Lucent Technologies
Bell Labs Innovations

B-STDX, CBX, and GX ATM Services Configuration Guide

Product Code: 80191
Revision 000
April 2003

Copyright© 2003 Lucent Technologies. All Rights Reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies.

For permission to reproduce or distribute, please contact: Technical Publications, Integrated Network Solutions/Core Switching Division at 978-692-2600.

Notice. Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Trademarks. NavisXtend and NavisCore are trademarks of Lucent Technologies. IP Navigator, Navis, CBX 500, GX 550, and B-STDX 9000 are registered trademarks of Lucent Technologies. Other trademarks and trade names mentioned in this document belong to their respective owners.

Limited Warranty. Lucent Technologies provides a limited warranty to this product. For more information, see the software license agreement in this document.

Ordering Information. To order copies of this document, use the online ordering instructions presented later in this guide.

Support Telephone Numbers. For technical support and other services, see the customer support contact information in the “About This Guide” section of this document.

LUCENT TECHNOLOGIES END-USER LICENSE AGREEMENT

LUCENT TECHNOLOGIES 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 LUCENT SWITCH(ES) CONTAINING THE SOFTWARE, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. OPENING THE PACKAGE(S) OR USING THE LUCENT 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, LUCENT 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 LUCENT, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Lucent 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 Lucent'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 Lucent'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. Lucent's Rights. You agree that the Software and the User Documentation are proprietary, confidential products of Lucent or Lucent'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 Lucent or Lucent'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 Lucent. Lucent may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Lucent, you agree to return to Lucent the Program and all copies or portions thereof. Termination of this License Agreement shall not prejudice Lucent's rights to damages or any other available remedy.

5. Limited Warranty. Lucent warrants, for your benefit alone, for a period of 90 days from the date of shipment of the Program by Lucent (the "Warranty Period") that the program diskettes in which the Software is contained are free from defects in material and workmanship. Lucent 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 Lucent of any warranties made under this Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM IS LICENSED "AS IS", AND LUCENT 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. Lucent'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 Lucent for the use of the Program. In no event shall Lucent be liable for any indirect, incidental, consequential, special, punitive or exemplary damages or lost profits, even if Lucent has been advised of the possibility of such damages.

7. Proprietary Rights Indemnification. Lucent 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 Lucent 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 Lucent to direct the defense and settlement of the claim, and (c) provide Lucent with the authority, information, and assistance that Lucent 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 Lucent's written consent. In any action based on such a claim, Lucent 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 Lucent, 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, Lucent 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 Lucent 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 Lucent 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 Lucent 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

About This Guide

What You Need to Know xxix
Reading Path xxxi
    Documentation for New Modules xxxiii
How to Use This Guide xxxiv
What's New in This Guide xxxvi
Conventions xxxviii
Related Documents xxxix
    Lucent xxxix
    Third Party xl
Ordering Printed Manuals Online xli
Customer Comments xli
Technical Support xli

Chapter 1 Overview

Logical Ports 1-1
CBX 500 ATM Flow Control Processor 1-2
ATM Trunks 1-2
PVCs 1-2
Network-wide Features 1-3
Fault-tolerant PVCs 1-3
Resilient Local Management Interface 1-3
SVCs 1-4
    SVC Proxy Signaling 1-4
    SPVCs 1-4
    Closed User Groups 1-5
    Port Security Screening 1-5
PNNI 1-5
Connection Admission Control 1-5
ATM Traffic Descriptors 1-6
CBX 500 Shared SP Threads 1-6
Priority Routing 1-6

Reliable Scalable Circuit....1-6
OSPF Name Aggregation....1-7
Customer Names....1-7
Abbreviations and Acronyms....1-7

Chapter 2 About ATM Logical Ports

ATM UNI Concepts....2-2
ATM UNI DCE and DTE....2-2
ATM UNI 4.0 Support....2-3
Using Interim Link Management Interface (ILMI)....2-4
ILMI VCC Trap Support....2-5
Using Logical Port Signaling....2-5
ILMI and Signaling Example....2-6
Configurable Control Circuits....2-6
ATM OPTimum Cell Trunk....2-7
Configuring the Virtual Path Identifier (VPI)....2-7
Configuring the OPTimum Trunk for VPCs....2-8
PVC/SVC VPC Connections....2-8
IP-Related Connections....2-8
ATM Direct Trunk....2-9
ATM CE....2-9
ATM NNI....2-9
Virtual UNI/NNI....2-10
Virtual Paths and Virtual Channels....2-11
Setting the Number of Valid Bits in the VPI/VCI....2-11
VPI/VCI Bit Allocation (CBX 500/GX 550)....2-12
Configuring VCC VPI Start and Stop Values for Virtual UNI/NNI....2-15
About Logical Port Bandwidth....2-16
Modifying Logical Port Bandwidth....2-17
CBX 500 SP Thread Bandwidth Available for Logical Ports....2-17
About the Oversubscription Factor....2-18
About VP Shaping on the CBX 500....2-19
About VP Shaping on the GX 550....2-20
Administrative Tasks....2-21
Using Templates....2-21
Modifying Switch Configuration Attributes....2-22
Non-Disruptive Logical Port and Trunk Attributes (CBX 500 and GX 550 Only)....2-22
Deleting ATM Logical Ports....2-24
Deleting Circuits....2-24
Deleting Trunks....2-25
Deleting Management VPI/VCIs....2-25
Deleting the Logical Ports....2-26

Chapter 3 Configuring CBX 500 or GX 550 Logical Ports

Accessing ATM Logical Port Functions....3-2
About the Set All Logical Ports in PPort Dialog Box....3-5
Defining a Logical Port....3-9
Selecting a Logical Port Type....3-10
About the Set Attributes Menu....3-11
Administrative Attributes....3-14
Configuring VP Shaping on CBX 500 Virtual UNI Logical Ports....3-19
Before You Begin....3-19
Virtual ATM UNI Logical Port Configuration Considerations....3-19
Modifying the VP Shaping Mode on GX 550 Virtual UNI Logical Ports....3-21
ATM Attributes....3-22
ILMI/Signaling/OAM Attributes....3-28
Setting Logical Port Signaling Tuning Parameters....3-33
ATM FCP Attributes....3-36
Traffic Descriptors Attributes....3-37
OPTimum Trunk VPI Range Attributes....3-38
Selectable Statistics Attributes....3-42
Completing the Logical Port Configuration....3-43
Setting Quality of Service Parameters....3-44
Setting SVC Quality of Service Parameters....3-47
Configuring Virtual ATM UNI/NNI Logical Ports....3-49
Configuring Logical Ports for Use With ATM SVCs....3-50
Defining SVC Connection ID Parameters Attributes....3-50
Defining SVC Parameters Attributes....3-52
Calling Party Parameters....3-52
Transit Network Parameters....3-56
CUG Parameters....3-57
Simultaneous SVC Limit Parameters....3-58
Additional Set SVC Parameters Attributes Menu Fields....3-59
Defining SVC Priorities Attributes....3-61
Defining SVC Traffic Descriptor (TD) Limits Attributes....3-64
Defining ATM SVC Parameters Attributes....3-67

Chapter 4 Configuring ATM Logical Ports on the B-STDX 8000/9000

About ATM Logical Ports....4-2
ATM UNI DCE....4-2
ATM UNI DTE....4-2
ATM Direct Trunk/Direct Cell Trunk....4-2
ATM OPTimum Cell Trunk....4-3
ATM OPTimum Frame Trunk....4-4
Network Interworking for Frame Relay Network-to-Network Interface....4-4
Setting the Number of Valid Bits in VPI/VCI for B-STDX 8000/9000....4-5
Using VP Shaping....4-6
I/O Modules for ATM Services....4-7
Configuring Ports for ATM DXI/FUNI and ATM Services....4-8
I/O Modules for ATM Interworking Services....4-8

Logical Port Congestion Thresholds....4-9
About ATM Logical Port Functions....4-10
About the Set Attributes Menu....4-10
Selecting an ATM Logical Port Type....4-13
Defining ATM UNI DCE/DTE Logical Ports....4-14
Administrative Attributes....4-15
Congestion Control Attributes....4-18
Trap Control Attributes....4-20
Priority Frame Attributes....4-22
ATM Attributes....4-23
ILMI/Signaling/OAM Attributes....4-25
Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports....4-27
Using Direct Cell Trunks....4-27
Using ATM OPTimum Cell Trunks....4-28
Administrative Attributes....4-29
Discard/Congestion Mapping Attributes....4-33
OPTimum Trunk VPI Range Attributes....4-35
Defining ATM OPTimum Frame Trunk Logical Ports....4-37
Defining ATM Network Interworking for Frame Relay NNI Logical Ports....4-42
Link Mgmt Attributes....4-44
Discard/Congestion Mapping Attributes....4-48
Completing the Logical Port Configuration....4-50

Chapter 5 About the ATM Flow Control Processor (FCP)

Modules Supported....5-2
Supported ATM Service Classes....5-3
ATM FCP Architecture....5-4
Closed-Loop Flow Control....5-5
Flow Control Mechanisms....5-5
RM Cell Generation....5-6
RM Cell Termination....5-6
CCRM Closed-Loop Flow Control....5-8
CCRM Closed-Loop Flow Control on a Trunk....5-8
CCRM Closed-Loop Flow Control on a UNI (Traffic Shaping)....5-9
CCRM Cell Generation....5-9
CCRM Cell Termination....5-9
BCM Closed-Loop Flow Control....5-10
BCM Closed-Loop Flow Control on a Trunk....5-10
BCM Closed-Loop Flow Control on a UNI....5-11
BCM Cell Generation....5-11
BCM Cell Termination....5-12
ABR RM Closed-Loop Flow Control....5-13
Cell Rate Adjustment....5-13
Initial Cell Rate (ICR) and ICR Constant....5-13
Idle Circuits and Idle VC Factor....5-13
Allowed Cell Rate....5-14
Rate Profile Tables....5-15
Per-VC Traffic Shaping....5-15

ATM FCP Queues....5-16
ATM Flow-Control Discard Mechanisms....5-18
VP Shaping....5-19
Shaping Rates....5-20
QoS Classes for VP Shaping....5-20
Multicast Cells....5-20

Chapter 6 Working with the ATM Flow Control Processor (FCP)

Configuration Process Overview....6-2
Enabling the FCP....6-2
Downloading Buffer Threshold and Rate Profile Tables....6-5
Setting Logical Port FCP Attributes....6-7
Frequently Asked Questions About the FCP....6-11
What happens if I disable the FCP?....6-11
What are the performance limitations of the FCP?....6-12
How many logical ports can I configure?....6-12
Configuration Options....6-12
Is the CI bit set when BCM cells are generated?....6-13
Why are RM cells not generated even though I am using the Auto RM Generation option?....6-13
How is fair bandwidth determined?....6-14
Why does the Early Packet Discard (EPD) option only work when enabled for all circuit connections?....6-15

Chapter 7 Configuring Trunks

About Administrative Cost....7-2
About Link Trunk Protocol....7-3
Trunk Delay....7-3
Keep Alive Threshold....7-3
Static and Dynamic Delay....7-4
About Automatic Protection Switching....7-5
APS Options....7-5
Intra-card APS 1+1....7-6
APS Trunk Backup....7-6
APS Resilient UNI....7-7
Fast Inter-card APS 1+1....7-8
About Trunk Backup for the B-STDX 8000/9000....7-12
Configuring B-STDX Trunk Backup....7-13
Process for Switching Over to a Backup Trunk....7-13
Defining the Manual Trunk Backup Feature....7-13
Accessing Trunk Functions....7-14
About the Set All Trunks Dialog Box....7-15
Defining a Trunk....7-20
Using B-STDX 8000/9000 Trunk Backup....7-25
Configuring the Primary Trunk for Trunk Backup....7-25
Configuring the Backup Trunk for Trunk Backup....7-26
Creating a Trunk Line Connection....7-27
Displaying Multiple Trunks Between Switches....7-32

Understanding Trunk-Line Coloring....7-33
Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks....7-34
Before You Begin....7-34
Defining ATM Direct Trunk Logical Ports....7-34
Defining ATM Direct Trunks for APS Trunk Backup and Fast APS 1+1....7-36
Configuring the Primary Trunk for APS Trunk Backup....7-36
Configuring the Backup Trunk for APS Trunk Backup....7-37
Configuring the Primary Trunk for Fast APS 1+1....7-37
Configuring Fast APS 1+1 for PNNI Links (GX 550 to PSAX 4500 Only)....7-39
Before You Begin....7-39
Defining ATM NNI Logical Ports for PNNI Links....7-39
Configuring External Trunks....7-44
Adding an External Device Object to the Network Map....7-45
Configuring an External Interface....7-50
Adding an External Trunk....7-52
Configuring VNN OSPF....7-55
Configuring VNN OSPF Loopback Addresses....7-55
Configuring VNN Area Aggregates....7-57
Configuring VNN OSPF Virtual Links....7-59
Configuring VNN/OSPF External Route Aggregates....7-60
Configuring VNN External Route Aggregates....7-61
Configuring OSPF External Route Aggregates....7-64
Configuring VNN OSPF Optimized Flooding....7-66
About VNN OSPF Optimized Flooding....7-66
Interoperability in Lucent Switch Networks....7-68
Enabling and Disabling VNN OSPF Optimized Flooding....7-68
Monitoring VNN OSPF Optimized Flooding....7-69
Configuring VNN OSPF Name LSA Suppression....7-70
About VNN Name LSA Suppression....7-70
Enabling and Disabling VNN Name LSAs....7-70
Monitoring VNN Name LSA Suppression....7-72

Chapter 8 Configuring ATM PVCs

GX 550 VC Provisioning Guidelines....8-2
PVC Endpoint Rules....8-4
PVC Establishment Rate Control....8-5
VC Overload Control and PVC Establishment Rate Control....8-5
PVC Establishment Rate Control When VC Overload Control Is Enabled....8-5
PVC Establishment Rate Control When VC Overload Control Is Disabled....8-5
VC Overload Control....8-6
About VC Overload Control....8-6
About Overload Severity Levels....8-7
Reliable Scalable Circuit....8-8
Disabling the Reliable Scalable Circuit Feature....8-8
Setting the VPI/VCI Values for PVCs....8-9
Accessing the Set All PVCs On Map Dialog Box....8-10

About the Set All PVCs On Map Dialog Box....8-11
About Redirect PVCs....8-15
Accessing the Set All Redirect PVCs On Map Dialog Box....8-16
About the Set All Redirect PVCs On Map Dialog Box....8-17
Defining a PVC Connection....8-22
Configuring an ATM Service PVC....8-25
About the Set Attributes Menu....8-26
Administrative Attributes....8-27
How PVC Routing Thresholds Interact With LPort Routing Metrics....8-28
Traffic Type Attributes....8-30
User Preference Attributes....8-32
Frame Discard Attributes....8-36
Extended QoS Parameters Attributes....8-37
Selectable Statistics Attribute....8-39
Completing the PVC Configuration....8-40
Configuring Frame Relay-to-ATM Interworking Circuits....8-41
Frame Relay-to-ATM Service Interworking....8-41
Frame Relay-to-ATM Network Interworking....8-42
Configuring Link Management for the Frame Relay Logical Port....8-42
Special Network Interworking PVC Configuration Parameters....8-42
Rate Enforcement....8-45
Graceful Discard....8-46
Rate Enforcement Schemes....8-46
Frame Relay-to-ATM Parameters Conversion Formula....8-47
Defining Service or Network Interworking PVC Connections....8-48
Traffic Type Attributes....8-52
User Preference Attributes....8-57
Defining a Redirect PVC Connection....8-62
Completing the Redirect PVC Configuration....8-68
Setting the Redirect PVC Delay Time....8-68
Manually Defining the Circuit Path....8-69
Moving Circuits....8-73
Configuring Point-to-Multipoint Circuits....8-75
Defining a Point-to-Multipoint Circuit Root....8-79
Defining Point-to-Multipoint Circuit Leafs....8-84
Restrictions on Multiple Leafs on the Same Physical Port....8-85
Deleting a Point-to-Multipoint Circuit Root and Leafs....8-86
Using Templates....8-87
Deleting Circuits....8-87

Chapter 9 Configuring Management Paths

Using Management PVCs....9-3
Configuring a Management PVC....9-4
Defining a Standard MPVC Connection....9-4
Defining a Redirect MPVC Connection....9-6
Using Management VPI/VCI....9-8
Defining the Management VPI/VCI Connection....9-8
Using Management SPVCs....9-11

Using Management SPVCs in a PNNI Environment....9-11
Configuring Management SPVCs....9-11
Defining SVC Port Addresses....9-12
Defining the Management SPVC Connection....9-12
Completing the Management Configuration....9-15
Defining the NMS Path....9-15
Configuring the Attached Device....9-17

Chapter 10 Configuring ATM Traffic Descriptors

Overview....10-2
About Traffic Descriptors....10-3
About Quality of Service....10-3
About Logical Port Quality of Service Parameters....10-4
About Traffic Parameters....10-5
Configuring ATM Traffic Descriptors....10-9
Defining Network-wide Traffic Descriptors....10-9
Defining Traffic Descriptor Attributes....10-12
Deleting Traffic Descriptor Definitions....10-13
Control Channel Default Traffic Descriptors....10-14

Chapter 11 Configuring Layer2 VPNs

About Layer2 VPN....11-2
Configuring a Layer2 Virtual Private Network....11-4
Creating a Layer2 VPN....11-4
Adding Customers to the Layer2 VPN....11-5
Configuring a Logical Port for Layer2 VPN....11-7
Using the Layer2 VPN/Customer View Feature....11-8
Configuring a PVC for Layer2 VPN....11-10
Layer2 VPNs over PNNI....11-11
Layer2 Limitations on PNNI Links....11-11

Chapter 12 Configuring Fault-Tolerant PVCs

Configuring Fault-Tolerant PVCs....12-2
Creating a Primary Port....12-3
Creating a Backup Port....12-3
Creating Service Names....12-4
Activating a Backup Binding Port....12-6
Using APS with Resilient UNI....12-8
Working Port and Protection Port Configuration Guidelines....12-9
CBX 500 Considerations....12-9
GX 550 Considerations....12-9
APS Resilient UNI Over PNNI....12-9
Configuring APS Resilient UNI....12-10
Before You Begin....12-10
Defining ATM UNI Logical Ports on the Working Ports....12-10
Defining ATM UNI Logical Ports on the Protection Ports....12-11
Defining the APS Fault-tolerant PVC/Resilient UNI Configuration....12-12

Chapter 13 Configuring Resilient LMI

Resilient LMI Terms 13-2
Configuration Guidelines 13-4
Resilient LMI Configuration Sequence 13-5
Creating Service Names 13-6
Configuring the RLMI Switchover Mode 13-10

Chapter 14 About SVCs

Address Formats 14-2
ATM End System Address (AESA) Formats 14-2
Native E.164 Address Format 14-7
Designing an Address Format Plan 14-7
About Address Registration 14-8
About Route Determination 14-10
About Address Translation 14-12
Network ID Addressing 14-17

Chapter 15 Configuring SVC Parameters

Configuring Node Prefixes 15-2
Defining a Node Prefix 15-3
Native E.164 Node Prefix Format 15-5
DCC and ICD AESA Node Prefix Format 15-6
E.164 AESA Node Prefix Format 15-7
Custom AESA Node Prefix Format 15-9
Defining Address and Routing Options 15-10
Configuring SVC Port Prefixes 15-13
E.164 Native Prefixes Port Prefix Format 15-15
DCC and ICD AESA Port Prefix Format 15-16
E.164 AESA Port Prefix Format 15-17
Custom AESA Port Prefix Format 15-19
Setting the Local and Remote Gateway Address for Port Prefixes 15-21
Defining Default Routes for Network-to-Network Connections 15-23
Defining Port Prefix Options 15-24
Configuring SVC Port Addresses 15-26
About Automatic Assignment of ESI Bytes 15-26
Native E.164 SVC Address Format 15-31
DCC and ICD AESA SVC Address Format 15-32
E.164 AESA SVC Address Format 15-34
Custom AESA SVC Address Format 15-35
Defining SVC Port Address Options 15-36
Configuring PVP Termination 15-37
Configuring PVC Termination 15-38
Configuring the Port User Part of the Address 15-39
Defining a Port User Part 15-40

Defining Network ID Parameters 15-42
Adding Network IDs 15-42
Modifying a Network ID 15-45
Deleting a Network ID 15-45

Chapter 16 Configuring SVC Proxy Signaling

About Proxy Signaling 16-2
Proxy Signaling Agent 16-3
Proxy Signaling Client 16-3
VPCI/SVC Address Association 16-3
Configuring the Proxy Signaling Agent 16-4
Configuring the VPCI Table 16-5
Configuring the Proxy Signaling Client 16-7

Chapter 17 Configuring SPVCs

About SPVCs 17-2
Using PVC/PVP Termination 17-2
Specifying the Target Select Type 17-3
About Point-to-Point SPVCs 17-5
Setting the VPI/VCI Values for SPVCs 17-7
Adding a Point-to-Point SPVC 17-8
Configuring the Terminating Endpoint Address 17-13
Configuring Point-to-Multipoint SPVCs 17-15
Adding a Point-to-Multipoint SPVC 17-16
Defining the Point-to-Multipoint SPVC Root 17-16
Defining Additional SPVC Leafs 17-18

Chapter 18 Closed User Groups (CUGs)

About CUG Member Rules 18-2
Defining Incoming and Outgoing Access 18-2
Member Rule Example 18-3
Developing Closed User Groups (CUGs) 18-3
Using CUGs in the Network 18-4
Call Setup Examples 18-5
Configured Addresses and CUG Membership 18-6
Configuring Closed User Groups (CUGs) 18-7
Defining CUG Members 18-7
Defining a Closed User Group 18-10
Assigning Member Rules to CUGs 18-11
Modifying Call Access for CUG Members 18-13

Chapter 19 Port Security Screening

Implementing Port Security Screening 19-2
Default Screens 19-2
Security Screens 19-3
About Security Screen Addresses 19-3
Port Security Screening Sample Configuration 19-5
Port Security Screening Configuration Summary 19-7
Configuring Port Security Screening 19-7
Creating Port Security Screen Definitions 19-8
Assigning Security Screens to Logical Ports 19-11
Deleting Security Screen Assignments 19-13
Activating Default Screens 19-13
Activating and Deactivating Security Screens 19-14
Viewing Screen Assignments 19-15

Chapter 20 Configuring PNNI Routing

Supported PNNI Features 20-2
PNNI Routing Protocol Overview 20-7
Hierarchical Organization 20-7
PNNI Routing Example 20-9
PNNI Packets 20-11
Fast Inter-card APS 1+1 PNNI Interworking with the PSAX 4500 20-12
Logical Port and Protocol Types 20-13
PNNI Administrative Weight 20-13
UBR Load Balancing Over Parallel PNNI Links 20-14
PNNI Signaling Overview 20-14
UNI 4.0 Signaling Features 20-15
PNNI and CBX/GX PVCs 20-15
Lucent ATM SPVC Node Prefix 20-16
Integrating VNN OSPF and PNNI Networks 20-17
PNNI/VNN Gateway Support 20-17
Importing Exterior Addresses 20-17
PNNI and VNN OSPF Call Interworking 20-17
Interworking VNN ATM PVCs with PNNI 20-17
Native E.164 Address Advertisement 20-18
Filtering PNNI and VNN OSPF Address Advertisements 20-18
Disabling PNNI/VNN Gateway Support 20-18
Route Advertisement Suppression 20-18
Connection Trace 20-18
Frame Relay-to-PNNI Interworking 20-21
PNNI Reroute Load Balancing 20-22
PNNI Reroute Load Balancing Criteria 20-22
Defining Reroute Tuning 20-23
Load Balancing Example 20-23
Configuring Circuit Reroute-Tuning Parameters 20-23
Resilient UNI and APS Resilient UNI Over PNNI 20-25
About Resilient UNI and APS Resilient UNI Over PNNI 20-25

Configuring Resilient UNI and APS Resilient UNI....20-26
Using the show pnni names Command....20-26
Configuring PNNI Routing....20-27
Enabling Name LSA Flooding on the Switch....20-28
Configuring PNNI Node Parameters....20-29
Accessing PNNI Node Parameter Functions....20-29
About the Set All PNNI Node Parameters Dialog Box....20-30
Adding PNNI Node Parameters....20-36
Adding PNNI Summary Addresses....20-39
Configuring Global Variables....20-41
Completing the PNNI Node Parameter Configuration....20-43
Configuring an ATM NNI Logical Port....20-44
Creating a PNNI Link Line Connection....20-48
Understanding PNNI Link Line Coloring....20-50
Configuring PVCs....20-51
Configuring SVC and SPVC Parameters....20-51
Configuring Offnet PVCs Over PNNI....20-52
Adding an Offnet Circuit....20-58
Administrative Attributes....20-60
Traffic Type Attributes....20-62
User Preference Attributes....20-63
Selectable Statistics Attribute....20-64
Configuring Management PVCs....20-65
Configuring Management SPVCs....20-65
Viewing PNNI Links....20-65
PNNI Trap Support....20-66

Appendix A Adjusting the CAC

About the Customizable CAC Options....A-3
Customizable CAC Example....A-3
Configuring the CAC....A-4
Tuning the CAC....A-5
Customizing the CAC for the VBR-RT, VBR-NRT, and ABR Classes....A-7
Customizing the CAC for the VBR-NRT and ABR Classes....A-10

Appendix B ATM Traffic Descriptors

Peak Cell Rate (PCR) CLP=0 and PCR CLP=0+1....B-2
PCR CLP=0 and PCR CLP=0+1 With Tagging....B-3
PCR CLP=0+1....B-4
PCR CLP=0+1 With Best Effort....B-4
PCR CLP=0+1, SCR CLP=0, MBS CLP=0....B-4
PCR CLP=0+1, SCR CLP=0, MBS CLP=0 With Tagging....B-6
PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1....B-8

Appendix C Allocating Logical Port Bandwidth on CBX 500 Shared SP Threads

Shared SP Thread Example C-2

Appendix D ATM Flow Control Processor Rate Profile Tables

About FCP Rate Profile Tables..... D-1
Determining FCP Rate Profile Values..... D-2
MCR Class Mappings..... D-4
DS3/E3 IOM MCR Class Mapping..... D-4
T1/E1 IOM MCR Class Mapping..... D-8
OC-3/STM-1 IOM MCR Class Mapping..... D-10
OC-12/STM-4 IOM MCR Class Mapping..... D-14
IMA Group Configuration..... D-18

Appendix E Priority Routing

About Priority Routing E-1
Network Convergence Time E-1
Specifying Routing Priorities E-2
Using Restricted Priority Routing E-3
Routing Priority Rules E-4
Circuit Provisioning E-4
Trunk-Failure Recovery E-4
Balance Rerouting E-5
Priority Routing and Path Cost E-5
Priority Routing and Path Cost Example E-5
Restricted Priority Routing and Path Cost Example E-6

Appendix F Reliable Scalable Circuit

Circuit Add Errors..... F-3
Circuit Modify Errors F-5
Circuit Delete Errors F-7

Appendix G OSPF Name Aggregation

About OSPF Name Aggregation G-1
OSPF Names G-1
Name Limitations..... G-2
Using OSPF Name Aggregation..... G-2
Sample Network Scenario..... G-2
Port-Level Name Aggregation..... G-3
Switch-Level Name Aggregation G-4
Network Hierarchical Addressing Plans..... G-5
Monitoring Network OSPF Name Activity G-7
Viewing OSPF Names at the Network Level..... G-7
Viewing OSPF Names at the Switch Level..... G-8
Viewing OSPF Names at the Card Level..... G-10

Appendix H Customer Names

Configuring Customer Names H-1
Adding Customer Names H-2
Associating a Logical Port with a Customer Name H-3
Using the Layer2 VPN/Customer View Feature H-6

Abbreviations and Acronyms

Abbreviations 1-1
Acronyms 1-3

Index

List of Figures

Figure 2-1. Two Virtual UNIs Through Central Network 2-10
Figure 2-2. Virtual UNI with VP Multiplexer 2-10
Figure 3-1. Set All Logical Ports in PPort Dialog Box 3-4
Figure 3-2. Add Logical Port Type Dialog Box 3-10
Figure 3-3. Add Logical Port Dialog Box 3-11
Figure 3-4. Administrative Attributes Fields 3-14
Figure 3-5. Set ATM Attributes Fields (UNI Logical Ports) 3-22
Figure 3-6. Set ILMI/Signaling/OAM Attributes Fields (UNI LPorts) 3-28
Figure 3-7. Set Logical Port Signaling Tuning Parameters Dialog Box 3-33
Figure 3-8. Set Traffic Descriptors Attributes Fields 3-37
Figure 3-9. Set Opt Trunk VPI Range Attributes Fields 3-38
Figure 3-10. Selectable Statistics Attributes 3-42
Figure 3-11. Set Logical Port QoS Parameters Dialog Box 3-44
Figure 3-12. Set Logical Port SVC QoS Parameters Dialog Box 3-48
Figure 3-13. SVC Menu 3-50
Figure 3-14. Set SVC Connection ID Parameters Attributes Fields 3-51
Figure 3-15. Set SVC Parameters Attributes Fields 3-52
Figure 3-16. Set Insertion Address Dialog Box 3-54
Figure 3-17. CUG Fields 3-57
Figure 3-18. Simultaneous SVC Limit Fields 3-58
Figure 3-19. Set SVC Priorities Attribute Fields 3-62
Figure 3-20. Set SVC TD Limits Attributes Fields 3-64
Figure 3-21. Set ATM SVC Parameters Attributes Fields 3-67
Figure 3-22. Tunneling Through a Public Network 3-68
Figure 3-23. Calling Into a Public Network 3-69
Figure 4-1. Set Attributes Menu 4-10
Figure 4-2. Add Logical Port Type Dialog Box 4-13
Figure 4-3. Add Logical Port Dialog Box (ATM UNI DCE/DTE) 4-14
Figure 4-4. Set Congestion Control Attributes Fields 4-18
Figure 4-5. Set Trap Control Attributes Fields 4-20
Figure 4-6. Set Priority Frame Attributes Fields 4-22
Figure 4-7. Set ATM Attributes Fields 4-23
Figure 4-8. Set ILMI/Signaling/OAM Attributes Fields 4-25
Figure 4-9. Set Administrative Attributes Fields (Direct/OPTimum Cell, ATM CS/IWU Card) 4-29
Figure 4-10. Set [Administrative] Attributes Fields (ATM DS3 UNI) 4-31
Figure 4-11. Set [Discard/Congestion Mapping] Attributes Fields 4-33
Figure 4-12. Set [Opt Trunk VPI Range] Attributes Fields 4-35
Figure 4-13. Add Logical Port Dialog Box (OPTimum Frame) 4-38
Figure 4-14. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS) 4-40
Figure 4-15. Add Logical Port Dialog Box (ATM CS/IWU) 4-43
Figure 4-16. Set Link Mgmt Attributes Fields 4-44
Figure 4-17. Set Discard/Congestion Mapping Attributes Fields 4-48

Figure 5-1. CBX 500 Queues and the ATM FCP 5-4
Figure 5-2. Closed-Loop Flow Control 5-7
Figure 5-3. CCRM Closed-Loop Flow Control 5-8
Figure 5-4. BCM Closed-Loop Flow Control 5-10
Figure 5-5. Output UNI Logical Port RM Termination 5-11
Figure 5-6. ATM FCP Buffers 5-17
Figure 5-7. VP Shaping Network Architecture Example 5-19
Figure 6-1. FCP Attribute Fields (Set Card Attributes Dialog Box) 6-3
Figure 6-2. Load Rate Profile Tables Dialog Box 6-6
Figure 6-3. Set ATM FCP Attributes Dialog Box (3-Port Channelized DS3/1 IMA IOM) 6-7
Figure 7-1. Trunk Delay - OSPF Metric and Keep Alive Messaging 7-3
Figure 7-2. Set All Trunks Dialog Box 7-14
Figure 7-3. Select Logical Ports Dialog Box 7-21
Figure 7-4. Add Trunk Dialog Box 7-22
Figure 7-5. Primary Trunk Type Menu Fields 7-25
Figure 7-6. Add Connection Dialog Box 7-27
Figure 7-7. Add Connection Dialog Box With Connection Class Selected 7-28
Figure 7-8. Add Object Dialog Box 7-29
Figure 7-9. Add Object - Set Attributes Dialog Box 7-30
Figure 7-10. Trunk Submap Window 7-32
Figure 7-11. Set Traffic Descriptors Attributes Fields 7-35
Figure 7-12. Set PNNI Parameters Attributes Fields 7-41
Figure 7-13. External Trunk Configuration Sequence 7-44
Figure 7-14. Add Object Palette 7-45
Figure 7-15. Add Object Dialog Box (External Device) 7-46
Figure 7-16. Add Object – Set Attributes Dialog Box (External Device) 7-48
Figure 7-17. Set All External Interfaces Dialog Box 7-50
Figure 7-18. Add External Interface Dialog Box 7-50
Figure 7-19. Set All External Trunks Dialog Box 7-52
Figure 7-20. Select Interfaces Dialog Box 7-53
Figure 7-21. Add External Trunk Dialog Box 7-53
Figure 7-22. Set All VNN Loopback Addresses Dialog Box 7-56
Figure 7-23. Add VNN Loopback Address Dialog Box 7-56
Figure 7-24. Set All VNN Area Aggregates Dialog Box 7-57
Figure 7-25. Add VNN Area Aggregate Dialog Box 7-57
Figure 7-26. Set All VNN Virtual Links Dialog Box 7-59
Figure 7-27. Add VNN Virtual Link Dialog Box 7-59
Figure 7-28. Set All VNN External Routes Aggregates Dialog Box 7-61
Figure 7-29. Add VNN External Routes Aggregate Dialog Box 7-61
Figure 7-30. Set All OSPF External Routes Aggregates Dialog Box 7-64
Figure 7-31. Add OSPF External Routes Aggregate Dialog Box 7-65
Figure 7-32. Set All VNN Optimized Flooding Dialog Box 7-68
Figure 7-33. Set Switch Attributes Dialog Box (CBX 500) 7-71
Figure 8-1. Set All PVCs On Map Dialog Box 8-10
Figure 8-2. Set All Redirect PVCs On Map Dialog Box 8-16
Figure 8-3. Select End Logical Ports Dialog Box 8-22
Figure 8-4. Add PVC Dialog Box 8-24

Figure 8-5. Set Traffic Type Attributes Fields 8-30
Figure 8-6. Set User Preference Attributes Fields 8-32
Figure 8-7. Set Frame Discard Attributes Fields 8-36
Figure 8-8. Set Extended QoS Parameters Attributes Fields 8-37
Figure 8-9. Set Selectable Statistics Attributes Field 8-39
Figure 8-10. Add PVC Dialog Box (FR-ATM) 8-48
Figure 8-11. Set Traffic Type Attributes Fields (FR-ATM) 8-52
Figure 8-12. Set User Preference Attributes Fields (FR-ATM) 8-57
Figure 8-13. Select Redirect Circuit End Logical Ports Dialog Box 8-62
Figure 8-14. Add Redirect PVC Dialog Box 8-64
Figure 8-15. Pure VNN Define Circuit Path Dialog Box 8-70
Figure 8-16. VNN/PNNI Mixed Define Circuit Path Dialog Box 8-70
Figure 8-17. PNNI Node ATM Address Dialog Box 8-71
Figure 8-18. Lucent Node IP Address Dialog Box 8-72
Figure 8-19. Select Source & Destination LPorts Dialog Box 8-73
Figure 8-20. Move Circuit Endpoint Dialog Box 8-74
Figure 8-21. Set All Point-to-Multiple-Point Circuit Roots Dialog Box 8-75
Figure 8-22. Add Point-to-Multiple-Point Circuit Root (Select LPort) Dialog Box 8-79
Figure 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box 8-80
Figure 8-24. Modify Point-to-Multiple-Point Circuit Leaf Dialog Box 8-84
Figure 8-25. Point-to-Multipoint Circuit Example 8-86
Figure 9-1. Connecting a PNNI Network 9-2
Figure 9-2. Set All Management VPI/VCIs Dialog Box 9-8
Figure 9-3. Select End Logical Port Dialog Box 9-9
Figure 9-4. Add Management VPI/VCI Dialog Box 9-10
Figure 9-5. Select SPVC Endpoints Dialog Box 9-12
Figure 9-6. Add Soft PVC Dialog Box 9-13
Figure 9-7. Set All Management Paths Dialog Box 9-15
Figure 9-8. Add Management Path Dialog Box 9-16
Figure 10-1. Set All ATM Traffic Descriptors Dialog Box 10-9
Figure 10-2. Add Traffic Descriptor Dialog Box 10-10
Figure 10-3. Traffic Descriptors Fields 10-12
Figure 11-1. Layer2 VPN Restrictive Mode Example 11-2
Figure 11-2. Layer2 VPN Inclusive Mode Example 11-3
Figure 11-3. Set All Layer2 VPNs Dialog Box 11-4
Figure 11-4. Add Layer2 Virtual Private Network Dialog Box 11-5
Figure 11-5. Set All Customers Dialog Box 11-5
Figure 11-6. Add Customer Dialog Box 11-6
Figure 11-7. Select Customer and Layer2 VPN Dialog Box 11-7
Figure 11-8. Select Layer2 Customer/Layer2 VPN View Dialog Box 11-8
Figure 12-1. Set All Service Name Bindings Dialog Box 12-4
Figure 12-2. Select End Logical Port Dialog Box 12-5
Figure 12-3. Add Service Name Binding Dialog Box 12-5
Figure 12-4. Select End Logical Port Dialog Box 12-6
Figure 12-5. Set/Modify Backup Service Name Binding Dialog Box 12-7
Figure 13-1. Set All RLMI Service Name Bindings Dialog Box 13-6
Figure 13-2. Select End Logical Ports Dialog Box 13-7

Figure 13-3. Add Service Name Binding Dialog Box 13-9
Figure 13-4. Modify RLMI Service Name Dialog Box 13-10
Figure 14-1. Native E.164 Address Converted to BCD Format..... 14-3
Figure 14-2. Embedded E.164 AESA Format..... 14-3
Figure 14-3. AESA Address Formats..... 14-6
Figure 14-4. Address Registration..... 14-9
Figure 14-5. State of Connection SETUP Message Address Elements (1)..... 14-15
Figure 14-6. State of Connection SETUP Message Address Elements (2)..... 14-15
Figure 14-7. State of Connection SETUP Message Address Elements (3)..... 14-16
Figure 14-8. State of Connection SETUP Message Address Elements (4)..... 14-16
Figure 15-1. Set All Node Prefixes Dialog Box..... 15-3
Figure 15-2. Add Node Prefix Dialog Box (E.164 Native Format)..... 15-5
Figure 15-3. Add Node Prefix Dialog Box (DCC or ICD AESA Format)..... 15-6
Figure 15-4. Add Node Prefix Dialog Box (E.164 AESA Format)..... 15-7
Figure 15-5. Add Node Prefix Dialog Box (Custom AESA Format)..... 15-9
Figure 15-6. Add Node Prefix Address and Routing Fields..... 15-10
Figure 15-7. Set All Port Prefixes Dialog Box..... 15-13
Figure 15-8. Add Prefix Dialog Box (E.164 Native Format)..... 15-15
Figure 15-9. Add Prefix Dialog Box (DCC and ICD AESA Format)..... 15-16
Figure 15-10. Add Prefix Dialog Box (E.164 AESA Format)..... 15-17
Figure 15-11. Add Prefix Dialog Box (Custom AESA Format)..... 15-19
Figure 15-12. Setting Local and Remote Gateway Addresses..... 15-21
Figure 15-13. Set Local Gateway Address Dialog Box..... 15-22
Figure 15-14. Add Prefix Dialog Box (Default Route)..... 15-23
Figure 15-15. Add Port Prefix Option Fields..... 15-24
Figure 15-16. Set All Port Addresses Dialog Box..... 15-28
Figure 15-17. Add Address Dialog Box..... 15-29
Figure 15-18. Add Address Dialog Box (Native E.164 SVC Address Format)..... 15-31
Figure 15-19. Add Address Dialog Box (DCC or ICD AESA Format)..... 15-32
Figure 15-20. Set All Node Prefix w/Auto ESI Dialog Box..... 15-32
Figure 15-21. Add Address Dialog Box (E.164 AESA Format)..... 15-34
Figure 15-22. Add Address Dialog Box (Custom AESA Format)..... 15-35
Figure 15-23. Add SVC Port Address Option Fields..... 15-36
Figure 15-24. PVP Termination Fields..... 15-37
Figure 15-25. PVC Termination Fields..... 15-38
Figure 15-26. Set All Port User Parts Dialog Box..... 15-40
Figure 15-27. Add User Part Dialog Box..... 15-41
Figure 15-28. Set All Port Network IDs Dialog Box..... 15-42
Figure 15-29. Add Network ID Dialog Box..... 15-44
Figure 16-1. Establishing SVCs for Endsystem via Proxy Signaling Agent (PSA)..... 16-2
Figure 16-2. Set ILMI/Signaling/OAM Attributes (Agent) Fields..... 16-4
Figure 16-3. Set VPCI Table in Logical Port Dialog Box..... 16-5
Figure 16-4. Add VPCI Attributes Dialog Box..... 16-6
Figure 16-5. Set ILMI/Signaling/OAM Attributes (Client) Fields..... 16-7
Figure 16-6. Select Agent Switch and Logical Port Dialog Box..... 16-8
Figure 17-1. Set All Point-to-Point SPVCs Dialog Box..... 17-5

Figure 17-2. Select SPVC Endpoints Dialog Box 17-8
Figure 17-3. Add Soft PVC Dialog Box 17-10
Figure 17-4. Set Traffic Type Attributes Fields 17-12
Figure 17-5. Set All Port Prefixes Dialog Box 17-13
Figure 17-6. Set All Port Addresses Dialog Box 17-14
Figure 17-7. Set All Point-to-Multipoint SPVCs Dialog Box 17-15
Figure 17-8. Add SPVC Leaf Dialog Box 17-18
Figure 18-1. Implementing CUGs 18-4
Figure 18-2. Set All SVC CUG Members Dialog Box 18-8
Figure 18-3. Add SVC CUG Member Dialog Box 18-8
Figure 18-4. Set All SVC CUGs Dialog Box 18-10
Figure 18-5. Add SVC CUG Dialog Box 18-11
Figure 18-6. Modify CUG (Assign Member Rules) Dialog Box 18-12
Figure 18-7. Modify CUG (Call Access) Dialog Box 18-13
Figure 19-1. Set All Port Security Screens Dialog Box 19-8
Figure 19-2. Adding Port Security Screens Dialog Box 19-9
Figure 19-3. Assigning and Activating Port Security Screens Dialog Box 19-12
Figure 19-4. Port Screen Activation Parameter Fields 19-14
Figure 19-5. Assigned Screens List Box 19-14
Figure 19-6. Assignments of Port Security Screens Dialog Box 19-15
Figure 20-1. Three-Tiered PNNI Routing Hierarchy Example 20-8
Figure 20-2. Two-Tiered PNNI Routing Hierarchy Example 20-9
Figure 20-3. Flow of PNNI Topology Information 20-10
Figure 20-4. Set All PVCs on Map Dialog Box (Connection Trace Information) 20-19
Figure 20-5. Set Switch Tuning Attributes Dialog Box 20-24
Figure 20-6. Configuring PNNI Routing 20-27
Figure 20-7. Set All PNNI Node Parameters Dialog Box 20-29
Figure 20-8. Add PNNI Node Instance Dialog Box 20-36
Figure 20-9. Add PNNI Summary Instance Dialog Box 20-39
Figure 20-10. Set PNNI Node Global Variables Dialog Box 20-41
Figure 20-11. Set PNNI Parameters Attributes Fields 20-45
Figure 20-12. Add Object - Set Attributes Dialog Box 20-49
Figure 20-13. Set All Offnet PVCs On Map Dialog Box 20-53
Figure 20-14. Select Offnet PVC Endpoints Dialog Box 20-58
Figure 20-15. Add Offnet Circuit Dialog Box 20-59
Figure 20-16. Set Traffic Type Attributes 20-62
Figure 20-17. User Preference Attributes 20-63
Figure 20-18. Set Selectable Statistics Attributes 20-64
Figure A-1. Set All CAC Parameters Dialog Box A-4
Figure G-1. Sample Network Addressing Scenario G-2
Figure G-2. Sample Network Showing Port and Network Prefixes G-5
Figure H-1. Set All Customers Dialog Box H-2
Figure H-2. Add Customer Dialog Box H-2
Figure H-3. Set All Logical Ports in PPort Dialog Box H-4
Figure H-4. Select Customer and Layer2 VPN Dialog Box H-5
Figure H-5. Select Layer2 Customer/Layer2 VPN View Dialog Box H-6

List of Tables

Table 2-1. Logical Ports and ILMI Settings....2-4
Table 2-2. Number of Valid Bits in VPI/VCI for CBX 500....2-13
Table 2-3. Number of Valid Bits in VPI/VCI for GX 550....2-14
Table 2-4. Physical and Logical Port Bandwidth Conversions....2-16
Table 2-5. Non-Disruptive Logical Port and Trunk Attributes....2-22
Table 3-1. Set All Logical Ports in PPort Dialog Box Buttons....3-5
Table 3-2. Set All Logical Ports in PPort Dialog Box Fields....3-7
Table 3-3. Defining a Logical Port....3-9
Table 3-4. Set Administrative Attributes Fields....3-14
Table 3-5. Configuring CBX and GX Logical Ports....3-18
Table 3-6. Set ATM Attributes Fields....3-22
Table 3-7. Set ILMI/Signaling/OAM Attributes Fields....3-29
Table 3-9. Set OPT Trunk VPI Range Attributes Fields....3-39
Table 3-10. Selectable Statistics Attributes Fields....3-42
Table 3-11. Select:Options: Menu....3-43
Table 3-12. Default Quality of Service Values for ATM UNI Logical Ports....3-44
Table 3-13. Set Logical Port SVC QoS Parameters Dialog Box Fields....3-48
Table 3-14. Set SVC Connection ID Parameters Attributes Fields....3-51
Table 3-15. Insertion Mode Options....3-53
Table 3-16. Presentation Mode Options....3-55
Table 3-17. Screening Mode Options....3-55
Table 3-18. Transit Network Selection Fields....3-56
Table 3-19. CUG Fields....3-57
Table 3-20. Simultaneous SVC Limit Fields....3-59
Table 3-21. Additional Set SVC Parameters Attributes Menu Fields....3-60
Table 3-22. Set SVC Priorities Attributes Fields....3-63
Table 3-23. Set SVC TD Limits Attributes Fields....3-65
Table 3-24. Set ATM SVC Parameters Attributes Fields....3-70
Table 4-1. I/O Modules for ATM Services....4-7
Table 4-2. Maximum Mono-Class Service Thresholds per Card Type....4-9
Table 4-3. Maximum Multi-Class Service Thresholds per Card Type....4-9
Table 4-4. Set Attributes Menu....4-11
Table 4-5. Configuring ATM Logical Port Types....4-13
Table 4-6. Add Logical Port Type Dialog Box Fields (UNI DCE/DTE)....4-14
Table 4-7. Set Administrative Attributes Fields....4-15
Table 4-8. Configuring UNI DCE/DTE Attributes....4-17
Table 4-9. Set Congestion Control Attributes Fields....4-18
Table 4-10. Set Trap Control Attributes Fields....4-20
Table 4-11. Set Priority Frame Attributes Fields....4-22
Table 4-12. Set ATM Attributes Fields....4-24
Table 4-13. Set ILMI/Signaling/OAM Attributes Fields....4-26
Table 4-14. Set [Administrative] Attributes (Direct/OPTimum Cell, ATM CS/IWU Card)....4-29

