavisCore process ID will be appended to the filename.

CV_ENFORCE_CBX500_THREAD_BW_LIMIT=TRUE — When set to True, this variable will restrict the sum of the logical port bandwidth on two IOMs sharing a common switching fabric thread to the thread's maximum supported bandwidth. A False setting will permit logical ports to oversubscribe the thread.

CV_PROFILE — These variables specify the location of the default buffer threshold and rate profile files used for the ATM FCP card. The ATM FCP uses these tables to determine the available bandwidth, the rate increase factor (RIF), and the rate decrease factor (RDF) for each VC on a port. See the *NavisCore ATM Configuration Guide* for more information.

CV_PROFILE_DISCARD_FILE=/opt/CascadeView/etc/cvDiscard.dat – Sets the location of the default discard file for NavisCore.

CV_PROFILE_CONGESTION_FILE=/opt/CascadeView/etc/cvCongestion.dat – Sets the location of the default congestion file for NavisCore.

CV_PROFILE_RIF_FILE=/opt/CascadeView/etc/cvRif.dat – Sets the location of the default RIF file for NavisCore.

CV_PROFILE_RDF_FILE=/opt/CascadeView/etc/cvRdf.dat – Sets the location of the default RDF file for NavisCore.

CV_CARD_STATS — This variable is used to disable the "Get Card Status" activity before an add, delete, or modify is performed on a circuit object. This feature is enabled by default.

CV_SAVE_STATS_DIR — This variable identifies the directory used for storing various configuration statistics. The directory must have write privileges.

CV_DEFAULT_TRUNK_OSPF_AREA — This variable identifies the default trunk OSPF area.

CV_CACHE_SET_ALL_LPORTS_DIALOG — This variable, when set to True, caches a dialog.

XENVIRONMENT=/opt/CascadeView/app-defaults/CVEnableDragDrop — This variable, when uncommented, enables drag and drop functionality. You may need to restart HP OpenView.

C

Configuring Poll Server

This release provides the optional Poll Server function, which does not run automatically until you configure and start it. By using Poll Server, you can reduce NavisCore's status-polling overhead when there are multiple NavisCore users monitoring the network simultaneously. If there are more than five NavisCore sessions running, using the Poll Server is the most efficient way to poll the switches without causing switch congestion.

The Poll Server acts like a daemon running in the background waiting for requests from an NMS session. When the Poll Server receives a request for status information, it polls the switch. Any additional NMS sessions requesting data receive status information from the Poll Server directly.

As a general guideline, with 40 consecutive users and 50 switches in the network, the Poll Server uses approximately 2 MB of RAM.

To use the Poll Server, you must set corresponding parameters in both NavisCore and the Poll Server's environment variables. NavisCore uses these environment variables to locate the Poll Server. If the environment variables are not set, NavisCore assumes that Poll Server is not present and therefore communicates directly with the switch(es).

NavisCore Environment Variables

The environment variables that configure Poll Server for NavisCore are set in the *cascadeview.cfg* file (default directory */opt/CascadeView/etc*). The *cascadeview.cfg* file sets these variables such that the Poll Server is disabled. If you make changes to these variables in *cascadeview.cfg*, you must start the Poll Server node and restart all NavisCore sessions for the changes to take effect. For information about modifying the *cascadeview.cfg* file, see Appendix B, "The NavisCore Configuration File".

Table C-1 describes the main parameters used to configure NavisCore to use the Poll Server function.

Table C-1. Poll Server Parameters (in cascadeview.cfg)

Parameter	Description
CV_POLL_SERVER_PORT	The port NavisCore polls when using the Poll Server. The default is 10888. This parameter is required and must match the POLL_SRV_SRV_PORT parameter (described in Table C-2). ***Note:*** *As a minimum configuration, set this parameter to 10888, and set* CV_POLL_SERVER_ADDRESS *to the node where the Poll Server is running.*
CV_POLL_SERVER_ADDRESS	IP address (in dot notation) of the node used to run the Poll Server. If the Poll Server runs on the same node as NavisCore, you can specify "localhost." To use Poll Server, you must set this variable. ***Note:*** *As a minimum configuration, set this parameter to the node where the Poll Server is running, and set* CV_POLL_SERVER_PORT *to 10888.*
CV_STATUS_POLL_INTERVAL	*(Optional)* Status polling interval used by NavisCore. The default is 300 seconds. This setting should be greater than the POLL_TIME_INTERVAL setting.