Table 4-15. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS) 4-32
Table 4-16. Configuring Direct Cell Trunk/OPTimum Cell Trunk Attributes 4-33
Table 4-17. Set [Discard/Congestion Mapping] Attributes Fields....4-34
Table 4-18. Set [OPT Trunk VPI Range] Attributes Field 4-36
Table 4-19. Set [Administrative] Attributes Fields (OPTimum Frame, ATM CS/IWU Card) 4-38
Table 4-20. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS) 4-41
Table 4-21. Configuring OPTimum Frame Trunk Attributes....4-42
Table 4-22. Configuring Network Interworking for Frame Relay NNI Attributes 4-43
Table 4-23. Set Link Mgmt Attributes Fields 4-44
Table 4-24. Set Discard/Congestion Mapping Attributes Fields 4-49
Table 5-1. Cell Scheduling....5-14
Table 6-1. Set Card Attributes Fields and Buttons (FCP)....6-3
Table 6-2. Set ATM FCP Attributes Fields and Buttons 6-8
Table 7-1. Fast APS 1+1 Options 7-8
Table 7-2. Set All Trunks Dialog Box Buttons....7-15
Table 7-3. Set All Trunks Dialog Box Fields 7-16
Table 7-4. Add Trunk Dialog Box Fields 7-23
Table 7-5. Primary Trunk Type Menu Fields 7-25
Table 7-6. Add Object Dialog Box Fields 7-29
Table 7-7. Add Object - Set Attributes Dialog Box....7-31
Table 7-8. Trunk Line Color Status Indicators 7-33
Table 7-9. Configuring an ATM NNI Logical Port 7-40
Table 7-10. PNNI Parameters Attributes Fields 7-42
Table 7-11. Add Object Dialog Box Fields (External Device)....7-47
Table 7-12. Add Object – Set Attributes Fields (External Device) 7-48
Table 7-13. Add External Interface Dialog Box Fields 7-51
Table 7-14. Add External Trunk Dialog Box Fields....7-54
Table 7-15. Add VNN Area Aggregate Dialog Box Fields....7-58
Table 7-16. VNN OSPF Virtual Link Fields 7-60
Table 7-17. Add VNN/OSPF External Routes Aggregate Dialog Box Fields .7-62
Table 7-18. VNN OSPF Optimized Flooding Console Commands 7-69
Table 8-1. PVC Endpoint Rules....8-4
Table 8-2. Set All PVCs On Map Dialog Box Buttons....8-11
Table 8-3. Set All PVCs On Map Dialog Box Fields 8-12
Table 8-4. Set All Redirect PVCs On Map Dialog Box Buttons....8-17
Table 8-5. Set All Redirect PVCs On Map Dialog Box Fields....8-18
Table 8-6. Select End Logical Ports Dialog Box Fields 8-23
Table 8-7. Set Administrative Attributes Fields 8-27
Table 8-8. Set Traffic Type Attributes Fields 8-30
Table 8-9. Set User Preference Attributes Fields....8-33
Table 8-10. Set Frame Discard Attributes Fields....8-37
Table 8-11. Set Extended QoS Parameters Attributes Fields 8-38
Table 8-12. Rate Enforcement and Discard Policy....8-45

Table 8-13. Rate Enforcement Schemes 8-46
Table 8-14. Add PVC Dialog Box Fields (FR-ATM) 8-49
Table 8-15. Set Administrative Attributes Fields 8-50
Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters) 8-53
Table 8-17. Set User Preference Attributes Fields 8-58
Table 8-19. Add Redirect PVC Dialog Box Fields 8-65
Table 8-20. Define Circuit Path Dialog Box Fields 8-71
Table 8-21. Set All Point-to-Multiple-Point Circuit Root Dialog Box Buttons 8-76
Table 8-22. Set All Point-to-Multiple-Point Circuit Root Dialog Box Fields 8-77
Table 9-1. Configuring Standard MPVC Attributes 9-5
Table 9-2. Configuring Redirect MPVC Attributes 9-6
Table 9-3. Select End Logical Port Dialog Box Fields 9-9
Table 9-4. Add Management VPI/VCI Dialog Box Fields 9-10
Table 10-1. Quality of Service Classes 10-4
Table 10-2. Traffic Parameters 10-5
Table 10-3. QoS Class Traffic Descriptors 10-7
Table 10-4. Traffic Descriptor Types 10-10
Table 10-5. UNI Signaling Control Channel Traffic Descriptor Defaults 10-14
Table 10-6. ILMI Control Channel Traffic Descriptor Defaults 10-15
Table 10-7. Trunk Control Channel Traffic Descriptor Defaults 10-16
Table 10-8. PNNI Routing Control Channel Traffic Descriptors 10-17
Table 13-1. Resilient LMI Terms 13-2
Table 13-2. RLMI Fields 13-8
Table 13-3. Modify RLMI Service Name Dialog Box Fields 13-10
Table 14-1. AFI Default Values 14-4
Table 14-2. IDI Default Values 14-4
Table 14-3. HO-DSP Default Values 14-5
Table 14-4. Calling Party Address Translation at Egress Port 14-13
Table 14-5. Called Party Address Translation at Egress Port 14-14
Table 15-1. Address Format Descriptions 15-4
Table 15-2. Add Node Prefix Address and Routing Fields 15-11
Table 15-3. Add Port Prefix Option Fields 15-24
Table 15-4. ESI Byte Assignments 15-26
Table 15-5. Add SVC Port Address Option Fields 15-36
Table 15-6. Set All Port Network IDs Dialog Box Fields 15-43
Table 15-7. Add Network ID Dialog Box Fields 15-44
Table 17-1. SPVC Target Select Type 17-3
Table 17-2. Set All Point-to-Point SPVCs Dialog Box Buttons 17-6
Table 17-3. Set All Point-to-Point SPVCs Dialog Box Fields 17-7
Table 17-4. Configuring the SPVC Terminating Endpoint Address 17-9
Table 17-5. Add Soft PVC Dialog Box Fields 17-11
Table 17-6. Add Point-to-Multipoint Fields 17-16
Table 17-7. Add SPVC Leaf Fields 17-19
Table 18-1. Incoming and Outgoing Calls Barred Example 18-5
Table 18-2. Configured Address and Corresponding CUG Membership 18-6
Table 18-3. Add SVC CUG Member Dialog Box Fields 18-9

Table 19-1. Default Screens 19-2
Table 19-2. Port Security Screen Examples 19-4
Table 19-3. Adding Port Security Screens Dialog Box Fields 19-9
Table 20-1. Supported PNNI Features 20-2
Table 20-2. Displaying Connection Trace Information for ATM Circuits 20-20
Table 20-3. Set Switch Tuning Attributes Fields 20-24
Table 20-4. Set All PNNI Node Parameters Dialog Box Buttons 20-30
Table 20-5. Set All PNNI Node Parameters Dialog Box Fields 20-31
Table 20-6. Add PNNI Node Instance Dialog Box Fields 20-37
Table 20-7. Add PNNI Summary Instance Dialog Box Fields 20-40
Table 20-8. Set PNNI Node Global Variables Dialog Box Fields 20-42
Table 20-9. Configuring an ATM NNI Logical Port 20-44
Table 20-10. PNNI Parameters Attributes Fields 20-46
Table 20-11. Add Object - Set Attributes Dialog Box 20-49
Table 20-12. PNNI Link Line Color Status Indicators 20-50
Table 20-13. Set All Offnet PVCs On Map Dialog Box Buttons 20-54
Table 20-14. Set All Offnet PVCs On Map Dialog Box Fields 20-55
Table 20-15. Add Offnet Circuit Dialog Box Fields 20-59
Table 20-16. Set Administrative Attributes Fields 20-60
Table 20-17. Allowable QoS Classes 20-63
Table 20-18. PNNI Traps 20-66
Table B-1. PCR CLP=0 and PCR CLP=0+1 ..... B-2
Table B-2. PCR CLP=0 and PCR CLP=0+1 With Tagging B-3
Table B-3. PCR CLP=0+1, SCR CLP=0, MBS CLP=0 ..... B-5
Table B-4. PCR CLP=0+1, SCR CLP=0, MBS CLP=0, With Tagging B-7
Table B-5. PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1 ..... B-9
Table D-1. FCP Rate Profile Values (by MCR class) D-2
Table D-2. DS3/E3 IOM MCR Class Mapping D-4
Table D-3. T1/E1 IOM MCR Class Mapping D-8
Table D-4. OC-3/STM-1 IOM MCR Class Mapping D-10
Table D-5. OC-12/STM-4 IOM MCR Class Mapping D-14
Table D-6. IMA Configuration MCR Formula Arguments D-18
Table F-1. Errors Encountered During Circuit Add Procedure F-3
Table F-2. Errors Encountered During Circuit Modify Procedure F-5
Table F-3. Errors Encountered During Circuit Delete Procedure F-7
Table G-1. Address Routing Requirements for Sample Network G-3

About This Guide

The *B-STDX, CBX, and GX ATM Services Configuration Guide* provides detailed instructions for using NavisCore™ to configure Asynchronous Transfer Mode (ATM) services in a Lucent switch network. Specifically, this guide describes how to configure logical ports, trunks, permanent virtual circuits (PVCs), and switched virtual circuits (SVCs) to support ATM services on a CBX 500 switch, GX 550 Multiservice WAN switch, and B-STDX 8000/9000 switch. This guide also explains how to configure a variety of features that enhance the ATM service platform, including Virtual Private Networks (VPNs), closed user groups (CUGs), and port security screening.

This guide supports the following Network Management System (NMS) and switch software releases:

- NavisCore™, Release 09.00.00.00 or greater
- CBX 500® Multiservice WAN switch software Release 09.00.00.00 or greater
- GX 550® Multiservice WAN switch software Release 09.00.00.00 or greater
- Prior supported releases of B-STDX 9000® Multiservice WAN switch software as noted in the Interoperability section of the NavisCore Software Release Notice (SRN).

What You Need to Know

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

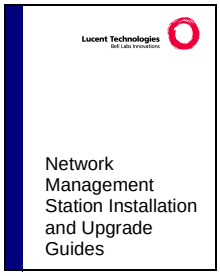
This guide assumes you have already installed the Lucent switch hardware, Network Management Station (NMS), and switch software. See the "Related Documents" section of this preface for a list of documents that describe these and other tasks.

Be sure to read the Software Release Notice (SRN) that accompanies each product. The SRN contains the most current feature information and requirements.

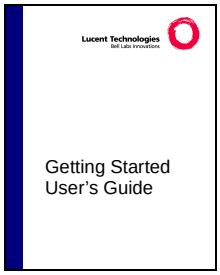
Reading Path

This section describes all of the documents that support the NavisCore NMS and switch software.

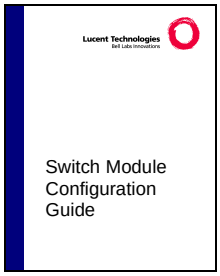
Read the following documents to install and operate NavisCore Release 09.00.00.00 or greater and the associated switch software. Be sure to review the accompanying SRNs for any changes not included in these guides.



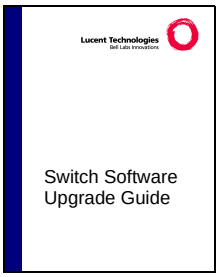
These guides describe prerequisite tasks, hardware and software requirements, and instructions for installing and upgrading Solaris, Sybase, HP OpenView, and NavisCore.



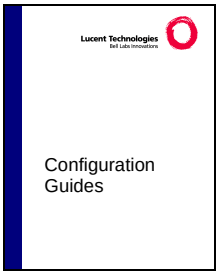
This guide describes how to configure and manage NavisCore, network maps, and Lucent switches. It also describes how to add third-party objects to the map and access them through NavisCore.



This guide describes the processor and input/output modules (IOMs) on each switch platform, and how to configure physical ports, timing, and other attributes through NavisCore.

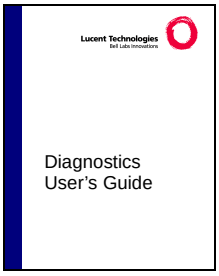


This guide describes procedures for upgrading a Lucent switch to the current software release.

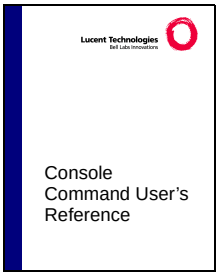


The following guides describe how to configure wide area network (WAN) services on the supported switch platforms:

- *B-STDX and CBX Frame Relay Services Configuration Guide*
- *B-STDX, CBX, and GX ATM Services Configuration Guide*
- *B-STDX and CBX IP Services Configuration Guide*



This guide describes how to monitor and diagnose problems in your NavisCore switch network.



This reference lists and describes the switch console commands.

Documentation for New Modules

The following guides provide information about hardware installation and switch software configuration for specific modules.

- *CBX 1-Port Channelized STM-1/E1 IMA I/O Module User's Guide* (Product Code: 80170)
- *GX BIO-C, OC-48c/STM-16c, and SF2 Modules User's Guide* (Product Code: 80199)

How to Use This Guide

This guide contains the following information:

Read	To Learn About
Chapter 1	How the information in this guide is organized.
Chapter 2	Concepts you need to understand before you configure ATM logical ports. These concepts include: virtual paths and channels, signaling, and Interim Link Management Interface (ILMI).
Chapter 3	Configuring ATM logical ports on a CBX 500 or GX 550 Multiservice WAN switch.
Chapter 4	Configuring ATM logical ports on a B-STDX 8000/9000 switch.
Chapter 5	The operation of the ATM Flow Control Processor (FCP) for supported CBX 500 I/O modules.
Chapter 6	Working with the ATM FCP and answers to frequently asked questions (FAQ).
Chapter 7	Configuring ATM trunks, Automatic Protection Switching (APS) trunk backup, and external trunks.
Chapter 8	Configuring point-to-point, point-to-multipoint, and redirect PVCs. This chapter also describes how to configure Frame Relay-to-ATM interworking circuits.
Chapter 9	Configuring NMS paths using a management PVC, management virtual path identifier/virtual channel identifier (VPI/VCI), or management soft permanent virtual circuit (SPVC) connection.
Chapter 10	Configuring traffic descriptors to manage Quality of Service (QoS) throughout your ATM network.
Chapter 11	Configuring your ATM services to provide Layer2 virtual private networks (VPNs).
Chapter 12	Configuring fault tolerant (resilient UNI/NNI) PVC services to provide backup services should a logical port endpoint fail. This chapter also describes APS Resilient User-to-Network Interface (UNI).
Chapter 13	Configuring Frame Relay Resilient Link Management Interface LMI (RLMI) on ATM Network Interworking for Frame Relay Network-to-Network Interface (NNI) logical ports on 1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 cards.
Chapter 14	ATM switched virtual circuit (SVC) concepts you need to understand before you can configure SVCs. These include address formats and registration, route determination, and address translation.

Read	To Learn About
Chapter 15	Configuring ATM SVCs on a CBX 500 or GX 550 switch.
Chapter 16	Configuring SVC Proxy Signaling.
Chapter 17	Configuring SPVCs within the network using signaling.
Chapter 18	Closed user groups (CUGs) that enable you to divide all network users into logically linked groups of users.
Chapter 19	Using the Port Security Screening function to create screens which allow/disallow incoming and outgoing calls.
Chapter 20	Configuring the ATM Private Network-to-Network Interface (PNNI) routing protocol in your Lucent network.
Appendix A	Tuning the Call Master Connection Admission Control (CAC) to achieve a desired cell loss ratio objective across all physical ports in your network.
Appendix B	How each traffic descriptor combination affects the cell streams under different traffic conditions.
Appendix C	Allocating logical port bandwidth on CBX 500 shared SP threads.
Appendix D	ATM FCP rate profile tables.
Appendix E	Using priority routing to prioritize PVC traffic.
Appendix F	Using the Reliable Scalable Circuit function to troubleshoot PVC provisioning problems.
Appendix G	Guidelines for using Open Shortest Path First (OSPF) name aggregation, which minimizes memory consumption when you provision prefixes and addresses for ATM SVC/SPVC or Frame Relay SVC connections across Lucent network switches.
Appendix H	Using the Customer Names feature to assign a logical port to a specific customer and use the customer name as a filter when viewing logical ports in a network.
Abbreviations and Acronyms	Abbreviations and acronyms used in this guide.

What's New in This Guide

This guide describes the following new product features in NavisCore Release 09.00.00.00 and includes the following changes and enhancements:

Feature or Enhancement	Description	See...
New Features in This Release		
True SONET/SDH APS	Bi-directional APS enhancements were added to provide true SONET/SDH APS for 4-port OC-3c/STM-1, 1-port OC-12c/STM-4, and 1-port OC-48/STM-16 modules on the GX 550 and the 4-port OC-3c/STM-1 and 1-port OC-12c/STM-4 modules on the CBX 500.	"About Automatic Protection Switching" on page 7-5
Unidirectional APS over PNNI	Uni-directional APS over PNNI is supported for the 4-port OC-3c/STM-1 and 1-port OC-12c/STM-4 modules on the GX 550 BIO1 module.	"Unidirectional APS Over PNNI" on page 7-9 and "Defining ATM Direct Trunk Logical Ports" on page 7-34
BIO2 support of 128 VCs	The GX 550 BIO2 card now supports a total of 128,000 virtual circuits for increased scalability.	"GX 550 VC Provisioning Guidelines" on page 8-2
Manual definition of the circuit path	The Define Circuit Path feature enables you to manually define a circuit path and the OSPF algorithm's circuit routing decisions. The circuit may cross PNNI peer groups, PNNI-VNN boundaries, VNN Areas, and Non-Lucent Networks (PNNI). If the alternate path option is defined, and a circuit failure occurs in the manually defined circuit path, the circuit can be routed based on VNN or PNNI information provided.	"Manually Defining the Circuit Path" on page 8-69
Layer2 VPN over PNNI and field name change from VNN VPN to Layer2 VPN	Layer 2 Virtual Private Networks (VPNs) can now be configured over PNNI links. Previously only VNN VPNs were supported.	Chapter 11, "Configuring Layer2 VPNs" Name change throughout
Automatic assignment of 6 ESI bytes	The 6-byte ESI portion of the SVC port address can be automatically assigned by NavisCore for both VNN and PNNI domains. The GX 550 and CBX 500 switches support the automatic ESI assignment feature for both VNN and PNNI. B-STDX 9000 switches support it only for VNN.	"About Automatic Assignment of ESI Bytes" on page 15-26

Feature or Enhancement	Description	See...
Offnet PVCs over PNNI	PNNI FRF.5 provides support for the FRF.5 standard over PNNI links. Endpoints can be configured to transmit data from a Lucent Frame Relay network to a third-party network and then back to an ATM or Frame Relay network via PNNI links.	"Configuring Offnet PVCs Over PNNI" on page 20-52
General Enhancements		
NavisCore dialog boxes and menu choices	Updated NavisCore dialog box illustrations and menu choice references to reflect recent additions and changes.	Throughout
3-Port DS3/1 IMA IOM	Incorporated relevant information from the *3-Port DS3/1 IMA IOM User's Guide* into this guide.	Throughout
MXOS 08.01.00.00 features	Incorporated relevant information from the *Feature Guide for MXOS Release 08.01.00* into this guide.	Throughout
Base Input/Output 2 (BIO2) Information	Incorporated relevant BIO2 information from the *Base Input/Output 2 (BIO2) Module User's Guide* into this guide.	Throughout
ATM Flow Control Processor (FCP)	Combined new and existing FCP information into this guide.	Chapter 5, "About the ATM Flow Control Processor (FCP)" and Chapter 6, "Working with the ATM Flow Control Processor (FCP)"
VNN OSPF configuration and VNN OSPF External Route Aggregates	Incorporated VNN OSPF configuration and overview information from the *NavisCore IP Navigator Configuration Guide.*	"Configuring VNN OSPF" on page 7-55 and "Configuring VNN/OSPF External Route Aggregates" on page 7-60

Conventions

This guide uses the following conventions, when applicable:

Convention	Indicates	Example
`Courier Regular`	System output, filenames, and command names.	`Please wait...`
<Courier Bold Italics>	Variable text input; user supplies a value.	Enter ***<cdrompath>/docs/atmcfg.pdf*** to display...
<Courier Italics>	Variable text output.	*<cdrompath>*`/docs/atmcfg.pdf`
Courier Bold	User input.	> **show ospf names**
Menu ⇒ Option	A selection from a menu.	NavisCore ⇒ Logon
Italics	Book titles, new terms, and emphasized text.	*Network Management Station Installation Guide*
A box around text	A note, caution, or warning.	See examples below.

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

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

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

Related Documents

This section lists the related Lucent and third-party documentation that may be helpful to read.

Lucent

- *B-STDX 8000/9000 Multiservice WAN Switch Hardware Installation Guide* (Product Code: 80005)
- *CBX 500 Multiservice WAN Switch Hardware Installation Guide* (Product Code: 80011)
- *GX 550 Multiservice WAN Switch Hardware Installation Guide* (Product Code: 80077)
- *GX 550 ES Hardware Installation Guide* (Product Code: 80149)
- *B-STDX, CBX, and GX Network Management Station Installation Guide* (Product Code: 80200)
- *B-STDX, CBX, and GX Network Management Station Upgrade Guide* (Product Code: 80201)
- *B-STDX, CBX, and GX Getting Started User's Guide* (Product Code: 80195)
- *B-STDX, CBX, and GX Switch Module Configuration Guide* (Product Code: 80196)
- *CBX and GX Switch Software Upgrade Guide* (Product Code: 80198)
- *B-STDX and CBX Frame Relay Services Configuration Guide* (Product Code: 80193)
- *B-STDX and CBX IP Services Configuration Guide* (Product Code: 80194)
- *B-STDX, CBX, and GX Switch Diagnostics User's Guide* (Product Code: 80192)
- *B-STDX, CBX, and GX Switch Troubleshooting User's Guide* (Product Code: 80197)
- *B-STDX, CBX, and GX Console Command User's Reference* (Product Code: 80190)
- *NavisXtend Statistics Server User's Guide* (Product Code: 80215)
- *NavisXtend Accounting Server Administrator's Guide* (Product Code: 80203)
- *NavisXtend Report Generator User's Guide* (Product Code: 80214)

All manuals for the Core Switching Division and the *Master Glossary* are available on the Core Switching Division Technical Publications Documentation Library CD-ROM (Product Code: 80025).

Third Party

- *Solaris 8 Advanced Installation Guide*
- *Solaris 8 (SPARC Platform Edition) Release Notes*
- *Solaris 8 Sun Hardware Platform Guide*
- *Installation Guide Sybase Adaptive Server™ Enterprise on Sun Solaris*
- *HP OpenView Managing Your Network*
- *HP OpenView 6.2 NNM Migration Guide*
- *Quick Start Installation Guide for HP OpenView Network Node Manager and HP OpenView Customer Views for NNM on Solaris*
- *HP OpenView 6.2 Release Notes*

Ordering Printed Manuals Online

You can order Core Switching manuals online. Use the following URL to access the Lucent Bookstore:

http://www.lucentdocs.com

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@lucent.com.
- FAX your comments to 978-692-1510, attention Technical Publications.

Technical Support

The Lucent Technical Assistance Center (TAC) is available to assist you with any problems encountered while using this Lucent product. Log on to our Customer Support web site to obtain telephone numbers for the Lucent TAC in your region:

http://www.lucent.com/support

1

Overview

This chapter gives an overview of the information described in this guide. It provides a suggested reading path to follow, depending on your network needs. Some chapters provide information on ATM network basics such as logical ports, trunks, and PVCs; other chapters explain how to configure optional features such as Virtual Network Navigator Virtual Private Networks (VPNs) and closed user groups (CUGs).

Logical Ports

The following chapters describe ATM logical ports:

- Chapter 2 provides an overview of ATM logical port types and features. Read this chapter if you are unfamiliar with basic ATM UNI concepts such as ILMI and signaling, or if you need more information on ATM VPI/VCI addresses. This chapter also describes the administrative tasks you perform for all logical ports.
- Chapter 3 describes how to configure ATM logical ports on a CBX 500 switch or a GX Multiservice WAN switch platform. This chapter includes information on configuring the logical port options you need if you plan to use SVCs in your network.
- Chapter 4 describes how to configure ATM logical ports on either the B-STDX 8000/9000 or the CBX 500 frame-based modules. Note that since the B-STDX is not a true ATM switch, many of the parameters you need to configure for the various ATM logical port types are different from the CBX or GX; in addition, the B-STDX does not provide ATM features for signaling and SVCs. These same ATM exceptions exist for the CBX 500 frame-based modules.

CBX 500 ATM Flow Control Processor

Chapter 5 provides information about the CBX 500 ATM Flow-Control Processor (FCP), which supports ATM traffic management through binary, hop-by-hop, closed-loop flow-control algorithms that shift network congestion to the edge of the network. In addition, the CBX 500 ATM Flow-Control Processor uses several per-Virtual Circuit (VC) cell/packet queuing and discarding mechanisms for additional network congestion control.

Based on the ATM Forum's *Traffic Management Specification*, Version 4.0, the ATM Flow-Control Processor delivers a fair, deterministic service for bursty ATM traffic, including: dynamically adjusting the Allowable Cell Rate (ACR) in response to Resource Management (RM) cell feedback; reducing congestion in the network by adjusting the data rate at which a VC sends cells fair resource allocation based on the minimum cell rate (MCR); and per VC-queuing with Early Packet Discard/Partial Packet Discard (EPD/PPD) capability.

Chapter 6 provides step-by-step instructions for configuring the ATM FCP as well as answers to frequently-asked questions (FAQ) about working with the ATM FCP.

Note – Contact a qualified Lucent organization for network design validation before enabling the FCP.

ATM Trunks

Chapter 7 describes how to configure the following types of ATM trunks:

- ATM Direct Trunks
- ATM OPTimum (Cell) Trunks
- ATM OPTimum Frame Trunks (B-STDX only)

For information on each of these trunk types, review the trunk logical port descriptions in Chapter 2 and Chapter 4. Chapter 7 also describes how to configure external trunks and provides instructions for using trunk backup and Fast APS.

PVCs

Chapter 8 describes how to configure point-to-point, redirect, and point-to-multipoint PVCs. In addition, Chapter 9 explains how to configure optional Management VPI/VCI, Management PVC, and Management SPVC connections.

Network-wide Features

The following chapters explain how to configure features that you can use throughout your ATM network.

- Chapter 10 describes how the CBX 500 and GX 550 use traffic descriptors to define a service contract that guarantees that a specified amount of data is delivered. You configure a set of traffic descriptors that you can use when you define PVCs throughout your ATM network; this *configurable control circuit* feature enables you to ensure Quality of Service (QoS). Note that ATM services for a B-STDX do not use traffic descriptors.
- Chapter 11 describes a Layer2 Virtual Private Network (VPN) which is an *optional* software feature that enables network providers to dedicate resources for those customers who require guaranteed performance, reliability, and privacy. Use the instructions in this chapter to configure Layer2 VPN services.

Fault-tolerant PVCs

Chapter 12 describes an *optional* logical port feature called fault-tolerant PVC (sometimes referred to as resilient UNI/NNI). A fault-tolerant PVC configuration enables a UNI data communications equipment (DCE) or data terminal equipment (DTE) logical port to serve as a backup for any number of active UNI ports. If a primary port fails or if you need to take a primary port offline for maintenance, you activate the backup port.

Using this feature, a logical port is given a service name. When you configure a PVC, select this service name as the logical port endpoint. If you activate the backup port, all PVCs on the failed primary port are automatically rerouted.

Note – You should not configure SVCs on a logical port that is also designated as a backup port.

If you use resilient UNI features in conjunction with the automatic protection switching (APS) functions available on the CBX and GX optical modules, you can configure a PVC to automatically revert to the backup port if the primary port fails.

Resilient Local Management Interface

Chapter 13 describes the Frame Relay Resilient LMI (RLMI) feature and how to configure RLMI on ATM Network Interworking for Frame Relay NNI logical ports on ATM IWU and ATM CS cards.

Resilient LMI provides resiliency by monitoring LMI link status. RLMI enables a pair of Frame Relay UNI, NNI or ATM Network Interworking for Frame Relay NNI logical ports configured on a B-STDX or CBX switch to serve as preferred and backup ports. If the primary port fails, a switchover to the backup port occurs.

SVCs

The CBX 500 and GX 550 offer switched virtual circuit (SVC) features. With SVCs, connections are not predefined as they are for PVCs. Instead, end stations use a signaling protocol to indicate to the ATM network the endpoint to which it routes the SVC request. To support SVC services, each user endpoint is assigned a unique address that identifies the endpoint and enables the network to route the SVC request.

The following chapters describe basic SVC concepts and configuration:

- Chapter 14 provides an overview of SVC concepts. Read this chapter if you are unfamiliar with SVC address formats and registration or need more information on route determination or address translation. This chapter also describes how to use network ID addressing.
- Chapter 15 describes how to configure SVC node and port prefixes and port addresses for each SVC address format. This chapter includes information on configuring network ID addressing.

The following sections describe *optional* SVC features you can use in your network to take advantage of ATM signaling functions.

SVC Proxy Signaling

Chapter 16 describes SVC proxy signaling. SVC proxy signaling is an *optional* CBX 500/GX 550 feature that enables a single signaling entity to signal on behalf of multiple endpoints. You can use proxy signaling to allow end systems that do not understand ATM signaling to set up SVCs via a proxy signaling agent (PSA). The PSA performs all signaling functions on behalf of the end system, known as the proxy signaling client (PSC).

SPVCs

Chapter 17 describes soft permanent virtual circuits (SPVCs). The network uses signaling to establish an SPVC. The network management system provisions one end of the SPVC with the address identifying the egress interface from the network. Once the SPVC configuration is in place, the switch at one end of the SPVC initiates the signaling. This calling end is responsible for establishing, releasing, and re-establishing the SVC request.

Closed User Groups

Chapter 18 describes closed user groups (CUGs). You can use CUGs to divide all SVC network users into logically linked groups of users. Members of the same CUG have particular calling privileges that members of different CUGs may not have. CUGs form one level of security between users of a network, allowing only those users who are members of the CUG to set up calls to each other. Information about CUG membership and rules is available throughout the network.

Port Security Screening

Chapter 19 describes the Port Security Screening feature. This feature is a mechanism you can use to ensure that your network cannot be compromised by unauthorized SVC access. You do this by creating screens that can allow/disallow incoming and outgoing SVCs.

PNNI

Chapter 20 describes how to configure the ATM PNNI routing protocol in your Lucent network. Table 20-1 on page 20-2 lists the supported PNNI features included in this release.

Private Network-to-Network Interface (PNNI) is a standard designed by the ATM Forum. This standard defines both an ATM routing protocol and an ATM signaling protocol. Lucent supports PNNI on both the CBX 500 and GX 550 switch platforms. For a detailed explanation of PNNI routing, see the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0* (af-pnni-0055.000), available from the ATM Forum's Web site (**`http://www.atmforum.com`**).

Connection Admission Control

Appendix A describes how to tune the Lucent Call Master Connection Admission Control (CAC) to achieve a desired cell loss ratio objective across all physical ports in your network. The Lucent CAC is responsible for the bandwidth allocation on all ATM cards on the CBX 500, GX 550, and B-STDX. It is also responsible for bandwidth allocation on all frame cards with the priority frame capability.

ATM Traffic Descriptors

Appendix B describes how each traffic descriptor combination affects the cell streams under different traffic conditions. When you create either a PVC or a point-to-multipoint circuit, you select one of several traffic descriptor combinations. The traffic descriptor combination specifies which traffic parameters are used for traffic control. It also determines the number and type of cells that are admitted into a congested queue, and whether or not high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds.

CBX 500 Shared SP Threads

Appendix C provides information on shared SP threads. CBX 500 chassis slots 3-4, 5-6, 7-8, 9-1, 10-2, 11-12, 13-14, and 15-16 are associated with the SP threads. This means that if you have an IOM installed in slots 3 and 4, you are “sharing” an SP thread. If you have an IOM in slot 9 or 10, you are sharing a thread with the SP itself. In this case, there are no thread limitations; the IOM has the full 599.040 Mbps of bandwidth available.

Priority Routing

Appendix E details priority routing, which enables you to prioritize virtual circuits (PVCs and SVCs) in your network. Priority routing can provide the following advantages: higher up time for high-priority circuits; optimal paths for high-priority circuits; and higher capacity to burst past the guaranteed QoS rates for high-priority circuits. The switch treats priority routing, QoS class, and circuit priority as independent elements. Priority routing rules are used for connection setup. QoS class is applied after the connection is set up. Circuit priority rules are applied once QoS class is established. Keep in mind that you must assign a higher priority to real-time QoS classes.

Reliable Scalable Circuit

Appendix F lists the NMS SNMP set errors that can occur during Circuit Add, Modify, and Delete operations for standard and redirect permanent virtual circuits (PVCs). When you perform these operations, the errors and, when possible, the circuit end point that caused the error are reported to you. When an error occurs, the Abort, Retry, and Ignore options available to you are sensitive to the end point that caused the failure.

OSPF Name Aggregation

Appendix G provides guidelines for using Open Shortest Path First (OSPF) name aggregation to minimize memory consumption when you provision prefixes and addresses for ATM SVC/SPVC or Frame Relay SVC connections across Lucent network switches.

Customer Names

Appendix H describes Customer Names, an *optional* software feature that enables network providers to assign ATM logical ports to a specific customer so that they can then use the customer name as a filter when viewing logical ports. You can configure the Customer Names feature with or without the use of Virtual Private Network (VPN).

Abbreviations and Acronyms

Abbreviations and Acronyms lists abbreviations for units of measure (in specifications) and terms and acronyms used in Lucent documentation.

2

About ATM Logical Ports

This chapter describes ATM concepts you need to understand before you can configure ATM services for a B-STDX 8000/9000 or CBX 500 switch, or for a GX Multiservice WAN switch.

Note – The B-STDX 8000/9000 switch does not support all ATM features. For specific information about the B-STDX ATM implementation, see Chapter 4.

For details on configuring an ATM NNI logical port for PNNI routing, see Chapter 20.

ATM UNI Concepts

This chapter describes the following CBX and GX logical port types:

- User-to-Network Interface (UNI) Data Communications Equipment (DCE) and Data Terminal Equipment (DTE)
- OPTimum Cell Trunk
- Direct (Cell) Trunk
- Circuit Emulation (CE)
- Network-to-Network Interface (NNI)

For information about the logical port types you can configure on a B-STDX and the CBX 500 frame-based modules, see Chapter 4, "Configuring ATM Logical Ports on the B-STDX 8000/9000."

ATM UNI DCE and DTE

This section describes some of the concepts you need to know when defining ATM UNI DCE and ATM UNI DTE logical ports for CBX and GX switches. You can configure a single ATM UNI logical port on a physical port to support the following standard protocol functions:

- ATM UNI 3.0, 3.1, and 4.0 (see "ATM UNI 4.0 Support" on page 2-3 for more information)
- International Telecommunications Union (ITU) UNI
- Interim Inter-switch Signaling Protocol (IISP) 3.0 and 3.1

You use the ATM UNI DCE logical port type to communicate with most ATM customer premise equipment (CPE). An ATM UNI DCE logical port represents the "network side" equipment. This logical port supports all types of PVCs as well as SVCs. For SVC applications, the ATM UNI DCE logical port assumes the role of the network side of the UNI signaling interface.

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

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

ATM UNI 4.0 Support

This release supports the ATM Forum's UNI Signaling 4.0 Specification. The following capability list from this specification outlines support on a per-feature basis.

Item Number	Capability
1	Point-to-point Calls
2	Point-to-multipoint Calls
3	Signaling of Individual QoS Parameters
4	Leaf Initiated Join[a]
5	ATM Anycast
6	ABR Signaling for Point-to-point Calls
7	Generic Identifier Transport
8	Virtual UNIs
9	Switched Virtual Path (VP) service
10	Proxy Signaling
11	Frame Discard
12	Traffic Parameter Negotiation
13	Supplementary Services
13.1	Direct Dialing In (DDI)
13.2	Multiple Subscriber Number
13.3	Calling Line Identification Presentation (CLIP)
13.4	Calling Line Identification Restriction (CLIR)
13.5	Connected Line Identification Presentation (COLP)
13.6	Connected Line Identification Restriction (COLR)
13.7	Subaddressing (SUB) Currently Available
13.8	User-user Signaling (UUS) Currently Available

[a] The ATM Forum *UNI Signaling 4.0* specification feature of Leaf Initiated Join (LIJ) support is under consideration. Industry demand does not exist yet to support this feature and no current CPE device supports this feature. The actual implementation of LIJ will likely correspond with the implementation of PNNI Version 2.0, which also introduces support of this feature.

Using Interim Link Management Interface (ILMI)

ILMI is a Management Information Base (MIB) that provides status and communication information to ATM UNI devices. This information includes status and statistics for virtual paths, connections, and address registration. The CBX, GX, and B-STDX switches support the ILMI MIB.

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

If you intend to use ILMI on the logical port (and the attached device supports ILMI), Lucent recommends that you enable ILMI support *before* you provision circuits. Under certain conditions, enabling ILMI after you provision circuits on a logical port may cause negative bandwidth with the associated QoS classes (including constant bit rate [CBR]).

Note – If you enable ILMI on a logical port, and for some reason the ILMI state is down, the logical port does not go down.

Table 2-1 describes the differences between UNI DCE and DTE logical ports with ILMI enabled and disabled.

Table 2-1. Logical Ports and ILMI Settings

Port Type	Effect On	With ILMI Enabled	With ILMI Disabled
UNI DCE	Address Registration	• Sends node prefixes • Sends port prefixes • Accepts addresses (qualified against configured prefixes)	None
	Remainder of ILMI MIB	Switch responds to `get` and `get next` commands sent by attached devices.	None
UNI DTE	Address Registration	Accepts prefixes (and optionally qualifies prefixes against configured prefixes).	None
	Remainder of ILMI MIB	Switch responds to `get` and `get next` commands sent by attached devices.	None

ILMI VCC Trap Support

CBX 500, GX 550, and B-STDX 8000/9000 switches can receive ILMI traps that report virtual channel connection (VCC) status from ATM UNI 3.1 end system devices. If a Lucent switch receives an ILMI trap indicating a change in PVC status, the information is transmitted over one or more Lucent switches to the PVC endpoint at a remote ATM UNI 3.1 device.

- If the remote interface is Frame Relay, the PVC status change (inactive or active) is transmitted by Frame Relay to ATM Service Interworking to the remote interface, and is reported by LMI protocol to the remote circuit endpoint.
- If the remote interface is ATM, the PVC status change is reported to the remote circuit endpoint by presence of (inactive) or absence of (active) virtual channel level (F5) Operations, Administration, and Maintenance (OAM) alarm indication signal (AIS).

To receive ILMI traps from ATM UNI 3.1 devices, you must enable the ILMI Administrative Status attribute. For information about enabling the ILMI Administrative Status attribute for logical ports, see Chapter 3, "Configuring CBX 500 or GX 550 Logical Ports," and Chapter 4, "Configuring ATM Logical Ports on the B-STDX 8000/9000."

Using Logical Port Signaling

This section describes the default signaling tuning parameters for an ATM UNI logical port.

Note – ATM logical ports on B-STDX modules or the CBX 500 frame-based modules do not support signaling.

In an ATM network, signaling is responsible for establishing and releasing SVCs. Signaling is used only on ingress and egress ports, including user-to-network, network-to-user, and network-to-network ports.

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

ILMI and Signaling Example

Under certain conditions, enabling ILMI and/or signaling after you provision circuits on a logical port may cause negative bandwidth for the associated QoS classes.

For example, you create an ATM logical port with both ILMI and signaling disabled. You then create a full-bandwidth CBR circuit (PCR = 96000 cps) on this logical port. If you later enable ILMI and/or signaling on the logical port, the bandwidth now appears to be negative. The circuit will no longer come back up due to insufficient bandwidth if you modify the logical port admin status or circuit.

Configurable Control Circuits

The CBX 500 and GX 550 configurable control circuit feature enables you to configure forward and reverse traffic descriptors for the following:

- ATM UNI ILMI and signaling control channels
- ATM Direct and OPTimum trunk signaling and node-to-node management traffic

The switch software views a control circuit as a virtual circuit link (VCL) between the logical port and the internal switch processor. When you configure a control circuit, the switch creates a VCL between this port and the switch processor. The logical port uses the forward traffic descriptor to police traffic flowing into the switch (UNI ILMI and signaling control channels only). It uses the backward traffic descriptor to determine the service category and equivalent bandwidth for the control circuit. The backward traffic descriptor is also used to calculate the effective bandwidth of the circuit to be used for bandwidth management on the logical port.

For control channels between a Lucent switch and another vendor device (including the ILMI, UNI signaling, and PNNI routing control channels), the traffic descriptor (TD) values calculate both the amount of bandwidth reserved by CAC and the rate at which the control channels are policed.

Control channels are not policed by default. When you enable the UPC or network parameter control (NPC) for the particular logical port, the control channel is policed at the traffic descriptor rate. Similar to the trunk control channels, the TD values associated with the ILMI, UNI signaling, and PNNI routing control channels do not affect the traffic shaping rate.

For more information about traffic descriptors, see Chapter 10, “Configuring ATM Traffic Descriptors.”

ATM OPTimum Cell Trunk

The CBX 500, GX 550, and B-STDX 8000/9000 ATM OPTimum cell trunk carries all types of PVC, SVC, and management data. The ATM OPTimum trunk logical port type provides trunk connectivity between two Lucent switches that are not directly connected. In this application, some other network elements are separating the two Lucent switches. These network elements usually consist of ATM switches in another network. The network provider who manages the other ATM switches provisions a virtual path connection (VPC) to carry the Lucent trunk traffic. This VPC supports the trunk and carries all the associated trunk protocol, management data, PVCs, and SVCs between the two Lucent switches (see "Configuring the Virtual Path Identifier (VPI)" on page 2-7).

Before you can configure an ATM OPTimum trunk logical port, *you must first configure an ATM UNI or NNI logical port with a minimal amount of bandwidth*; this logical port acts as the feeder port. The feeder port serves the following purposes:

- Enables interoperability between Lucent and non-Lucent switches by providing a standard interface type over which a link management protocol can run
- Controls the valid range of virtual path identifier/virtual channel identifier (VPI/VCI) values that you can use

Using switch software release 3.0 or greater on the CBX switch and 1.0 or greater on the GX switch enables VPCs to traverse OPTimum trunks. This capability depends on the logical port configuration as well as the configuration of the interfacing network. Prior to this release, VPCs could not traverse OPTimum trunks.

Configuring the Virtual Path Identifier (VPI)

The VPI is the identifier used for all VCC circuits routed over the OPTimum trunk. The range of valid VPI values depends upon the number of valid VPI bits you set for the ATM UNI feeder port (see Table 2-2 on page 2-13). Enter a number from 0-*nnnn* to identify the virtual path for the ATM logical port; *nnnn* is equal to 2^{P}-1, where *P* is the value specified in the Valid Bits in VPI field for the UNI feeder port that shares this physical port (see the example on page 2-12).

For example, if you entered 4 in the Valid Bits in VPI field for the UNI feeder port, you can have up to 15 virtual paths on this port (2^{4}-1=15); if you entered 8 in the Valid Bits in VPI field, you can have up to 255 virtual paths on this port (2^{8}-1=255). The highest value you can enter (and therefore, the greatest number of virtual paths you can configure on the port) depends on the value you entered in the Valid Bits in VPI field for the ATM UNI feeder port. The OPTimum trunk's VPI must be unique to the port.

Configuring the OPTimum Trunk for VPCs

Permanent virtual circuit (PVC) and switched virtual circuit (SVC) VPCs and IP-related connections can traverse OPTimum trunks. The following section describes each configuration.

PVC/SVC VPC Connections

The VPC VPI start and VPC VPI stop values define the range of VPIs to be used for all connection-based VPC circuits (that is, PVC, SVC, and SPVC) over this OPTimum trunk.

The valid range of VPI values depends on the number of valid VPI bits you set for the ATM UNI feeder port (see Table 2-2 on page 2-13). The specified range may not overlap the ranges specified for OPTimum trunk Internet Protocol (IP) connections.

Example

Assume that the following conditions are in place:

- The number of valid VPI bits set from the ATM UNI feeder port is 4.
- The VPI value is set to 0.

Using these assumptions, if you want to configure two VPIs on the OPTimum trunk to support PVC, SVC, or SPVC VPC circuits, you could specify a VPC VPI start of 1 and a VPC VCI stop of 2.

Note – The network that interfaces with the OPTimum trunk must be configured to accept circuits with this VPI and any of its valid VCIs. To accomplish this, create a PVC in the interfacing network using this VPI and define the PVC circuit type as VPC (see Table 8-7 on page 8-27).

IP-Related Connections

You can configure label switch paths (LSPs) over OPTimum cell trunks on B-STDX and CBX switches.

- On CBX 500 switches, IP automatically assigns a permanent virtual path (PVP) to each LSP crossing an OPTimum trunk. These point-to-point PVPs carry LSP traffic in both directions, which reduces the number of paths required to interconnect switches in two given clusters.
- On B-STDX switches, IP assigns a virtual channel connection (VCC) to each LSP crossing an OPTimum trunk.

Before IP can assign PVPs and VCCs, you must specify specific VPI values and ranges of VPI values for each logical port endpoint of the OPTimum trunk. You specify these values on the OPT Trunk VPI Range Attributes dialog box. See the *B-STDX and CBX IP Services Configuration Guide* for more information.

ATM Direct Trunk

The CBX 500, GX 550, and B-STDX 8000/9000 ATM direct trunk is used to provide trunk connectivity between two directly connected Lucent switches. The ATM direct trunk carries all types of PVC, SVC, trunk protocol, and management data between the Lucent switches.

ATM CE

The GX 250 ATM Circuit Emulation (CE) logical port type is configured only on a GX 250 DS3 CE Transport card physical port. You can configure one ATM CE logical port on each DS3 physical port. The ATM CE logical port can be used as a PVC endpoint.

The ATM CE physical port, logical port, and circuit are used to provide an unstructured DS3 service that emulates a point-to-point DS3 circuit configuration. The CE service enables two devices to transparently pass a DS3 bitstream through an ATM network, so that the two devices appear to be directly connected to each other. The ATM network, in effect, is the wire used to pass the bitstream from one device to the other.

Note – The product formerly called the GX 250 Multiservice Extender is now referred to as the GX 550 ES (Extender Shelf) in the NavisCore NMS interface.

The NavisCore NMS may display features that are not available in this release. For a complete list and explanation of each of the features that are supported in this release, see the NavisCore Software Release Notice.

ATM NNI

The CBX 500 and GX 550 ATM Network-to-Network Interface (NNI) logical port type enables you to connect ATM-based public networks belonging to two different carriers. This logical port type implements the Broadband-Inter-Carrier Interface (B-ICI) protocol, which facilitates the multiplexing of services for inter-carrier (Regional Bell Operating Company [RBOC] and inter-exchange carrier [IXC]) delivery. You can use an ATM NNI logical port as a feeder port for Lucent OPTimum trunks and virtual UNIs.

ATM NNI logical ports also support the PNNI routing protocol. To configure PNNI routing in your Lucent network, see Chapter 20. For a detailed explanation of PNNI routing, see the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0 (af-pnni-0055.000)*, available from the ATM Forum's web site (**`http://www.atmforum.com`**).

Virtual UNI/NNI

A Virtual UNI/NNI forms an extension of the standard “direct” UNI DCE/DTE or NNI logical port types. In an ATM network, you can use virtual UNI/NNI logical ports to enable VP tunneling or to connect to a VP multiplexer. VP tunneling allows you to connect two switches (using signaling) via a virtual path through the ATM network (network-to-network connection class). See the example in Figure 2-1.

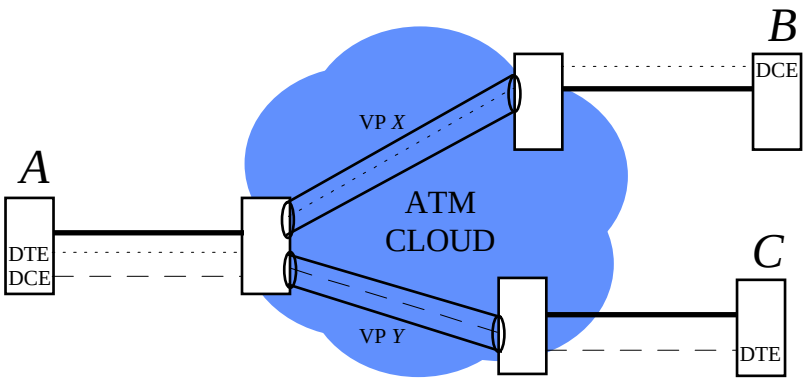


Figure 2-1. Two Virtual UNIs Through Central Network

VP multiplexing enables you to connect a GX 550 or CBX 500 switch to a VP multiplexer using a direct UNI (or NNI) logical port on which you have configured several “virtual” UNI (or NNI) ports. The VPI address range you define for each virtual UNI/NNI port corresponds to a port on the VP multiplexer. This method does not use VPCs and the configured logical port bandwidth can be used by any PVC on any VPI (network-to-endsystem connection class). See the example in Figure 2-2.

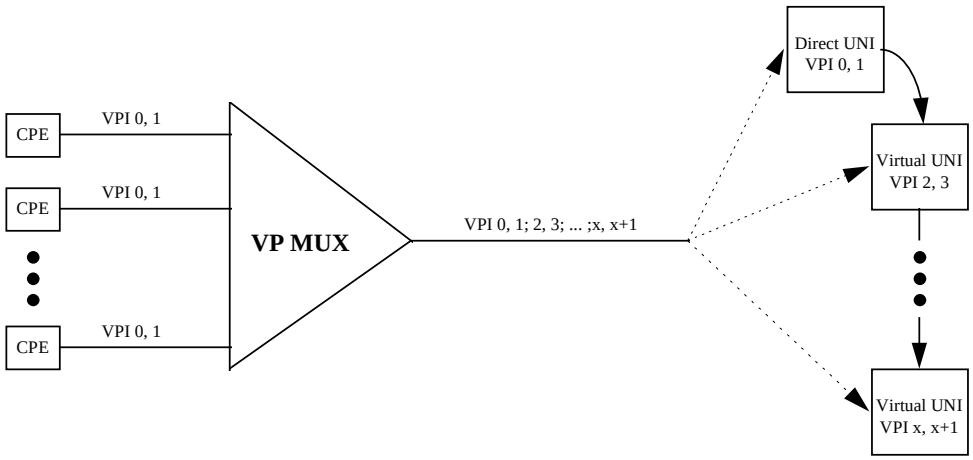


Figure 2-2. Virtual UNI with VP Multiplexer

Virtual Paths and Virtual Channels

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

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

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

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

Setting the Number of Valid Bits in the VPI/VCI

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

For the CBX 500, the valid range for the VPI field is 0 – 8 and the valid range for the VCI field is 6 – 14; for the GX 550, the valid range of the VPI field is 0 – 12 and the VCI field is 6 – 13. You may have to adjust these values in the following situations:

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

  This OPTimum trunk/circuit trade-off is shown by the following formulas:

  Maximum virtual paths = 2^P – 1
  (^{P} represents the value in the Valid Bits in VPI field)

  Maximum virtual channels = 2^C – 32
  (^{C} represents the value in the Valid Bits in VCI field)

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

Note – On a CBX 500 only, **P+C ≤ 14**.

VPI/VCI Bit Allocation (CBX 500/GX 550)

When configuring a Direct Trunk or UNI logical port, you select the number of bits in the Number of Valid bits in VPI/VCI field. The highest order bit set (1) is used for reserving address space for Multipoint-to-Point Tunnel (MPTs). It does not matter what the bit allocation for VPI/VCI is, a set portion of the bit is used for establishing 16 MPTs across a trunk. The number of bits configured for VPI will directly affect the total number of transit VCs.

The total number of VCCs, MPTs, and VPCs supported varies because of dynamic address allocation; however, the maximum number supported is 15360 VCCs/VPCs and 1024 MPTs. With dynamic address allocation, VPI bits are no longer dedicated for use with VPCs.

Use Table 2-2 as a guide to set the VPI/VCI values on a CBX 500. Use Table 2-3 as a guide to set the VPI/VCI values on a GX 550.

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

Table 2-2. Number of Valid Bits in VPI/VCI for CBX 500

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

[a] Only 8 bits of the VPI are available on UNI type interfaces per ATM Forum standards.

[b] VCI 0 - 31 are reserved and should not be used for user traffic per ATM Forum standards.

Table 2-3. Number of Valid Bits in VPI/VCI for GX 550

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

[a] Only 8 bits of the VPI are available on UNI type interfaces per ATM Forum standards.

[b] VCI 0 - 31 are reserved and should not be used for user traffic per ATM Forum standards.

Configuring VCC VPI Start and Stop Values for Virtual UNI/NNI

The CBX 500 and GX 550 switches provide a virtual UNI/NNI feature. The direct UNI/NNI provides the range of VCC VPI start and stop values. The range of VPI start and stop values you define for the first virtual UNI/NNI must fall within this range; it cannot overlap with the range you define for subsequent virtual UNI/NNI ports.

For example:

Logical Port	VPI Start	VPI Stop
First Virtual UNI/NNI	2	5
Second Virtual UNI/NNI	6	10

The switch handles SVCs differently, depending on how you configure the Connection Type field of the virtual UNI/NNI (see Table 3-6 on page 3-22). If the logical port is set to the Network <-> Network Connection Type, it implies a network scenario as shown in Figure 2-1 on page 2-10. In this case, the first VPI is used for VCCs only. Additional VPIs can only be used for signaled VPCs with the best effort QoS. If the logical port is set to the Network <=> Endsystem Connection Type, it implies a network scenario as shown in Figure 2-2 on page 2-10. In this case, all available VPIs can be used for either signaled VCCs or VPCs of any QoS class.

The restrictions described above only apply to SVCs. When using virtual UNI/NNIs in conjunction with PVCs, there are no restrictions and the Connection Type field on the logical port is not used.

About Logical Port Bandwidth

The maximum amount of logical port bandwidth does not equal the physical port bandwidth due to the overhead associated with packaging ATM cells into the physical layer frames. This overhead is different for each physical media type as well as the different packaging methods. Table 2-4 provides a guide to mapping and converting physical layer bandwidth to logical port bandwidth.

Table 2-4. Physical and Logical Port Bandwidth Conversions

Physical Port Media Type	Physical Port Bandwidth (Kbps)	Exact Logical Port Bandwidth (Kbps)	Exact Logical Port Bandwidth (cps)	NMS Rounded Maximum Logical Port Bandwidth (Kbps)	NMS Rounded Maximum Logical Port Bandwidth (cps)
OC-12c/STM-4	622080	599040	1412830.19	599040	1412830
OC-3c/STM-1	155520	149760	353207.55	149760	353207
ATM DS3 (with Physical Layer Convergence Protocol [PLCP])	44736	40704	96000	40704	96000
ATM DS3 (with header check sequence [HCS] direct mapping)	44736	44209.694	104268.15	44209	104266
ATM E3 (with HCS direct mapping)	34368	33920	80000	33920	80000
ATM E3 (with G.751 PLCP)	34368	30528	72000	30528	72000
T1	1544	1536	3622.64	1536	3622
E1	2048	1920	4528.3	1920	4528

In some cases, due to the way the switch stores logical port bandwidth, the NMS may have to round down non-integer maximum logical port bandwidth values to the nearest kbps value.

Note – For most applications, rounding down non-integer maximum logical port bandwidth does not cause any problems. However, if you need to run 100% line rate traffic through a policed PVC where you have rounded values, policing may cause minor cell loss.

Example

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

Modifying Logical Port Bandwidth

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

CBX 500 SP Thread Bandwidth Available for Logical Ports

The NMS and CAC enforce the switch processor (SP) fabric thread bandwidth such that each SP fabric thread is limited to 599.040 Mbps. This enforcement ensures that service is guaranteed even when two IOMs are placed on the same SP fabric thread. The 599.040 Mbps number is derived from the maximum user cell bandwidth that the OC-12c/STM-4 interface supports (the OC-12c/STM-4 physical layer bandwidth is 622.080 Mbps, but the maximum user traffic that any OC-12c/STM-4 port can support is 599.040 Mbps). This 599.040 thread limitation is also derived from the maximum user cell bandwidth that the four OC-3c/STM-1 interfaces support (the OC-3c/STM-1 physical layer bandwidth is 155.020 Mbps, but the maximum user traffic that any OC-3c/STM-1 port can support is 149.76 Mbps).

For example, this NMS enforcement is noticeable whenever you attempt to provision two OC-3c/STM-1 cards on the same SP fabric thread. As you provision logical ports, the NMS subtracts the assigned bandwidth from the 599.040 Mbps total. After you provision four OC-3c/STM-1 logical ports at the maximum 149.76 Mbps bandwidth value, there is no bandwidth left for the other OC-3c/STM-1 card and its logical ports. Because of this, when you use two cards on the same fabric thread, Lucent recommends you allocate the bandwidth accordingly across all of the IOM ports.

Note – You can oversubscribe the logical ports to avoid any negative implications associated with this restriction. You can use the Set QoS Parameters dialog box (accessible from the Add Logical Port dialog box) to oversubscribe a logical port.

About the Oversubscription Factor

The oversubscription factor percentage enables you to optimize the number of PVCs and SVCs you can configure on the network by allowing you to oversubscribe the logical ports. If you configure oversubscription for the variable bit rate (VBR) classes of service (CoS), QoS is no longer guaranteed.

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

The CAC algorithm determines effective bandwidth of a virtual circuit (PVC and SVC). For a VBR circuit, the CAC uses the circuit's PCR, sustainable cell rate (SCR), and maximum burst size (MBS) values. For CBR circuits, the CAC uses the PCR of the circuit. UBR circuits are assigned 100 cps of bandwidth for load and reroute purposes, since it is a "best effort" service.

Note – Appendix A describes how to tune the CAC to optimize your network. If you tune the CAC properly, you can optimize network resources without adversely affecting QoS.

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

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

Since inter-local area network (LAN) traffic is bursty in nature, not all network traffic uses the network resources at precisely the same time. Basically, the higher you set the oversubscription factor, the less guarantee there is that user data will get through on the port; the trade-off is that you can provision more circuits on that port. If, however, all network traffic attempts to use the network resources at precisely the same time (for example, during multiple file transfer sessions over the same trunk), some traffic may be delayed or even dropped.

If you leave the oversubscription factor set for the minimum value of 100%, the port delivers all user data for that CoS without unanticipated delays or excessive cell loss. A value of 200% effectively doubles the virtual bandwidth available for that CoS.

Note – Lucent reserves a certain percentage of bandwidth for network management, routing updates, and other management traffic.

About VP Shaping on the CBX 500

Virtual path (VP) shaping provides the ability to shape OPTimum trunk connections at a specified PCR while preserving QoS integrity. This feature is useful when multiple OPTimum trunk logical ports exist on one physical port and each trunk must traverse a VP of a fixed PCR. This feature ensures that the maximum rate of the OPTimum trunk traffic does not exceed the specified PCR. See either the CBX 500 or NavisCore Software Release Notices (SRNs) for appropriate revision levels.

On a CBX 500, you can enable VP shaping only if the host IOM is equipped with certain revisions of the ATM Flow Control Processor (FCP) module. The FCP supports flow control or VP shaping on a per-logical port basis. See either the CBX 500 or NavisCore SRNs for appropriate revision levels.

Shaping is performed by assigning each VP a single queue on the FCP. Shaping is only performed on the first VP; FCP treats the other VPs (used for VP switching) as VCs (which are shaped at their initial cell rate [ICR]). One PCR is provisioned for the first VP of the lport and the aggregate traffic is scheduled with this rate. As a result, the aggregate rate of the traffic on the first VP never exceeds the provisioned PVC rate. Four queues are maintained for each shaped VP. The CBR queue has the highest priority, followed by VBR-RT, VBR-NRT, and available bit rate/unspecified bit rate (ABR/UBR) queues. VCCs within a shaped VP are mapped to the four queues according to their QoS.

For additional information and configuration instructions, see "Configuring VP Shaping on CBX 500 Virtual UNI Logical Ports" on page 3-19.

Note – Lucent recommends that you do not mix shaped and non-shaped logical ports on a physical port.

About VP Shaping on the GX 550

When you configure OPTimum trunk, Virtual UNI, or Virtual NNI logical ports on phy modules attached to GX 550 Multiservice WAN Base Input/Output 2 (BIO2) modules, you can enable VP shaping to provide egress traffic shaping. The VP shaping feature enables multiple VPs that are destined to multiple endpoints to be shaped from a single physical port at the egress. Traffic is shaped based on a user-defined shaping rate that is defined on the Add Logical Port dialog box during logical port configuration.

VP shaping on the GX 550 BIO2 module:

- Enables GX 550 traffic sent to your network to comply with your purchased traffic contract.
- Enables GX 550 traffic to traverse over other networks that cannot handle bursts in cell traffic.
- Ensures that the maximum rate of the OPTimum trunk traffic does not exceed the specific cells per second (CPS).

When you define Administrative attributes for an OPTimum trunk, Virtual UNI, or Virtual NNI logical port on the BIO2 module, you can enable VP shaping by setting the VP Shaping and VP Shaping Rate attributes. For more information, see the descriptions of these attributes in Table 3-4 on page 3-14.

Due to hardware restrictions, you cannot dynamically modify (enable or disable) the configured VP Shaping mode for BIO2 virtual UNI logical ports on which circuits are provisioned. If you plan to enable VP Shaping on virtual UNI logical ports, Lucent recommends that you set the VP Shaping attribute *before* configuring circuits on the logical port.

To modify the VP Shaping mode for GX 550 virtual UNI logical ports on which circuits are provisioned, use the procedure described in "Modifying the VP Shaping Mode on GX 550 Virtual UNI Logical Ports" on page 3-21.

Administrative Tasks

This section describes how to:

- Use templates to define a new logical port
- Modify switch configuration attributes
- Delete ATM logical port components, including:
  - Circuits
  - Trunks
  - Management VPI/VCI

Using Templates

If you defined a logical port configuration and saved it as a template (see *Is Template* field), you can define a new logical port using the same parameters.

To define a logical port from a template:

1. Choose the *Add Using Template* command on the Set All Logical Ports in PPort dialog box (see Figure 3-1 on page 3-4).
2. Perform one of the following tasks:
   - Choose *Last Template* to use the last template you defined for this switch.
   - Choose *Template List* to display a list of templates defined for this map. Select a template and choose OK.

Modifying Switch Configuration Attributes

When you modify CBX 500, GX 550, and B-STDX 8000/9000 switch attributes, you usually need to perform a PRAM Sync to synchronize the configuration information between switch PRAM and the NMS database. See the *B-STDX, CBX, and GX Getting Started User's Guide* for information about using PRAM features.

Non-Disruptive Logical Port and Trunk Attributes (CBX 500 and GX 550 Only)

Certain logical port and trunk attributes are defined as *non-disruptive*. When you modify any of these attributes on CBX 500 or GX 550 switches, the NMS sends the appropriate SNMP SET commands to the switch without bringing down the logical port. Switch PRAM and the NMS database are synchronized automatically, without interrupting network traffic.

Note – When you modify any attributes other than non-disruptive attributes, the NMS will bring down the logical port.

Non-disruptive attributes appear in ***bold italicized*** text on NavisCore dialog boxes.

Table 2-5 lists the non-disruptive logical port and trunk attributes, with references to additional information. This guide does not illustrate all the dialog boxes that can display these attributes.

Table 2-5. Non-Disruptive Logical Port and Trunk Attributes

Attribute	See
Net Overflow	"Administrative Attributes" on page 3-14 "Defining ATM UNI DCE/DTE Logical Ports" on page 4-14 "Defining ATM OPTimum Frame Trunk Logical Ports" on page 4-37 "Defining ATM Network Interworking for Frame Relay NNI Logical Ports" on page 4-42
Redirect PVC Delay Time	"Administrative Attributes" on page 3-14 "Defining ATM UNI DCE/DTE Logical Ports" on page 4-14 "Defining ATM Network Interworking for Frame Relay NNI Logical Ports" on page 4-42
VP Shaping (FCP for CBX 500)	"Administrative Attributes" on page 3-14

Table 2-5. Non-Disruptive Logical Port and Trunk Attributes (Continued)

Attribute	See
Call Admission Control	"ATM Attributes" on page 3-22 "ATM Attributes" on page 4-23
Loss Threshold	"ILMI/Signaling/OAM Attributes" on page 3-28 "ILMI/Signaling/OAM Attributes" on page 4-25
DTE Prefix Screen Mode	"ILMI/Signaling/OAM Attributes" on page 3-28
NTM Congestion Thresholds (T, Notification Time; CT1, CT2, CT3, CT4 Thresholds)	"Completing the Logical Port Configuration" on page 3-43 See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for information about configuring these parameters.
CBR, VBR-RT, VBR-NRT, ABR/UBR Routing Metric Options and Oversubscription %	"Setting Quality of Service Parameters" on page 3-44
Hold Down Timer (0..255)	"Defining SVC Parameters Attributes" on page 3-52
Discard Priority Mapping (DE/CLP) and Congestion Mapping (FECN/EFCI)	"Discard/Congestion Mapping Attributes" on page 4-33 and page 4-48.
LMI Update Delay	"Link Mgmt Attributes" on page 4-44
CIR Policing Enabled	"Link Mgmt Attributes" on page 4-44
RLMI Max Full Status Attempts	"Link Mgmt Attributes" on page 4-44
Static Delay	"Configuring an ATM NNI Logical Port" on page 20-44 "Accessing Trunk Functions" on page 7-14
Trunk Admin Cost	"Accessing Trunk Functions" on page 7-14
Subscription Factor (%)	"Accessing Trunk Functions" on page 7-14
Area ID	"Accessing Trunk Functions" on page 7-14
Customer Name	"Configuring a Logical Port for Layer2 VPN" on page 11-7 "Associating a Logical Port with a Customer Name" on page H-3

Deleting ATM Logical Ports

Perform the following steps before deleting an ATM logical port:

Step 1. Ensure the logical port is not defined as part of a circuit.

Step 2. Ensure the logical port is not defined as part of a trunk.

Step 3. Ensure the logical port is not defined as the feeder (ATM UNI DCE/DTE or ATM NNI) for an existing ATM OPTimum trunk logical port.

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

- Circuits
- Trunks
- Logical port

Deleting Circuits

To delete a circuit:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits. The Set All PVCs On Map dialog box appears (see Figure 8-1 on page 8-10).
2. To view the list of circuits, select the *Search by Name* field and press Return. If necessary, select each circuit and review each logical port endpoint.
3. Select the circuit to delete.
4. Choose Delete.
5. Choose Close to return to the network map.

Deleting Trunks

To delete a trunk:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Trunks. The Set All Trunks dialog box appears (see Figure 7-2 on page 7-14).
2. To view the list of trunks, select the *Search by Name* field and press Return. If necessary, go to the Defined Trunk Name window, individually select each trunk, and review each logical port endpoint.
3. Select the trunk to delete.
4. Choose Delete.
5. Choose Close to return to the network map.

Deleting Management VPI/VCIs

To delete a management VPI/VCI:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Management VPI/VCIs. The Set All Management VPI/VCIs dialog box appears (see Figure 9-2 on page 9-8), listing the defined management VPI/VCIs in the network configuration in the Defined Management Connection window.
2. Select the management VPI/VCI to delete.
3. Choose Delete.
4. Choose Close to return to the network map.

Deleting the Logical Ports

To delete the logical port:

1. Select the switch from which to delete the logical port.
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the physical port on which the logical port resides, and press the right mouse button to display a popup menu. Select Logical Port. The Set All Logical Ports in PPort dialog box appears (see Figure 3-1 on page 3-4).
4. Select the logical port to delete. Make sure the Loopback Status field displays NONE.

Note – Make sure this logical port is not the logical port used as the feeder for an ATM OPTimum trunk. If this is the case, either delete the OPTimum trunk logical port or first define another feeder before you delete this logical port.

5. Choose Delete.
6. Choose Close.

3

Configuring CBX 500 or GX 550 Logical Ports

This chapter provides instructions for configuring ATM logical ports on a CBX 500 switch or a GX 550 Multiservice WAN switch. For additional configuration information and a description of Lucent's ATM logical port service, see the following chapters:

- For an overview of ATM logical port service, see Chapter 2.
- For information about configuring ATM logical ports on a B-STDX switch, see Chapter 4.
- For details on configuring an ATM NNI logical port for PNNI routing, see Chapter 20.

Accessing ATM Logical Port Functions

To access the logical port functions in NavisCore:

1. Select the switch to which you want to add a logical port.
2. Log in to NavisCore using either a provisioning or operator password.
3. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The CBX 500 or GX 550 Switch Back Panel dialog box appears.

   To access a GX 250 switch and logical port functions:

   a. From the GX 550 Switch Back Panel dialog box, select the SwDwLn module.

   b. Choose GX 250. The GX 250 Switch Back Panel dialog box appears.

Note – The product formerly called the GX 250 Multiservice Extender is now referred to as the GX 550 ES (Extender Shelf) in the NavisCore NMS interface.

The NavisCore NMS may display features that are not available in this release. For a complete list and explanation of each of the features that are supported in this release, see the NavisCore Software Release Notice.

---

4. Select the physical port you want to configure and press the right mouse button to display a pop-up menu.
5. Perform one of the following sets of steps, depending on your configuration:

   To define the logical port for a DS1 (T1) channel on the 3-Port Channelized DS3/1 IMA IOM:

   a. Select Physical Port Attributes from the popup menu. The Set DS3 Physical Port Attributes dialog box appears.

   b. Select the button for the channel you want to configure.

   c. Choose Set Chan Attr. The Set Channel Attributes dialog box appears.

   d. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears, as shown in Figure 3-1 on page 3-4. (For a T1 channel, the Channel ID field appears in this dialog box instead of the IMA Group ID field. All other fields are identical.)

To define the logical port for an IMA group on the 3-Port Channelized DS3/1 IMA IOM:

a. Select Physical Port Attributes from the popup menu. The Set DS3 Physical Port Attributes dialog box appears.

b. Choose IMA groups. The Set IMA Group Attributes dialog box appears.

c. Select the name of the IMA group for which you want to define the logical port. The buttons of the T1 links belonging to that IMA group become highlighted.

d. Choose Logical Port. The Set All Logical Ports in PPort dialog box appears, as shown in Figure 3-1 on page 3-4. (For an IMA group, the IMA Group ID field appears in this dialog box instead of the Channel ID field. All other fields are identical.)

Note – See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for information about using the Set DS3 Physical Port Attributes dialog box, Set Channel Attributes dialog box, and Set IMA Group Attributes dialog box to configure physical port, channel, and IMA group attributes for the 3-Port Channelized DS3/1 IMA IOM.

To define the logical port for any other I/O module:

a. Select Logical Ports ⇒ All on Physical Port.

b. Review the fields in the Set All Logical Ports in PPort dialog box that appears (Figure 3-1 on page 3-4).

Note – If you are defining a logical port on an OC-48/STM-16 phy module attached to a GX 550 Multiservice WAN Base Input/Output 2 (BIO2) module, you can only access the Set All Logical Ports in PPort dialog box by choosing the Logical Port button on the Set SubPort Attributes dialog box. To access the Set SubPort Attributes dialog box, select a subport from the Subports section on the Set ATM OC-48/STM-16 Physical Port Attributes dialog box, and choose the Attributes button.

For more information about configuring OC-48/STM-16 subports, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

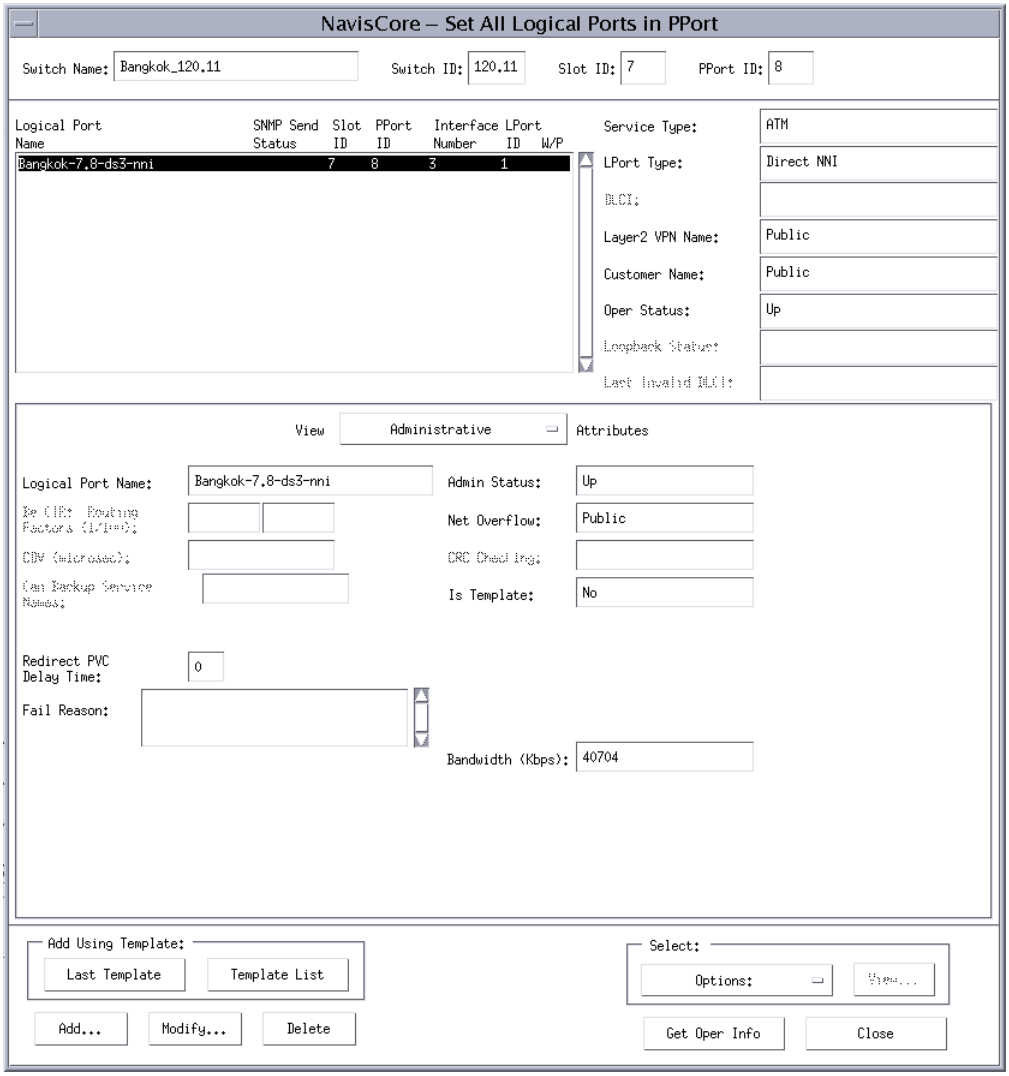


Figure 3-1. Set All Logical Ports in PPort Dialog Box

To learn more about the Set All Logical Ports in PPort fields dialog box, continue with the next section, "About the Set All Logical Ports in PPort Dialog Box." To begin defining a logical port, proceed to "Defining a Logical Port" on page 3-9.

About the Set All Logical Ports in PPort Dialog Box

The Set All Logical Ports in PPort dialog box displays information about existing logical ports and enables you to add a new logical port. It also provides several buttons that you can use to access additional logical port functions, such as add, modify, and delete.

Table 3-1 describes the required buttons on the Set All Logical Ports in PPort dialog box.

Table 3-1. Set All Logical Ports in PPort Dialog Box Buttons

Button	Action/Description
Last Template/ Template List	If you have already defined a logical port configuration and saved it as a template, use this option to define a new logical port using similar parameters. See "Using Templates" on page 2-21 for more information.
Add	Adds a new logical port.
Modify	Modifies the selected logical port. The Modify button displays dialog boxes that are similar to those displayed when you add a logical port; however, you cannot modify the logical port name and the logical port type.
Delete	Deletes the selected logical port. For more information on deleting ATM logical ports, see page 2-24.
Get Oper Info	Updates the logical port screen with current information from the switch and logical port.

Table 3-1. Set All Logical Ports in PPort Dialog Box Buttons (Continued)

Button	Action/Description
Select: Options	Use the Select: Options menu to view logical port options. Once you select an option from this list, choose View to access the information. The following fields describe the options you can select. *Statistics* – Displays the summary statistics for the selected logical port. *Diagnostics* – Accesses diagnostic tests for the selected logical port. *Layer2 VPN/Customer Info* – Accesses Layer2 VPN and customer name information for the logical port. See Chapter 11, "Configuring Layer2 VPNs," and Appendix H, "Customer Names," for more information. *QoS Parameters* – Displays the quality of service parameters (including bandwidth and routing metrics) for the selected logical port. See "Setting Quality of Service Parameters" on page 3-44 for more information. *NTM Parameters* (CBX 500 and GX 550 only) – Displays the network traffic management (NTM) parameters for the selected logical port. *NTM Statistics* (CBX 500 and GX 550 only) – Displays the NTM statistics for the selected logical port. *NDC Statistics* (CBX 500 and GX 550 only) – Displays the network data collection (NDC) statistics for the selected logical port. *IP Parameters* – Accesses the NavisCore IP logical port functions. See the *B-STDX and CBX IP Services Configuration Guide* for more information. *Accounting* (B-STDX and CBX 500 only) – Accesses the NavisXtend Accounting server logical port functions. For more information, see the *NavisXtend Accounting Server Administrator's Guide*. *Screen Assignments* – Displays the SVC port security screen assignments for the selected logical port. See Chapter 19, "Port Security Screening" for more information. *SVC QoS Parameters* – Displays the SVC quality of service parameters (including bandwidth) for the selected logical port. See "Setting SVC Quality of Service Parameters" on page 3-47 for more information.

Table 3-2 describes the required field on the Set All Logical Ports in PPort dialog box.

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

Field	Action/Description
Switch Name	Displays the name of the switch in which the I/O module resides.
Switch ID	Displays the switch number used as the host assignment in the switch's internal Internet Protocol (IP) address.
Slot ID	Displays the slot number in which the I/O module resides.
PPort ID	Displays the number of the physical port on which you want to add a logical port.
IMA Group ID *(3-Port Channelized DS3/1 IMA IOM only)*	Displays the ID number of the IMA group on which you want to define a logical port. ***Note:*** *This field appears only when you are defining a logical port for an IMA group. If you are defining a logical port for an individual DS1 (T1) channel, the Channel ID field appears instead.*
Channel ID *(3-Port Channelized DS3/1 IMA IOM only)*	Displays the number of the DS1 (T1) channel for which you want to define a logical port. ***Note:*** *This field appears only when you are defining a logical port for an individual DS1 (T1) channel. If you are defining a logical port for an IMA group, the IMA Group ID field appears instead.*
Logical Port Name	Displays a list of the configured logical ports on this physical port, channel, or IMA group. This field also lists the Simple Network Management Protocol (SNMP) and send status if an SNMP request failed. The reason for the failure is displayed in the Fail Reason field. For more information about possible failure reasons, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
Service Type	Displays ATM.
LPort Type	Displays the logical port type: UNI DCE, UNI DTE, CE, Direct Trunk, or OPTimum Trunk.
Layer2 VPN Name	Displays the Layer2 Virtual Private Network (VPN) name to which this logical port belongs. See Chapter 11, "Configuring Layer2 VPNs," for more information.
Customer Name	Displays the name of the customer to which this logical port is dedicated. (The default name is Public.)
Oper Status	Indicates whether this port is operationally Up, Down, or Unknown. Unknown indicates that the NMS is unable to contact the switch to retrieve status.

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

Field	Action/Description
Loopback Status	Indicates whether loopback testing is enabled on this logical port. The default is None (no testing).
Fail Reason	Displays the reason for the logical port failure if an SNMP request was not sent successfully. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information.
View Attributes (option menu)	Displays the appropriate attributes configured for the selected option. See one of the following sections for more information: • "Administrative Attributes" on page 3-14 • "ATM Attributes" on page 3-22 • "ILMI/Signaling/OAM Attributes" on page 3-28 • "ATM FCP Attributes" on page 3-36 • "Traffic Descriptors Attributes" on page 3-37 • "OPTimum Trunk VPI Range Attributes" on page 3-38 • "Selectable Statistics Attributes" on page 3-42 • "Configuring Logical Ports for Use With ATM SVCs" on page 3-50

Defining a Logical Port

Table 3-3 directs you to the process for defining logical ports. Before you begin to define logical ports, read "Selecting a Logical Port Type" on page 3-10 and "Administrative Attributes" on page 3-14.

Table 3-3. Defining a Logical Port

To Configure	Read
ATM CE	"ATM Attributes" on page 3-22
ATM UNI DCE ATM UNI DTE ATM NNI	"ATM Attributes" on page 3-22 "ILMI/Signaling/OAM Attributes" on page 3-28 "ATM FCP Attributes" on page 3-36 (*Optional*) "Configuring Logical Ports for Use With ATM SVCs" on page 3-50
ATM NNI (BICI only)	"ATM Attributes" on page 3-22 "ILMI/Signaling/OAM Attributes" on page 3-28
ATM Direct Trunk	"ATM Attributes" on page 3-22 "ILMI/Signaling/OAM Attributes" on page 3-28
ATM OPTimum Trunk	"Traffic Descriptors Attributes" on page 3-37 "OPTimum Trunk VPI Range Attributes" on page 3-38

Selecting a Logical Port Type

To select an ATM logical port type:

1. On the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4), choose Add to define a new logical port. The Add Logical Port type dialog box appears (Figure 3-2).

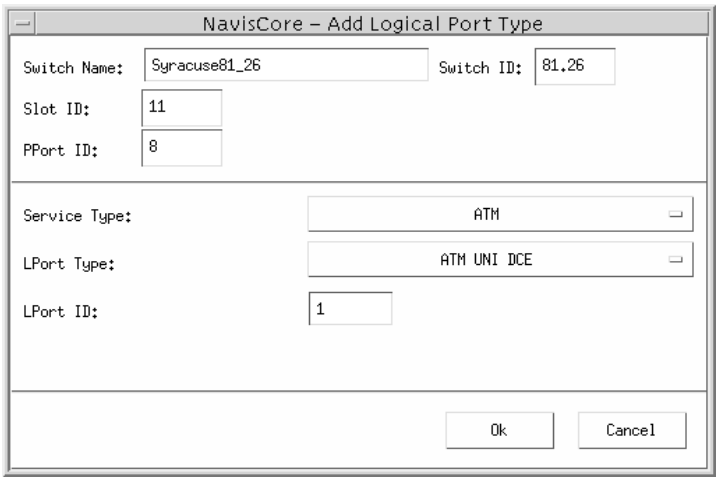


Figure 3-2. Add Logical Port Type Dialog Box

2. In the Service Type field, select *ATM* (if it is not already selected).
3. In the LPort Type field, select the ATM logical port type you want to configure.

   The available options in the LPort Type field differ depending on the supported ATM logical port types for your module. Possible options include:

   - ATM CE
   - ATM UNI DCE
   - ATM UNI DTE
   - ATM NNI
   - ATM OPTimum Trunk
   - ATM Direct Trunk

Note – If you are configuring a logical port on a 4CeDS3 physical port, the Service Type and LPort Type default to ATM circuit emulation (CE).

For instructions on configuring an ATM NNI logical port for use with the PNNI routing protocol, see Chapter 20.

4. Choose OK. The Add Logical Port dialog box appears (Figure 3-3).

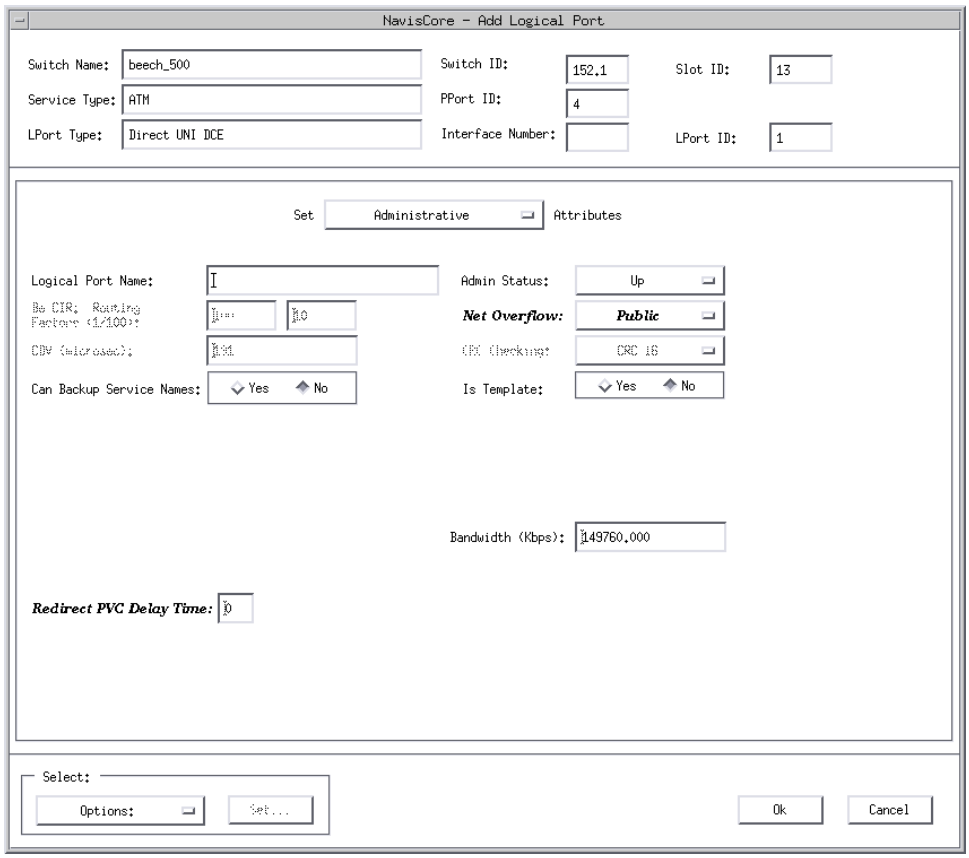


Figure 3-3. Add Logical Port Dialog Box

About the Set Attributes Menu

When you configure logical ports, the Add Logical Port dialog box (Figure 3-3) contains a variety of parameters that you must specify. During this procedure, use the Set Attributes menu on the Add Logical Port dialog box to configure the following parameters:

Administrative — Displays the Set Administrative Attributes fields, including Logical Port Name, Admin Status, and Bandwidth. See Table 3-4 on page 3-14 to set these attributes.

ATM — Displays the Set ATM Attributes fields, including the Number of Valid Bits in VCI, Number of Valid Bits in VPI, and ATM Protocol. You can also enable or disable the Call Admission Control (CAC) or usage parameter control (UPC) functions from this display. See Table 3-6 on page 3-22 to set these attributes.

ILMI/Signaling/OAM — Displays the Set ILMI/Signaling/OAM Attributes fields, which allow you to fine-tune your ATM service. See Table 3-7 on page 3-29 to set the following attributes:

ILMI – A Management Information Base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep-alive protocol. This selection also provides an option to configure the traffic characteristics for the ILMI control channel.

Signaling – A signaling protocol that supports the dynamic creation of ATM virtual circuits. To configure SVC signaling parameters, access the Set Logical Port Signaling Tuning Parameters dialog box (Figure 3-7 on page 3-33). This selection also provides an option to configure the traffic characteristics for the signaling control channel.

OAM – A parameter that enables the logical port to generate Operations, Administration, and Maintenance (OAM) alarms.

Proxy Signaling – Switched virtual circuit (SVC) proxy signaling is an *optional* CBX 500/GX 550 feature that enables a single signaling entity to signal on behalf of multiple endpoints. You can use proxy signaling to allow end systems that do not understand ATM signaling to set up SVCs via a proxy signaling agent (PSA). The PSA performs all signaling functions on behalf of the end system, known as the proxy signaling client (PSC). See Chapter 16, "Configuring SVC Proxy Signaling" for more information.

ATM FCP — Displays the Set ATM FCP Attributes fields, which allow you to configure logical ports for the CBX 500 ATM Flow Control Processor (FCP). See Chapter 5, "About the ATM Flow Control Processor (FCP)," to learn about the operation of the ATM FCP. See Chapter 6, "Working with the ATM Flow Control Processor (FCP)," for details about configuring the ATM FCP and for answers to frequently-asked questions. See Appendix D, "ATM Flow Control Processor Rate Profile Tables," for information about the ATM FCP rate profile tables.

Traffic Descriptors — Displays the Set Traffic Descriptors Attributes fields, which allow you to configure ATM traffic descriptors for the trunk logical ports. See page 3-37 to set these attributes.

OPTimum Trunk VPI Range — Displays the Set Opt Trunk VPI Range Attributes fields, which allow you to specify the range of VPIs that can be created over an OPTimum trunk. These options work in conjunction with IP's Label Switch Path (LSP), a feature that is used to switch IP traffic through a Lucent cloud using ATM VP switching. You also use this option to configure the OPTimum trunk to handle VPCs. See Table 3-9 on page 3-39 to set these attributes.

Selectable Statistics — Displays the Set Selectable Statistics Attributes fields, which allow you to enable/disable statistics collection from the logical port. This option is available with the NavisXtend Statistics Server. See Table 3-10 on page 3-42 to set these attributes.

SVC Connection ID Parameters — Displays the Set SVC Connection ID Parameters Attributes fields, which allow you to configure a separate SVC VPI/VCI address range contained within the PVC VPI/VCI address range. By creating two separate address ranges, you can use one VPI/VCI range for PVCs on a logical port and a different (smaller) VPI/VCI range for SVCs on the same logical port. This addressing scheme enables a CBX 500/GX 550 to interoperate with an SVC-capable CPE that only supports VPI 0 for SVCs. You can set the VPI/VCI range to limit SVCs to VPI 0, while allowing PVCs to utilize the full VPI range. See Table 3-14 on page 3-51 to set these attributes.

SVC Parameters — Displays the Set SVC Parameters Attributes fields, which allow you to define various SVC screening and handling parameters for each logical port on the switch. See "Defining SVC Parameters Attributes" on page 3-52 to set these attributes.

SVC Priorities — Displays the Set SVC Priorities Attributes fields, which allow you to assign bandwidth and bumping priority to SVCs based on the ingress QoS class. The network routes SVCs originating from this logical port according to the SVC ingress QoS class. See Table 3-22 on page 3-63 to set these attributes.

SVC TD Limits — Displays the Set SVC TD Limits Attributes fields, which allow you to set the CBR, VBR-RT, VBR-NRT, and ABR maximum traffic descriptor values for each service class. See Table 3-23 on page 3-65 to set these attributes.

ATM SVC Parameters — Displays the Set ATM SVC Parameters Attributes fields, which allow you to set the Ingress and Egress Address Translation Mode parameters. This option also enables you to configure the cell delay variation (CDV), minimum cell rate (MCR) value, and frame discard parameters. See Table 3-24 on page 3-70 to set these attributes.

Continue with the following sections to configure these attributes. To configure SVC attributes, see "Configuring Logical Ports for Use With ATM SVCs" on page 3-50.

Administrative Attributes

From the Add Logical Port dialog box (Figure 3-3 on page 3-11), select Set [Administrative] Attributes and complete the fields described in Table 3-4.