Poll Server Environment Variables

You configure the "pollsrv" environment variables in the *run-pollsrv.sh* file, which is located in the */opt/CascadeView/bin* directory.

Table C-2 describes the main parameters used to configure the Poll Server function.

Table C-2. Poll Server Parameters (in run-pollsrv.sh)

Parameter	Description
POLL_SRV_SRV_PORT	*(Optional)* The port used to receive polls from NavisCore. This setting must match the CV_POLL_SERVER_PORT setting (described in Table C-1). The default is 10888.
POLL_SRV_COMMUNITY	*(Optional)* The default value for the community name used to poll switches. The default is "public."
POLL_TIME_INTERVAL	*(Optional)* The polling interval used to poll switches. This setting should be less than the CV_STATUS_POLL_INTERVAL setting. The default is 20 seconds.

Table C-2. Poll Server Parameters (in run-pollsrv.sh) (Continued)

Parameter	Description
POLL_SRV_DEV_PORT	*(Optional)* The port used when polling switches. This value is normally not changed. The default is 161.
POLL_SRV_DEV_TIMEOUT	*(Optional)* The timeout value used when polling switches. The default is 1500 milliseconds.
POLL_SRV_DEV_RETRIES	*(Optional)* The number of retry attempts for polling. This value is normally not changed. The default is 4.

Minimum Configuration

The minimal configuration that enables NavisCore to use the Poll Server is to set CV_POLL_SERVER_PORT to 10888 and CV_POLL_SERVER_ADDRESS to the node where the Poll Server is running. If the Poll Server runs on the same node, a value of “localhost” can be used. If these environment variables are not set, NavisCore will poll the switches directly.

The Poll Server expects that the community string to be sent to the switch will be embedded in the string that is sent from the client. If this is not found, it will use the environment variable POLL_SRV_COMMUNITY as the community name for the switches. The same value is used for all switches.

The Poll Server periodically refreshes its cached values. The expiration time for a value is given by POLL_TIME_INTERVAL. This value should be lower than the CV_STATUS_POLL_INTERVAL, because values collected more frequently than the POLL_TIME_INTERVAL will not reflect changes.

Starting and Stopping Poll Server

This section describes how to start and stop the Poll Server function. The following steps assume the default NavisCore directory is */opt/CascadeView.* If your default directory is in a different location, substitute accordingly.

When starting and stopping Poll Server (pollsrv), be sure to exit and restart all NavisCore sessions to take advantage of the configured polling service.

Starting Poll Server

To start the Poll Server:

1. As the root user, enter the following command to start the Poll Server (pollsrv):

   `/opt/CascadeView/bin/start-pollsrv.sh`

   This command adds the "run-pollsrv.sh" entry in the */etc/inittab* file and starts the pollsrv process.

2. Edit */opt/CascadeView/etc/cascadeview.cfg* as follows:

   Locate and uncomment the following CV_POLL_SERVER environment variables:

   ```
   CV_POLL_SERVER_PORT
   CV_POLL_SERVER_ADDRESS
   export CV_POLL_SERVER_PORT CV_POLL_SERVER_ADDRESS
   ```

   Verify there is no **#** sign before the three environment variables.

3. (*Optional*) You may customize the Poll Server-related variables at this point.
4. Press the Escape key.
5. Enter **:wq!**

Any NavisCore sessions started after you complete these steps will use the Poll Server.

Stopping Poll Server

To stop the Poll Server:

1. As the root user, enter the following command:

   `/opt/CascadeView/bin/stop-pollsrv.sh`

   This command removes the “run-pollsrv.sh” entry in the */etc/inittab* file and stops the pollsrv process.

2. Edit */opt/CascadeView/etc/cascadeview.cfg* as follows:

   Locate and comment out the following CV_POLL_SERVER environment variables:

   `CV_POLL_SERVER_PORT`

   `CV_POLL_SERVER_ADDRESS`

   Any NavisCore sessions started after you complete these steps no longer use the Poll Server.

Glossary

A

absolute congestion

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

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).

alarm

Message notifying an operator or administrator of a network problem.

Alarm Indication Signal

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

alternate path

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

amber frames

Ascend's own class of packet frames used to identify packets as they travel through the Frame Relay network. The network forwards amber frames with the Discard Eligible bit set; therefore the packet is eligible for discard if it passes through a congested node.

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.

ANSI

See *American National Standards Institute*.

ASCII

See *American Standard Code for Information Interchange*.

ASCII text file

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

Asynchronous Transfer Mode

A method used for transmitting voice, video, and data over high-speed LAN and WAN networks. See also *cell relay*.

ATM

See *Asynchronous Transfer Mode*.

B

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.

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.

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*.

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.

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

CBR

See *Constant Bit Rate*.

cell

Any fixed-length data packet. For example, ATM uses fixed-length, 53-byte cells. See also *cell relay*.

Cell Loss Priority

A field in the ATM cell header that indicates the eligibility of the cell for discard by the network under congested conditions.

cell relay

A form of packet transmission that uses a fixed-length, 53-byte cell over a packet-switched network; also known as Asynchronous Transfer Mode (ATM).

CIR

See Committed Information Rate.

circuit

A communications channel or path between two devices.

circuit switching

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

client

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

CLP

See Cell Loss Priority.

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.

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).

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.

Constant Bit Rate

A Quality of Service class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery of bits.

Control Processor

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

CP

See *Control Processor*.

D

daemon

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

data bits

In asynchronous transmission, the bits that actually contain the data being sent. Also called “payload” in some transmission methods.

Data Link Connection Identifier

A 10-bit address that identifies PVCs.

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.

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.

destination address

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

DLCI

See *Data Link Connection Identifier*.

domain

A network community of users sharing the same database information.

E

Explicit Forward Congestion Indication

One of the congestion feedback modes allowed in the Available Bit Rate (ABR) service. In the EFCI marking mode, the switch sets a bit in the headers of forward cells to indicate congestion; these are then turned around at the destination end system and sent back to the source end system.

EFCI

See Explicit Forward Congestion Indication.

environment variable

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

Extended Superframe Format

In Frame Relay, a frame structure that extends the DS1 superframe structure from 12 to 24 frames, for a total of 4632 bits. This format redefines the 8-Kbps channel consisting of framing bits previously used only for terminal and robbed-bit signaling synchronization.

F

failed LED

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

Flow Control Processor

A processor that supports ATM traffic management through binary, hop-by-hop, closed-loop flow-control algorithms.

FCP

See Flow Control Processor.

Frame Relay

A type of data transmission based on a packet-switching protocol, with transmission rates up to 2 Mbps. Frame Relay provides for bandwidth-on-demand.

Frame Relay Assembler/Disassembler

A function that enables a logical port to perform Frame Relay encapsulation/de-encapsulation for HDLC/SDLC-based protocols. The FRAD function encapsulates HDLC/SDLC traffic entering an Ascend Frame Relay network and de-encapsulates it upon exiting the network. This function is restricted to one point-to-point PVC.

Frame Relay RFC1294 Multi-protocol Encapsulation

A specification allowing for a single circuit to be established between two devices.

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.

globally significant DLCI

A feature of the Local (or Link) Management Interface (LMI) enhancement to Frame Relay that enables DLCIs to use the same connection-identification scheme across the network (global values) to specify individual end devices.

good LED

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

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

HDLC

See *High-level Data Link Control.*

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.

host name

A unique name identifying a host system.

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*.

I

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 Module

A module in a switch that manages the lowest level of a node's trunk or user interface. HSSI can operate over a 50-ft (15m) shielded twisted-pair cable.

Input/Output Processor

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

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.

Internet Protocol

The TCP/IP session-layer protocol that regulates packet forwarding.

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.