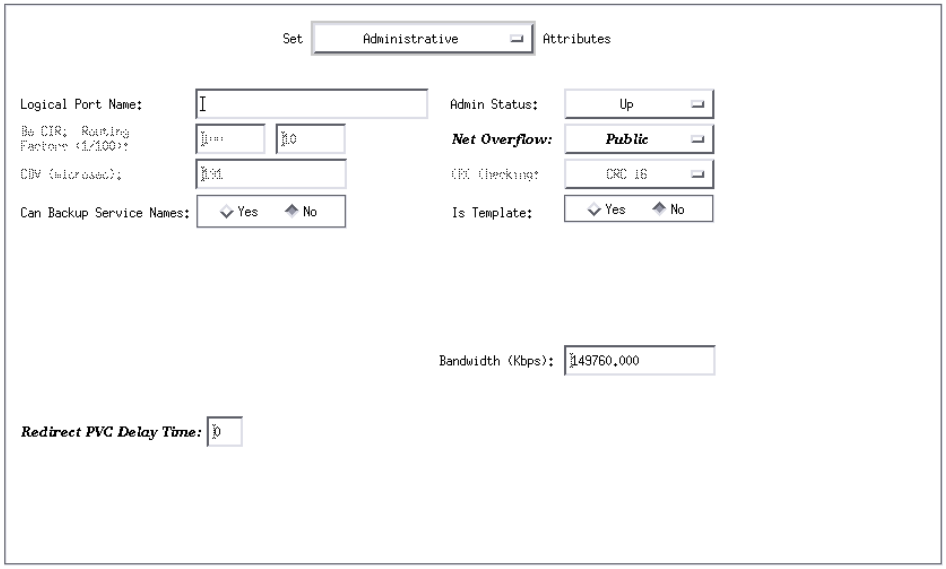


Figure 3-4. Administrative Attributes Fields

Table 3-4. Set Administrative Attributes Fields

Field	Logical Port	Action/Description
Logical Port Name	All	Enter a unique alphanumeric name for this port. NavisCore uses this name to reference the logical port.
Admin Status	All	Set the Admin Status as follows: *Up* – (default) Activates the port. *Down* – Saves the configuration in the database without activating the port, or takes the port offline to run diagnostics. When only one logical port exists on a physical port, and you set the admin status for the logical port to Down, the physical port is also considered down. If more than one logical port exists on a physical port, and you set the admin status for each of these logical ports to Down, the physical port is also considered down.

Table 3-4. Set Administrative Attributes Fields (Continued)

Field	Logical Port	Action/Description
Can Backup Service Names	UNI DCE/DTE	Select *Yes* to configure a logical port for backup service in a fault-tolerant PVC configuration. A fault-tolerant PVC configuration enables a logical port to serve as a backup for any number of active UNI ports. For more information about fault-tolerant PVCs, see Chapter 12, "Configuring Fault-Tolerant PVCs." ***Note**: Lucent recommends that you do not configure SVCs on a logical port that is also designated as a backup port in a fault-tolerant PVC configuration.*
Net Overflow	UNI DCE/DTE and NNI	Determines how SVC traffic originating from this logical port is managed during trunk overflow or failure conditions. This feature is used with Layer2 Virtual Private Networks (VPN). To assign this logical port to a specific Layer2 VPN and customer, see "Configuring a Logical Port for Layer2 VPN" on page 11-7. Select one of the following options: *Public* – (default) SVCs originating from this port are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – SVCs originating from this port can only use dedicated Layer2 VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures. ***Note:** Modifying the value for this attribute does not admin down the logical port.*
Is Template	All	*(Optional)* Saves these settings as a template to configure another logical port with similar options. To create a template, choose *Yes*. (*No* is the default value for this field.)

Table 3-4. Set Administrative Attributes Fields (Continued)

Field	Logical Port	Action/Description
Bandwidth (Kbps)	All	Enter the amount of bandwidth for this logical port. The default is the amount of bandwidth remaining from the physical clock rate less any logical ports already configured. • If you are defining more than one ATM UNI or NNI logical port type on this port (*Virtual UNI/NNI*), be sure to adjust the bandwidth value to accommodate these virtual ports. • If you are defining an OPTimum cell trunk on this port, configure this UNI logical port with a minimal amount of bandwidth. For specific guidelines on configuring bandwidth with the various physical port types, see page 2-17.
VP Shaping	*CBX 500* – Virtual UNI and OPTimum Trunk logical ports on I/O modules with FCP enabled *GX 550* – Virtual UNI, Virtual NNI, and OPTimum Trunk logical ports on BIO2 modules	Enables or disables VP shaping. VP shaping provides a method for traffic sent over a Lucent switch through another network to comply with the purchased traffic contract in that other network. This feature shapes individual cell trunk or virtual UNI/NNI logical port traffic at the configured VP shaping rate. For more information about the VP shaping feature on CBX 500 modules, see "About VP Shaping on the CBX 500" on page 2-19. For configuration instructions, see "Configuring VP Shaping on CBX 500 Virtual UNI Logical Ports" on page 3-19. For more information about the VP shaping feature on GX 550 modules, see "About VP Shaping on the GX 550" on page 2-20. ***Note:*** *Modifying the value for this attribute does not admin down the logical port.*

Table 3-4. Set Administrative Attributes Fields (Continued)

Field	Logical Port	Action/Description
VP Shaping Rate (cells per second)	*CBX 500* – Virtual UNI and OPTimum Trunk logical ports on I/O modules with FCP enabled *GX 550* – Virtual UNI, Virtual NNI, and OPTimum Trunk logical ports on BIO2 modules	If you enable VP shaping, enter a value between 100 and the *maximum logical port bandwidth* in cells per second. See Table 2-4 on page 2-16 for these values. **Notes:** *Due to hardware restrictions, you cannot dynamically modify (enable or disable) the configured VP Shaping mode for BIO2 virtual UNI logical ports on which circuits have been provisioned. The NMS will not allow changes to the VP Shaping field if circuits are provisioned on the logical port.* *To modify the VP Shaping mode for virtual GX 550 UNI logical ports on which circuits are provisioned, see "Modifying the VP Shaping Mode on GX 550 Virtual UNI Logical Ports" on page 3-21.* *When you enable VP shaping for a logical port on the GX 550 BIO2 module, the VP Shaping Rate field is read-only. The VP shaping rate is automatically calculated based on the Bandwidth entered in the Bandwidth (Kbps) field, described earlier in this table.*
CDV (microsec)	OPTimum trunk	Enter a cell delay variation (CDV) value (in µsecs) that will be added to the Lucent default trunk CDV. For constant bit rate (CBR) traffic, this default is 250 µsecs. For variable bit rate (VBR) traffic, the default value is 500 µsecs. The logical port CDV value is zero (0) by default. If you believe that the path through the network providing the OPTimum trunk connectivity will introduce additional cell delay variation (exceeding the value provided by the Lucent default), enter the appropriate value in this field.

Table 3-4. Set Administrative Attributes Fields (Continued)

Field	Logical Port	Action/Description
Redirect PVC Delay Time	UNI DCE/DTE and NNI	Enter a value between 0-255 seconds. This value represents the number of seconds to wait before the network initiates call clearing after a circuit goes down. The default value is zero. You configure this value only for the primary endpoint and you can reset it at any time. A value of 0 causes the network to initiate call clearing immediately, which can trigger the switch over between a working redirect PVC endpoint and its primary or secondary endpoint. Increasing the value can minimize the PVC redirection as a result of temporary data terminal equipment (DTE) state changes. For more information about redirect PVCs, see Chapter 8. ***Note:*** *Modifying the value for this attribute does not admin down the logical port.*

See Table 3-5 to continue this configuration. If you are configuring an ATM CE logical port, choose OK from the Set Administrative Attributes dialog box (Figure 3-3 on page 3-11) and continue with Chapter 8 to define the PVC connection.

Table 3-5. Configuring CBX and GX Logical Ports

Logical Port Type	See
UNI or NNI	"ATM Attributes" on page 3-22.
Direct Trunk	"ATM Attributes" on page 3-22 (direct trunk logical port on GX 550 only) and "Traffic Descriptors Attributes" on page 3-37.
OPTimum Trunk	"Traffic Descriptors Attributes" on page 3-37 and "OPTimum Trunk VPI Range Attributes" on page 3-38.

Note – This release supports the ATM Forum UNI 4.0 Signaling Standard. For more information, see "ATM UNI 4.0 Support" on page 2-3.

Configuring VP Shaping on CBX 500 Virtual UNI Logical Ports

This section describes how to configure the VP shaping feature on virtual ATM UNI logical ports on the CBX 500 switch. For more information, see "About VP Shaping on the CBX 500" on page 2-19.

Before You Begin

Before you configure VP shaping on a virtual ATM UNI logical port, verify that you have completed the following tasks:

- Enabled the ATM Flow Control Processor (FCP) on a supported CBX 500 module. See "Enabling the FCP" on page 6-2 for more information on configuring the FCP attributes on an IOM.
- Configured an ATM UNI DCE or NNI logical port with a minimum amount of bandwidth; this logical port acts as the feeder port. When used as a feeder port, you can still use the ATM UNI CE or NNI logical port for PVC and SVC applications, providing enough bandwidth has been assigned to the feeder port.

Virtual ATM UNI Logical Port Configuration Considerations

To configure a virtual ATM UNI logical port, see "Configuring Virtual ATM UNI/NNI Logical Ports" on page 3-49. In addition, be aware of the special considerations described in the following sections.

Configuring the Virtual Path Identifier

The Virtual Path Identifier (VPI) is the identifier used for all VCC circuits routed over the Virtual UNI. The range of valid VPI values depends upon the number of valid VPI bits you set for the ATM UNI feeder port. (see Table 2-2 on page 2-13). Enter a number from 0-*nnnn* to identify the virtual path for the ATM logical port; *nnnn* is equal to 2^{P}-1, where *P* is the value specified in the Valid Bits in VPI field for the UNI feeder port that shares this physical port (see the example on page 2-12).

For example, if you entered 4 in the Valid Bits in VPI field for the UNI feeder port, you can have up to 15 virtual paths on this port (2^{4}-1=15); if you entered 8 in the Valid Bits in VPI field, you can have up to 255 virtual paths on this port (2^{8}-1=255). The highest value you can enter (and therefore, the greatest number of virtual paths you can configure on the port) depends on the value you entered in the Valid Bits in VPI field for the ATM UNI feeder port. The virtual UNI's VPI must be unique to the port.

Configuring VCC VPI Start and Stop Values for Virtual UNI

The CBX 500 and GX 550 switches provide a virtual UNI feature. The direct UNI provides the range of VCC VPI start and stop values (see "Configuring the Virtual Path Identifier" on page 3-19). The range of VPI start and stop values you define for the first virtual UNI must fall within this range; it cannot overlap with the range you define for subsequent virtual UNI ports.

For example:

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

The switch handles SVCs differently, depending on how you configure the Connection Type field of the virtual UNI (see Table 3-6 on page 3-22). If the logical port is set to the Network <-> Network Connection Type, it implies a network scenario as shown in Figure 2-1 on page 2-10. In this case, the first VPI is used for VCCs only. Additional VPIs can only be used for signaled VPCs with the best effort QoS. If the logical port is set to the Network <=> Endsystem Connection Type, it implies a network scenario as shown in Figure 2-2 on page 2-10. In this case, all available VPIs can be used for either signaled VCCs or VPCs of any QoS class.

The restrictions described above only apply to SVCs. When using virtual UNIs in conjunction with PVCs, there are no restrictions and the Connection Type field on the logical port is not used.

Enabling the VP Shaping Option

When you set Administrative Attributes for the virtual UNI logical port, verify that the VP Shaping option is enabled (see page 3-16). For additional information on VP shaping rates used by the FCP, see "Shaping Rates" on page 5-20.

Modifying the VP Shaping Mode on GX 550 Virtual UNI Logical Ports

Due to hardware restrictions, you *cannot* dynamically modify (either enable or disable) the configured VP Shaping mode for GX 550 BIO2C virtual UNI logical ports on which circuits are already provisioned. To reset the VP Shaping mode for virtual UNI logical ports:

1. Follow the steps described in "Deleting Circuits" on page 2-24 to delete all circuits provisioned on the virtual UNI logical port.
2. Follow the steps described in "Defining a Logical Port" on page 3-9 to access the VP Shaping field in the Set Administrative Attributes menu for the virtual UNI logical port. Modify the configured VP Shaping mode as needed by enabling or disabling the option.
3. Re-create the previously configured circuits.

ATM Attributes

The Set ATM Attributes menu is available for UNI and NNI logical port types, as well as for ATM Direct Trunk logical ports residing on the GX 550.

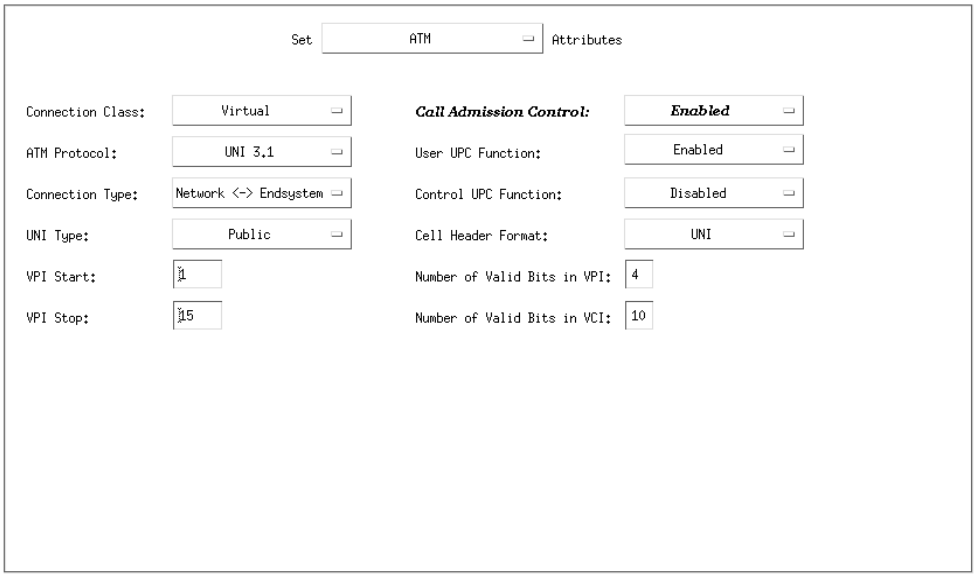


Figure 3-5. Set ATM Attributes Fields (UNI Logical Ports)

Note – For the ATM Direct Trunk logical port type, the Number of Valid Bits in VCI field is the only field you need to configure.

Select Set [ATM] Attributes and complete the fields described in Table 3-6.

Table 3-6. Set ATM Attributes Fields

Field	Logical Port	Action/Description
Connection Class	UNI DCE/DTE, or NNI	Displays the logical port connection type, either direct or virtual. This field is set to Direct when you configure the first UNI/NNI logical port on this physical port. When you configure subsequent UNI/NNI ports on this physical port, this field displays Virtual. For Trunk logical port types, this field defaults to Direct and cannot be changed.

Table 3-6. Set ATM Attributes Fields (Continued)

Field	Logical Port	Action/Description
ATM Protocol	UNI DCE/DTE and NNI	The equipment to which you connect this port must support the protocol you select. Lucent logical ports support the following protocols: UNI 4.0 UNI 3.1 UNI 3.0 IISP 3.1 IISP 3.0 ITU UNI BICI 1.1 (*NNI only*) PNNI 1.0 (*NNI only*) The default Signaling Tuning parameters are based on the ATM Protocol you select. If you change the Signaling Tuning parameters for this port and later change the UNI version, the default Signaling Tuning parameters for the ATM Protocol you selected will overwrite these changes. For more information on Signaling Tuning parameters, see page 3-33.
Connection Type	UNI DCE	This option lets the switch know whether or not to send a configured node prefix over the ILMI channel to the attached device. This setting has no effect if ILMI is not enabled, or ILMI is enabled but you will not use ILMI address registration. Use one of the following options: • Select Network <–> Endsystem if this port connects to a CPE device and you want a compliant configured node prefix sent over the ILMI channel to the device for ILMI address registration. • Select Network <–> Network if this port connects to another network switch and you do not want the node prefix sent over the ILMI channel to the attached device.
UNI Type	UNI DCE/DTE	Select *Public* if at least one end of this connection attaches to a public network. Select *Private* if this connection resides completely within a private network.
VPI Start	Virtual UNI/ NNI	For a virtual UNI/NNI logical port, this field represents the virtual channel connection (VCC) VPI of the control channels (that is, signaling and ILMI). For more information on VPI Start and Stop values, see page 2-15.

Table 3-6. Set ATM Attributes Fields (Continued)

Field	Logical Port	Action/Description
VPI Stop	Virtual UNI	To configure this value, use the following formula: `VCC VPI Stop <= (2 numvpibits - 1)` where "numvpibits" equals the value you configure for the Number of Valid Bits in VPI field (page 3-27). ***Note**: This value does not apply to Virtual NNI logical ports. You can assign one VCC VPI value for Virtual NNI logical ports (not a range).*
Call Admission Control	UNI DCE/DTE and NNI	When enabled (default), the port rejects a circuit creation request if there is not enough available bandwidth. When disabled, the port attempts to create a circuit even if there is not enough available bandwidth (for VBR Non-Real Time queue only). ***Notes:** If you disable Call Admission Control for a logical port, you are effectively disabling Lucent's Call Master Connection Admission Control (CAC) function on that logical port. For more information about the CAC function, see Appendix A.* *Modifying the value of this attribute does not admin down the logical port.*
User UPC Function	UNI DCE/DTE	Enables or disables the usage parameter control (UPC) function for PVCs and SVCs. You can also enable or disable the UPC function for individual PVCs. If you want to use the UPC function on a per-PVC basis, you must enable the UPC function on the logical port. *Enabled* – (default) Enables the UPC function for circuits on this logical port for all QoS classes, except ABR. Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – All traffic, including non-conforming traffic, passes in through the port. If you disable the UPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. For this reason, *Lucent recommends that you leave the UPC function enabled on all logical ports*. *Enabled with ABR* – Enables the UPC function for circuits on this logical port for all QoS classes, including ABR. For information on UPC traffic parameters, see Chapter 10, "Configuring ATM Traffic Descriptors."

Table 3-6. Set ATM Attributes Fields (Continued)

Field	Logical Port	Action/Description
Control UPC Function	UNI DCE/DTE	Enables or disables policing on a user port for control circuits (signaling and ILMI) independent of user traffic. The default is disabled. Enable policing to prevent an attached device from overloading the switch with data on the control circuit. The switch polices the control circuit to pre-defined default traffic characteristics (see Chapter 10). The attached device typically needs to support per-VC shaping on the control channels. ***Note**: If the attached device is another Lucent switch, do not enable policing since the CBX 500 and GX 550 do not support per-VC shaping on the control channels.*
User NPC Function	NNI	Enables or disables the Network Parameter Control (NPC) function for user circuits. You can also enable or disable the NPC function for individual PVCs. If you want to use the NPC function on a per-PVC basis, you must enable the NPC function on the logical port. *Enabled* – Enables the NPC function for circuits on this logical port for all QoS classes, except ABR. Cells that do not conform to the traffic parameters are dropped or tagged as they come into the port. *Disabled* – (default) All traffic, including non-conforming traffic, passes in through the port. If you disable the NPC function on a logical port, quality of service is no longer guaranteed on the network due to the potential for increasing the cell loss ratio on network circuits. With NPC disabled, Lucent recommends *that all ATM UNI ports have UPC enabled*. Traffic entering the network should have traffic shaping performed. *Enabled with ABR* – Enables the NPC function for circuits on this logical port for all QoS classes, including ABR. For information on NPC traffic parameters, see Chapter 10, "Configuring ATM Traffic Descriptors."

Table 3-6. Set ATM Attributes Fields (Continued)

Field	Logical Port	Action/Description
Control NPC Function	NNI	Enables or disables policing on a user port for control circuits (signaling and ILMI) independent of user traffic. The default is disabled. Enable policing to prevent an attached device from overloading the switch with data on the control circuit. The switch polices the control circuit to pre-defined default traffic characteristics (see Chapter 10). The attached device typically needs to support per-VC shaping on the control channels. ***Note**: If the attached device is another Lucent switch, do not enable policing since the CBX 500 and GX 550 do not support per-VC shaping on the control channels.*
Cell Header Format	All	This field controls the number of VPI bits in the ATM cell header for VPCs on the CBX 500 and VCCs and VPCs on the GX 550. Select UNI to use a range of 0 through 8. Select NNI to use valid bits in a VPI range of 0 through 12. See page 2-11 for more information.
Number of Valid Bits in VPI	UNI DCE/DTE and NNI	Specify a value that is within the valid range for either the NNI or UNI call header format. The default is 4. See page 2-11 for details. ***Note:** If you are using the 3-Port Channelized DS3/1 IMA IOM configured in UNI mode, the default value for Number of Valid Bits in VPI is 8, based on an SVC Connection ID Range of 0 (zero) to 255. When the 3-Port Channelized DS3/1 IMA IOM is configured in IMA mode, the standard ATM default value is used.*

Table 3-6. Set ATM Attributes Fields (Continued)

Field	Logical Port	Action/Description
Number of Valid Bits in VCI	UNI DCE/DTE and NNI	Specify a value that is compatible with the desired VCI range on the port. The default is 10. See page 2-11 for details. ***Note:*** *If you are using the 3-Port Channelized DS3/1 IMA IOM configured in UNI mode, the default value for Number of Valid Bits in VCI is 6, based on an SVC Connection ID Range of 0 (zero) to 255. When the 3-Port Channelized DS3/1 IMA IOM is configured in IMA mode, the standard ATM default value is used.*
	GX 550 Direct Trunk only	This field affects the amount of connection entry resource that is reserved for VCs that traverse this trunk endpoint. The default value of 10 translates into a value of 2^10 or a minimum of 1024 connection entries being reserved for VCs on the trunk. The default value of 10 is the most efficient usage of the connection entry resource for OC3 ports. A value of 12 is the most efficient usage of the connection entry resource for OC-12c/STM-4 and OC-48/STM-16 ports.

When you finish configuring the Set ATM Attributes fields, proceed to the next section, "ILMI/Signaling/OAM Attributes."

ILMI/Signaling/OAM Attributes

The Set ILMI/Signaling/OAM attributes selection menu is only available for ATM UNI and ATM NNI logical port types. ATM UNI and PNNI 1.0 (NNI) logical ports support ILMI, Signaling, OAM, and Proxy; NNI logical ports configured for Broadband Inter-Carrier Interface (BICI) 1.1 support OAM and Proxy Signaling, only; ATM UNI logical ports configured for Fast APS support ILMI and OAM, only.

For more information about ILMI and Signaling, see page 2-4. The fields on this dialog box also enable you to configure *optional* proxy signaling features for a UNI logical port. See Chapter 16, "Configuring SVC Proxy Signaling," for instructions on using proxy signaling.

Select Set [ILMI/Signaling/OAM] Attributes and complete the fields described in Table 3-7 on page 3-29.

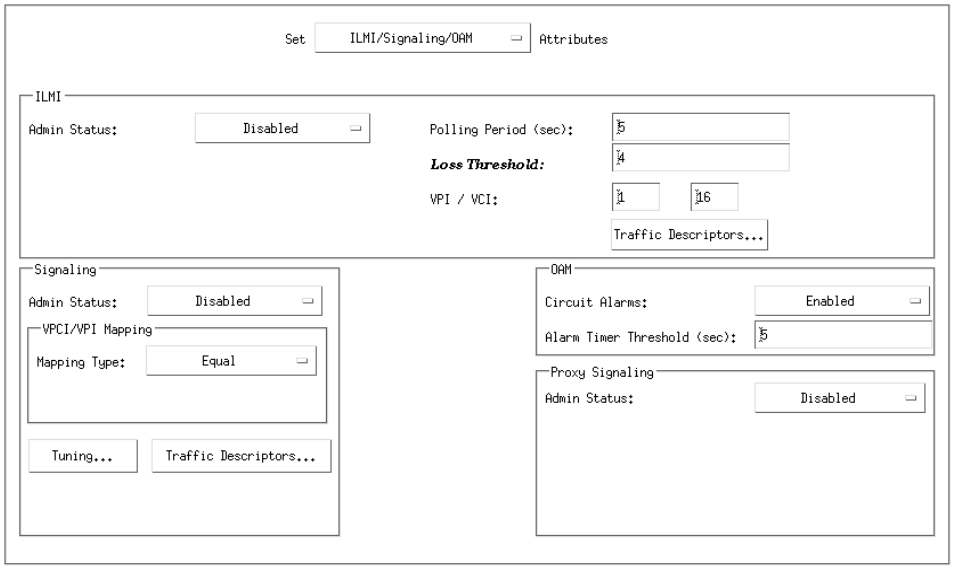


Figure 3-6. Set ILMI/Signaling/OAM Attributes Fields (UNI LPorts)

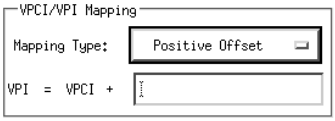
Table 3-7. Set ILMI/Signaling/OAM Attributes Fields

Field	Action/Description
ILMI Attributes ***(UNI DCE/DTE logical ports only)***	
Admin Status	Choose *Enabled* to reserve a percentage of bandwidth in the VBR-NRT QoS class for ILMI. You can override the bandwidth and QoS class default values by choosing the Traffic Descriptors button and assigning traffic descriptors for the ILMI channel. When ILMI is *Disabled* (default), this bandwidth is not reserved. If the attached device cannot run ILMI, leave ILMI disabled. To receive ILMI virtual channel connection (VCC) status traps from non-Lucent ATM UNI 3.1 devices, you must enable ILMI Admin Status. For information about ILMI support, see "Using Interim Link Management Interface (ILMI)" on page 2-4. ***Note:*** *If you are using line loopback diagnostics, you must disable ILMI support. See the* B-STDX, CBX, and GX Switch Diagnostics User's Guide *for more information.*
Traffic Descriptors	Choose this field to access the Set ILMI Traffic Descriptors dialog box. This option enables you to modify the traffic characteristics for the control channel. This feature is known as *configurable control channel.* See "Defining Traffic Descriptor Attributes" on page 10-12 to complete the fields on this dialog box.
Polling Period (sec)	Specify the polling period (T) for an ILMI poll. The switch generates an ILMI poll every (T) seconds. The default is 5 seconds.
Loss Threshold	Specify the number of times (K) the logical port will issue an ILMI poll before the link is considered down. If no responses are seen in K x T seconds, the link is considered down. The default is 4. ***Note:*** *Modifying the value of this attribute does not admin down the logical port.*
VPI/VCI	Enter the ID of the virtual path identifier (VPI) or virtual channel identifier (VCI) you want to use for ILMI polling. The default is zero for VPI, 16 for VCI.

Table 3-7. Set ILMI/Signaling/OAM Attributes Fields (Continued)

Field	Action/Description
DTE Prefix Screen Mode (DTE ports)	When a DTE port receives network prefixes from an external network, you can perform various levels of screening on them against the list of prefixes configured on the node and/or port. Select one of the following options: *Accept All* – No screening occurs; accepts all prefixes. *Node Prefix* – (default) Accepts only network prefixes that partially or fully match a configured node prefix. *Port Prefix* – Accepts only network prefixes that partially or fully match a configured port prefix. *Node or Port Prefix* – Accepts only network prefixes that partially or fully match either a configured node prefix or a configured port prefix. *Reject All* – Rejects all network prefixes received from an external network. For more information about node and port prefixes, see Chapter 14, "About SVCs." ***Note:*** *Modifying the value of this attribute does not admin down the logical port.*
Signaling Attributes *(UNI DCE/DTE logical ports only)*	
Admin Status	Choose *Enabled* to reserve a percentage of bandwidth in the VBR-NRT QoS class to support the UNI signaling protocol. You can override default values for bandwidth and QoS class by choosing the Traffic Descriptors button to assign traffic descriptors for the signaling channel. Use the default setting (Disabled) if you will only use this logical port for PVCs (that is, you will not create SVCs on the port). When signaling is *Disabled* (default), this bandwidth is not reserved. If the attached device cannot run signaling, leave signaling disabled. For information about ILMI support, see page 2-5. ***Note:*** *To use line loopback diagnostics, you must disable signaling support. See the* B-STDX, CBX, and GX Switch Diagnostics User's Guide *for more information.*

Table 3-7. Set ILMI/Signaling/OAM Attributes Fields (Continued)

Field	Action/Description
Mapping Type (*Virtual UNI/NNI only*)	Use this button to configure the virtual path connection identifier (VPCI). See Chapter 16 for more information on VPCI mapping. *Equal* – (default) The VPI equals the VPCI. *Positive Offset* – The VPI of the corresponding circuit equals the VPCI plus the value you enter.  *Negative Offset* – The VPI of the corresponding circuit equals the VPCI minus the value you enter. *Table* – This option has additional functions that are used with Proxy Signaling. For information on configuring them, see Chapter 16.
Traffic Descriptors	Choose this field to access the Set Logical Port Signaling Traffic Descriptors dialog box. This option enables you to modify the traffic characteristics for the control channel. This feature is known as *configurable control channel.* See "Traffic Descriptors Attributes" on page 3-37 to complete the fields on this dialog box.
Tuning	Choose the Tuning field to display the Set Logical Port Signaling Tuning Parameters dialog box. For information about Tuning parameters, see "Setting Logical Port Signaling Tuning Parameters" on page 3-33.
OAM Attributes	
Circuit Alarms	Select *Enabled* (default) to allow this logical port to generate OAM alarms. The switch uses these alarms to signal when the circuits have gone down. Select *Disabled* to disable OAM alarms on this logical port.
Alarm Timer Threshold (sec)	Before generating an OAM alarm, the switch waits until the circuit has been down for the time period you specify in this field. The default is 5 seconds.
Proxy Signaling	
Admin Status	Specifies the proxy signaling administrative status if you want to use this optional feature for a UNI logical port. Proxy signaling allows end systems that do not understand ATM signaling to set up SVCs via a proxy signaling agent (PSA). The PSA performs all signaling functions on behalf of the end system, known as the proxy signaling client (PSC). Choose Disabled, Agent, or Client. For instructions on using proxy signaling, see Chapter 16, "Configuring SVC Proxy Signaling."

When you finish configuring the ILMI, Signaling, and OAM attributes for this logical port, do one of the following:

- If the logical port you are configuring supports *optional* ATM Flow Control Processor (FCP) functions, continue with "ATM FCP Attributes" on page 3-36.
- If this is a UNI or PNNI 1.0 (NNI) logical port and you plan to use ATM SVCs in your network, continue with "Configuring Logical Ports for Use With ATM SVCs" on page 3-50. Otherwise, continue with "Completing the Logical Port Configuration" on page 3-43.
- If this is a BICI 1.1 (NNI) logical port, proceed to "Completing the Logical Port Configuration" on page 3-43.

Setting Logical Port Signaling Tuning Parameters

This section describes how to modify the signaling parameters for an ATM UNI logical port. For more information on signaling, see page 2-5.

To modify the signaling tuning parameters:

1. From the Set ILMI/Signaling/OAM Attributes menu (Figure 3-6 on page 3-28), choose the Tuning button in the Signaling field. The Set Logical Port Signaling Tuning dialog box appears (Figure 3-7).

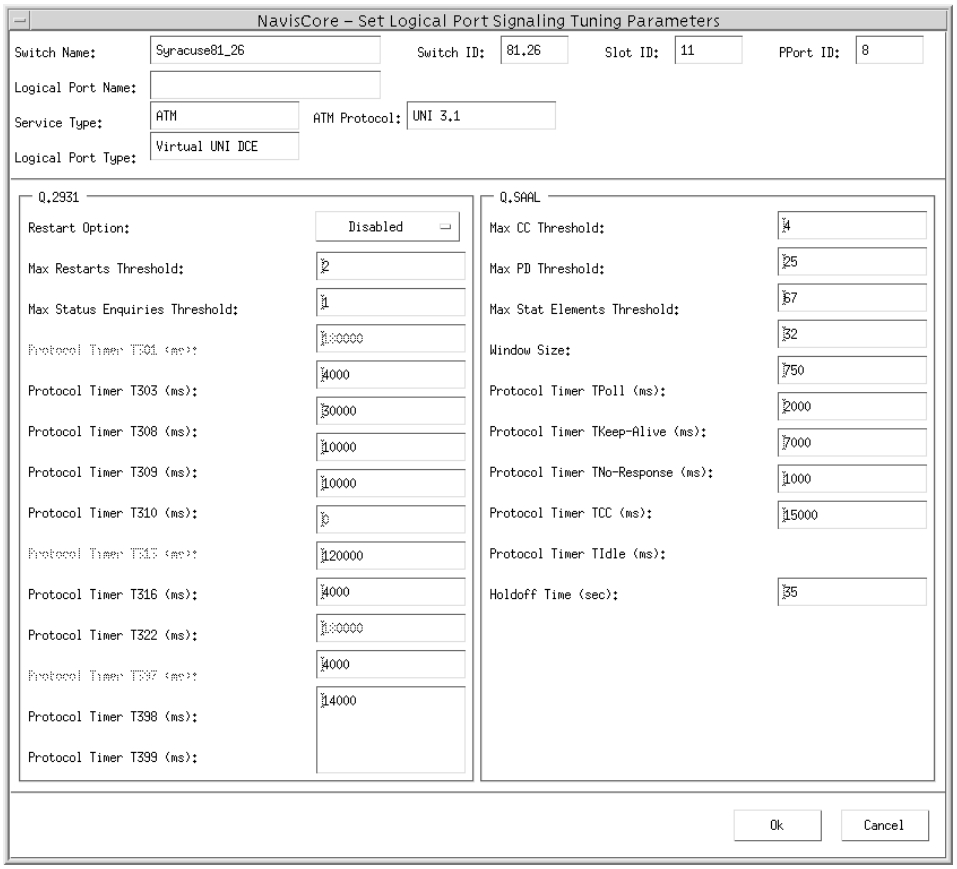


Figure 3-7. Set Logical Port Signaling Tuning Parameters Dialog Box

Use the Set Logical Port Signaling Tuning Parameters dialog box to set the Q.2931 thresholds and timers, and the Q.SAAL protocol data unit (PDU) thresholds and timers. In general, you should not change the default values. The displayed defaults are based on the ATM protocol you selected for the logical port (see page 3-23).

2. Complete the fields in Table 3-8. All timer field values are specified in milliseconds (1/1000 of a second).

Table 3-8. Set Logical Port Signaling Tuning Parameters Fields

Field	Action/Description
Q.2931	
Restart Option	Select either *Enabled* or *Disabled* (default). Enabling this option sends a restart message whenever Q.SAAL is connected and there are no active calls on a link.
Max Restarts Threshold	The maximum number of restarts to send without a response. The default is 2.
Max Status Enquiries Threshold	The maximum number of status enquiries that can be unacknowledged before the SVC is dropped. The default is 1.
Protocol Timer T301 (ms)	How long to wait for a CONNECT after ALERTING has been received. The default is 180000 msec. (UNI 4.0, Q.2931/Q.2971 protocol only.)
Protocol Timer T303 (ms)	How long to wait for a response after a SETUP protocol data unit (PDU) has been sent. The default is 4000 msec.
Protocol Timer T308 (ms)	How long to wait for a response after a RELEASE PDU has been sent. The default is 30000 msec.
Protocol Timer T309 (ms)	If Q.SAAL is down, how long to wait before SVCs are dropped. The default is 10000 msec for the UNI 3.1 ATM protocol and 90000 msec for UNI 3.0.
Protocol Timer T310 (ms)	How long to wait for the next response after a CALL PROCEEDING PDU has been received. The default is 10000 msec.
Protocol Timer T313 (ms)	How long to wait for a response after a CONNECT PDU has been sent. This function defaults to 4000 msec for DTE logical ports; it is disabled for DCE logical ports.
Protocol Timer T316 (ms)	How long to wait for a response after a RESTART PDU has been sent. The default is 120000 msec.
Protocol Timer T322 (ms)	How long to wait for a response after a STAT ENQUIRY PDU has been sent. The default is 4000 msec.
Protocol Timer T397 (ms)	How long to wait for an ADD PTY ACK after PTY ALERTING has been received. The default is 180000 msec. (UNI 4.0, Q.2931/Q.2971 protocol only.)

Table 3-8. Set Logical Port Signaling Tuning Parameters Fields (Continued)

Field	Action/Description
Protocol Timer T398 (ms)	How long to wait for a response after a DROP PTY PDU has been sent. The default is 4000 msec.
Protocol Timer T399 (ms)	How long to wait for a response after an ADD PTY PDU has been sent. The default is 14000 msec.
Q.SAAL	
Max CC Threshold	The maximum number of transaction retries for control PDUs. The default is 4.
Max PD Threshold	The maximum number of data PDUs without a POLL. The default is 25.
Max Stat Elements Threshold	The maximum number of missing elements in a STATUS PDU. The default is 67.
Window Size	The maximum number of unacknowledged PDUs that can exist at any time. The default is 32. If you decrease this value, peer signaling slows down.
Protocol Timer TPoll (ms)	How often a poll is sent when the Q.SAAL is active. The default is 100 msec if this port uses the UNI 3.0 or IISP 3.0 ATM protocol; the default is 750 msec for all others.
Protocol Timer TKeep-Alive (ms)	How often a poll is sent when the Q.SAAL is in the transient state. The default is 2000 msec.
Protocol Timer TNoResponse (ms)	The maximum amount of time that can pass without a STATUS PDU being received. The default is 7000 msec.
Protocol Timer TCC (ms)	The retry time for control PDUs. The default is 1000 msec.
Protocol Timer TIdle (ms)	How often a poll is sent when Q.SAAL is idle. This parameter does not apply to UNI 3.0 connections. The default is 15000 msec.

Table 3-8. Set Logical Port Signaling Tuning Parameters Fields (Continued)

Field	Action/Description
Holdoff Time (sec)	The ATM signaling holdoff timer holds off the re-establishment of the ATM signaling connection after you modify a physical or logical port or after a physical port alarm is detected. This mechanism essentially converts SAAL reset conditions into SAAL failure conditions (also described in Q.2931). The default is 35 seconds. ***Note:*** *For PNNI logical port types, the default value for Holdoff Time is zero seconds. Configuring a value higher than 0 may result in an extra delay of 30 seconds in establishing logical group node (LGN) switched virtual channel connections (SVCCs) between neighboring LGNs.*

3. When you finish, choose OK to return to the Add Logical Port dialog box (Figure 3-3 on page 3-11).
4. Continue with page 3-31 to configure the remaining OAM attributes.

ATM FCP Attributes

Cascade Communications Resource Management (CCRM) cells are a subset of the ATM Forum's *ATM Traffic Management, Version 4.0*, available bit rate (ABR) resource management (RM) cells. The backward congestion message (BCM) cells provide interoperability with other manufacturers' ATM switches.

Note – Contact a qualified Lucent organization for network design validation before enabling the FCP.

For information about basic concepts, configuration procedures, and frequently-asked questions for the ATM FCP, see the following chapters in this guide:

- Chapter 5, "About the ATM Flow Control Processor (FCP)," describes the operation of the ATM FCP.
- Chapter 6, "Working with the ATM Flow Control Processor (FCP)," provides detailed configuration procedures and answers to frequently-asked questions about using the ATM FCP.
- Appendix D, "ATM Flow Control Processor Rate Profile Tables," describes the organization and default values for the ATM FCP rate profile tables.

If this is a UNI logical port, continue with "Configuring Logical Ports for Use With ATM SVCs" on page 3-50. If this is an NNI logical port, proceed to "Completing the Logical Port Configuration" on page 3-43.

Traffic Descriptors Attributes

The Set Traffic Descriptors Attributes menu is only available for ATM Direct and OPTimum Trunk logical port types. The fields in this menu selection enable you to modify the traffic characteristics for the configurable control channel. These traffic descriptors are used for bandwidth allocation, not for policing.

Select Set [Traffic Descriptors] Attributes to configure node and card traffic descriptors.

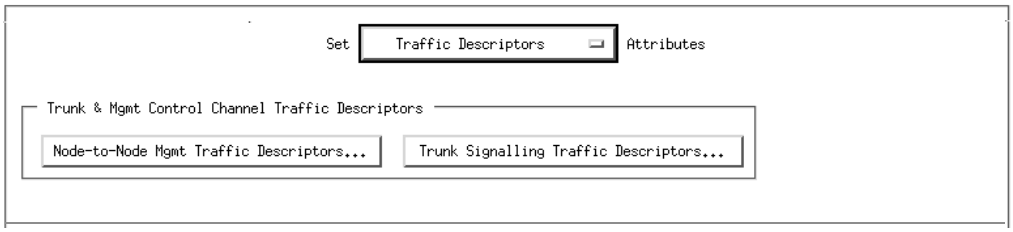


Figure 3-8. Set Traffic Descriptors Attributes Fields

1. Choose Node-to-Node Mgmt Traffic Descriptors. The Set Logical Port Node-to-Node Management Traffic Descriptor dialog box appears. (See Figure 10-3 on page 10-12 for an example.)
2. See "Defining Traffic Descriptor Attributes" on page 10-12 to complete the fields on this dialog box.
3. Choose OK to return to the Add Logical Port dialog box.
4. Choose Trunk Signaling Traffic Descriptors.
5. Repeat step 2 and step 3 to configure trunk signaling traffic descriptors.

Note – If there are currently *no* traffic descriptors configured, the Add Traffic Descriptor dialog box (Figure 10-2 on page 10-10) appears when you choose Node-to-Node Mgmt Traffic Descriptors or Trunk Signaling Traffic Descriptors. To use the Add Traffic Descriptors dialog box to define a new traffic descriptor, see "Defining Network-wide Traffic Descriptors" on page 10-9.

To complete this trunk logical port configuration, do one of the following:

- If this is an OPTimum Trunk logical port, continue with the next section, "OPTimum Trunk VPI Range Attributes."
- If this is a Direct Trunk logical port, proceed to "Completing the Logical Port Configuration" on page 3-43.

OPTimum Trunk VPI Range Attributes

Select Set [Opt Trunk VPI Range] Attributes and complete the fields described in Table 3-9.

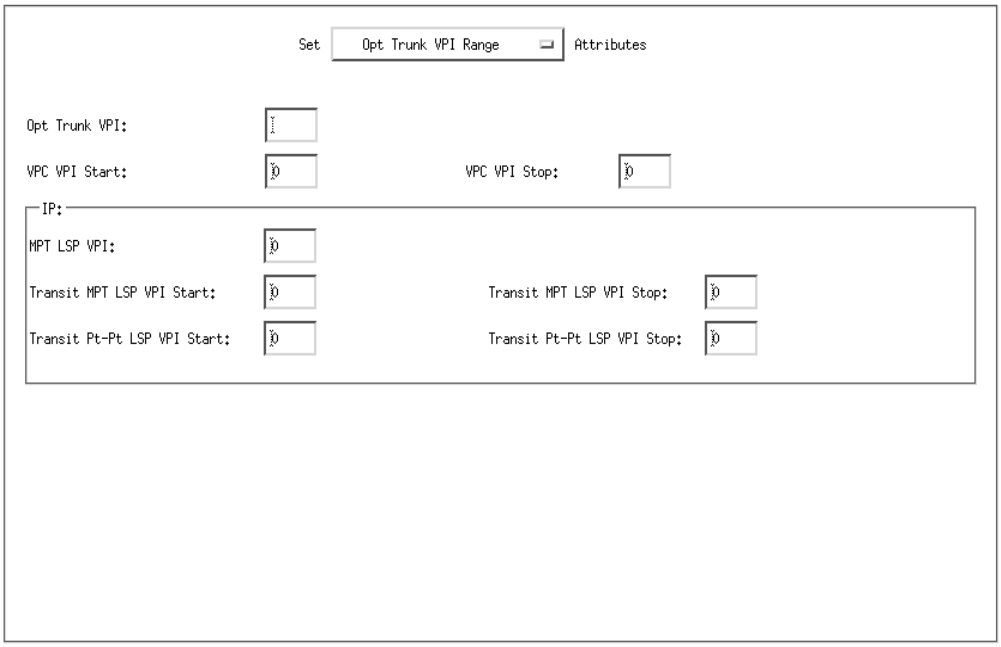


Figure 3-9. Set Opt Trunk VPI Range Attributes Fields

Note – Several of the OPTimum Trunk VPI Range attributes in Table 3-9 relate to the values you specify for transit multipoint-to-point label switched path (MPT LSP) connections and transit point-to-point label switched path (point-to-point LSP) connections. For details about configuring LSPs, see the *B-STDX and CBX IP Services Configuration Guide*.

Table 3-9. Set OPT Trunk VPI Range Attributes Fields

Field	Action/Description
Opt Trunk VPI *(OPTimum cell trunk logical port endpoints on CBX 500 switches only)*	Specify the virtual path identifier (VPI) value for the default virtual channel connection (VCC), which is used for network management and virtual circuit control on the OPTimum trunk. The Opt Trunk VPI value: • Must be outside the VPI value ranges you configure for transit MPT LSPs, transit point-to-point LSP connections, and virtual UNIs. • Must *not* conflict with the MPT LSP VPI value.
VPC VPI Start *(OPTimum cell trunk logical port endpoints on CBX 500 and GX 550 switches only)*	Specify the first virtual path connection (VPC) virtual path identifier (VPI) value in the range of VPI values for virtual UNI logical ports that use the OPTimum trunk. For example, if the desired range is 155 to 255, you would specify 155 in this field. The default is zero (0). The range that you specify: • Must *not* overlap the ranges that you specify for transit multipoint-to-point label switched paths (MPT LSPs), and transit point-to-point LSP connections. • Must *not* conflict with the Opt Trunk VPI value. For more information, see "Configuring the OPTimum Trunk for VPCs" on page 2-8.
VPC VPI Stop *(OPTimum cell trunk logical port endpoints on CBX 500 and GX 550 switches only)*	Specify the last VPC VPI value in the range of VPI values for virtual UNI logical ports that use the OPTimum trunk. For example, if the desired range is 155 to 255, you would specify 255 in this field. The range that you specify: • Must *not* overlap the ranges that you specify for transit multipoint-to-point label switched paths (MPT LSPs) and transit point-to-point LSP connections. • Must *not* conflict with the Opt Trunk VPI value and the MPT LSP VPI value. For more information, see "Configuring the OPTimum Trunk for VPCs" on page 2-8.

Table 3-9. Set OPT Trunk VPI Range Attributes Fields (Continued)

Field	Action/Description
MPT LSP VPI *(OPTimum cell trunk logical port endpoints on CBX 500 and GX 550 switches only)*	Specify the VPI value for the MPT LSP root. If the switch where the OPTimum cell trunk logical port endpoint resides is also the root of an MPT LSP, a VPI is needed for the MPT LSP root. The value must be an even value between 2 and 30 (for example, 4). The default is 0 (zero). The MPT LSP VPI value: • Must be outside the VPI value ranges you configure for transit MPT LSPs, transit point-to-point LSP connections, and virtual UNI logical ports. • Must *not* conflict with the Opt Trunk VPI value.
Transit MPT LSP VPI Start *(OPTimum cell trunk logical port endpoints on CBX 500 and GX 550 switches only)*	Specify the first VPI value in the range of VPI values for transit MPT LSPs. The default is 0 (zero). The range that you specify: • Must *not* overlap the ranges that you specify for virtual UNI logical ports and transit point-to-point LSP connections. • Must *not* conflict with the Opt Trunk VPI value.
Transit MPT LSP VPI Stop	Specify the last VPI value in the range of VPI values for transit MPT LSPs. The default is 0 (zero). The range that you specify: • Must *not* overlap the ranges that you specify for virtual UNI logical ports and transit point-to-point LSP connections. • Must *not* conflict with the Opt Trunk VPI value and the MPT LSP VPI value.

Table 3-9. Set OPT Trunk VPI Range Attributes Fields (Continued)

Field	Action/Description
Transit Pt-Pt LSP VPI Start	Specify the first VPI value in the range of VPI values for transit point-to-point LSP connections. If you enter 0 (zero), the transit point-to-point LSP connection is disabled. The range that you specify: • Must *not* overlap the ranges that you specify for virtual UNI logical ports and transit MPT LSPs. • Must *not* conflict with the Opt Trunk VPI value and the MPT LSP VPI value.
Transit Pt-Pt LSP VPI Stop	Specify the last VPI value in the range of VPI values for transit point-to-point LSP connections. If you enter 0 (zero), the transit point-to-point LSP connection is disabled. The range that you specify: • Must *not* overlap the ranges that you specify for virtual UNI logical ports and transit MPT LSPs. • Must *not* conflict with the Opt Trunk VPI value and the MPT LSP VPI value.

Selectable Statistics Attributes

The Selectable Statistics option is available with the NavisXtend Statistics Server. This feature allows you to enable and disable statistics collection from the logical port.

Select Set [Selectable Statistics] Attributes and complete the fields described in Table 3-10.

Figure 3-10. Selectable Statistics Attributes

Table 3-10. Selectable Statistics Attributes Fields

Field	Action/Description
Bulk Statistics for the Logical Port	Enable to configure statistics collection from the logical port using the NavisXtend Statistics Server. Choices are Enable or Disable. The default setting is Disable. See the *NavisXtend Statistics Server User's Guide* for more information.
Bulk Statistics for All PVCs on the Lport	Enable to configure statistics collection for all PVCs on the logical port using the NavisXtend Statistics Server. Bulk Statistics for the logical port must be enabled before enabling this option. Choices are Enable or Disable. The default setting is Disable. See the *NavisXtend Statistics Server User's Guide* for more information.

Completing the Logical Port Configuration

Use the following steps to complete the logical port configuration:

1. (*Optional*) To configure this logical port for a specific Layer2 VPN and customer, see "Configuring a Logical Port for Layer2 VPN" on page 11-7.
2. From the Add Logical Port dialog box, use the Select: Options: menu to review additional options. Choose Set to configure this information. Table 3-11 describes these options.

Table 3-11. Select:Options: Menu

Options	Action/Description
QoS Parameters	To review default QoS parameters and, if necessary, modify these defaults, see "Setting Quality of Service Parameters" on page 3-44.
SVC QoS Parameters	To review default SVC QoS parameters and, if necessary, modify these defaults, see "Setting SVC Quality of Service Parameters" on page 3-47.
NTM Parameters (*Optional - CBX and GX*)	To configure network traffic management (NTM) parameters for this logical port, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
Accounting Parameters (*Optional*)	Enables you to configure NavisXtend Accounting server parameters. See the *NavisXtend Accounting Server Administrator's Guide* for details.

3. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 3-1 on page 3-4).
4. Choose Close to return to the Set Physical Port Attributes dialog box. Then choose Cancel to return to the Switch Back Panel dialog box.

Setting Quality of Service Parameters

This section describes how to set the Quality of Service (QoS) parameters for a logical port. These parameters enable you to specify the bandwidth and routing metrics (if applicable) for the various traffic service classes. Lucent recommends that you set the logical port QoS fixed and dynamic options before you provision circuits. Under certain conditions, if you change the bandwidth from dynamic to fixed after you provision circuits, one or more QoS classes (including CBR) may display negative bandwidth. For more information about QoS, see "About Quality of Service" on page 10-3.

Table 3-12 lists the default QoS parameters. The switch routes circuits depending on the logical port routing metric you select.

Table 3-12. Default Quality of Service Values for ATM UNI Logical Ports

Service Type	Bandwidth Allocation	Routing Metric	Oversubscription Factor
CBR	Dynamic	Admin Cost	100%
VBR-RT	Dynamic	Admin Cost	100%
VBR-NRT	Dynamic	Admin Cost	100%
ABR/UBR	Dynamic	Admin Cost	100%

To modify these settings, from the Select: Options: menu (see page 3-43) select QoS Parameters and choose Set. The Set Logical Port QoS Parameters dialog box appears.

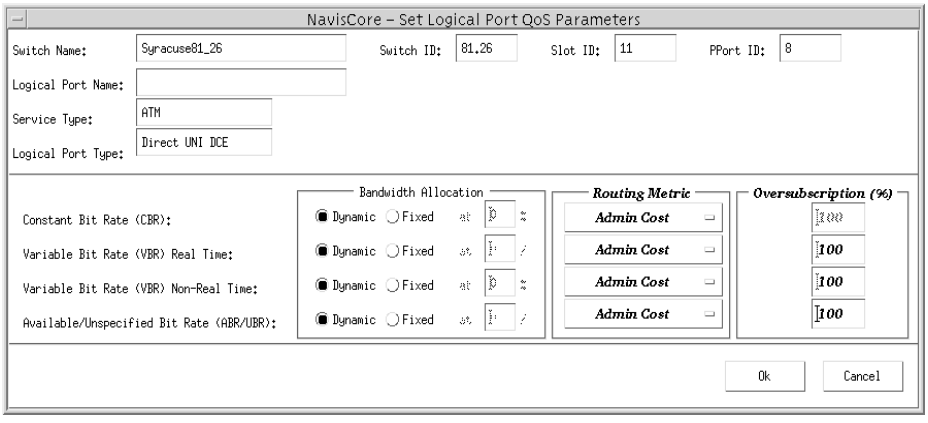


Figure 3-11. Set Logical Port QoS Parameters Dialog Box

To set the QoS parameters:

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

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

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

   - If you set the CBR or VBR service class bandwidth to Fixed, you are specifying the maximum bandwidth to reserve for this type of traffic; if the network requests a circuit that exceeds the fixed value, the circuit cannot be created.
   - If you set the ABR/UBR service class to Fixed, you are guaranteeing that amount of service (at a minimum) for the UBR queue, provided that the VBR queues are not oversubscribed. 100 cells per second of bandwidth is allocated for ABR/UBR connections.

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

2. The switch routes circuits depending on the logical port routing metric you select. Routing metrics apply only if the port is configured as UNI DCE, UNI DTE, or NNI logical port.

   Changing the routing metrics does not admin down the logical port. Select one of the following Routing Metrics for each class of service.

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

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

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

3. (*Optional*) Specify the Oversubscription factor percentage for each class of service (except CBR, which is set to 100% and cannot be modified). This value must be between 100% and 10000%.

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

   After monitoring your network, if users of a particular service class are reserving more bandwidth than they are actually using, you can adjust the oversubscription values to suit your needs. By doing so, however, you may adversely impact the quality of service for this and lower priority service classes. For more information on the oversubscription factor, see page 2-18.

   Changing the value of the Oversubscription percentage does not admin down the logical port.

4. Choose OK to return to the Add Logical Port dialog box.

Setting SVC Quality of Service Parameters

The SVC QoS feature enables you to limit the percentage of logical port bandwidth that SVCs are allowed to consume. This feature is useful in cases when you want to offer both SVC and PVC services on a logical port yet limit the amount of bandwidth available for SVCs. When you configure a logical port for use with SVCs, you have the ability to set the percentage of bandwidth available for SVCs for each class of service (CBR, VBR-RT, VBR-NRT, ABR/UBR).

The values entered on the Set Logical Port SVC QoS Parameters dialog box (Figure 3-12 on page 3-48) work in conjunction with the service class bandwidth allocation values entered on the Set Logical Port QoS Parameters dialog box (Figure 3-11 on page 3-44). On the Set Logical Port QoS Parameters dialog box, the Bandwidth Allocation field is set to Dynamic by default. If you change the Bandwidth Allocation field to *Fixed* and enter a value of (for example) 40% for VBR-NRT, the logical port bandwidth available for SVCs would be a maximum of 40%. You can limit the VBR-NRT bandwidth further by entering a value in the SVC Allowed (%) field on the Set Logical Port SVC QoS Parameters dialog box (Figure 3-12 on page 3-48).

If you accept the default SVC Allowed percentage of 100% for all QoS classes, then SVCs will have the same access as PVCs to the logical port bandwidth in each QoS class. If you want to limit the amount of logical port bandwidth that SVCs consume, you must enter a value lower than 100% in the SVC Allowed (%) field. For example, if you want to limit CBR SVCs to consume 50% of the logical port bandwidth available to CBR connections, enter 50% in the SVC Allowed (%) field.

Note – A transit SPVC at a UNI or NNI endpoint is treated as an SVC and is subject to the entered SVC Allowed percentage. An originating or terminating SPVC at a UNI or NNI endpoint is treated as a PVC and is not subject to the entered SVC Allowed percentage.

The values entered on the Set Logical Port SVC QoS Parameters dialog box (Figure 3-12 on page 3-48) will also work in conjunction with port oversubscription. For example, if you oversubscribe a logical port class of service to 200%, the associated increase in bandwidth is fully available for SVCs (by default). If you want to limit access to the increased level of bandwidth such that only 50% is available for SVCs, you would enter 50% in the SVC Allowed (%) field (for the appropriate class of service) on the Set Logical Port SVC QoS Parameters dialog box.

To set the SVC QoS parameters:

1. Using the Select:Options: button on the Add Logical Port dialog box (Figure 3-3 on page 3-11), select SVC QoS Parameters and choose Set. The Set Logical Port SVC QoS Parameters dialog box appears.

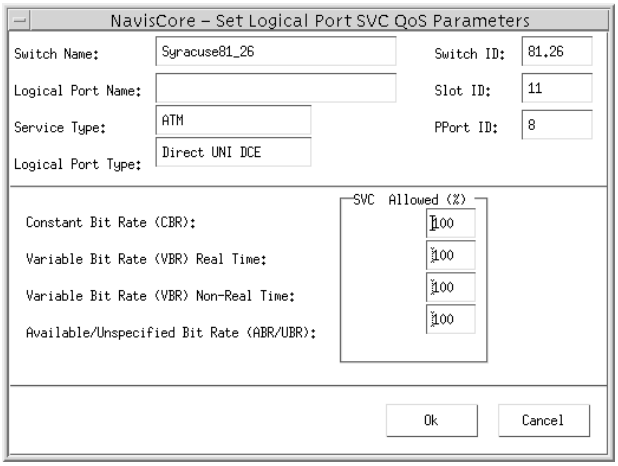


Figure 3-12. Set Logical Port SVC QoS Parameters Dialog Box

2. Complete the fields in Table 3-13 and then choose OK

Table 3-13. Set Logical Port SVC QoS Parameters Dialog Box Fields

Field	Action/Description
Constant Bit Rate (CBR)	Specify the percent of CBR bandwidth on this logical port available to SVCs. Enter a value between 0-100%. The default is 100%.
Variable Bit Rate (VBR) Real Time	Specify the percent of VBR-RT bandwidth on this logical port available to SVCs. Enter a value between 0-100%. The default is 100%.
Variable Bit Rate (VBR) Non-Real Time	Specify the percent of VBR-NRT bandwidth on this logical port available to SVCs. Enter a value between 0-100%. The default is 100%.
Available/Unspecified Bit Rate (ABR/UBR)	Specify the percent of ABR/UBR bandwidth on this logical port available to SVCs. Enter a value between 0-100%. The default is 100%.

Configuring Virtual ATM UNI/NNI Logical Ports

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

Note – The maximum number of virtual UNI logical ports per physical port can be verified by using the show pram <card #> command at the switch console. Note that one logical port is reserved for each physical port. For example, a 4-Port OC-3c card supports a maximum of 120 lports, but since four (one per physical port) are reserved, there are 116 configurable logical ports.

If you need to configure an ATM Virtual NNI logical port using PNNI 1.0 routing, see Chapter 20.

To add a virtual ATM UNI/NNI logical port:

1. Complete the steps in "Accessing ATM Logical Port Functions" on page 3-2. Make sure you access a physical port on which you have already defined a UNI logical port.
2. Choose Add to define a new logical port. The Add Logical Port Type dialog box (Figure 3-2 on page 3-10) appears.
3. Select the LPort Type, either ATM UNI DCE, ATM UNI DTE, or ATM NNI.
4. Choose OK. The Add Logical Port dialog box appears. The LPort Type field displays a virtual ATM UNI DCE/DTE (or NNI) logical port type.
5. Continue with the instructions beginning with Table 3-4 on page 3-14 to configure attributes for this virtual UNI/NNI logical port.

Note – For additional information on configuring VP shaping on virtual ATM UNI logical ports, see "Configuring VP Shaping on CBX 500 Virtual UNI Logical Ports" on page 3-19.

Configuring Logical Ports for Use With ATM SVCs

If you plan to use ATM SVCs in your network, there are additional Set Attributes functions you must configure. You configure these SVC attributes for ATM UNI DCE, ATM UNI DTE, and ATM NNI logical port types. You can configure the following SVC attributes shown in Figure 3-13:

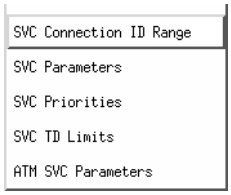


Figure 3-13. SVC Menu

For a detailed description of these attributes, see "About the Set Attributes Menu" on page 3-11.

For more information about SVCs, see Chapter 14, "About SVCs" and Chapter 15, "Configuring SVC Parameters."

Defining SVC Connection ID Parameters Attributes

The VPI/VCI address range fields allow you to design a VPC VPI or VCC VPI/VCI address range to match the capability of the equipment attached to this port.

From the Add Logical Port dialog box (Figure 3-3 on page 3-11), select Set [SVC Connection ID Parameters] Attributes and complete the fields described in Table 3-14.

Note – If you are using the 3-Port Channelized DS3/1 IMA IOM configured in UNI mode, the default SVC Connection ID Range is 0 (zero) to 255. The corresponding default values for Number of Valid Bits in VCI (6) and Number of Valid Bits in VPI (8) are displayed in the Set ATM Attributes fields, as described in Table 3-6 on page 3-22. When the 3-Port Channelized DS3/1 IMA IOM is configured in IMA mode, the standard SVC Connection ID Parameters default values are used.

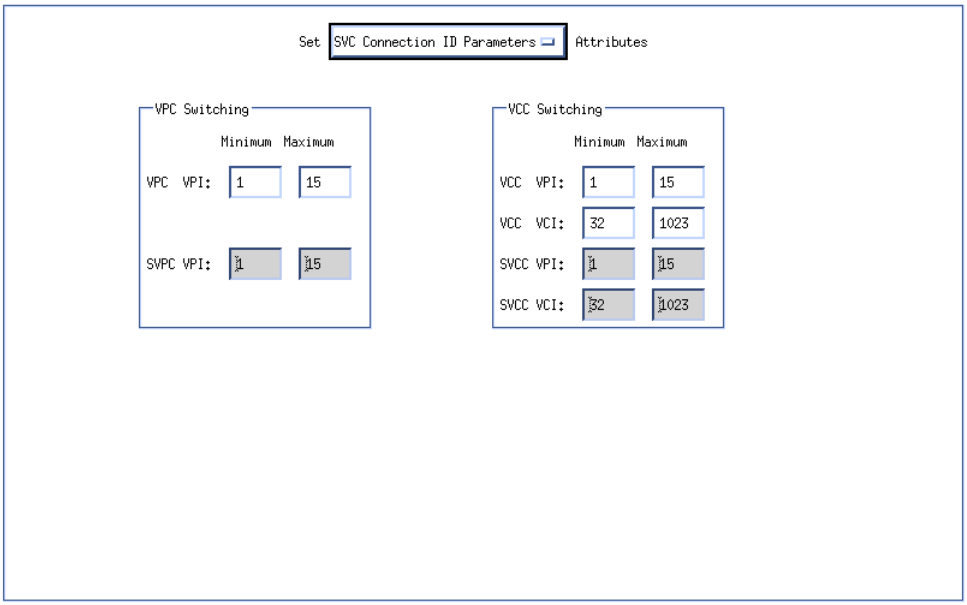


Figure 3-14. Set SVC Connection ID Parameters Attributes Fields

Table 3-14. Set SVC Connection ID Parameters Attributes Fields

Field	Action/Description
VPC VPI	Displays the VPI range for a VPC.
SVPC VPI (*UNI 4.0 only*)	Enter the range of SVPC VPI values. *Direct UNI* – This range corresponds to the Cell Header Format field (see page 3-26). For UNI cell header types, the range is from 0 - 255; for NNI, the range is from 0 - 4095.
VCC VPI	Displays the VPI range for a VCC.
VCC VCI	Displays the VCI range for a VCC.
SVCC VPI	Enter the range of SVCC VPI values. *Direct UNI* – This range corresponds to the value you entered for Number of Valid Bits in VPI (see page 3-26).
SVCC VCI	Enter the range of SVCC VCI values. *Direct UNI* – This range corresponds to the value you entered for Number of Valid Bits in VCI (see page 3-27). *Virtual UNI/NNI* – This range depends on the number of VCI bits configured on the feeder (direct) logical port.

Defining SVC Parameters Attributes

From the Add Logical Port dialog box (Figure 3-3 on page 3-11), select Set [SVC Parameters] Attributes and complete the fields shown in Figure 3-15.

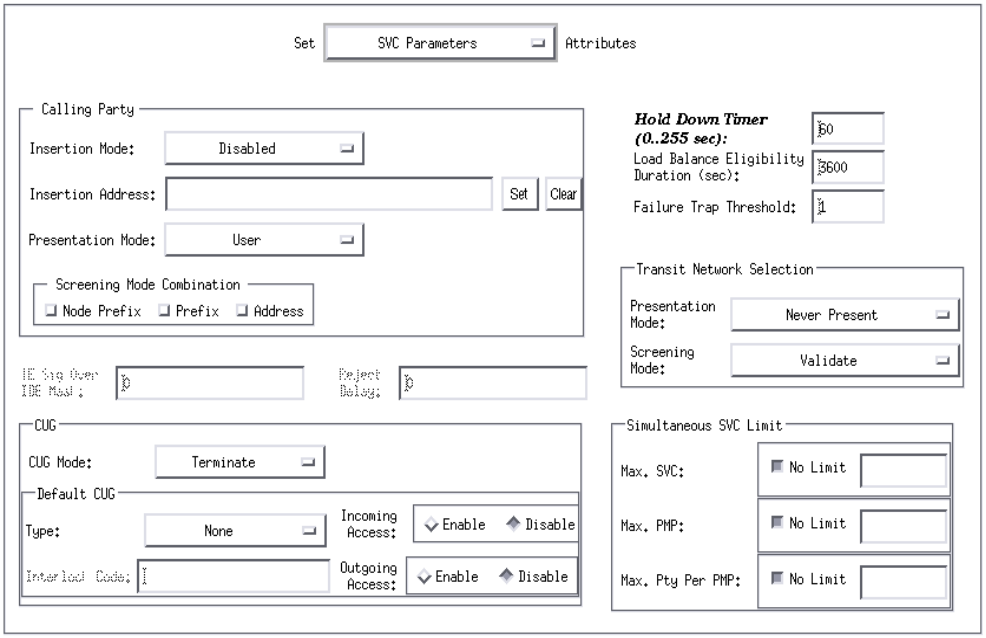


Figure 3-15. Set SVC Parameters Attributes Fields

Calling Party Parameters

Use the following parameters to configure the logical port for various address and screening options:

Insertion Mode and Insertion Address — Specifies how the logical port handles the calling party address in SVC requests.

Presentation Mode — Specifies whether or not to include the calling party address on egress SVCs and processes the connected number address in an ingress Connect message.

Screening Mode Combination — Determines whether or not to process an ingress call at this logical port.

Insertion Mode/Insertion Address

For calling party screening to occur, set the Insertion Mode field to Disabled or Insert. If you select Replace, calling party screening is effectively disabled because the Calling Party Insertion Address is always considered valid. If you select Insert, calling party screening occurs only when the caller signals the calling party address. If the caller does not signal the calling party address, the Calling Party Insertion Address, which is always considered valid, is used.

1. Select one of the Insertion Mode options described in Table 3-15.

Table 3-15. Insertion Mode Options

Option	Action/Description
Disabled	The logical port does not insert or replace the calling party address. If you set the Insertion Mode field to Disable (default), skip to "Presentation Mode" on page 3-55.
Insert	If the logical port receives an SVC request that does not have a calling party information element, it inserts the address that is specified in the Calling Party Insertion Address field.
Replace	When the logical port receives an SVC request: • If there is no calling party address, it inserts the calling party address specified in the Calling Party Insertion Address field. • If there is a calling party address, it overwrites the existing calling party information element with the address specified in the Calling Party Insertion Address field.

2. Choose the Set button to the right of the Insertion Address field. The Set Insertion Address dialog box appears.

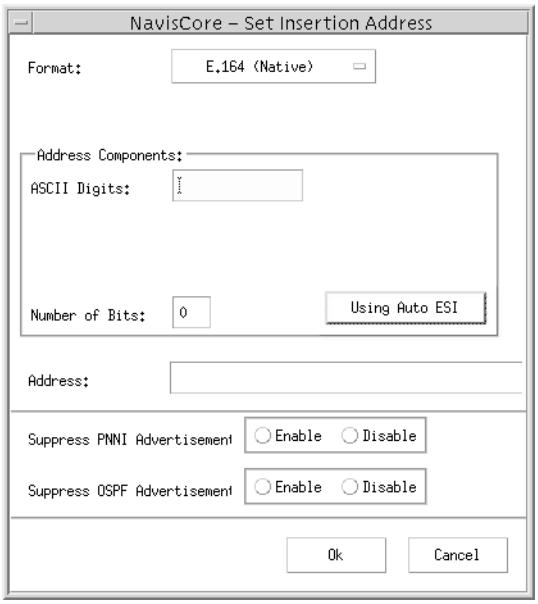


Figure 3-16. Set Insertion Address Dialog Box

Note – The calling party insertion address is not used to route SVCs to this port. To use the calling party insertion address to route SVCs to this port, configure the address (or a prefix corresponding to the address) on this port. For more information, see "Configuring SVC Port Addresses" on page 15-26.

3. Select the appropriate options in the Format field. See the following list of applicable sections for instructions.
   - For Native E.164 Addresses, see page 15-31.
   - For DCC or ICD AESA addresses, see page 15-32.
   - For E.164 AESA addresses, see page 15-34.
   - For Custom AESA addresses, see page 15-35.
4. To advertise this address across the PNNI routing domain if the local switch is connected to a PNNI peer group, select Disable (default).
5. To advertise this address across the VNN OSPF routing domain, select Disable (default).
6. Proceed to "Presentation Mode" on page 3-55.

Presentation Mode

In the Calling Party field of the Set [SVC Parameters] Attributes menu (Figure 3-15 on page 3-52), select one of the Presentation Mode options described in Table 3-16. The Presentation Mode is applied at egress to the calling party and ingress to the connected number.

Table 3-16. Presentation Mode Options

Button	Action/Description
User	Include the calling party (connected number) address at egress (ingress) based on the Presentation Indicator in the SETUP (Connect) message of the user's SVC request (confirm).
Always	Always include the calling party (connected number) address at egress (ingress), regardless of the Presentation Indicator in the SETUP (connect) message of the user's SVC request (confirm).
Never	Never include the calling party (connected number) address at egress (ingress), regardless of the Presentation Indicator in the SETUP (connect) message of the user's SVC request (confirm).

Screening Mode Combination

In the Calling Party section of the Set [SVC Parameters] Attributes fields (Figure 3-15 on page 3-52), configure one or more of the Screening Mode Combination options described in Table 3-17. If you select more than one item, the ingress call is processed if it meets one or more of the selected criteria (for example, if you select both Node Prefix and Address, the calling party address must match either a valid node prefix or a valid port address).

Note – If you enable screening at any level, and the calling party has no calling party address, the SVC fails unless you set the Calling Party Insertion Mode to Insert or Replace, and configure a Calling Party Insertion Address.

Table 3-17. Screening Mode Options

Option	Action/Description
Node Prefix	Screens the calling party against all of the configured node prefixes. If a match is found, the screen is successful.
Prefix	Screens the calling party against all of the configured port prefixes. If a match is found, the screen is successful.
Address	Screens the calling party against all of the configured port addresses. If a match is found, the screen is successful.

Transit Network Parameters

The Set [SVC Parameters] Attributes menu (Figure 3-15 on page 3-52), provides the Transit Network Selection shown in Table 3-18.

Table 3-18. Transit Network Selection Fields

Option	Action/Description
Presentation Mode	Select the egress presentation mode for the selected logical port. Options include: *Never Present* – (default) Never signal transit network selection (TNS) in egress SVC requests. *Present Signaled TNS Only* – Signal TNS in egress SVC requests only if TNS was signaled by the user in the ingress SVC request. *Signaled or Source Default* – Signal TNS in egress SVC requests if TNS was signaled by the user in the ingress SVC request or a source default network ID was provisioned at the ingress user's logical port. ***Note**: Network IDs that do not match the adjacent network ID (see the Adjacent Network field in Table 15-7 on page 15-44) are processed according to the configured presentation mode; however, a network ID that matches the adjacent network ID will never be signaled in egress calls (presentation mode is Never Present).*
Screening Mode	Select the screening mode for the selected logical port. Options include: *Ignore* – Ignore the signaled TNS. *Accept* – Always accept the signaled TNS. *Validate* – (default) Screens the signaled TNS and ignores it if there is no match.

CUG Parameters

The Set [SVC Parameters] Attributes menu (Figure 3-15 on page 3-52) provides the following CUG fields, as shown in Table 3-19:

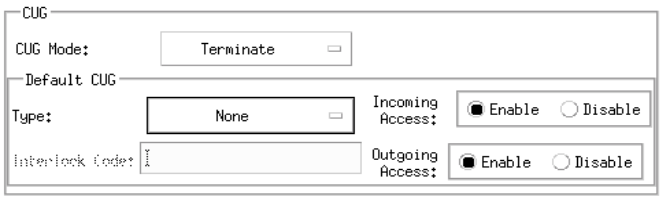


Figure 3-17. CUG Fields

Use Table 3-19 to configure these fields.

Table 3-19. CUG Fields

Field	Action/Description
CUG	
CUG Mode	The CUG Mode allows you to enable address-based or port-based CUG. Options include: *Terminate* – (default) Enables Address-based CUG when you set the Default CUG Type to *None*. Enables Port-based CUG when you set the Default CUG Type to anything but none. *Disabled* – Disables CUG. *Signal* – The port signals the port-based CUG interlock code at the FR UNI or NNI.
Default CUG	
Type	The type of default CUG configured on this logical port for port-based CUG. Options include: *None* (default) *E.164* *DNIC* *AESA*
Interlock Code	The interlock Code for the default CUG configured on this logical port. Available interlock codes include: • E.164 and DNIC interlock codes are typically 13 numerical digits encoded as T.50 (ASCII) characters, however, interlock codes of length 1-13 are allowed. • AESA interlock codes are typically 24 binary octets, where the first 20 resemble an AESA; however, interlock codes of length 1-24 are allowed.

Table 3-19. CUG Fields (Continued)

Field	Action/Description
Incoming Access	Specifies how ingress calls from non-CUG users or users of a different CUG are handled. Options include: *Enable* – Accepts calls from users that do not belong to the same CUG. *Disable* – (default) Rejects calls from users that do not belong to the same CUG.
Outgoing Access	Specifies how egress calls to non-CUG users or users of a different CUG are handled. Buttons include: *Enable* – Allows calls to users that do not belong to the same CUG. *Disable* – (default) Blocks calls to users that do not belong to the same CUG.

Simultaneous SVC Limit Parameters

The Set [SVC Parameters] Attributes menu (Figure 3-15 on page 3-52) provides the following Simultaneous SVC Limit fields, shown in Table 3-20:

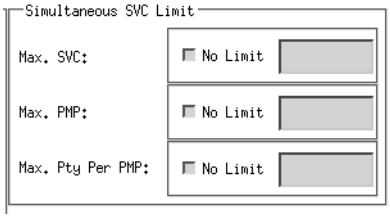


Figure 3-18. Simultaneous SVC Limit Fields

Use Table 3-20 to configure the Simultaneous SVC Limit fields. The No Limit check box is selected by default. If you want to enter a value between 0 - 16777215 cells per second, you must deselect the No Limit check box.

Table 3-20. Simultaneous SVC Limit Fields

Field	Action/Description
Max. SVC	The maximum number of SVCs allowed on the logical port. Originating and terminating SVCs are summed for this purpose. Each point-to-multipoint SVC is counted as one SVC, no matter how many leaves it may have. Enter a value between 0-16777215 or accept the default, No Limit.
Max. PMP	The maximum number of Point-to-Multipoint SVCs allowed on the logical port. Only root SVCs are summed for this purpose. Enter a value between 0-16777215 or accept the default, No Limit.
Max. Pty Per PMP	The maximum number of parties allowed per Point-to-Multipoint SVC on the logical port. Enter a value between 0-16777215 or accept the default, No Limit. ***Note:*** *The value displayed in this field shows the number of leaves, without the root leaf. However, the actual established SVC calls will be leaves plus root leaf (that is, one more than the value displayed in this field).*

Additional Set SVC Parameters Attributes Menu Fields

The Set [SVC Parameters] Attributes dialog box (Figure 3-15 on page 3-52) provides the following additional SVC options:

- Hold Down Timer
- Load Balance Eligibility
- Failure Trap Threshold
- IE Sig Overide Mask
- Reject Delay

Use Table 3-21 to configure the remaining Set [SVC Parameters] Attributes menu fields options.

Note – Although you can modify these fields, Lucent recommends you use the default parameters.

Table 3-21. Additional Set SVC Parameters Attributes Menu Fields

Field	Action/Description
Hold Down Timer (sec)	Enter the number of seconds to wait before the network initiates SVC clearing when a trunk has gone down. If you enter 0 (zero), the network clears the SVC immediately upon detection of a trunk outage. ***Note:*** *Modifying the value of this attribute does not admin down the logical port.*
Load Balance Eligibility Duration (sec)	Enter the number of seconds an SVC must be established before it is eligible for load balance rerouting. The default is 3600 seconds. This feature is useful for those SVCs that are long term and may encounter a forced reroute due to trunk failure.
Trap Failure Threshold	Enter the threshold crossing alarm value for SVC failure traps. The switch generates a trap if the internal SVC failure counter crosses this threshold during the current 15-minute time period. The internal counter is reset every 15 minutes. The default value of 1 means that if one SVC failure occurs on a logical port, a trap is issued and no additional traps are issued until the next 15-minute period. If you change the threshold value to 100, it means that 100 SVC failures must occur in a 15-minute window in order to trigger a trap. If you enter0 (zero) the switch never generates a failure trap.

Table 3-21. Additional Set SVC Parameters Attributes Menu Fields (Continued)

Field	Action/Description
IE Sig Overide Mask	Enter a value to prevent the incoming SVC ATM Adaptation Layer (AAL) information element (IE) parameter from overiding the logical port setting. The default value is 0 (zero). The range of values is 0 - 2147483647 (mask bits).
Reject Delay	Enter the number of milliseconds to wait for a RELEASE PDU after a SETUP PDU has been received. The default value is 30000 msec. The range of values is 0 - 30000 msec.

Defining SVC Priorities Attributes

From the Add Logical Port dialog box (Figure 3-3 on page 3-11), select Set [SVC Priorities] Attributes and complete the fields described in Table 3-22. You can set routing priorities for the following:

- CBR
- VBR (Real Time)
- VBR (Non Real Time)
- UBR/ABR

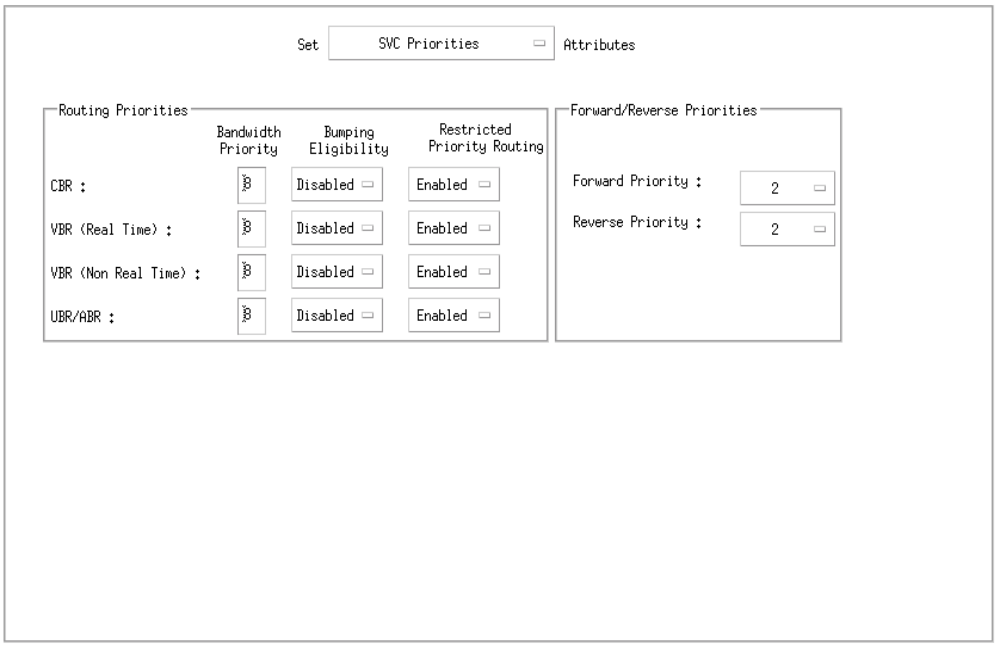


Figure 3-19. Set SVC Priorities Attribute Fields

Table 3-22. Set SVC Priorities Attributes Fields

Field	Action/Description
Routing Priorities	
Bandwidth Priority	For each of the QoS queues, specify a value from 0 through 15, where 8 is the default and 0 indicates the highest priority. See Appendix E, "Priority Routing," for more information.
Bumping Eligibility	If restricted priority routing is disabled, specify Disabled (default) to keep non-real time SVCs originating at this logical port in retry mode until sufficient bandwidth is available. Specify Enabled for non-real time SVCs to become active, whether or not sufficient bandwidth exists. If restricted priority is enabled, non-real time circuits that are bumped remain in retry mode until sufficient bandwidth is available, regardless of the bumping eligibility setting (Disabled or Enabled). Bumping eligibility is valid only for non-real time circuits, based on QoS classes. Real-time circuits ignore this setting. See Appendix E, "Priority Routing," for more information.
Restricted Priority Routing	Set to Enabled (default) to provision new SVCs at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings. Set to Disabled if you want to use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits. See Appendix E, "Priority Routing" for more information.
Forward/Reverse Priorities	
Forward Priority	Forward priority applies to the caller to callee direction of an SVC. When a particular service category's output queue becomes congested, it must discard cells. This logical port attribute sets the discard priority for the SVC in the forward direction. The lower the number, the higher the priority. Set this attribute from 1 (high priority) to 3 (low priority). The default is 2.
Reverse Priority	Reverse priority applies to the callee to caller direction of an SVC. When a particular service category's output queue becomes congested, it must discard cells. This logical port attribute sets the discard priority for the SVC in the reverse direction. The lower the number, the higher the priority. Set this attribute from 1 (high priority) to 3 (low priority). The default is 2.

Defining SVC Traffic Descriptor (TD) Limits Attributes

From the Add Logical Port dialog box (Figure 3-3 on page 3-11), select Set [SVC TD Limits] Attributes. The Set [SVC TD Limits] Attributes fields appears (see Figure 3-20 on page 3-64).

Note – The No Limit check box is selected by default. If you want to enter a value between 0 - 2147483647 cells per second, you must deselect the No Limit check box.

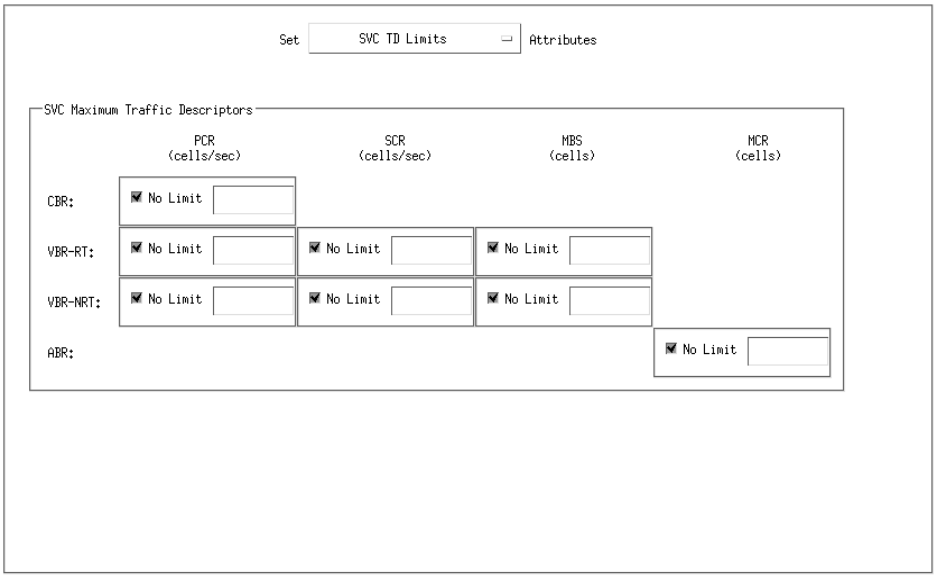


Figure 3-20. Set SVC TD Limits Attributes Fields

Complete the fields described in Table 3-23.

Table 3-23. Set SVC TD Limits Attributes Fields

Field	Action/Description
CBR	
PCR (cells/sec)	The maximum PCR, in cells per second, that may be signaled for a CBR ATM SVC. This object is used to qualify the forward PCR signaled at this ingress logical port and the backward PCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
VBR-RT	
PCR (cells/sec)	The maximum PCR, in cells per second, that may be signaled for a VBR-RT ATM SVC. This object is used to qualify the forward PCR signaled at this ingress logical port and the backward PCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
SCR (cells/sec)	The maximum SCR, in cells per second, that may be signaled for a VBR-RT ATM SVC. This object is used to qualify the forward SCR signaled at this ingress logical port and the backward SCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
MBS (cells)	The maximum MBS, in cells, that may be signaled for a VBR-RT ATM SVC. This object is used to qualify the forward MBS signaled at this ingress logical port and the backward MBS signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.

Table 3-23. Set SVC TD Limits Attributes Fields (Continued)

Field	Action/Description
VBR-NRT	
PCR (cells/sec)	The maximum PCR, in cells per second, that may be signaled for a VBR-NRT ATM SVC. This object is used to qualify the forward PCR signaled at this ingress logical port and the backward PCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
SCR (cells/sec)	The maximum SCR, in cells per second, that may be signaled for a VBR-NRT ATM SVC. This object is used to qualify the forward SCR signaled at this ingress logical port and the backward SCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
MBS (cells)	The maximum MBS, in cells, that may be signaled for a VBR-NRT ATM SVC. This object is used to qualify the forward MBS signaled at this ingress logical port and the backward MBS signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.
ABR	
MCR (cells)	The maximum MCR, in cells per second, that may be signaled for an ABR ATM SVC. This object is used to qualify the forward MCR signaled at this ingress logical port and the backward MCR signaled at this egress logical port. Enter a value between 0 - 2147483647 or accept the default value, No Limit.

Defining ATM SVC Parameters Attributes

The Set [ATM SVC Parameters] Attributes menu enables you to set the Egress and Ingress Address Translation Mode parameters.

From the Add Logical Port dialog box (Figure 3-3 on page 3-11):

1. Select Set [ATM SVC Parameters] Attributes. The Set [ATM SVC Parameters] Attributes fields appear.

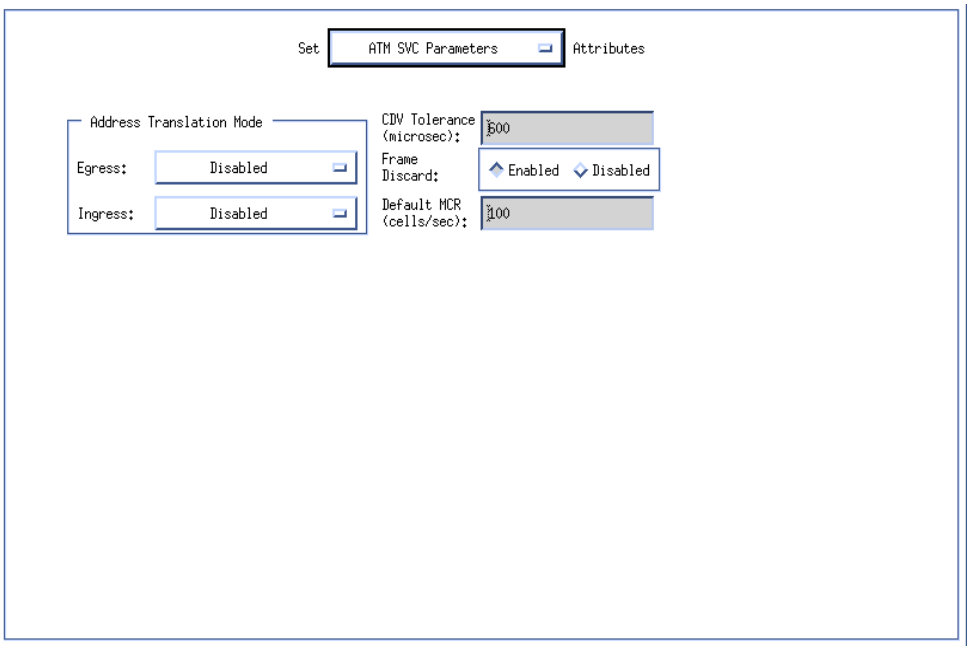


Figure 3-21. Set ATM SVC Parameters Attributes Fields

2. Select one of the following Egress Address Translation Mode options:

   Disabled — No address translation occurs on egress from the logical port.

   Tunnel — Select this option if the call is being routed through another network that is using a different address domain (see Figure 3-22). If the calling party address matches a port prefix and the port prefix has a gateway address defined, substitute the local gateway address for the calling party address, and substitute the remote gateway address for the called party address on egress from the logical port. The original addresses are then carried as sub-addresses. If you select this option, you should also select Tunnel for the Ingress Address Translation Mode.

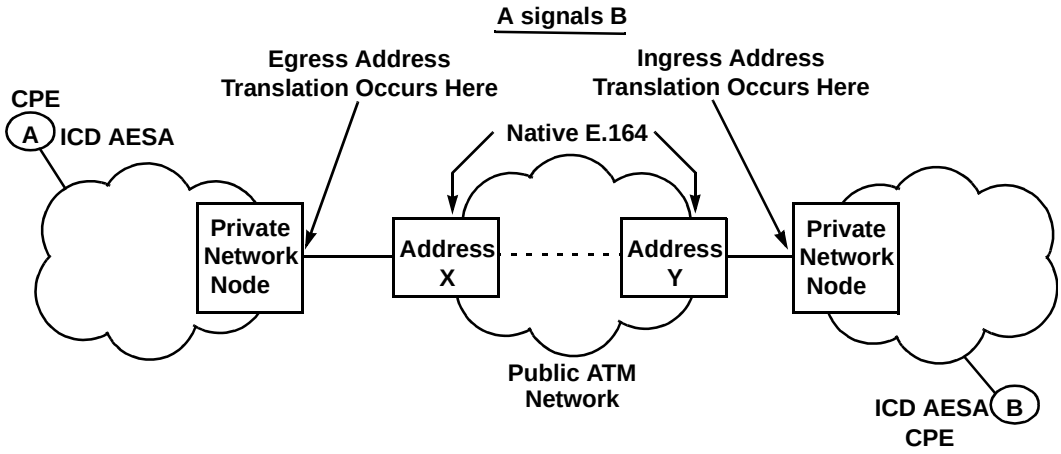


Figure 3-22. Tunneling Through a Public Network

E.164 Native to AESA — Select this option to convert native E.164 addresses to E.164 AESA format. With this option, the high-order domain-specific part (HO-DSP), end system identifier (ESI), and SEL octets of the ATM end system address (AESA) are filled with zeros at the network's egress logical port. Also, leading zeros and the trailing Fh are added to the initial domain port (IDP) portion. For example, the native E.164 address 5085551234 would be converted to AESA E.164 address 45-000005085551234F-00000000-000000000000-00.

E.164 AESA to Native — Select this option to convert E.164 AESAs to native E.164 format. If you select this option, the authority and format indicator (AFI), HO-DSP, ESI, and SEL octets of the address are removed at the network's egress logical port. Also, all leading zeros and the trailing Fh in the IDP portion of the address are removed. For example, the AESA E.164 address 45-000005085551234F-1A2B3C- 0000050F0601-00 would be converted to the native E.164 address 5085551234.

Replace — Select this option if the SVC is being routed into an attached network that is using a different address domain (see Figure 3-23). With this option, the calling party address is replaced with the local gateway address and the called party address is replaced with the remote gateway address at the network's egress logical port.

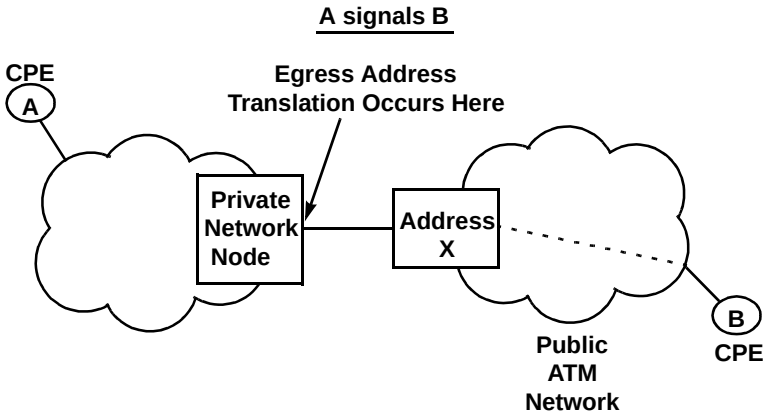


Figure 3-23. Calling Into a Public Network

For more information on egress address translation, see "About Address Translation" on page 14-12.

3. Select one of the following Ingress Address Translation Mode options. These options should match those specified for the Egress Address Translation Mode.

   Disabled — No address translation occurs at the ingress port.

   Tunnel — Select this option if a sub-address is present in the SETUP message, to promote it to the address information element at the ingress port.