ISDN

See Integrated Services Digital Network.

IOA

See *Input/Output Adapter*.

IOM

See Input/Output Module.

IOP

See *Input/Output Processor*.

IP

See *Internet Protocol*.

IP address

See *Internet Protocol address*.

K

Kbps

Kilobits per second.

keep-alives

A series of polling messages used in the Local (or Link) Management Interface (LMI) of a Frame Relay port to verify link integrity between devices.

L

LAN

See *Local Area Network*.

LAP

See *link-state routing 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-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*.

locally significant DLCI

In Frame Relay, an identifier or address that specifies a local router, PVC, SVC, or endpoint device. It is reusable at non-overlapping endpoints and allows for scalability. Compare with *globally significant DLCI*.

logical port

A configured circuit that defines protocol interaction.

M

management DLCI

A value that specifies a PVC or SVC from a LAN connected via a router to a Ascend switch over a Frame Relay network.

Management Information Base

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

marginal LED

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

Mbps

Megabits per second.

MIB

See *Management Information Base*.

mild congestion

In Frame Relay, the state of a link when the threshold (more than 16 buffers by default) is exceeded.

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 Management Station

A device used to configure and manage the network.

NMS

See Network Management Station.

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.

node processor

A control module present in the GX 550 switch that controls the switch and interacts with multiple input/output processor (IOP) modules.

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.

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.

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-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.

Parameter Random Access Memory

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

path

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

PDU

See Protocol Data Unit.

Permanent Virtual Circuit

A logical connection across a packet-switched network that is always in place and always available along a predetermined network path. See also *Virtual Circuit*.

Point-to-Point Protocol

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

polling

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

PPP

See *Point-to-Point Protocol*.

PRAM

See *Parameter Random Access Memory*.

Protocol Data Unit

A unit of data consisting of control information and user data exchanged between peer layers.

PVC

See *Permanent Virtual Circuit*.

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

RADIUS

See Remote Authentication Dial-In User Service.

Random Access Memory

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

RAM

See *Random Access Memory*.

red alarm

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

red frames

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

redundancy

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

Remote Authentication Dial-In User Service

A distributed security system which uses an authentication server to solve the security problems associated with remote computing.

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.

S

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

In Frame Relay, 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.

shortest path routing

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

Simple Network Management Protocol

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

SLIP

See *Serial Line over Internet Protocol*.

SNMP

See *Simple Network Management Protocol*.

SP

See Switch Processor.

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.

SVC

See *Switched Virtual Circuit*.

Switch Processor

A control module present in the CBX 500 switch that controls the switch and interacts with multiple input/output processor (IOP) modules.

Switched Multimegabit Data Services

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

Switched Virtual Circuit

A logical connection across a packet-switched network providing as-needed connections to any other node in the network. See also *Virtual Circuit*.

synchronization

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

synchronous transmission

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

T

telnet

The Internet standard protocol for remote terminal-connection services.

throughput

The actual speed of the network.

traffic shaping

In Frame Relay, a set of rules that describes traffic flow. The sender has a mechanism to ensure that the transmission of its guaranteed packets behaves in a certain way. The network knows what kind of traffic to expect, and can monitor the behavior of the traffic.

Transmission Control Protocol

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

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.

U

UDP

See User Datagram Protocol.

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.

V

VC

See *Virtual Circuit*.

VCI

See Virtual Circuit Identifier.

Virtual Circuit

A logical circuit set up to ensure reliable communication between two network devices. See also *PVC* and *SVC*.

Virtual Circuit Identifier

A 16-bit field in the ATM cell header that is used as an addressing identifier to route cell traffic.

Virtual Path Identifier

An 8-bit field in the ATM cell header that is used as an addressing identifier to route cell traffic.

Virtual Private Network

A network configuration that provides dedicated bandwidth and guaranteed performance, reliability, and privacy.

VPI

See Virtual Path Identifier.

VPN

See Virtual Private Network.

W

WAN

See *Wide Area Network*.

Wide Area Network

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

Index

A

B

C

D

E

G

H

I

K

L

M

N

O

P

R

S

T

U

V

X