   E.164 Native to AESA — Select this option if you selected E.164 AESA to Native as the Egress Address Translation Mode. If you select this option, the AFI, HO-DSP, ESI, and SEL octets of the address are removed at the network's ingress logical port. Also, all leading zeros and the trailing Fh in the IDP portion of the address are removed. For example, the AESA E.164 address 45-000005085551234F-1A2B3C-0000050F0601-00 would be converted to the native E.164 address 5085551234.

   E.164 AESA to Native — Select this option if you selected E.164 Native to AESA as the Egress Address Translation Mode. With this option, the HO-DSP, ESI, and SEL octets of the AESAs are filled with zeros at the network's ingress logical port. Also, leading zeros and the trailing Fh are added to the IDP portion. For example, the native E.164 address 5085551234 would be converted to AESA E.164 address 45-000005085551234F-00000000-000000000000-00.

   For more information on ingress address translation, see "About Address Translation" on page 14-12.

4. Complete the additional Set [ATM SVC Parameters] Attributes fields described in Table 3-24.

   Keep the following points in mind as you set the Frame Discard parameters:

   - If the incoming SVC includes the ATM Adaptation Layer (AAL) parameter information element (IE), there are cases where the information in the AAL IE overrides the logical port setting. This only occurs when requesting a non-UBR AAL 1 and AAL 3/4 connection. For all other cases, including those where an AAL 5 IE, user-defined AAL IE, or no AAL IE is signaled in, the logical port setting will be in effect.
   - In cases where the incoming SVC does not include the AAL IE or includes a user-defined AAL IE, you may want to disable Frame Discard as user traffic may be unintentionally discarded if the AAL type of user traffic is not compatible with early packet discard/partial packet discard (EPD/PPD).
   - If you are running UNI 4.0 on the logical port and the user signals in a Frame Discard preference (enabled or disabled), the signaled request will override the logical port setting. This functionality is not applicable in earlier UNI versions as it is not possible to signal in a frame discard preference.
   - When configuring NNI or virtual NNI logical ports on GX 550 BIO2 modules, you should only enable Frame Discard if the traffic traversing the NNI or virtual NNI port is encapsulated using ATM Adaptation Layer 5 (AAL-5). If Frame Discard is enabled on an NNI or virtual NNI port that is *not* using AAL-5 encapsulation, all traffic traversing the NNI or virtual NNI port may be discarded.

Table 3-24. Set ATM SVC Parameters Attributes Fields

Field	Action/Description
CDV Tolerance (microsec)	Configure the cell delay variation tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. Enter a value between 1 - 65535 µsec, which represents cell delay tolerance. The default is 600 µsec. ***Note:*** *If you are using the 3-Port Channelized DS3/1 IMA IOM, the recommended minimum CDV tolerance value is 1000 microseconds.*
Frame Discard	Enable (default) or Disable Frame Discard. When you enable Frame Discard, the network performs early packet discard (EPD) and partial packet discard (PPD) on traffic that traverses SVCs using this logical port. This field affects both the CBX 500 FCP-based EPD/PPD functionality and the CBX 500 and GX 550 output buffer EPD/PPD functionality. If you have FCP enabled on a CBX 500 IOM, the FCP-based EPD/PPD function takes precedence over the IOM output buffer EPD/PPD function.
Default MCR (cells/sec)	The default MCR, in cells per second, to be used for both directions of ABR calls when no MCR has been signaled. Enter a value between 0 - 16777215. The default value is 100.

4

Configuring ATM Logical Ports on the B-STDX 8000/9000

This chapter describes how to configure logical ports for ATM services on a B-STDX 8000/9000. Most I/O modules in the B-STDX 8000/9000 perform a type of "frame-based" ATM switching. The 1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 modules are capable of performing ATM cell-switching. Keep in mind that the dialog boxes that appear while you configure logical ports display different attributes depending on the type of module, frame- or cell-based.

In addition, the CBX 500 frame-based modules are also capable of providing frame-based ATM switching. ATM logical ports for these modules are configured the same as a B-STDX 8000/9000 frame-based module.

For information about the basic elements of ATM service, see one of the following sections in Chapter 2, "About ATM Logical Ports":

- "Using Interim Link Management Interface (ILMI)" on page 2-4
- "Virtual Paths and Virtual Channels" on page 2-11
- "About the Oversubscription Factor" on page 2-18
- "Administrative Tasks" on page 2-21

About ATM Logical Ports

The following sections describe the types of logical ports you can configure using either a B-STDX module or the CBX 500 frame-based modules. For an outline of the logical port types that each module supports, see Table 4-1 on page 4-7.

ATM UNI DCE

The ATM UNI DCE logical port type configures the logical port to communicate with an ATM CPE over ATM PVCs. The Lucent switch acts as an access concentrator feeding multiple Frame Relay and/or ATM PVCs to the CPE via the logical port.

ATM UNI DTE

The ATM UNI DTE logical port type configures the logical port to communicate with an ATM switch over ATM PVCs. The Lucent switch acts as an access concentrator feeding multiple Frame Relay and/or ATM PVCs to the ATM network via the logical port.

ATM Direct Trunk/Direct Cell Trunk

An ATM direct cell trunk (“direct trunk”) logical port type supports the transmission of virtual path connection (VPC) data. Like OPTimum cell trunks, direct trunks have no Lucent header. A unique VPI/VCI identifies the circuit and controls traffic using a separate channel. A cell trunk uses a virtual path through the ATM cloud as a channel. When configuring a direct trunk, no DTE feeder is required. Since the direct trunk uses all of the physical port’s bandwidth, you can only configure one direct trunk logical port type on a single physical port; no other logical port types can be configured on this port.

Direct trunks enable you to create a trunk between either two B-STDX switches, or between a CBX 500 or GX 550 and a B-STDX. This logical port type enables a single OSPF routing domain in a mixed network that includes both B-STDX or GX 550 switches.

The following modules support direct trunk connections between B-STDX switches:

- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1
- 1-port ATM UNI DS3/E3

The following modules support direct trunk connections between a B-STDX and either a CBX 500 or GX 550 switch:

- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1

ATM OPTimum Cell Trunk

An OPTimum cell trunk is a virtual path that supports the transmission of virtual circuit connection (VCC) data. Virtual circuits may be established between any B-STDX 8000/9000 and CBX 500, or GX 550 user interface via B-STDX 8000/9000 frame/cell trunks and CBX 500 or GX 550 cell trunks.

An OPTimum cell trunk establishes a single OSPF routing domain in a mixed network that includes both B-STDX 8000/9000 and CBX 500 or GX 550 switches. Routing decisions allow frame-based traffic to traverse either frame- or cell-based trunks. Cell-based traffic is restricted to routes that traverse Direct Cell trunks. OPTimum Cell trunks have no Lucent trunk header. A unique VPI/VCI identifies the circuit and control traffic using a separate channel. A cell trunk uses a virtual path through the ATM cloud as a trunk.

You can configure an ATM OPTimum cell trunk to create a switch-to-switch Lucent trunk through a public data network (PDN) into another Lucent network. The Lucent OPTimum trunk allows private enterprises to purchase low-cost, public-carrier services as the trunk between two Lucent switches, rather than use a more expensive leased-line service.

An OPTimum cell trunk enables you to create a trunk between either two B-STDX 8000/9000 switches or between a CBX 500 or GX 550 and a B-STDX 8000/9000. The following modules support OPTimum cell trunk connections between B-STDX 8000/9000 switches:

- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1
- ATM UNI DS3/E3

The following modules support OPTimum cell trunk connections between a B-STDX 8000/9000 and either a CBX 500 or GX 550 switch:

- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1

ATM OPTimum Frame Trunk

An ATM Open Packet Trunk (OPTimum) logical port enables you to use public ATM networks as trunk lines between two Lucent switches. You can configure an ATM OPTimum frame trunk logical port to:

- Connect to a peer Lucent switch over an ATM PVC.
- Connect to a peer Lucent switch over an ATM PVC, using an ATM data service unit (DSU).
- Multiplex Frame Relay PVCs and Switched Multimegabit Data Service (SMDS) “connections” over the ATM PVC.

You can configure an ATM OPTimum frame trunk to create a switch-to-switch Lucent trunk through a public data network (PDN) into another Lucent network. The Lucent OPTimum trunk allows private enterprises to purchase low-cost, public-carrier services as the trunk between two Lucent switches, rather than use a more expensive leased-line service.

Use this logical port type to do the following:

- Optimize performance and throughput in situations where both ends are connected by Lucent switches.
- Enable the logical port to communicate with a Lucent switch peer over an ATM PVC.
- Multiplex multiple Frame Relay PVCs and SMDS “connections” over the ATM PVC.

Network Interworking for Frame Relay Network-to-Network Interface

The Network Interworking for Frame Relay Network-to-Network Interface (FR NNI) logical port type provides the following access:

- Enables an ATM broadband circuit to interconnect two Frame Relay networks.
- Enables the logical port to communicate with a peer Frame Relay switch over an ATM PVC.
- Multiplexes multiple Frame Relay PVC segments over the ATM PVC.
- Supports many-to-one connection multiplexing.
- Facilitates inter-Local Access and Transport Area (LATA) FR NNI connections.
- Supports Frame Relay/ATM PVC Network Interworking Implementation Agreement FRF.5.

Setting the Number of Valid Bits in VPI/VCI for B-STDX 8000/9000

The Number of Valid Bits setting applies to the VPI and VCI range that you can use for VCCs (both PVCs and SVCs). The default values of VPI = 4 and VCI = 8 mean that you can use VCCs over the range of VPI = 0 – 15 (4 bits of VPI) and a VCI range of VCI = 32 – 255 (bits of VCI).

The valid range for the *number of valid bits in VPI* field is 0 – 6; the valid range for the *number of valid bits in VCI* field is 6 – 12. You may have to adjust these values in the following situations:

- In cases where the required VPI/VCI(s) of the attached devices are outside the default range of VPI = 0 – 15 and VCI = 32 – 255.
- If you use this logical port as a feeder for OPTimum trunks, the VPI value limits the number of OPTimum trunks you can create on this physical port. The VCI value limits the number of circuits you can route over each OPTimum trunk.

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

  Maximum virtual paths = $2^P - 1$
  Maximum virtual channels = $2^C - 32$
  $P + C \leq 12$

  Keep in mind that the default values and range for this setting are different from the CBX 500/GX 550. For an overview of virtual paths and channels, see page 2-11.

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

Using VP Shaping

The VP Shaping feature provides a method of enabling Lucent switch traffic sent to a customer network to comply with the customer's purchased traffic contract. By using VP Shaping, all circuits assigned to the shaper are set to the configured SCR, peak cell rate (PCR), and MBS rates. The 1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 support VP Shaping.

For ATM Direct and OPTimum Cell Trunk logical ports, you can only configure shaper attributes when VP shaping is selected (see Figure 4-9 on page 4-29). Once you select Shaping Type = VP, the pull-down list is enabled. For ATM OPTimum Frame Trunk logical ports, you can select both VP and VC shaping attributes from the pull-down list.

Keep in mind that you must first configure the 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 physical port shaper attributes before you can specify these attributes for the logical port. For information about configuring VP shaping on the 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 physical ports, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

I/O Modules for ATM Services

You can configure most ATM logical port types for B-STDX 8000/9000 I/O modules. Table 4-1 lists any exceptions.

Table 4-1. I/O Modules for ATM Services

I/O Module Type	ATM Logical Port Support
Frame-based I/O Modules	
8-port Universal I/O 4-port Unchannelized T1 4-port Unchannelized E1 2-port HSSI 10-port DSX-1	ATM UNI DCE ATM UNI DTE OPTimum Frame trunk ATM FR NNI
4-port 24 Channel T1 4-port 30 Channel E1	ATM UNI DCE ATM UNI DTE
ATM-based I/O Modules	
ATM DS3/E3 UNI 12-port ATM T1 12-port ATM E1	ATM UNI DTE ATM UNI DCE Direct trunk OPTimum Cell trunk OPTimum Frame trunk ATM FR NNI ***Note:*** *Because the ATM DS3/E3 UNI, 12-port ATM T1 and 12-port ATM E1 cards are not cell- based, you configure the same logical port attributes as the frame-based cards.*
1-port ATM CS DS3/E3 1-port ATM IWU OC-3c/STM-1	ATM UNI DCE ATM UNI DTE Direct trunk OPTimum Cell trunk OPTimum Frame trunk ATM FR NNI

Configuring Ports for ATM DXI/FUNI and ATM Services

Low-speed ATM *Data Exchange Interface/Frame User-to-Network Interface* (DXI/FUNI) service enables a Lucent switch to interoperate between Frame Relay and ATM technology on a single platform. ATM DXI/FUNI is a frame-based protocol that is designed to map easily to Frame Relay. Lucent supports ATM DXI/FUNI, Mode 1A features for the ATM DXI/FUNI standard. These features include:

- Provisioning for up to 938 virtual connections per card
- Support for AAL Type 5 data packaging only
- Frame sizes up to 8192 octets (DTE DSU)
- 16-bit frame checking sequence between the DTE and the DCE

I/O Modules for ATM Interworking Services

You can configure ATM FR NNI logical port services on the following B-STDX 8000/9000 I/O modules:

- 8-port Universal I/O
- 2-port High-Speed Serial Interface (HSSI)
- 10-port DSX-1

ATM-based I/O Modules

- ATM UNI DS3/E3
- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1
- 12-port ATM E1
- 12-port ATM T1

Logical Port Congestion Thresholds

Logical port maximum and default congestion threshold values vary depending on the type of service class configured for the logical port. You can configure congestion thresholds for both mono-class and Priority Frame QoS multi-class variable frame rate-non-real time (VFR-NRT) services. See "Priority Frame Attributes" on page 4-22 for information about configuring mono- and multi-class services.

Table 4-2 shows the maximum mono-class service threshold values you can configure for each frame-based and ATM-based module that supports ATM services.

Table 4-2. Maximum Mono-Class Service Thresholds per Card Type

Card Type	56-Byte Buffers	Bytes
8-Port UIO	5450	305200
10-Port DSX	4668	261408
4-Port Unchannelized T1	5408	302848
4-Port Unchannelized E1	5408	302848
12-Port Unchannelized E1	1922	107632
2-Port HSSI	23632	1323392
1-Port ATM UNI	60799	3404744

Table 4-3 shows the maximum multi-class service threshold values you can configure for each frame-based and ATM-based module that support ATM services.

Table 4-3. Maximum Multi-Class Service Thresholds per Card Type

Card Type	56-Byte Buffers	Bytes
8-Port UIO	2800 (if port speed is < or = 2048 Kbps)	156800
	5600 (if port speed is > 2048 and < or = 4096 Kbps)	313600
	11200 (if port speed is > 4096 and < or = 8192 Kbps)	627200
10-Port DSX	2080	116480
4-Port Unchannelized T1	1600	89600
4-Port Unchannelized E1	1600	89600

Table 4-3. Maximum Multi-Class Service Thresholds per Card Type

Card Type	56-Byte Buffers	Bytes
12-Port Unchannelized E1	2069	115864
2-Port HSSI	22400	1254400
1-Port ATM UNI	54504	3052224

About ATM Logical Port Functions

Chapter 3 contains instructions for accessing the Set All Logical Ports in PPort dialog box and provides an overview of the fields and functions contained in this dialog box.

- To access the Set All Logical Ports in PPort dialog box, complete the steps in "Accessing ATM Logical Port Functions" on page 3-2.
- To review information about this dialog box, see "About the Set All Logical Ports in PPort Dialog Box" on page 3-5.

About the Set Attributes Menu

When you define a new logical port, the Add Logical Port dialog box contains a variety of parameters that you must specify. During the process, use the Set Attributes menu on the Add Logical Port dialog box to configure them.

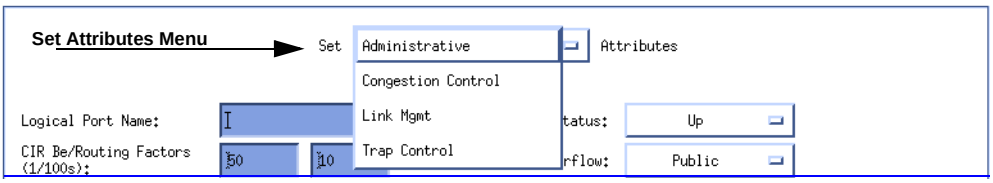


Figure 4-1. Set Attributes Menu

Table 4-4 describes the options you can configure for each ATM logical port type. Keep in mind that some options are only available for certain card types.

Table 4-4. Set Attributes Menu

Option Menu	Description	Logical Port Type	Card Types
Administrative	Specifies the number of channels allocated to each port and sets the admin status, net overflow, and bandwidth parameters. The administrative attribute fields may vary depending on the type of service and card type.	All	All
Congestion Control	Sets the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network.	• UNI DCE/DTE • Interworking for FR NNI	Frame-based cards (see Table 4-1 on page 4-7)
Trap Control	Sets the congestion threshold percentage in which traps are generated, and the number of frame errors per minute on each logical port.	All	Frame-based cards (see Table 4-1 on page 4-7)
Priority Frame	Specifies the service class type that the logical port can support. The valid values and their corresponding definitions are mono-class and multi-class. When you configure the port for mono-class operation, it only supports VFR-NRT mode; when configured for multi-class operation, it can support constant frame rate (CFR), VFR-RT, VFR-NRT, and unspecified frame rate (UFR) services.	All	Frame-based cards (see Table 4-1 on page 4-7)
ATM	Sets the ATM parameters, which include the number of valid bits in the VPI/VCI, the ATM protocol, and the UNI type.	UNI DCE/DTE	ATM CS and IWU cards

Table 4-4. Set Attributes Menu (Continued)

Option Menu	Description	Logical Port Type	Card Types
ILMI/Signaling/ OAM	Specifies the ILMI and OAM parameters. *ILMI* – Management Information Base (MIB) that provides status and communication information to ATM UNI devices and provides a port keep-alive protocol. *OAM* – Sets the alarm functions that generate Operations, Administration, and Maintenance (OAM) alarms. ***Note**: The B-STDX 8000/9000 does not support ATM SVC signaling functions.*	UNI DCE/DTE	ATM CS and IWU cards
Discard/ Congestion Mapping	Provides support for configurable mapping of discard eligible/cell loss priority (DE/CLP) and forward explicit congestion notification (FECN)/EFCI bits for both ingress and egress traffic.	• Direct trunk • OPTimum cell trunk • OPTimum frame trunk • Interworking for FR NNI	ATM CS and IWU cards
Link Mgmt	Sets the DCE and DTE polling timer and interval values.	Interworking for FR NNI	All
OPTimum Trunk VPI Range	Specifies the VPI of an OPTimum cell trunk.	OPTimum cell trunk	All

Selecting an ATM Logical Port Type

To select an ATM logical port type:

1. Complete the steps in "Accessing ATM Logical Port Functions" on page 3-2.
2. Choose Add to define a new logical port. The Add Logical Port Type dialog box appears.

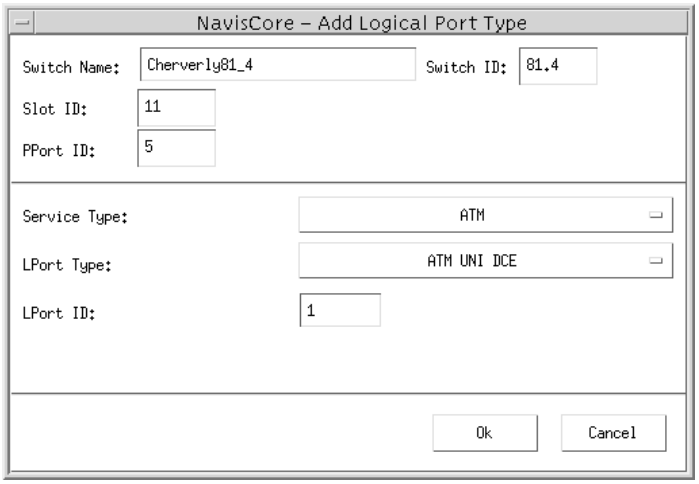


Figure 4-2. Add Logical Port Type Dialog Box

3. Select a logical port type. See Table 4-5 to continue this configuration.

Table 4-5. Configuring ATM Logical Port Types

Logical Port Type	See...
ATM UNI DTE or ATM UNI DCE	"Defining ATM UNI DCE/DTE Logical Ports" on page 4-14.
ATM OPTimum Cell Trunk or ATM Direct Trunk	"Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports" on page 4-27.
ATM OPTimum Frame Trunks	"Defining ATM OPTimum Frame Trunk Logical Ports" on page 4-37.
ATM Network Interworking for FR NNI	"Defining ATM Network Interworking for Frame Relay NNI Logical Ports" on page 4-42.

Defining ATM UNI DCE/DTE Logical Ports

To define an ATM UNI-DCE or ATM UNI-DTE logical port:

1. Complete the Add Logical Port Type dialog box (Figure 4-2 on page 4-13) fields described in Table 4-6.

Table 4-6. Add Logical Port Type Dialog Box Fields (UNI DCE/DTE)

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

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

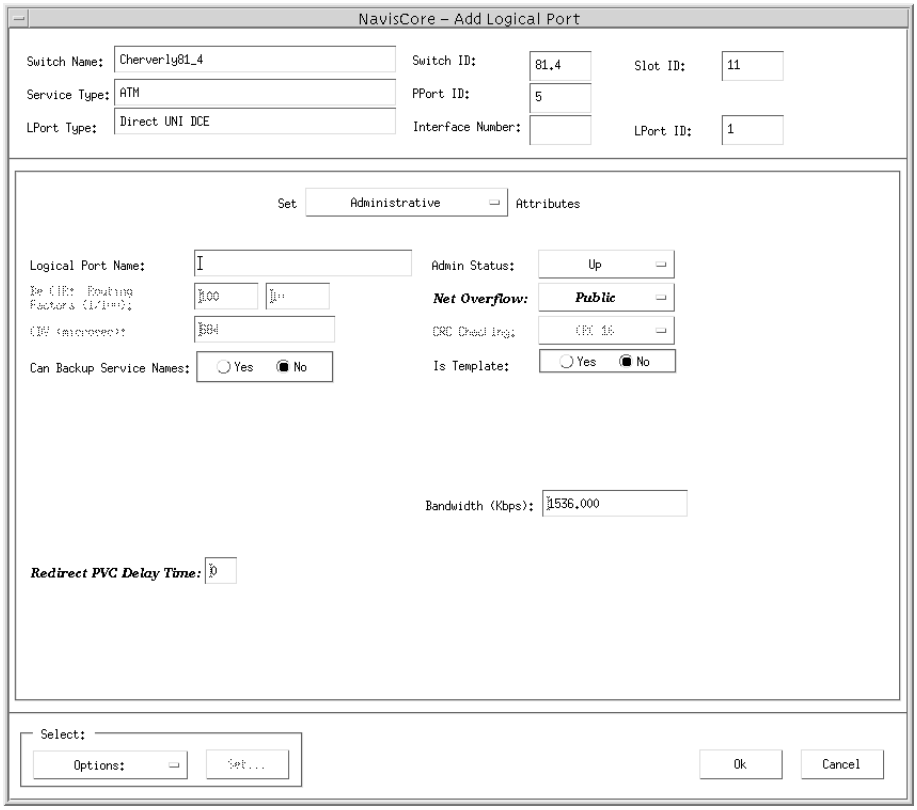


Figure 4-3. Add Logical Port Dialog Box (ATM UNI DCE/DTE)

Administrative Attributes

Select Set [Administrative] Attributes (see Figure 4-3 on page 4-14), and complete the fields described in Table 4-7.

Table 4-7. Set Administrative Attributes Fields

Field	Action/Description
Logical Port Name	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Can Backup Service Names	*Fault-tolerant PVC only* – Select Yes to configure a logical port for backup service. For more information, see Chapter 12, "Configuring Fault-Tolerant PVCs." *Primary or Backup RLMI Port only* – Select Yes to configure this port as the Resilient Link Management Interface (RLMI) backup port. Select No to configure this port as the RLMI primary port. ***Note:*** *When a backup port is not in use, the port is idle and does not use network resources.* For more information about RLMI, see Chapter 13, "Configuring Resilient LMI."
Admin Status	Set the Admin Status as follows: *Up* – (default) Activates the port. *Down* – Saves the configuration in the database without activating the port, or takes the port offline to run diagnostics. When only one logical port exists on a physical port, and you set the admin status for the logical port Down, the physical port is also considered "Down." If more than one logical port exists on a physical port, and you set the admin status for each of these logical ports to Down, the physical port is also considered Down.
Net Overflow	Set the Net Overflow parameters to one of two modes: *Public* – (default) Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network. See "Configuring a Logical Port for Layer2 VPN" on page 11-7 for more information. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*
CRC Checking (HSSI modules only)	Set this value to match the number of error checking bits used by the CPE connected to this port. Performs a cyclic redundancy check (CRC) on incoming data. Data is checked in either 4K (CRC 16) or 8K (CRC 32) frames.

Table 4-7. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Is Template	(*Optional*) You can save these settings as a template, which you can use again to quickly configure a logical port with the same options. To create a template, choose Yes.
Channels allocated for a Logical Port are marked by their IDs	Specify the DS0 (for T1) or TS0 (for E1) channel(s) allocation for this logical port. The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel to remove the X. Use the following Channel Allocation editing buttons to select/deselect channels: -- To deselect all channels ++ To select all channels - To deselect a specific channel + To select a specific channel ***Note**: The logical port bandwidth either increments or decrements depending on the number of channels you select or deselect. You can configure other logical ports with different attributes to other DS0/TS0 channels on this same physical port.*
Bit Stuffing	Select the bandwidth that matches the bandwidth capability of the customer premise equipment (CPE) connected to this logical port. Enables bit stuffing on T1/E1/DSX-1 ports. Bit stuffing affects the available bandwidth of each DS0/TS0 channel on this port. *On* – Provides 56 Kbps of bandwidth. *Off* – Provides 64 Kbps of bandwidth.
Bandwidth (Kbps)	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth remaining from the physical clock rate, less any logical ports already configured. To define a trunk logical port on this same physical port, decrease the amount of bandwidth on this logical port to ensure sufficient remaining bandwidth. For example: *Physical port clock speed*: 1536 Kbps *Logical port UNI-DTE/NNI Feeder Bandwidth*: 56 Kbps *Logical port Frame Relay Trunk Bandwidth*: 1480 Kbps The example configuration allocates a PDN trunk with 1480 Kbps bandwidth between two Lucent switches, each attached to a PDN network.

Table 4-7. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Redirect PVC Delay Time	Enter a value between 0-255 seconds. This value represents the number of seconds to wait before the network initiates call clearing after a circuit goes down. The default value is 0 (zero). You configure this value only for the primary endpoint and you can reset it at any time. A value of zero causes the network to initiate call clearing immediately, which can trigger the switch over between a working redirect PVC endpoint and its primary or secondary endpoint. Increasing the value can minimize the PVC redirection as a result of temporary data terminal equipment (DTE) state changes. For more information on redirect PVCs, see Chapter 8, "Configuring ATM PVCs." ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

See Table 4-8 to continue this configuration.

Table 4-8. Configuring UNI DCE/DTE Attributes

For 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 cards see...	For frame-based cards see...
"ATM Attributes" on page 4-23	"Congestion Control Attributes" on page 4-18
"ILMI/Signaling/OAM Attributes" on page 4-25	"Trap Control Attributes" on page 4-20
	"Priority Frame Attributes" on page 4-22

When you finish setting the attributes in Table 4-8, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

Congestion Control Attributes

Select Set [Congestion Control] Attributes and complete the fields described in Table 4-9.

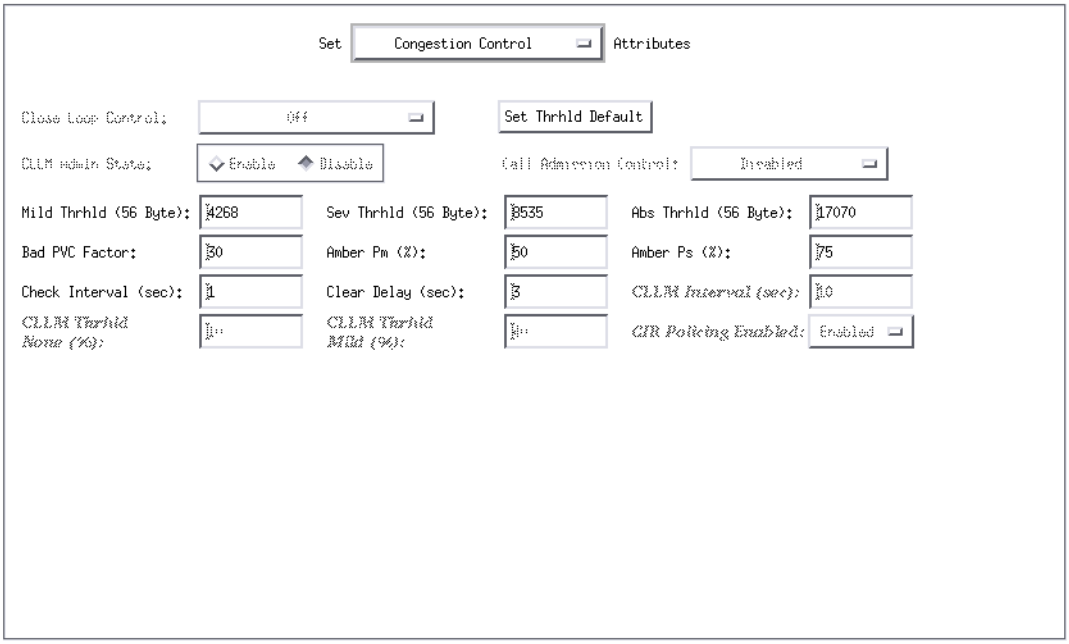


Figure 4-4. Set Congestion Control Attributes Fields

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

Table 4-9. Set Congestion Control Attributes Fields

Field	Action/Description
Set Thrhld Default	Set the Mild, Severe, and Absolute threshold settings to the default settings.
Mild Thrhld (56 Byte) Sev Thrhld (56 Byte) Abs Thrhld (56 Byte)	Accept the defaults or enter values for the mild, severe, and absolute threshold fields. ***Note:*** *If you set threshold parameters on a T1/E1 card, the default values do not appear until you set the bit stuffing and bandwidth allocation. See Table 4-7 on page 4-15 for more information on bit stuffing and bandwidth allocation.*

Table 4-9. Set Congestion Control Attributes Fields (Continued)

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

Trap Control Attributes

Select Set [Trap Control] Attributes and complete the fields described in Table 4-10.

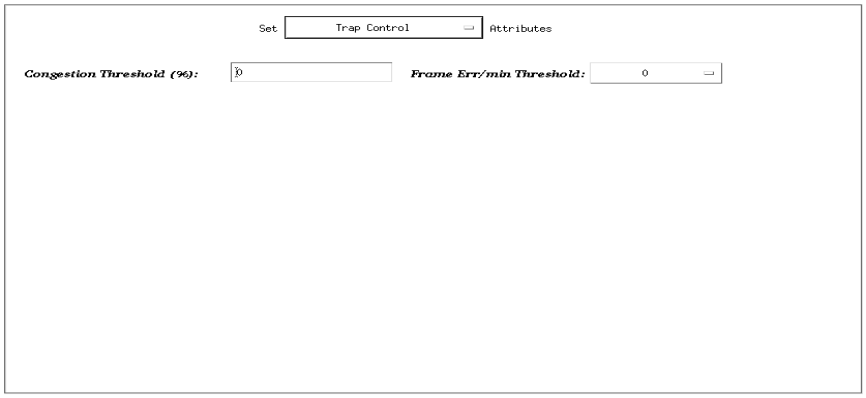


Figure 4-5. Set Trap Control Attributes Fields

Table 4-10. Set Trap Control Attributes Fields

Fields	Action/Description
Congestion Threshold (%)	Enter a value between 0 and 100 to indicate the threshold percentage for generating and sending traps to the NMS for this logical port. A congestion trap is generated and sent to the NMS if the rate of congestion over a one-minute period exceeds the percentage value you enter. Adjust the entered value according to how sensitive this port needs to be to network congestion. Options include: *Zero* – (default) Disables the congestion threshold. If you enter0 (zero), no traps are generated for this logical port. *Low* – Generates a trap at the first sign of congestion. *High* – Only generates traps for serious network congestion. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

Table 4-10. Set Trap Control Attributes Fields (Continued)

Fields	Action/Description
Frame Err/min Threshold	Enter a value from 0 to 16384 to configure the frame error threshold on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS. Adjust this value according to how sensitive this port needs to be to frame errors. Options include: *Zero* – (default) Disables this feature, which prevents traps from being generated for this logical port. *Low* – Port is sensitive to frame errors. *High* – Only generates traps when a significant number of frame errors occurs within a one-minute period. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*
SMDS PDU Violation Threshold (0-255) (*OPTimum Frame Trunks only*)	Specify the number of PDU violations that can occur before a trap is sent to the NMS. The software increments a counter every time an SMDS PDU violation takes place on a logical port. The software polls these counters every 60 seconds. If a particular counter exceeds the specified SMDS PDU violation threshold for the logical port, it generates a trap corresponding to that particular violation. The default is 10 PDU violations. Options include: *Low* – Sensitive to SMDS PDU violations. *High* – Only issue traps when there is a significant number of SMDS PDU violations.
SMDS PDU Violation Traps (*OPTimum Frame Trunks only*)	Enable or disable this field. An SMDS PDU violation can be either an SIP 3 SMDS address failure or an invalid DXI2 frame header. These errors mean incoming frames are bad, indicating problems with the CPE configuration. Options include: *Disable* – (default) Turns off traps. *Enable* – Issues traps for PDU violations.

Priority Frame Attributes

Select Set [Priority Frame] Attributes and complete the fields described in Table 4-11.

Figure 4-6. Set Priority Frame Attributes Fields

Table 4-11. Set Priority Frame Attributes Fields

Field	Action/Description
LPort Service Class Type	*Mono-class* – (default) PVC traffic maps to a VFR-NRT service class. *Multi-class* – Allows PVC traffic to utilize all ATM services classes. You must also specify Transmit Scheduling Mode.
Transmit Scheduling Mode	The transmit scheduling mode determines the method used to schedule transmission among the service classes. If you select the Multi-class LPort Service Class, select one of the following queue management options: *Fixed Priority* – Empties the CFR queue first and then the VFR-RT, VFR-NRT, and UFR queues in fixed order. *Weighted Round Robin* – Empties the CFR queue first, VFR-RT and VFR-NRT queues in weighted order, and the UFR queue last.

Table 4-11. Set Priority Frame Attributes Fields (Continued)

Field	Action/Description
Allow Vfr-Rt Negative (*Trunk logical port types only)*	This field becomes available if you select the Multi-class Lport Service Class. If you choose enable, the trunk can be oversubscribed. This option is useful in cases where a trunk has failed and PVCs must be rerouted to a new trunk. When this happens, trunk bandwidth can become negative and service may be slow, but PVCs stay up. With this option disabled (default), PVCs from the failed trunk will not be rerouted and remain down; however, existing trunk bandwidth and service remain stable.

When you finish setting these attributes, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

ATM Attributes

The Set ATM Attributes menu is only available for the 1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 cards. Select Set [ATM] Attributes and complete the fields described in Table 4-12.

Figure 4-7. Set ATM Attributes Fields

Table 4-12. Set ATM Attributes Fields

Field	Action/Description
Connection Class	Defaults to Virtual and cannot be changed.
ATM Protocol	Select the ATM protocol. Options include: • UNI 3.1 (default) • UNI 3.0
UNI Type	Select Public if at least one end of this connection attaches to a public network. Select Private if this connection resides completely within a private network.
Connection Type	Select Network - Network if this port connects to another switch or an end system. Select Network - End system if this port connects to a router or host (UNI DCE ports only).
Number of Valid Bits in VPI	Set the number of valid bits in VPI. This field applies to virtual channel connections (VCCs) only. Specify the number of bits used in the ATM cell header for storing the virtual path identifier (VPI). The total of both number of valid bits in VPI/VCI values cannot exceed 12. The default of 4 is recommended; this setting enables you to configure 15 OPTimum trunks, with up to 223 virtual channels on a given virtual path. The valid range for the VPI field is 0-6. For more information about setting these values, see page 4-5.
Number of Valid Bits in VCI	Set the number of valid bits in VCI. This field applies to VCCs only. Specify the number of bits used in the ATM cell header for storing the virtual channel identifier (VCI). The total of both number of valid bits in VPI/VCI values cannot exceed 12. The default of 8 is recommended; this setting enables you to configure 15 OPTimum trunks, with up to 223 virtual channels on a given virtual path. The valid range for the VCI field is 6-12. For more information about setting these values, see page 4-5.

Table 4-12. Set ATM Attributes Fields (Continued)

Field	Action/Description
Call Admission Control	Set the Call Admission Control parameter to: *Enabled* – (default) Port rejects a circuit creation request if there is not enough available bandwidth. *Disabled* – Port attempts to create a circuit even if there is not enough available bandwidth (for VBR NRT and UBR queues only). ***Notes:*** *If you disable Call Admission Control on a UNI logical port, you are effectively disabling Lucent's Call Master Connection Admission Control (CAC) function on that logical port.* *Changing the value of this attribute does not admin down the logical port.*

ILMI/Signaling/OAM Attributes

The Set [ILMI/Signaling/OAM] Attributes menu is only available for the 1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 cards.

Select Set [ILMI/Signaling/OAM] Attributes and complete the fields described in Table 4-13.

Figure 4-8. Set ILMI/Signaling/OAM Attributes Fields

Table 4-13. Set ILMI/Signaling/OAM Attributes Fields

Field	Action/Description
Admin Status	Enable or disable the admin status. *Enabled* – Provides ILMI support. When ILMI is *Disabled* (default), the logical port state is the same as the physical port state. *Disabled* – Disables ILMI support. To receive ILMI VCC status traps from non-Lucent ATM UNI 3.1 devices, you must enable ILMI Admin Status. For information about ILMI support, see "Using Interim Link Management Interface (ILMI)" on page 2-4. ***Note:*** *If you are using line loopback diagnostics, you must disable ILMI support. See the* B-STDX, CBX, and GX Switch Diagnostics User's Guide *for more information.*
Polling Period (sec)	Specify the polling period (T) for an ILMI poll. The switch generates an ILMI poll every (T) seconds. The default is *5 seconds*.
Loss Threshold	Specify the number of times (K) the logical port will issue an ILMI poll before the link is considered down. If no responses are seen in K x T seconds, the link is considered down. The default is 4. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*
VPI/VCI	Enter the virtual path identifier (VPI) or virtual channel identifier (VCI) you want to use for ILMI polling. The default is 0 (VPI) or 16 (VCI).
Circuit Alarms	Set the circuit alarm status. *Enabled* – (default) Allows this logical port to generate OAM alarms. The switch uses these alarms to signal when the circuits have gone down or come back up. *Disabled* – Disables OAM alarms on this logical port.
Alarm Timer Threshold (sec)	Set the alarm timer threshold (in seconds). The switch waits until the circuit has been down for the time period you specify in this field before generating an OAM alarm. The default is *5 seconds*.

To complete a logical port configuration for a 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 card, proceed to "Completing the Logical Port Configuration" on page 4-50.

Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports

This section describes how to configure an ATM direct trunk or ATM OPTimum cell trunk. These logical port types are only available for the 1-port ATM CS DS3/E3, 1-port ATM IWU OC-3c/STM-1, and ATM UNI DS3/E3 cards.

Using Direct Cell Trunks

To configure an ATM direct cell trunk, perform the following steps:

Step 1. Configure the physical port you want to use for the direct trunk (see the *B-STDX, CBX, and GX Switch Module Configuration Guide*). You can configure direct trunks on any of the following ATM modules:

- 1-port ATM CS DS3/E3
- 1-port ATM IWU OC-3c/STM-1
- ATM DS3/E3 UNI

Step 2. Configure an ATM direct cell trunk logical port on the physical port.

Step 3. Configure the trunk (see Chapter 7, “Configuring Trunks”).

Using ATM OPTimum Cell Trunks

To implement the ATM OPTimum cell trunk, first configure a UNI DTE feeder logical port on the same physical port. (1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 ports can also use a UNI DCE port for this purpose.)

To configure an ATM OPTimum cell trunk, perform the following steps:

Step 1. Configure the physical port you want to use for the ATM OPTimum cell trunk (see the *B-STDX, CBX, and GX Switch Module Configuration Guide*).

Step 2. Configure a UNI DTE feeder logical port (page 4-14) for the ATM OPTimum cell trunk on this physical port. Assign this logical port a minimum amount of bandwidth.

Step 3. Configure the ATM OPTimum cell trunk logical port on the same physical port. Assign the remaining bandwidth to this logical port (if there is only one ATM OPTimum cell trunk configured on the physical port).

Step 4. Configure the trunk (see Chapter 7, “Configuring Trunks”).

To configure an ATM direct trunk or ATM OPTimum cell trunk logical port:

1. Complete the Add Logical Port Type dialog box as follows:

   Service Type — Select ATM. The available ATM Logical port types appear.

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

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

3. Select Set [Administrative] Attributes and complete the fields in Table 4-14.

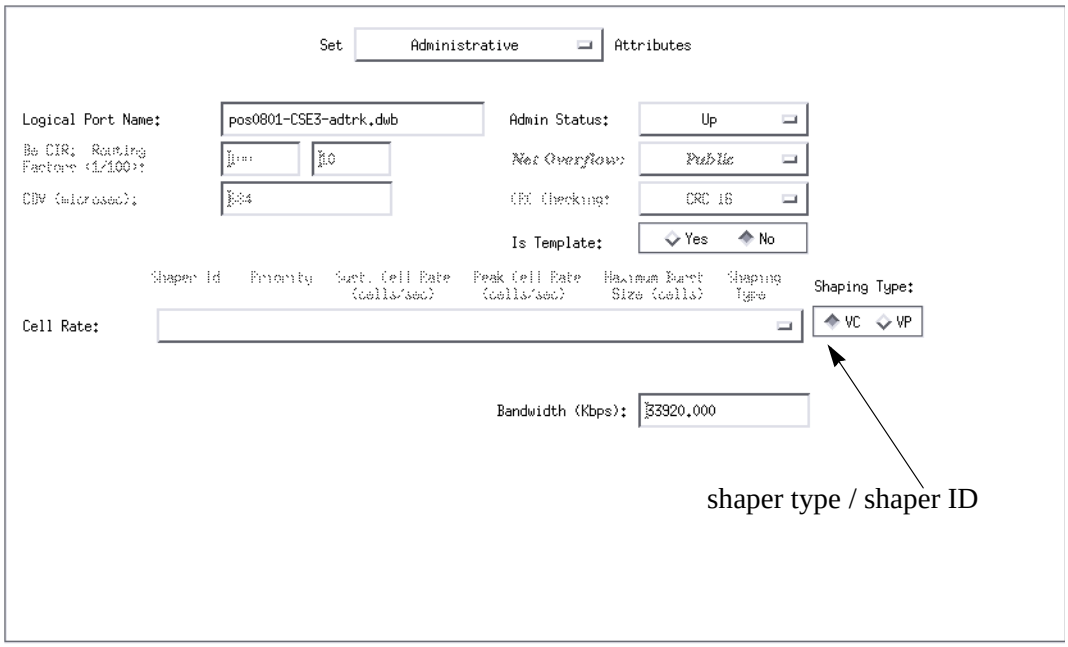


Figure 4-9. Set Administrative Attributes Fields (Direct/OPTimum Cell, ATM CS/IWU Card)

Administrative Attributes

Complete the administrative attributes fields described in Table 4-14. Note that Table 4-14 lists all possible administrative attributes for a Direct and OPTimum Cell logical port. The attributes vary depending on your type of I/O module.

Table 4-14. Set [Administrative] Attributes (Direct/OPTimum Cell, ATM CS/IWU Card)

Field	Card/Logical Port Type	Action/Description
Logical Port Name	All	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Admin Status	All	Set the Admin Status as follows: *Up* – (default) Activates the port. *Down* – Saves the configuration in the database without activating the port, or takes the port offline to run diagnostics.

Table 4-14. Set [Administrative] Attributes (Direct/OPTimum Cell, ATM CS/IWU Card) (Continued)

Field	Card/Logical Port Type	Action/Description
CDV (microsec)	ATM CS/ IWU card OPTimum and Direct Cell Trunks	Specify the maximum cell delay variation (in µsecs) for this logical port. This value applies only to CBR traffic, and it specifies the maximum variation in time delays between cells going out of this logical port. The default value is 684 for 1-port ATM IWU OC-3c/STM-1 ports, or 191 for 1-port ATM CS DS3/E3 ports. To change the default, you need to know the maximum CDV for PVCs on the port, as well as the hardware traffic requirements at the opposite end of the connection.
Net Overflow	All	Set the Net Overflow parameters to either: *Public* – (default) Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own virtual private network. See "Configuring a Logical Port for Layer2 VPN" on page 11-7 for more information. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*
Is Template	All	(*Optional*) You can save these settings as a template, which you can use again to quickly configure a logical port with the same options. To create a template, choose Yes. See "Using Templates" on page 2-21 for more information.
Shaping Type	ATM CS/IWU card	The Add Logical Port dialog box defaults to a VC Shaping Type (see Figure 4-9 on page 4-29). Using VC Shaping, the shaper pick list is grayed out and the switch uses a method of dynamically selecting a shaper for each circuit routed over the cell trunk. To use the default VC shaping method, at least one VC shaper must exist in the shaper range 1 – 5, at least one in the range 6 – 10, and at least one in the range 11 – 15. To enable VP shaping, select Shaping Type VP, then select a Shaper ID. For more information about VP Shaping, see "Setting the Number of Valid Bits in VPI/VCI for B-STDX 8000/9000" on page 4-5.

Table 4-14. Set [Administrative] Attributes (Direct/OPTimum Cell, ATM CS/IWU Card) (Continued)

Field	Card/Logical Port Type	Action/Description
Cell Rate	ATM UNI DS3/E3 cards	Specify the cell transmission rate that is allowed over a given period of time on a given circuit. Cell Rate allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR traffic; it does not apply to CBR or UBR traffic.
Bandwidth (Kbps)	All	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth available on the port. If you are configuring more than one ATM OPTimum cell trunk on this logical port, enter the appropriate amount of bandwidth to reserve for the ATM OPTimum cell trunk you are currently configuring. Leave enough bandwidth for any remaining ATM OPTimum cell trunks you need to configure on this logical port. ***Note**: Multipoint VCCs are limited over ATM OPTimum cell trunks. You cannot configure more than one circuit leaf of a point-to-multipoint circuit on the same logical port, since multiplexing cannot be performed at the port level. If you configure more than one OPTimum trunk on a logical port, set up a circuit leaf for a given circuit root on only one of the OPTimum trunks.*
Shaper ID	ATM CS/IWU card	If you enable VP shaping, choose a value from 1 through 15 to specify the Shaper ID and associated priority, sustainable cell rate, peak cell rate, and maximum burst size values (see Figure 4-9). Make sure you assign only one trunk logical port per shaper ID. Assigning more than one trunk logical port to a given shaper ID decreases circuit performance.

If you are configuring an ATM DS3/E3 UNI module, Figure 4-9 on page 4-29 displays the following fields in place of the Shaping Type/Shaper ID. To complete these fields, see Table 4-15. Otherwise, continue with the instructions in Table 4-16 on page 4-33.

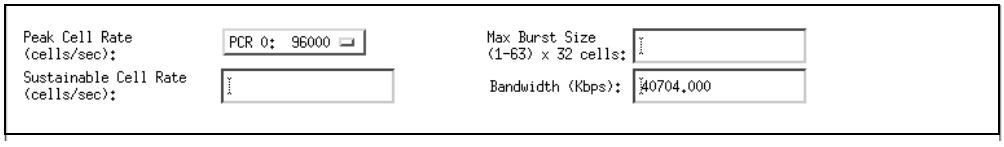


Figure 4-10. Set [Administrative] Attributes Fields (ATM DS3 UNI)

Table 4-15. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS)

Field	Card/Logical Port Type	Action/Description
Peak Cell Rate (cells/sec)	ATM UNI DS3/E3 cards	Specify the maximum allowed cell transmission rate (expressed in cells per second). The PCR defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
Sustainable Cell Rate (cells/sec)	ATM UNI DS3/E3 cards	Specify the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. SCR allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR traffic; it does not apply to CBR or UBR traffic.
Max Burst Size	ATM UNI DS3/E3 cards	Specify the maximum number of cells that can be received at the peak cell rate. This allows a burst of cells to arrive at a rate higher than the SCR. If the burst is larger than anticipated, the additional cells are either tagged or dropped. This parameter applies only to VBR traffic; it does not apply to CBR or UBR traffic.
Bandwidth (Kbps)	All	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth available on the port. If you are configuring more than one ATM OPTimum cell trunk on this logical port, enter the appropriate amount of bandwidth to reserve for the ATM OPTimum cell trunk you are currently configuring. Leave enough bandwidth for any remaining ATM OPTimum cell trunks you need to configure on this logical port. ***Note**: Multipoint VCCs are limited over ATM OPTimum cell trunks. You cannot configure more than one circuit leaf of a point-to-multipoint circuit on the same logical port, since multiplexing cannot be performed at the port level. If you configure more than one OPTimum trunk on a logical port, set up a circuit leaf for a given circuit root on only one of the OPTimum trunks.*

See Table 4-16 to continue this configuration:

Table 4-16. Configuring Direct Cell Trunk/OPTimum Cell Trunk Attributes

For 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 cards see...	For ATM DS3/E3 UNI cards see...
"Discard/Congestion Mapping Attributes" on page 4-33	"Trap Control Attributes" on page 4-20
"OPTimum Trunk VPI Range Attributes" on page 4-35	"Priority Frame Attributes" on page 4-22
	"OPTimum Trunk VPI Range Attributes" on page 4-35

When you finish setting these attributes, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

Discard/Congestion Mapping Attributes

The Set [Discard/Congestion Mapping] Attributes menu enables you to select discard and congestion priority bit mappings on data sent to and from the logical port. Egress mapping takes place just before the ATM interface transmits the data; ingress mapping takes place after the ATM interface receives the data. These options provide support for configurable mapping of the DE/CLP and FECN/EFCI bits.

Select Set [Discard/Congestion Mapping] Attributes and complete the fields described in Table 4-17 on page 4-34. When you finish, continue with "Completing the Logical Port Configuration" on page 4-50.

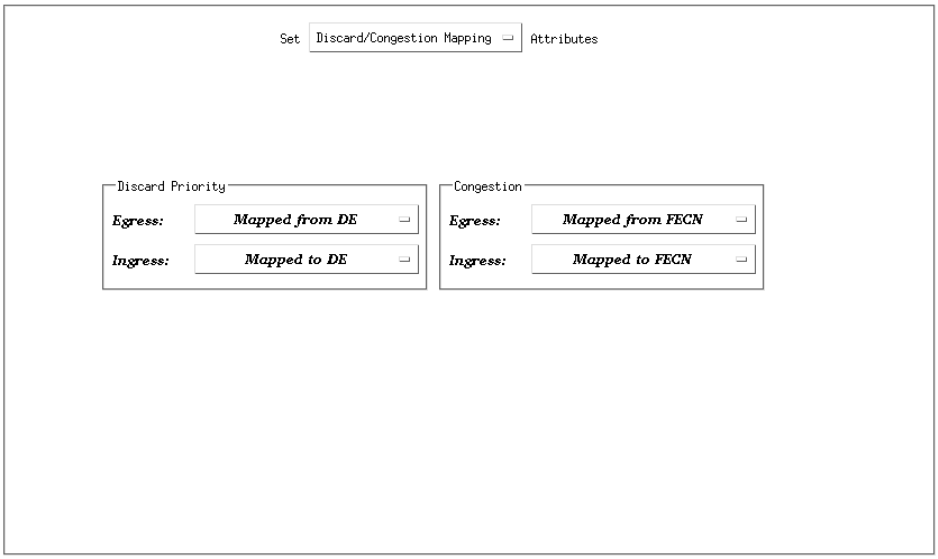


Figure 4-11. Set [Discard/Congestion Mapping] Attributes Fields

Table 4-17. Set [Discard/Congestion Mapping] Attributes Fields

Field	Action/Description
Discard Priority – Egress	Select one of the following options: *Mapped from DE* – (default) The value of the Discard Priority bit is used to set the CLP bit when the frame is segmented into cells. The mapping is done just before the frame is presented to the hardware for segmentation. The Discard/ Priority bit is a product of the ingress data stream's Discard Priority bit setting and whatever modifications are made to this bit due to rate enforcement processing. *Always 0* – The value of the CLP bit is always set to zero (0) for all cells transmitted on this trunk. *Always 1* – The value of the CLP bit is always set to 1 for all cells segmented from all frames transmitted on this trunk. ***Note:*** *Changing the value of this attribute does not admin down the logical port.*
Discard Priority – Ingress	Select one of the following options: *Mapped to DE* – (default) The value of the CLP bit received in the cells that make up the ingress frame is transferred directly to the internal Discard Priority bit. The Discard Priority bit is transferred with the frame to the egress card for subsequent transmission. If the egress packet format is Frame Relay, then the Discard Priority bit is included in the Q.922 header as the DE bit; if the egress packet format is ATM, then the CLP bit is set from the Discard Priority bit. *Not mapped* – The value of the Discard Priority bit is always set to zero (0), ignoring the CLP setting received in the frame. This setting is transferred to the egress card. ***Notes****: These Discard Priority settings are used by the rate enforcement and congestion control processing on the egress card. The egress card may change the Discard Priority bit due to congestion or rate enforcement.* *Changing the value of this attribute does not admin down the logical port.*
Congestion – Egress	Select one of the following options: *Mapped from FECN* – (default) The value of the forward explicit congestion notification (FECN) bit is used to set the EFCI bit when the frame is segmented into cells. The mapping takes place just before the frame is presented to the hardware for segmentation. *Always 0* – The value of the EFCI bit is always set to zero for all cells segmented from all frames transmitted on this trunk. ***Note:*** *Changing the value of this attribute does not admin down the logical port.*

Table 4-17. Set [Discard/Congestion Mapping] Attributes Fields (Continued)

Field	Action/Description
Congestion – Ingress	Select one of the following options: *Mapped to FECN* – (default) The value of the EFCI bit received in the cells that comprise the ingress frame is transferred directly to the FECN bit. The congestion bit is transferred with the frame to the egress card for subsequent transmission. If the egress packet format is Frame Relay, then the congestion bit is included in the Q.922 header as the FECN bit; if the egress packet format is ATM, then the EFCI bit is set from the congestion bit. Note that the egress card can modify the congestion bit due to congestion. *Always 0* – The value of the congestion bit is always set to zero (0), ignoring the setting of the EFCI bit in the cells that comprise the frame. This setting is forwarded to the egress card along with the frame. ***Note:*** *Changing the value of this attribute does not admin down the logical port.*

OPTimum Trunk VPI Range Attributes

Select Set [Opt Trunk VPI Range] Attributes and complete the field described in Table 4-18.

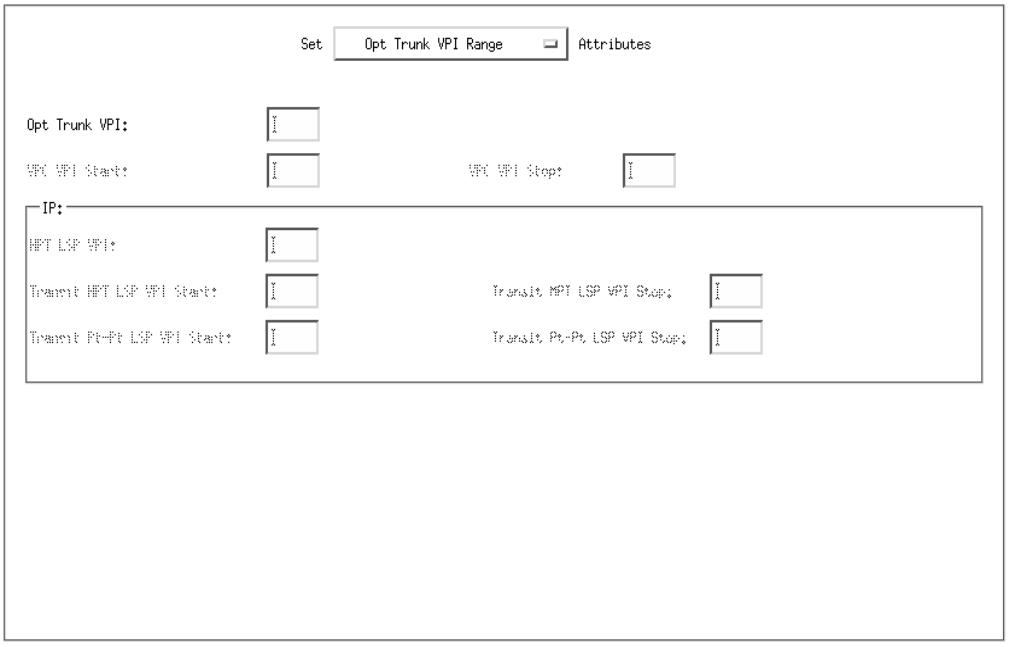


Figure 4-12. Set [Opt Trunk VPI Range] Attributes Fields

Table 4-18. Set [OPT Trunk VPI Range] Attributes Field

Field	Action/Description
Opt Trunk VPI	Enter a number from 0 – *nnnn* to identify the virtual path for the ATM logical port. This is the VPI used for all circuits routed over this OPTimum trunk. Entering a value of 0 (Zero) enables 4096 circuits to be routed over the trunk. The range of valid VPI values depends upon the number of valid VPI bits you set for the ATM UNI feeder port. For more information, see page 4-5.

When you finish setting these attributes, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

Defining ATM OPTimum Frame Trunk Logical Ports

To implement the ATM OPTimum frame trunk, first configure a UNI DTE feeder logical port on the same physical port. To configure an ATM OPTimum frame trunk, perform the following steps:

Step 1. Configure the physical port you want to use for the ATM OPTimum frame trunk (see the *B-STDX, CBX, and GX Switch Module Configuration Guide*).

Step 2. Configure a UNI DTE feeder logical port for the ATM OPTimum frame trunk on this physical port (page 4-14). Assign this logical port a minimum amount of bandwidth.

Step 3. Configure the ATM OPTimum frame trunk logical port on the same physical port. Assign the remaining bandwidth to this logical port.

Step 4. Configure the trunk (see Chapter 7, "Configuring Trunks").

To configure an ATM OPTimum frame trunk logical port:

1. Complete the Add Logical Port Type dialog box fields as follows:

   Service Type — Select ATM. The available ATM Logical Port Types appear.

   LPort Type — Select ATM OPTimum Frame Trunk.

   VPI — Enter a number from 0 – nnnn to identify the virtual path for the ATM logical port. This is the VPI used for all circuits routed over this ATM OPTimum frame trunk. Entering a value of 0 (zero) enables 4096 circuits to be routed over the trunk.

   The range of valid VPI values depends upon the number of valid VPI bits you set for the ATM UNI feeder port. For more information, see page 4-5.

   VCI — If this logical port resides on the ATM DS3/E3 UNI, enter a value from 32 to 255. Otherwise, enter a value in the range of 32 - xxx, where xxx is determined by the Number of Valid Bits in VCI setting on the feeder port (see page 4-5).

   Make sure the number you enter matches the VCI value of the equipment connected to this port. You may have received this value from the ATM network provider.

Note – You must provision a VPC in another ATM network between two Lucent switches. This VPC acts like a physical line. Specify the VPI of this VPC in the Virtual Path ID field.

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

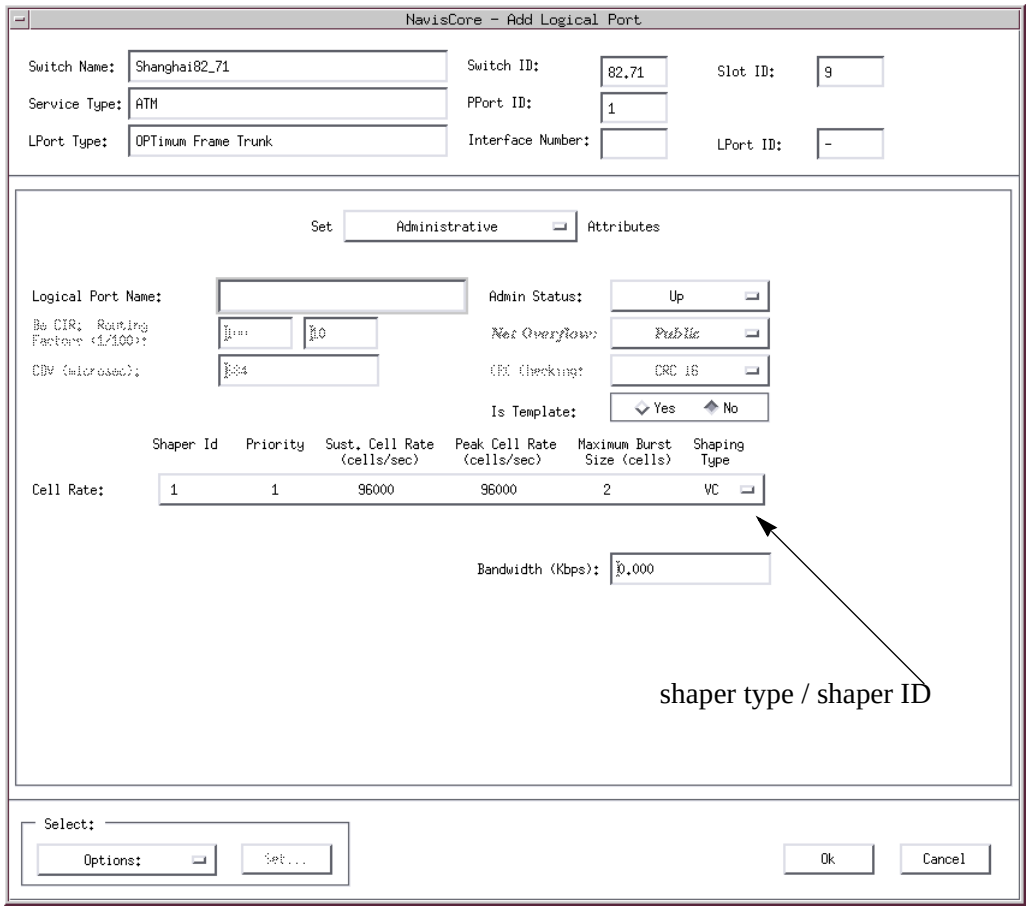


Figure 4-13. Add Logical Port Dialog Box (OPTimum Frame)

3. Select Set [Administrative] Attributes, and complete the fields described in Table 4-19.

Table 4-19. Set [Administrative] Attributes Fields (OPTimum Frame, ATM CS/IWU Card)

Field	Card Type	Action/Description
Logical Port Name	All	Enter an alphanumeric logical port name (up to 32 characters in length) to assign this port.
Admin Status	All	Set the Admin Status as follows: *Up* – (default) Activates the port. *Down* – Saves the configuration in the database without activating the port, or takes the port offline to run diagnostics.

Table 4-19. Set [Administrative] Attributes Fields (OPTimum Frame, ATM CS/IWU Card) (Continued)

Field	Card Type	Action/Description
Net Overflow	All	Set the Net Overflow parameters to one of two modes: *Public* – (default) Enables the circuit to use public trunks during traffic overflow or trunk failure conditions. *Restrict* – Restricts trunks to their own VPN. See "Configuring a Logical Port for Layer2 VPN" on page 11-7 for more information. ***Note:*** *Changing the value of this attribute does not admin down the logical port.*
Can Backup Service Names	All	*(Fault-tolerant PVC only)* To configure a logical port for backup service in a fault-tolerant PVC configuration, select Yes. For more information, see Chapter 12, "Configuring Fault-Tolerant PVCs".
Is Template	All	(*Optional*) Save these settings as a template to use again to quickly configure a logical port with the same options. To create a template, choose Yes. See "Using Templates" on page 2-21 for more information.
Shaper ID	CS/IWU	(*See Figure 4-13*) Choose a value from 1 through 16 to specify the Shaper ID and associated priority, sustainable cell rate, peak cell rate, and burst tolerance values. This list provides both VP and VC shaping attributes. Make sure you assign only one trunk logical port per shaper ID. Assigning more than one trunk logical port to a given shaper ID decreases circuit performance. For more information, see "Setting the Number of Valid Bits in VPI/VCI for B-STDX 8000/9000" on page 4-5.

Table 4-19. Set [Administrative] Attributes Fields (OPTimum Frame, ATM CS/IWU Card) (Continued)

Field	Card Type	Action/Description
Bandwidth (Kbps)	All	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth available on the port. If you are configuring more than one OPTimum frame trunk on this logical port, enter the appropriate amount of bandwidth for the ATM OPTimum frame trunk you are currently configuring. Remember to leave bandwidth for any remaining ATM OPTimum frame trunks you need to configure on this logical port.

If you are configuring an ATM DS3/E3 UNI module, Figure 4-13 on page 4-38 displays the following fields in place of the Shaping Type/Shaper ID. Complete the fields in Table 4-20. Then, continue with the instructions in Table 4-21 on page 4-42.

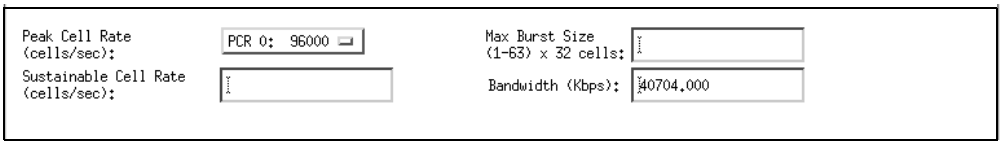


Figure 4-14. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS)

Table 4-20. Set [Administrative] Attributes Fields (ATM DS3 UNI PCR/SCR/MBS)

Field	Card/Logical Port Type	Action/Description
Peak Cell Rate (cells/sec)	ATM UNI DS3/E3	Select a PCR between 0 (zero) and 7. This value represents the maximum allowed cell transmission rate (expressed in cells per second). It defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
Sustainable Cell Rate (cells/sec)	ATM UNI DS3/E3	Specify the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. The SCR allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR traffic; it does not apply to CBR or UBR traffic.
Maximum Burst Size (cells)	ATM UNI DS3/E3	Specify the maximum number of cells that can be received at the peak cell rate (PCR). MBS allows a burst of cells to arrive at a rate higher than the SCR. If the burst is larger than anticipated, the additional cells are either tagged or dropped. This parameter applies only to VBR traffic; it does not apply to the CBR or UBR traffic.
Bandwidth (Kbps)	All	Enter the amount of bandwidth you want to configure for this logical port. The default is the amount of bandwidth available on the port. If you are configuring more than one OPTimum frame trunk on this logical port, enter the appropriate amount of bandwidth for the ATM OPTimum frame trunk you are currently configuring. Remember to leave bandwidth for any remaining ATM OPTimum frame trunks you need to configure on this logical port.

See Table 4-21 to continue this configuration.

Table 4-21. Configuring OPTimum Frame Trunk Attributes

For 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 cards see...	For frame-based cards see...
"Discard/Congestion Mapping Attributes" on page 4-33	"Trap Control Attributes" on page 4-20
	"Priority Frame Attributes" on page 4-22

When you finish setting these attributes, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

Defining ATM Network Interworking for Frame Relay NNI Logical Ports

Before you configure an ATM Network Interworking for FR NNI logical port, first configure an ATM UNI DTE feeder logical port with a minimal amount of bandwidth on the same physical port.

To define an ATM Network Interworking for FR NNI logical ports:

1. Complete the Add Logical Port Type dialog box fields as follows:

   Service Type — Select ATM.

   LPort Type — Select ATM Network Interworking for FR NNI.

   VPI — Enter the VPI of the ATM VCC that carries the NNI data.

   VCI — Enter the VCI of the ATM VCC used to carry the NNI data. (NNI is a single ATM circuit that can be used to carry a single Frame Relay circuit or many Frame Relay circuits multiplexed over a single ATM circuit.)

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

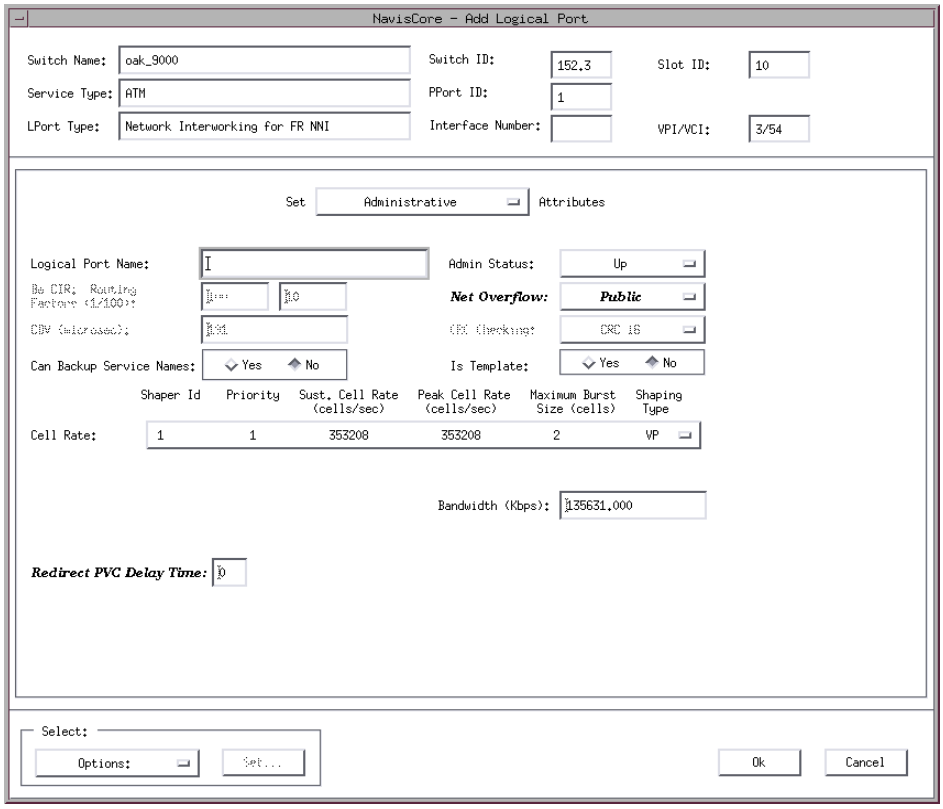


Figure 4-15. Add Logical Port Dialog Box (ATM CS/IWU)

Select [Set Administrative] Attributes, and complete the fields described in Table 4-22.

Table 4-22. Configuring Network Interworking for Frame Relay NNI Attributes

For 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 cards see...	For frame-based cards see...
"Administrative Attributes" on page 4-15	"Administrative Attributes" on page 4-29
"Link Mgmt Attributes" on page 4-44	"Congestion Control Attributes" on page 4-18
"Trap Control Attributes" on page 4-20	"Link Mgmt Attributes" on page 4-44
"Discard/Congestion Mapping Attributes" on page 4-48	"Trap Control Attributes" on page 4-20
	"Priority Frame Attributes" on page 4-22

When you finish setting these attributes, continue with the section, "Completing the Logical Port Configuration" on page 4-50.

Link Mgmt Attributes

Select Set [Link Mgmt] Attributes and complete the fields described in Table 4-23.

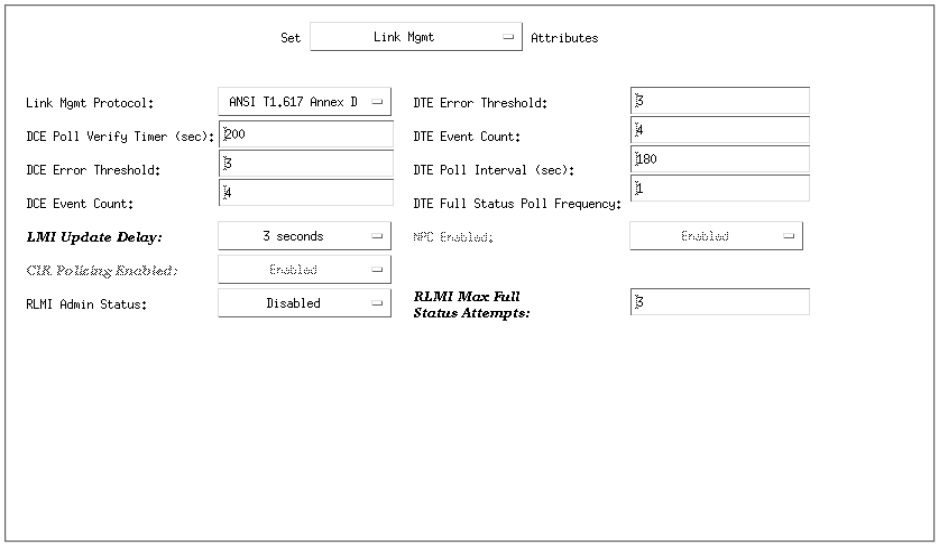


Figure 4-16. Set Link Mgmt Attributes Fields

Table 4-23. Set Link Mgmt Attributes Fields

Field	Action/Description
Link Mgmt Protocol	Select the link management protocol used by the Frame Relay equipment connected to this port. Options include: *ANSI T1.617 Annex D* – (default) The network uses DLCI 0 for link management. *LMI Rev1* – The network uses DLCI 1023 for link management. *CCITT Q.933 Annex A* – For international standard (European) use only. The network uses DLCI 0 for link management. *Auto Detect* – Use this option only if the attached customer premise equipment (CPE) provides the link management protocol. This logical port can then automatically detect which protocol is in use. *Disabled* – Use this option only if the attached CPE does not support link management or to disable link management for troubleshooting purposes. If you disable LMI, you cannot enable RLMI.

Table 4-23. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
DCE Poll Verify Timer (sec)	Specify the value of the T392 timer, which sets the length of time the network should wait between status inquiry messages. If the network does not receive a status inquiry message within the number of seconds you specify, the network records an error. The default value is 200 seconds. Increase this value if the DTE device has a poll frequency that is greater than or equal to the DCE Poll Verify Timer. Decrease this value if the DTE's poll frequency is less than or equal to 1/2 of the DCE poll verify timer.
DCE Error Threshold	Specify the DCE error threshold (392). This parameter is used with the DCE Events Count (N393) parameters. The Local Management protocol monitors the number of events you specify for the DCE Event Count. If the number of events found in error exceeds the DCE Error Threshold you specify, the link is declared inactive. The default value is 3.
DCE Event Count[1]	Specify the DCE event count. This field specifies the number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or invalid status inquiry message or expiration of the T392 timer. For example, use the default DCE Error Threshold value of three and the default DCE Event Count value of four. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.
LMI Update Delay	Set a timer from 1 to 9 seconds to enable asynchronous LMI updates. The default is three (3) seconds. When you set this timer, the switch sends a signal (known as an *event*) to notify other customer premise equipment (CPE) when a circuit on this logical port goes up or down. The specified time interval creates a buffer. If the circuit recovers within this period of time, no event is issued. • If you choose *No Updates*, the switch does not send a signal to the CPE. • If you choose *No Delay*, the switch sends an update immediately to the CPE. For example, if the network takes a significant amount of time to recover from trunk outages, increase the LMI update delay. This delay minimizes network downtime visibility to end-users. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

Table 4-23. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
DCE Poll Verify Timer (sec)	Specify the value of the T392 timer, which sets the length of time the network should wait between status inquiry messages. If the network does not receive a status inquiry message within the number of seconds you specify, the network records an error. The default value is 200 seconds. Increase this value if the DTE device has a poll frequency that is greater than or equal to the DCE Poll Verify Timer. Decrease this value if the DTE's poll frequency is less than or equal to 1/2 of the DCE poll verify timer.
DCE Error Threshold	Specify the DCE error threshold (392). This parameter is used with the DCE Events Count (N393) parameters. The Local Management protocol monitors the number of events you specify for the DCE Event Count. If the number of events found in error exceeds the DCE Error Threshold you specify, the link is declared inactive. The default value is 3.
DCE Event Count[1]	Specify the DCE event count. This field specifies the number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or invalid status inquiry message or expiration of the T392 timer. For example, use the default DCE Error Threshold value of three and the default DCE Event Count value of four. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.
LMI Update Delay	Set a timer from 1 to 9 seconds to enable asynchronous LMI updates. The default is three (3) seconds. When you set this timer, the switch sends a signal (known as an *event*) to notify other customer premise equipment (CPE) when a circuit on this logical port goes up or down. The specified time interval creates a buffer. If the circuit recovers within this period of time, no event is issued. • If you choose *No Updates*, the switch does not send a signal to the CPE. • If you choose *No Delay*, the switch sends an update immediately to the CPE. For example, if the network takes a significant amount of time to recover from trunk outages, increase the LMI update delay. This delay minimizes network downtime visibility to end-users. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

Table 4-23. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
RLMI Admin Status (1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 *modules*)	Enables or disables the RLMI administrative state. *Enabled* – Enables Resilient LMI. If you enable RLMI on a Frame Relay UNI DTE or NNI port, you can configure the RLMI Max Full Status Attempts. If you enable RLMI, you cannot set LMI to Disabled. *Disabled* – (default) Disables Resilient LMI. ***Notes**: You cannot disable RLMI or delete a logical port if the logical port is configured in an RLMI service name binding. If the lport is configured as a member of a "Master" RLMI service name binding, you can change the lport type to Frame Relay UNI DTE or NNI. If the lport is configured as a member of a "Slave" RLMI service name binding, you can change the lport type to Frame Relay UNI DCE or NNI.* *Changing the value for this attribute does not admin down the logical port.* See Chapter 13 for more information about RLMI.
DTE Error Threshold	Specify an error threshold (N392). This parameter is used with the DTE Events Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DTE Event Count. If the number of events found in error exceeds the specified DTE Error Threshold, the link is declared inactive. The default value is 3.
DTE Event Count	Specify the number of events in a sliding window of events monitored by the network. The default is 4. An event is the receipt of a valid or invalid status message or expiration of the T391 timer. For example, use the default DTE Error Threshold value of 3 and the default DTE Event Count value of 4. If three (N392) of the last four (N393) events are bad, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.
DTE Poll Interval (sec)	Specify the number of seconds between the transmission of status inquiry messages (T391). Set the DTE poll interval to a value that is less than the DCE poll verify timer on the attached device. (This value must be greater than 1/2 the value of the DCE poll verify timer.) The default is 180 seconds for one-to-one mapping.
DTE Full Status Poll Frequency	Specify the number of T391 polling cycles between full status inquiry messages. Reduce this value to absorb more bandwidth, since the more frequent full status requests increase overhead. The default value is 1 for one-to-one mapping.

Table 4-23. Set Link Mgmt Attributes Fields (Continued)

Field	Action/Description
RLMI Max Full Status Attempts (1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 *modules*)	The number of LMI full status inquiry attempts used to bring up the working interface. The default is 3 attempts. Enter a value greater than 0 (zero). See Chapter 13 for more information about RLMI. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

[1] The DCE/DTE Error Threshold and the DCE/DTE Event Count work together. The lower you set these values, the more sensitive the logical port is to LMI poll errors. To make the logical port less sensitive to errors, increase these values.

Discard/Congestion Mapping Attributes

The Set Discard/Congestion Mapping Attributes menu enables you to select discard and congestion priority bit mappings on data sent to and from the logical port. Egress mapping takes place just before the ATM interface transmits the data; ingress mapping takes place after the ATM interface receives the data. These options provide support for configurable mapping of the DE/CLP and FECN/EFCI bits.

Select Set [Discard/Congestion Mapping] Attributes and complete the fields described in Table 4-24 on page 4-49.

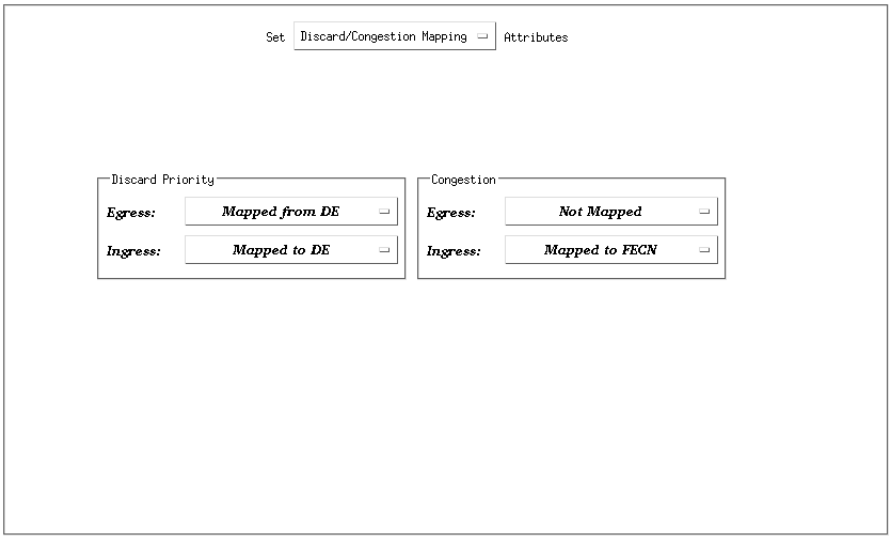


Figure 4-17. Set Discard/Congestion Mapping Attributes Fields

Table 4-24. Set Discard/Congestion Mapping Attributes Fields

Field	Action/Description
Discard Priority – Egress	Select one of the following options: *Mapped from DE* – (default) The value of the Discard Priority bit is used to set the CLP bit when the frame is segmented into cells. The mapping is done just before the frame is presented to the hardware for segmentation. The Discard Priority bit is a product of the ingress data stream's Discard Priority bit setting and whatever modifications are made to this bit due to rate enforcement processing. *Always 0* – The value of the CLP bit is always set to 0 (zero) for all cells transmitted on this trunk. *Always 1* – The value of the CLP bit is always set to 1 for all cells segmented from all frames transmitted on this trunk. ***Note:*** *Changing the value for this attribute does not admin down the logical port.*
Discard Priority – Ingress	Select one of the following options: *Mapped to DE* – (default) The value of the CLP bit received in the cells that make up the ingress frame is transferred directly to the internal Discard Priority bit. The Discard Priority bit is transferred with the frame to the egress card for subsequent transmission. If the egress packet format is Frame Relay, then the Discard Priority bit is included in the Q.922 header as the DE bit; if the egress packet format is ATM then the CLP bit is set from the Discard Priority bit. *Not mapped* – The value of the Discard Priority bit is always set to 0 (zero), ignoring the CLP setting received in the frame. This setting is transferred to the egress card. ***Notes****: These Discard Priority settings are used by the rate enforcement and congestion control processing on the egress card. The egress card may change the Discard Priority bit due to congestion or rate enforcement.* *Changing the value for this attribute does not admin down the logical port.*
Congestion – Egress	Set to *Not mapped*. The value of the EFCI bit is always set to 0 (zero) for all cells segmented from all frames transmitted on this trunk.
Congestion – Ingress	Set to *Mapped to FECN*. The value of the EFCI bit received in the cells that comprise the ingress frame is transferred directly to the internal Congestion bit (FECN bit). The Congestion bit is transferred with the frame to the egress card for subsequent transmission. If the egress packet format is Frame Relay, then the Congestion bit is included in the Q.922 header as the FECN bit; if the egress packet format is ATM, then the EFCI bit is set from the Congestion bit. Note that the egress card can change the Congestion bit due to congestion.

Completing the Logical Port Configuration

Use the following steps to complete the logical port configuration:

1. (*Optional*) To configure this logical port for a specific Layer2 VPN and customer, see "Configuring a Logical Port for Layer2 VPN" on page 11-7.
2. (*Optional*) If this is an ATM UNI, ATM OPTimum Cell Trunk, or ATM Direct Cell Trunk logical port type on a 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 card, you can configure QoS parameters.

   From the Add Logical Port dialog box, use the Select: Options: menu to select QoS. Choose Set.

   See "Setting Quality of Service Parameters" on page 3-44 for more information.
3. Choose OK. The Set All Logical Ports in PPort dialog box reappears (Figure 3-1 on page 3-4).
4. Choose Close to return to the Set Physical Port Attributes dialog box. Then choose Cancel to return to the Switch Back Panel dialog box.

Configure the remaining logical ports for this physical port. See the instructions in this chapter for the specific type of logical port you want to add.

- When you finish configuring a DTE logical port, you can add either an ATM OPTimum cell trunk logical port or an ATM OPTimum frame trunk logical port.
- To configure logical ports on another physical port, select the port, then see the appropriate section for the logical port type you want to configure.
- After you configure both logical port endpoints for a trunk, you can add the trunk line connection between them. See Chapter 7, "Configuring Trunks," for more information.
- After you configure both endpoints of an ATM UNI logical port connection, you can add PVCs between the logical port endpoints. See Chapter 8, "Configuring ATM PVCs," for more information.

5

About the ATM Flow Control Processor (FCP)

The ATM Flow Control Processor (FCP) is an optional feature that supports ATM traffic management through binary, hop-by-hop, closed-loop flow control algorithms that shift network congestion to the edge of the network. In addition, the FCP uses several per-virtual circuit (VC) cell/packet queuing and discarding mechanisms for additional network congestion control.

Based on the ATM Forum's *Traffic Management Specification, Version 4.0*, the ATM FCP delivers a fair, deterministic service for bursty ATM traffic, including:

- Dynamically adjusting the allowable cell rate (ACR) in response to resource management (RM) cell feedback
- Reducing congestion in the network by adjusting the data rate at which a VC sends cells
- Fair resource allocation based on the minimum cell rate (MCR)
- Per-VC queuing with early packet discard/partial packet discard (EPD/PPD) capability

Modules Supported

The FCP is available on the following CBX 500 I/O modules:

- 8-Port T1 and E1 modules
- 8-Port DS3 and E3 ATM UNI modules
- 4-Port ATM UNI OC-3c/STM-1 module
- 1-Port OC-12c/STM-4 module
- 3-Port Channelized DS3/1 IMA module

Note – Contact a qualified Lucent organization for network design validation before enabling the FCP.

Supported ATM Service Classes

The ATM FCP manages traffic in the unspecified bit rate (UBR), available bit rate (ABR), and variable bit rate-non-real time (VBR-NRT) service classes by applying:

Closed-loop flow control — See "Closed-Loop Flow Control" on page 5-5 for more information.

Dynamic cell rate adjustment — The Allowed Cell Rate (ACR) is adjusted by the rate increase factor (RIF) and the rate decrease factor (RDF). The RDF and RIF can be configured in proportion to the MCR. Refer to "Allowed Cell Rate" on page 5-14 for more information about configuring the RDF and RIF.

MCR guarantee — The MCR guarantee varies by Quality of Service (QoS) class as follows:

- *Unspecified Bit Rate (UBR) Class* – The MCR is set at a rate of 100 cells per second. Note that UBR is a best effort service, and cannot be guaranteed.
- *Available Bit Rate (ABR) Class* – The MCR is set during circuit configuration.
- *Variable Bit Rate-Non-Real Time (VBR-NRT) Class* – The sustainable cell rate (SCR) is configured during circuit admission. The SCR is used in the same way as the MCR during ACR adjustments.

Note – The ATM FCP can manage the VBR-NRT QoS class. The management of VBR-NRT is a configurable parameter through NavisCore.

ATM FCP Architecture

The ATM FCP provides per-VC queuing, and supports the CBX 500 quad-plane buffer architecture. Figure 5-1 shows the ATM FCP output buffers relative to the CBX 500 IOM quad-plane output buffers.

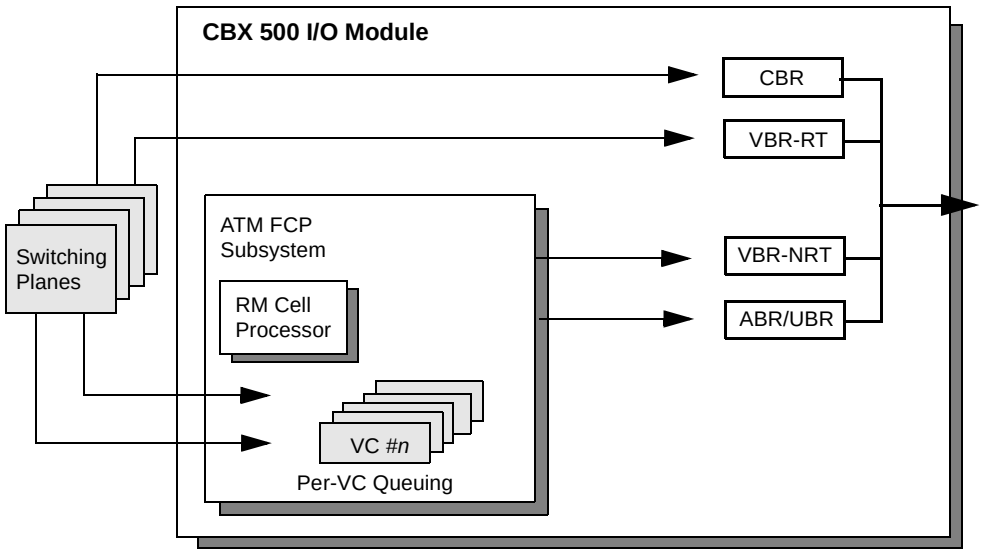


Figure 5-1. CBX 500 Queues and the ATM FCP

Cells from the CBX 500 switching fabric are transmitted through the ATM FCP to the IOM output buffer. Note that the ATM FCP only manages non-real time traffic.

In the FCP, cells are queued and dequeued based on the configured rate for the VC. Each VC is subject to discard mechanisms. Cells entering the output CBX 500 quad-plane queues are transmitted in the same manner as on an IOM that does not have an FCP.

Closed-Loop Flow Control

Lucent's closed-loop, flow control architecture is based on hop-by-hop control loops with binary feedback. The hop-by-hop control loops push congestion at central nodes to switches at the edge of the network, thereby providing more efficient use of network bandwidth. In addition, with less network congestion at central nodes, there is increased network throughput.

Flow Control Mechanisms

The ATM FCP supports three closed-loop, flow control mechanisms:

Cascade Communications Resource Management (CCRM) Cells — A subset of the ABR RM cells described in the ATM Forum's *ATM Traffic Management Specification, Version 4.0*. The Protocol ID field in each RM cell is defined as the CCRM ID, indicating that it is a CCRM cell. The default value for the CCRM ID is always set at a value of 6 and cannot be modified. Refer to "Enabling the FCP" on page 6-2 for more information about CCRM cells.

Backward Congestion Message (BCM) Cells — Provide a different RM cell mechanism and may also provide interoperability with non-Lucent ATM switches. The Protocol ID field in each BCM cell is defined as the BCM ID. The default value for the BCM ID is always set at a value of 5 and cannot be modified. Refer to "Enabling the FCP" on page 6-2 for more information about BCM cells.

Note – Because the FCP communicates with both CCRM and BCM cells for hop-by-hop control loops, CCRM and BCM cells are both configured within a single network to allow for conversion between one closed-loop, flow control algorithm to another.

Available Bit Rate (ABR) RM Cells — The Protocol ID for an ABR RM cell is one (1). The ATM FCP identifies any RM cell with a Protocol ID of 1 as an ABR RM cell. ABR RM cells received by a Lucent switch will be passed transparently through the network.

RM Cell Generation

Any port on an IOM can generate CCRM and BCM cells and can be configured to *not* generate RM-type cells (the No Loop option). These types of cells let you configure different closed-loop, flow control algorithms on the same IOM.

Note – Because RM cells are generated in the backward direction, the type of RM cells generated depends on the configuration of the logical port through which they are transmitted.

In general, RM-type cells can be generated at 30 to 250 millisecond (msec) intervals per VC. The default value for this parameter is 100 msec.

RM Cell Termination

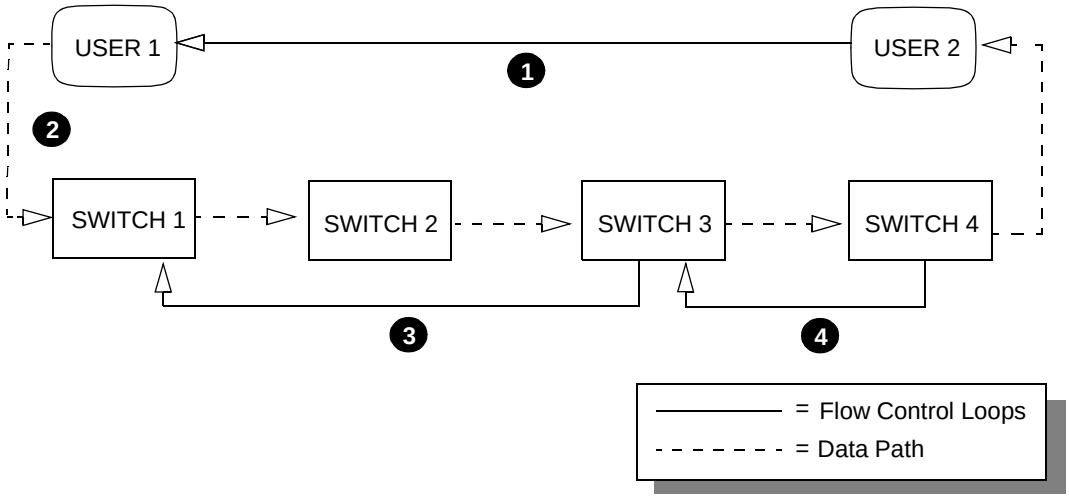
RM cells generated by other vendors are passed through Lucent switches transparently. Other vendors may have implementations of the ATM Forum Traffic Management 4.0 standard that can conflict with Lucent's implementation of this standard. Other vendors can set the Protocol ID to any number between 1-255.

RM cells are terminated by Lucent switches under the following conditions:

- If the RM cell received is a backward RM cell, has a Protocol ID of 5, and is transversing a Virtual Circuit (VC), then it is designated as a BCM cell and may be terminated.
- If the RM cell received is a backward RM cell, has a Protocol ID of 6, and is transversing a Virtual Circuit (VC), then it is designated as a CCRM cell and may be terminated.
- For RM cells that are traversing a Virtual Path (VP), the above conditions apply if the VCI of the RM cell is 6.

If any of the above conditions are not met, the RM cell will be passed through the network transparently.

Figure 5-2 shows hop-by-hop, closed-loop flow control between four CBX 500 switches. The flow control loops are shown as solid lines. The data paths are shown as dotted lines.



1 End-to-End User Control Loops

End-to-end user flow control loops are “outer” loops. The switches do not change their cell rates in response to this flow control loop. Rather, they mark the congestion indication (CI) and no increase (NI) bits based on the local congestion state, as defined in the ATM Forum’s *Traffic Management Specification*, *Version 4.0*.

2 Different Logical Port Types on the Same I/O Module

The ATM FCP supports different types of flow control loops on the same I/O module. USER 1 has a user-to-network interface (UNI) connection. SWITCH 2 has a trunk connection to a different port on the same I/O module in SWITCH 1. Enabling and disabling of loop control is provisioned per port.

3 Switches Without Flow Control Loops

SWITCH 2 does not generate or terminate flow control loops to the other switches. SWITCH 2 generates a forward notification of congestion to SWITCH 3. Explicit forward congestion indication (EFCI) marking can be configured on a CBX 500 switch through NavisCore. When SWITCH 2 marks EFCI in the data cells, SWITCH 3 can be configured to include EFCI notification in the decision of the backward notification to SWITCH 1.

4 Rate Control at the Output Switch

SWITCH 4’s cell rate fills the available bandwidth and is adjusted based on local congestion. The flow control loop between SWITCH 4 and USER 2 can be configured as either BCM or CCRM termination. If configured as BCM, SWITCH 4 will adjust rates according to the port congestion. If configured as CCRM, SWITCH 4 will perform traffic shaping to the initial cell rate (ICR) of each VC.

Figure 5-2. Closed-Loop Flow Control

CCRM Closed-Loop Flow Control

Lucent's closed-loop, flow control architecture can use CCRM cells to notify other FCPs of network congestion or availability. CCRM cells are normally generated at the RM cell generation rate if the circuit is active.

CCRM Closed-Loop Flow Control on a Trunk

Figure 5-3 shows an example of CCRM closed-loop flow control between two CBX 500 switches.

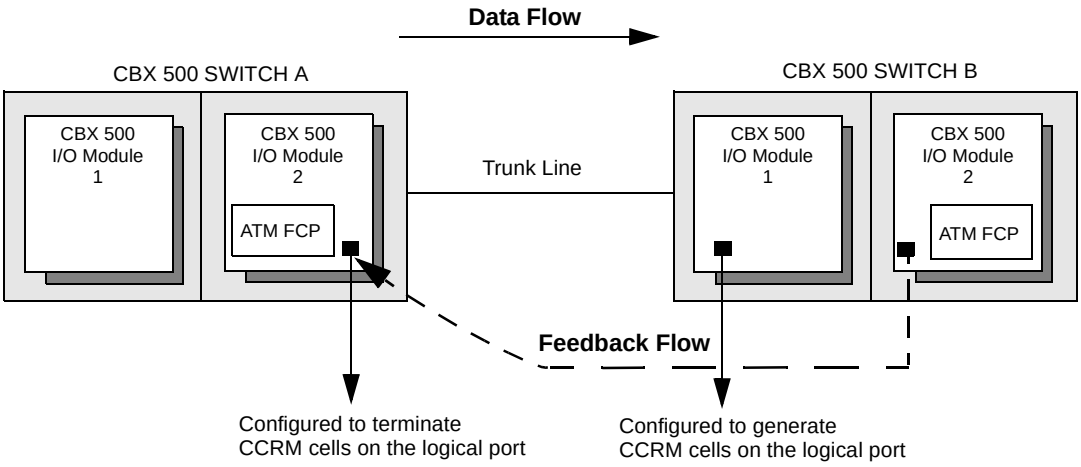


Figure 5-3. CCRM Closed-Loop Flow Control

On Switch B, the FCP in IOM 2 generates RM cells to control the rate of data transmitted by IOM 2 on Switch A. IOM 2 on Switch B also determines the type of RM cell to generate by looking at the logical port setting on IOM 1 on Switch B.

CCRM Closed-Loop Flow Control on a UNI (Traffic Shaping)

For information on CCRM Closed-Loop Flow Control on a UNI, see "Per-VC Traffic Shaping" on page 5-15.

CCRM Cell Generation

Any port on an IOM can generate CCRM cells. CCRM cells are generated at the RM cell generation rate.

When a CCRM cell is generated:

- The direction (DIR) and backward indicator (BI) bits are set, indicating that this is a switch-generated backward RM cell.
- The congestion indication (CI) and no increase (NI) bits are set according to the current congestion status of the VC.

The destination ATM switch periodically sends backward binary notification through CCRM cells to the source ATM switch, indicating the state of the destination ATM switch's queue for a VC. The binary notification is reflected in the CI and NI bits of the CCRM cell. The CCRM cell indicates either a cell rate increase or decrease. The source ATM switch then responds by adjusting the cell rate accordingly for that VC and terminates the CCRM cell.

CCRM Cell Termination

When you configure the FCP to terminate CCRM cells, the FCP decides whether or not to increase or decrease the ACR. This decision is based upon one or more of the following:

- The local port congestion state
- The current ACR being above the fair bandwidth for the VC
- The CI and NI state in the CCRM cell

The fair bandwidth for a VC is the proportional allocation of the total bandwidth for managed (non-real time) circuits. This allocation is based on the MCR of the VC relative to all of the managed VCs. The total, non-real time bandwidth is the total port bandwidth, less the bandwidth allocated to unmanaged (real-time) circuits and PMP non-real time circuits.

Note that the FCP can increase the ACR well beyond its fair bandwidth. Once other circuits attempt to use that bandwidth (which causes a congestion condition), the FCP will throttle back the ACR towards the fair bandwidth for the circuit until the congestion condition is removed.

For general RM cell termination considerations, see "RM Cell Termination" on page 5-6.

BCM Closed-Loop Flow Control

The FCP can also use a BCM closed-loop, flow control algorithm. Unlike CCRM cells, BCM cells only indicate cell rate decreases. BCM cells are sent at periodic intervals only when congestion exists.

BCM Closed-Loop Flow Control on a Trunk

Figure 5-4 shows an example of BCM closed-loop flow control between two CBX 500 switches.

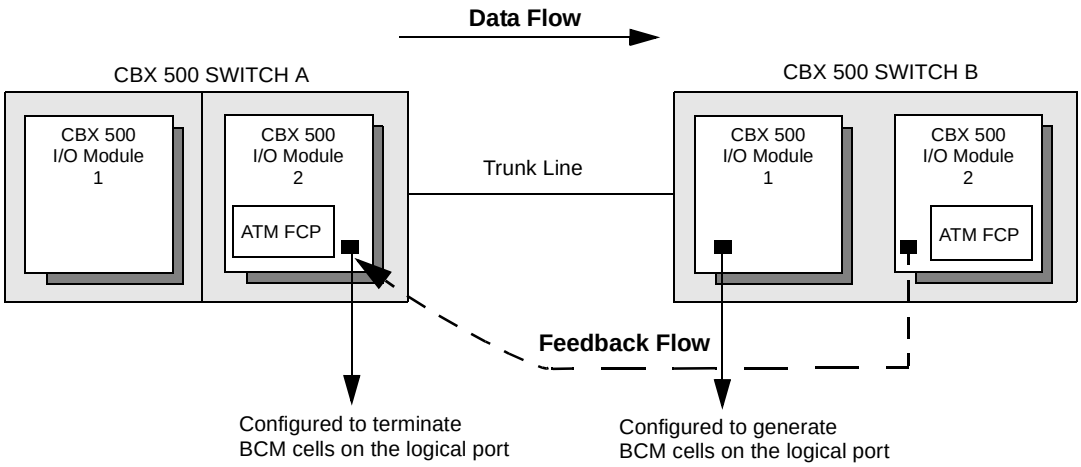


Figure 5-4. BCM Closed-Loop Flow Control

On Switch B, the FCP in IOM 2 generates RM cells to control the rate of data transmitted by IOM 2 on Switch A. IOM 2 on Switch B also determines the type of RM cell to generate by looking at the logical port setting on IOM 1 on Switch B.

BCM Closed-Loop Flow Control on a UNI

You can configure an output UNI logical port to allow FCP-managed VCs using that logical port to adjust their cell rates to use the available non-real time bandwidth. This is done by setting the RM termination type on that logical port to BCM, as shown in Figure 5-5.

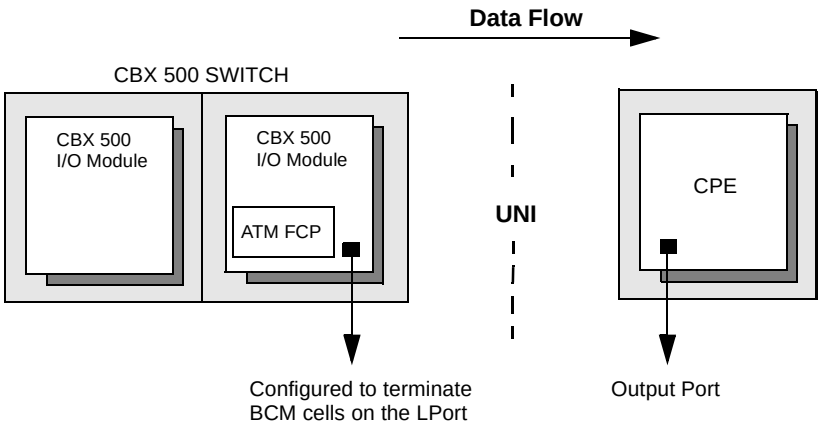


Figure 5-5. Output UNI Logical Port RM Termination

Because the logical port does not receive any BCM cells from the customer premise equipment (CPE), the ACR of the VCs keeps increasing until the logical port becomes congested. The ACR will increase fairly, corresponding to the RIF and PCR values of the VCs. See Table 6-2 on page 6-8 for information on setting the RM Cell Termination attribute.

BCM Cell Generation

You can configure any port on an IOM to generate BCM cells. If you select the BCM generation option when configuring the ATM FCP, BCM cells are only generated when the port is congested. See "Enabling the FCP" on page 6-2 for information on configuring the BCM generation option.

BCM Cell Termination

When you configure the FCP to terminate BCM cells, the FCP decides whether to increase or decrease the ACR. This decision is based upon one or more of the following conditions:

- The local port congestion state
- The current ACR being above the fair bandwidth for the VC
- Whether or not any BCM cells were received within the RM cell generation interval

Note – If BCM cells are received, but the port is not configured for BCM termination, the BCM cells are forwarded.

The fair bandwidth for a VC is the proportional allocation of the total bandwidth for managed (non-real time) circuits, based on the MCR of the VC relative to all of the managed VCs. The total, non-real time bandwidth is the total port bandwidth, less the bandwidth allocated to unmanaged (real-time) circuits and point-to-point NRT circuits.

Note that the FCP can increase the ACR well beyond its fair bandwidth. Once other circuits attempt to use that bandwidth (which causes a congestion condition), the FCP will throttle back the ACR towards the fair bandwidth for the circuit until the congestion condition is removed.

For general RM cell termination considerations, see “RM Cell Termination” on page 5-6.

ABR RM Closed-Loop Flow Control

ABR RM closed-loop flow control is an additional flow-control loop for switches that generate ABR RM cells. Because the ABR RM flow-control loop is an end-to-end loop, the CBX 500 does not generate or terminate ABR RM cells. The FCP forwards the ABR RM cells through the network transparently.

Cell Rate Adjustment

The ATM FCP performs rate adjustments on each circuit that it manages by distributing the available bandwidth fairly among the managed circuits. A circuit is initially granted an Initial Cell Rate (ICR); its rate is then adjusted continuously. The rate at any given time is referred to as the allowed cell rate (ACR).

Initial Cell Rate (ICR) and ICR Constant

When a VC initially becomes active, its ACR is set to its ICR. The ICR for a VC is determined by its peak cell rate (PCR), minimum cell rate (MCR), and initial cell rate (ICR) Constant.

The ICR Constant is configurable through NavisCore. The default value is 0 (zero). The following formula shows how to calculate the ICR:

$$ICR = MCR + \frac{PCR - MCR}{2^{ICR\ CONSTANT}}$$

See Table 6-1 on page 6-3 for information on configuring the ICR Constant.

Idle Circuits and Idle VC Factor

A circuit transitions from an active to an idle state when no data cells are received for that circuit for a period of time. This time period is determined by multiplying the Idle VC Factor by the RM cell generation interval.

The specified number of RM cell generation intervals that cause a VC to go idle (called the Idle VC Factor) is configurable through NavisCore. The default value for the Idle VC Factor is 8, meaning the Idle VC time-out period is 800 ms. See Table 6-1 on page 6-3 for information about configuring the Idle VC Factor and RM cell generation interval.

Note – If no cells are received for a specified number of RM cell intervals, the VC is marked “idle,” and the ACR is set back to the ICR. RM cells are not generated for idle VCs.

Allowed Cell Rate

The FCP continuously adjusts the allowed cell rate (ACR) of the circuits.

The VC cell rate is increased according to the following formula:

$$ACR = ACR + (RIF \times PCR)$$

Where: $1/32768 \leq RIF \leq 1$

The ACR is upper-bounded by the PCR.

Note – The PCR used may be one of the following: the PCR configured for this VC or the smallest logical port bandwidth through which the VC is routed. The option that has the smallest value is used as the PCR.

The VC cell rate is decreased according to the following formula:

$$ACR = ACR - (RDF \times ACR)$$

Where: $1/32768 \leq RDF \leq 1$

The ACR is lower-bounded by the MCR. Table 5-1 lists the minimum allocated MCR for ABR and UBR circuits.

Table 5-1. Cell Scheduling

Port Bandwidth	Max. Port Cell Rate (cells/sec)	Max. Number of Circuits (connections/port)	Min. Allocated MCR (cells/sec)
OC-12	1412830	16K	256
OC-3	353207	4K	88
DS3	96000	2K	55
E3	80000	2K	40
DS1	3622	2K	8
E1	4528	2K	8

Rate Profile Tables

You can load four rate profile tables into the ATM FCP. The ATM FCP uses these tables to determine the Rate Increase Exponent (RIE) and the Rate Decrease Exponent (RDE) for each VC on a port. These, in turn, are used to compute the RIF and the RDF. The RIE and RDE values for any VC are obtained from indexing the corresponding rate profile table with the VC's MCR class. The MCR (SCR for VBR-NRT VCs) of any VC is mapped to one of 256 MCR classes. See "MCR Class Mappings" on page D-4 for information about MCR classes.

For information on downloading the tables using NavisCore, see "Downloading Buffer Threshold and Rate Profile Tables" on page 6-5.

The RIE and RDE are defined as follows:

Rate Increase Exponent (RIE) — The RIE is a configurable value that is the negative exponent for the RIF calculation ($RIF=2^{-RIE}$). For example, an RIE of 3 translates to an RIF of 1/8. The RIE must be less than 16.

Rate Decrease Exponent (RDE) — The RDE is a configurable value that is the negative exponent for the RDF calculation ($RDF=2^{-RDE}$). For example, a value of 3 translates to an RDF of 1/8. The RDE must be less than 16.

Per-VC Traffic Shaping

You can configure the ATM FCP to perform traffic shaping by turning off the control loop for VCs on a trunk or UNI port that is managed by the ATM FCP. For any direction of data flow, you configure the output logical port that will perform shaping to terminate CCRM cells. In addition, you need to configure the connected logical port (for shaping on a trunk) to *not* generate RM cells (the No Loop option). For a UNI port to perform traffic shaping, the connected CPE should not generate CCRM cells back to the FCP. See Table 6-2 on page 6-8 for information about configuring RM cell termination settings.

VCs are shaped at their ICR. Because control loops are disabled, the ACR will stay at the ICR if non-real time bandwidth is available.

See "Initial Cell Rate (ICR) and ICR Constant" on page 5-13 for a description of the ICR calculation.

ATM FCP Queues

The ATM FCP provides per-VC queueing. Per-VC queuing provides independent buffer allocation to each VC, thereby isolating congestion on one VC from other VCs. Each per-VC queue has two configurable thresholds:

- Local congestion threshold
- Local discard threshold

The local congestion and discard thresholds for a specific VC are obtained by indexing the congestion and discard profile tables with the MCR class of the VC. The MCR class of the VC is obtained from its MCR (or SCR for VBR-NRT circuits). See "MCR Class Mappings" on page D-4 for information about MCR classes.

For information on downloading the tables using NavisCore, see "Downloading Buffer Threshold and Rate Profile Tables" on page 6-5.

In addition to the local thresholds, each port on an FCP-enabled IOM is assigned the following:

- Global congestion threshold
- Global discard threshold
- Global cell loss priority 0+1 (CLP0+1) threshold

You can configure these global thresholds as ATM FCP attributes for a logical port. The EFCI attribute sets the global congestion threshold, The Discard attribute sets the global discard threshold, and the CLP0+1 attribute sets the global cell loss priority 0+1 threshold. See Table 6-2 on page 6-8 for details about configuring these attributes.

Both local and global thresholds are used for congestion notification and discarding. A VC is considered congested only if its local queue is above the local congestion threshold, and the global queue on the port is above the global congestion threshold.

Similarly, a VC enters a discard state only if the local queue length is greater than the local discard threshold, and the port queue length is greater than the global discard threshold.

Figure 5-6 shows the five ATM FCP buffer thresholds.

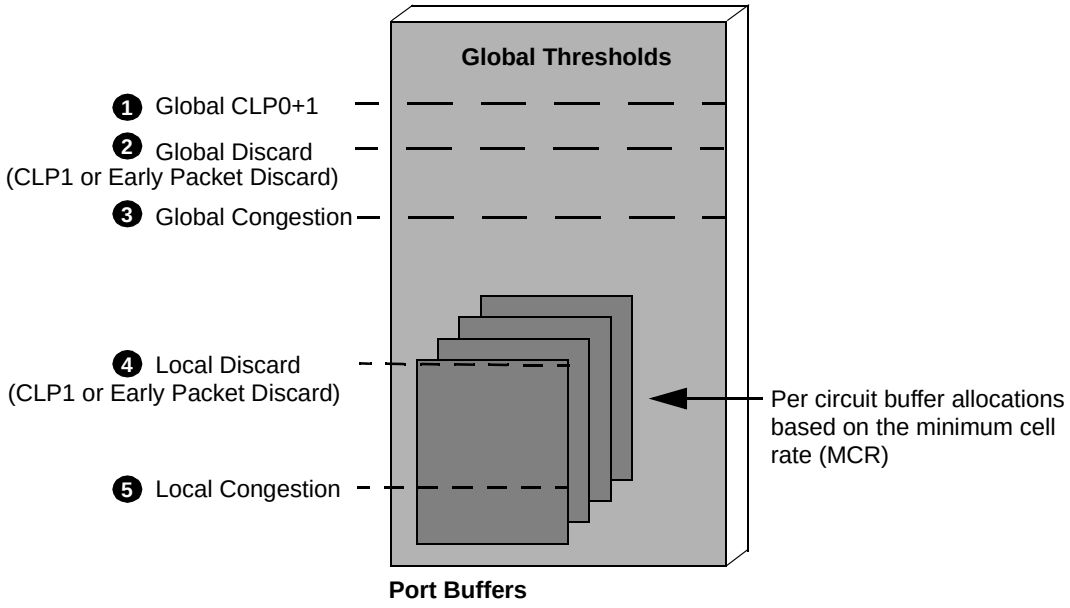


Figure 5-6. ATM FCP Buffers

The buffer space between the Global Discard and Global CLP0+1 thresholds allows the VCs on this port to continue to queue cells after the Global Discard threshold is exceeded. Any VC that has also exceeded its Local Discard threshold would continue to queue either CLP0 cells (if the circuit is using the CLP1 discard method) or cells from the current packet (if the circuit is using the early packet discard method). Circuits can continue to queue cells until the Global CLP0+1 threshold is reached.

The CLP0+1 threshold enables you to reserve buffers before the maximum buffer capacity is reached. Lucent recommends that you reserve a sufficient number of buffers to allow new and idle circuits to start up and get access to buffers.

ATM Flow-Control Discard Mechanisms

The ATM FCP supports three mechanisms for discarding cells:

Early Packet Discard (EPD) — The ATM FCP performs EPD for UBR, ABR, and VBR-NRT VCs. If a cell causes the queue for a VC to exceed the discard thresholds, the VC enters the EPD state. The cells in the current packet of the VC are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded for that VC.

Selective Cell Loss Priority 1(CLP1) Discard — Selective CLP1 discard can be provisioned for UBR, ABR, and VBR-NRT VCs. If the current cell causes the queue for a VC to exceed the discard thresholds and the cell has CLP set to 1, then the cell is discarded. Note that EPD is not performed in this case.

Partial Packet Discard (PPD) — If the global CLP0+1 threshold for a port is reached, PPD is performed for circuits that are configured for EPD. However, unlike EPD, all of the remaining cells in the current packet are discarded. Note that the End of Frame (EOF) cell is discarded as well. This results in the loss of the next packet even if the packet is transmitted.

Note – The PPD results in no further throughput for this circuit if both of the following conditions occur:

- A circuit is set for EPD and does not send ATM Adaptation Layer 5 (AAL-5) PDUs (for example, AAL0 data)
- A port becomes sufficiently congested (CLP 0+1 threshold is reached)

VP Shaping

Note – You must enable the FCP to use the VP shaping feature.

The VP Shaping feature is *not supported* on the 3-Port Channelized DS3/1 IMA I/O module.

In addition to the existing VC functionality, the FCP supports the VP shaping feature. VP shaping lets you configure the FCP to provide egress traffic shaping on OPTimum trunks and Virtual UNI logical ports on the CBX 500.

When the FCP is enabled, all logical ports that are not configured for VP shaping perform per-circuit flow control. No per-VC flow control is performed for VCs going over a shaped OPTimum trunk or Virtual UNI logical port.

VP shaping is typically used to limit the amount of traffic tunneling through a non-Lucent network on a virtual path. The core network enforces a VP traffic contract. If traffic leaving the CBX 500 is not shaped to the contract, this traffic is dropped by the UPC as it enters the core network.

Figure 5-7 shows an example of VP shaping network architecture.

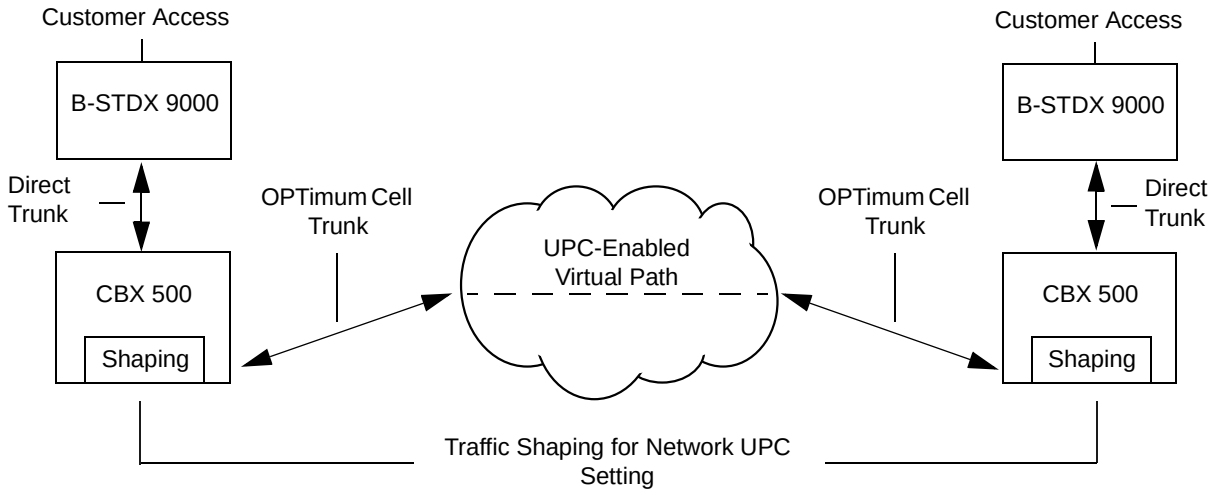


Figure 5-7. VP Shaping Network Architecture Example

Shaping Rates

When you configure an OPTimum trunk or Virtual UNI, you can enter a shaping rate for the logical port. All cells belonging to the first VP on the shaped logical port OPTimum trunk or Virtual UNI will be "shaped" or paced at the specified OPTimum trunk shaping rate. Any other VPs will be shaped at their initial cell rate.

See Chapter 3, "Configuring CBX 500 or GX 550 Logical Ports," for information about configuring OPTimum trunks and Virtual UNIs.

QoS Classes for VP Shaping

VP shaping is performed on all QoS classes. QoS support is provided within the logical port (OPTimum trunk or Virtual UNI) by priority scheduling in decreasing order of priority: CBR, VBR-RT, VBR-NRT, ABR/UBR.

Each QoS class has two configurable thresholds – a discard threshold, and a CLP0+1 threshold. The eight thresholds (two per service class) are configured on a per card basis. See the section on configuring VP shaping attributes in the *B-STDX, CBX, and GX Switch Module Configuration Guide* for information about the default VP shaping threshold values.

The discard threshold is used for EPD or CLP1 discards in the same manner as described in per-VC flow control. Per-VC queuing is not performed; there is no "fair share" bandwidth allocation among the VCs sharing a logical port.

Multicast Cells

All multicast cells are placed into a single queue. There is one queue per I/O module. Multicast cells are discarded when the ATM FCP multicast queue length reaches a certain threshold. You can configure this threshold for each installed I/O module.

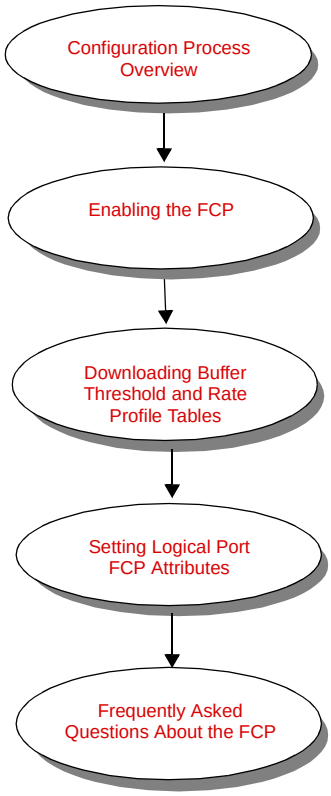
Multicast cells are dequeued at the assigned multicast cells shaping rate. This rate is configurable using NavisCore. See Table 6-1 on page 6-3 for more information about configuring the Multicast Rate attribute.

6

Working with the ATM Flow Control Processor (FCP)

You can configure the ATM Flow Control Processor (FCP) on an input/output module (IOM) after you set the module's attributes. This chapter describes how to configure the FCP. In addition, this chapter addresses frequently asked questions about the FCP.

This chapter describes the following topics and tasks:



Configuration Process Overview

Perform the following steps to configure the FCP:

Step 1. Enable the ATM Flow Control Processor (FCP). See "Enabling the FCP" on page 6-2.

Step 2. Download load rate profile tables. See "Downloading Buffer Threshold and Rate Profile Tables" on page 6-5.

Step 3. Configure logical port FCP attributes. See "Setting Logical Port FCP Attributes" on page 6-7.

Enabling the FCP

This section describes how to enable and configure the FCP on an IOM.

Note – Contact a qualified Lucent organization for network design validation before enabling the FCP.

To enable the FCP:

1. If you have not already done so, log in to the network map by selecting NavisCore ⇒ Logon from the Misc menu. Enter your operator password.
2. Select the CBX 500 switch object for which you are enabling the FCP.
3. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.

   See the *B-STDX, CBX, and GX Getting Started User's Guide* for information about the functions you can access on the Switch Back Panel dialog box.

Note – Slots 1 and 2 in a CBX 500 switch are reserved for the main switch processor module and the optional redundant switch processor module. Slot 1 is always configured as the main switch processor module.

4. Select the slot containing the IOM you are configuring and choose Attrs. The Set Card Attributes dialog box appears.

5. In the ATM Flow Control Processor field, select Enabled. The FCP attribute fields appear on the lower portion of the Set Card Attributes dialog box (Figure 6-1).

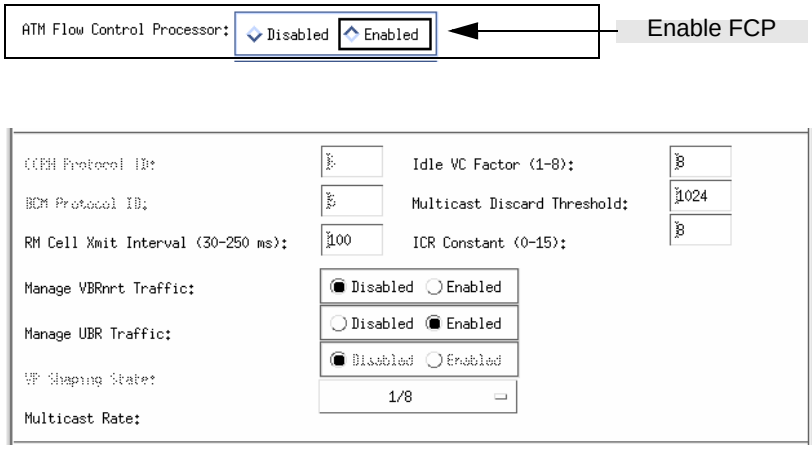


Figure 6-1. FCP Attribute Fields (Set Card Attributes Dialog Box)

Note – Enabling the ATM Flow Control Processor will make the IOM out of sync. Perform a PRAM Sync *after* loading the profile tables (described on page 6-5) to enable the ATM Flow Control Processor on an IOM.

See the *B-STDX, CBX, and GX Getting Started User's Guide* for PRAM Sync instructions.

6. Complete the fields described in Table 6-1.

   For more information about the ATM FCP fields, see "Closed-Loop Flow Control" on page 5-5.

   For information about other fields on the Set Card Attributes dialog box, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

Table 6-1. Set Card Attributes Fields and Buttons (FCP)

Field	Action/Description
CCRM Protocol ID	Displays the protocol number (6) in Cascade Communications Resource Management (CCRM) cells. This value is not configurable.
BCM Protocol ID	Displays the protocol ID number (5) in Backward Congestion Message (BCM) cells. This value is not configurable.
RM Cell Xmit Interval (30-250 ms)	Enter the resource management (RM) cell transmit interval. The default value is 100.

Table 6-1. Set Card Attributes Fields and Buttons (FCP) (Continued)

Field	Action/Description
Idle VC Factor (1-8)	Enter the Idle VC Factor. The default value is 8. For more information on the Idle VC Factor, see "Idle Circuits and Idle VC Factor" on page 5-13.
Multicast Discard Threshold	Enter the Multicast Discard Threshold. The default value is 1024.
ICR Constant (0-15)	Enter the Initial Cell Rate (ICR) constant. The default value is 8. For more information on the ICR Constant parameter, see "Initial Cell Rate (ICR) and ICR Constant" on page 5-13.
Manage VBR-NRT Traffic	Select one of the following options: *Disabled* – (default) VBR-NRT traffic is not managed by the FCP. *Enabled* – VBR-NRT traffic is managed by the FCP.
Manage UBR Traffic	Select one of the following options: *Disabled* – (default) UBR traffic is not managed by the FCP. *Enabled* – UBR traffic is managed by the FCP.
Multicast Rate	The multicast rate parameter determines the rate at which the multicast queue is dequeued on the ATM FCP. The default value is 1/8 (12.5%) of the channel rate. You can select the multicast shaping rate as a fraction of the line rate, from 1/15 to 1. The rate is configured per IOM. ***Note:*** *There is only one multicast queue per ATM FCP.*

7. When you finish setting FCP attributes, choose Ok.
8. Choose Ok to return to the Switch Back Panel dialog box.

Downloading Buffer Threshold and Rate Profile Tables

You can load four profile tables into the ATM Flow Control Processor. The ATM Flow Control Processor uses these tables to determine the local discard threshold, local congestion threshold, rate increase factor, and rate decrease factor for each VC that it manages.

Until you load the profile tables, the ATM Flow Control Processor does not contain default profile table values, and cannot calculate the required thresholds and rate factors to manage VCs.

The file names that initially appear by default on the Load Rate Profile Tables dialog box (Figure 6-2 on page 6-6) are always the default files for this dialog box. These defaults remain the same even after you select and load different files.

Note – To permanently change the file names that appear by default on this dialog box, you can edit the `cascadeview.cfg` file. If you are unfamiliar with the procedures for updating the `cascadeview.cfg` file, please contact the Lucent Technical Assistance Center for more information.

See Appendix D, "ATM Flow Control Processor Rate Profile Tables," for more information on the use and content of the profile tables.

To load the Buffer Threshold and Rate Profile tables:

1. Access the Set Card Attributes dialog box and enable the ATM FCP using the steps in "Enabling the FCP" on page 6-2.

Note – If the ATM Flow Control Processor field is not enabled in the Set Card Attributes dialog box, the Load Profile button will be grayed out on the dialog box. Once you set this field to Enabled, this button and the FCP attribute fields appear on the lower portion of the Set Card Attributes dialog box (see Figure 6-1 on page 6-3).

2. Choose Load Profile. The Load Rate Profile Tables dialog box (Figure 6-2) appears.

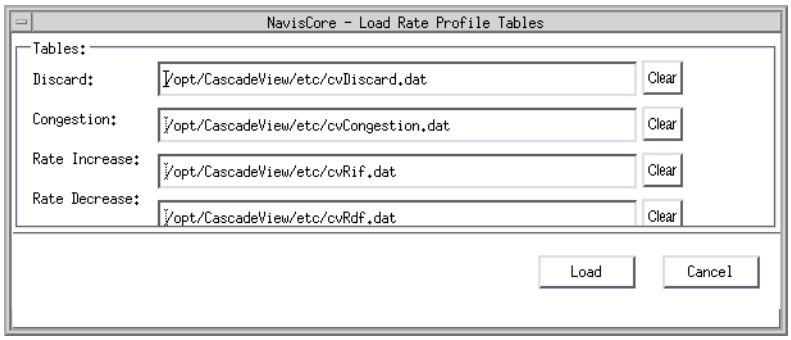


Figure 6-2. Load Rate Profile Tables Dialog Box

3. Select the full path and file name for each of the rate profile tables listed on the Load Rate Profile Tables dialog box, using one of the following options:
   - Manually enter a new file name, including directory path information, and go to Step 4.
   - Choose Clear if you do not want to load a particular rate profile table, and go to Step 4.
4. Choose Load. The files are loaded into the Sybase database.
5. Perform a PRAM Sync. See the *B-STDX, CBX, and GX Getting Started User's Guide* for PRAM Sync instructions.

Setting Logical Port FCP Attributes

When you define logical ports on an FCP-enabled module, you must configure additional ATM FCP attributes for the logical port.

To set ATM FCP attributes for a logical port:

1. Access the Add Logical Port dialog box (see Figure 3-3 on page 3-11) using the steps in "Selecting a Logical Port Type" on page 3-10.
2. Choose the ATM FCP attribute type from the Set Attributes option menu. The Set ATM FCP Attributes fields appear.

   The ATM FCP attributes and default values differ depending on the I/O module you are configuring. Figure 6-3 shows an example of the ATM FCP attributes for the 3-Port Channelized DS3/1 Inverse Multiplexing for ATM (IMA) I/O module.

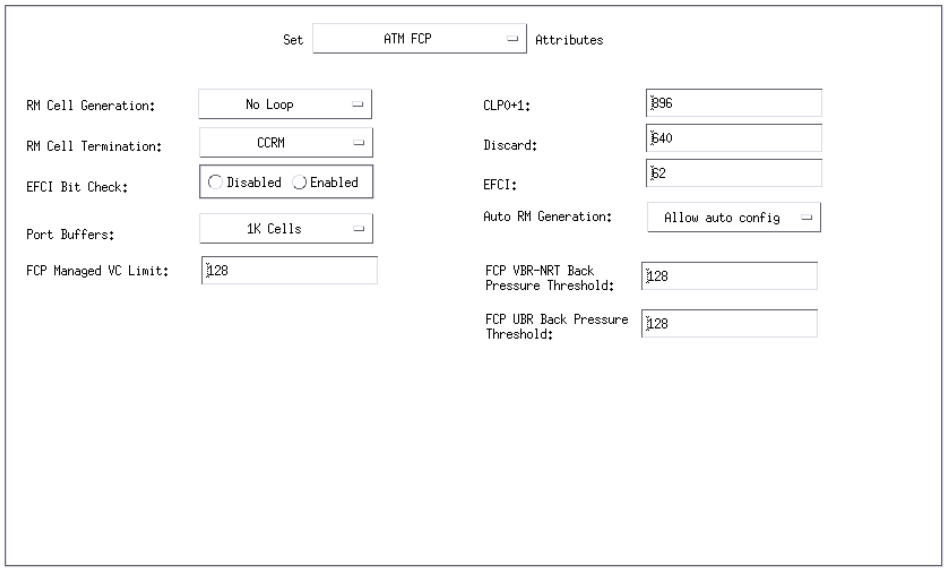


Figure 6-3. Set ATM FCP Attributes Dialog Box (3-Port Channelized DS3/1 IMA IOM)

3. Complete the fields and buttons described in Table 6-2.

Table 6-2. Set ATM FCP Attributes Fields and Buttons

Field/Button	Description
RM Cell Generation	Select the type of cell to generate for the virtual circuit (VC). Options include: *CCRM* – VC will generate Cascade Communications Resource Management (CCRM) cells. *BCM* – VC will generate backward congestion message (BCM) cells. *No Loop* (default) – VC will generate no RM cells.
RM Cell Termination	Select the type of RM cell to terminate for the port. Options include: *CCRM* (default) – VC will terminate CCRM cells only. *CCRM and BCM* – VC will terminate both BCM and CCRM cells.
EFCI Bit Check	Enables you to support control loops across switches that do not have the ATM FCP installed. These switches mark the explicit forward congestion indication (EFCI) bit in data cells to indicate network congestion. If this option is enabled, the ATM FCP reviews the EFCI bits in the cell stream when it generates a backward RM cell.
Port Buffers	Select the number of desired cell buffers per port. Port buffers enable you to configure the number of cell buffers for each port. The entire cell buffer can be divided among the ports on an IOM. Options include: • 1K (default) • 2K • 4K • 8K • 16K • 32K • 64K
FCP Managed VC Limit *(3-Port Channelized DS3/1 IMA IOM only)*	Enter the number of FCP-managed VCs supported for a logical port on the 3-Port Channelized DS3/1 IMA IOM. The range of possible values is 64 - 16384 VCs (multiples of 64), with the following defaults: • The default value is 64 for logical ports created on an IMA group with *one IMA link* configured. • The default value is 128 for logical ports created on a IMA group with *multiple IMA links* configured.

Table 6-2. Set ATM FCP Attributes Fields and Buttons (Continued)

Field/Button	Description
CLP0+1	Enter the value for the CLP0+1 buffer threshold. The CLP0+1 threshold enables you to reserve buffers before the maximum buffer capacity is reached. The default value differs depending on the module you are configuring.
Discard	Enter the value for the Global Discard buffer threshold. Global Discard. buffers enable you to reserve buffers for cell discard. The default value differs depending on the module you are configuring.
EFCI	Enter the value for the explicit forward congestion indication (EFCI) threshold. You can configure this threshold to allow for some margin before the Global Discard buffer threshold is reached. This margin compensates for some of the closed-loop, flow-control delay in the network prior to discarding cells. The default value differs depending on the module you are configuring.
Auto RM Generation	Select the mode for Auto RM Generation. Options include: *Allow Auto Config* (default) – RM cell generation is automatically disabled for a VC if no upstream FCP-enabled IOM is detected for the VC in the adjacent upstream switch. *Override Auto Config* – The switch continues to generate RM cells regardless of whether or not an adjacent upstream switch contains an FCP-enabled IOM.
FCP VBR Back Pressure Threshold *(3-Port Channelized DS3/1 IMA IOM only)*	Enter the value of the back-pressure (BP) threshold for VBR-NRT traffic on the egress. You can configure the BP Threshold for each logical port according to the ATM service class (either VBR/ABR or UBR-NRT.) The FCP subsystem intercepts traffic between the switch fabric and the IMA base card. The system monitors each of the 84 T1 channels for its buffer congestion state. If a channel exceeds the specified BP threshold value, a throttle mechanism is activated to reduce the rates on all active circuits to the fair-bandwidth value for the circuit. The default value is 128 cells.

Table 6-2. Set ATM FCP Attributes Fields and Buttons (Continued)

Field/Button	Description
FCP UBR Back Pressure Threshold *(3-Port Channelized DS3/1 IMA IOM only)*	Enter the value of the BP threshold for UBR/ABR traffic on the egress. See the FCP VBR BP Threshold description earlier in this table for a description of the purpose of the FCP BP threshold parameter. The default value is 128 cells.

Note – An additional ATM FCP logical port attribute, FCP Managed VC Number, is available for the 3-Port Channelized DS3/1 IMA IOM on the View ATM FCP Attributes dialog box. This read-only attribute displays the number of FCP-managed virtual circuits (VCs) currently available on the logical port. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for details about viewing this and other ATM FCP attributes for ATM logical ports.

Frequently Asked Questions About the FCP

This section provides guidelines for answering common customer questions regarding the ATM Flow Control Processor (FCP). Unless otherwise noted in the answer, these guidelines apply to *all* CBX 500 I/O modules (IOMs) that support the ATM FCP. These modules include:

- 8-Port T1 and E1 modules
- 8-Port DS3 and E3 ATM UNI modules
- 4-Port ATM UNI OC-3c/STM-1 module
- 1-Port OC-12c/STM-4 module
- 3-Port Channelized DS3/1 IMA module

If you experience difficulties that are not addressed in this section and require assistance, please contact the Lucent Technical Assistance Center (TAC). For contact information, see "Technical Support" on page xliii.

What happens if I disable the FCP?

The FCP is an optional feature that is available for the supported CBX 500 I/O modules listed above. See "Enabling the FCP" on page 6-2 for instructions on enabling and disabling the FCP.

When you disable the FCP, all of the I/O module and logical port attributes related to the FCP are reset to their default values. The only exception is the resource management (RM) Cell Generation Type, which remains configured whether or not an FCP is present.

If you disable the FCP, the I/O module is unable to:

- Perform intelligent discarding on a per-connection basis.
- Provide minimum rate guarantees on a per-connection basis.
- Minimize latency in the event of network congestion.

What are the performance limitations of the FCP?

Under certain conditions, the FCP experiences performance limitations. Possible performance-limiting conditions are:

- Increasing the number of virtual circuits (VCs) slightly affects performance on the FCP.
- Enabling the EFCI check affects performance because of increased processing requirements. There is an extra check to determine if the EFCI bit is set.
- The IOM performs RM cell generation as a background process. Therefore, decreasing the generation interval has little impact on data throughput. Increasing the data rate has an impact on RM cell generation, because there are fewer cycles left for background processing.

How many logical ports can I configure?

Note – This information applies only when using the ATM FCP on the 3-Port Channelized DS3/1 IMA IOM.

Based on performance testing, Lucent provides the following guidelines for logical port configuration when utilizing the ATM Flow Control Processor on the 3-Port Channelized DS3/1 IMA IOM.

Configuration Options

The Flow Control Processor subsystem for the 3-Port Channelized DS3/1 IMA IOM was designed to support a variety of distinct T1 channels and/or IMA groups. IMA groups can bundle up to eight T1 channels to form a single entity. The following logical port configuration options are available:

Default Configuration — The FCP allocates a default amount of 1K cell buffer memory per provisioned logical port, IMA group, or DS1 channel. Therefore, 64K cells (the maximum available port buffering on the FCP subsystem) are allocated per 3-Port DS3/1 IMA IOM. Each logical port can have either a distinct T1 channel or an IMA group containing up to eight T1 channels. Lucent does not recommend using the maximum default cell buffer threshold when provisioning more than 64logical ports.

User-Defined Configuration — You can configure more than 64logical ports with a corresponding number of T1 and/or IMA groups by assigning less than 1K to each logical port.

Is the CI bit set when BCM cells are generated?

Since Backward Congestion Message (BCM) cells are generated only when network congestion occurs, it is assumed that downstream congestion is present when a CBX 500 switch receives BCM cells. Accordingly, the CBX 500 switch reduces the rate of excess data into the network, regardless of the CI bit setting. Therefore, since the switch does not check the status of the CI bit when it receives BCM cells, it is unnecessary to change the CI bit setting from 0 to 1 for BCM cells.

Why are RM cells not generated even though I am using the Auto RM Generation option?

The Virtual Connection (VC) Manager establishes all circuits. During circuit setup, the VC Manager looks at the adjacent upstream switch to find an FCP-enabled IOM in the circuit path. If the VC Manager detects an FCP-enabled IOM, the FCP determines whether or not to generate RM cells on that circuit, according to congestion status.

The VC Manager prevents backward RM cells from being sent to upstream devices that may be unable to process RM cells. When the VC Manager does not detect an FCP-enabled interface, the system overrides the RM cell generation functionality.

The Auto RM Generation field on the Set ATM FCP Attributes dialog box (Figure 6-3 on page 6-7) provides the following two options for RM cell generation:

- To set RM cells to be generated automatically, select the default option, *Allow Auto Config*.
- To set RM cells to be generated even if no upstream FCP-enabled IOM is detected, select the *Override Auto Config* option.

See “Setting Logical Port FCP Attributes” on page 6-7 for more information on these options.

How is fair bandwidth determined?

Note – This information applies only when using the ATM FCP on the 3-Port Channelized DS3/1 IMA IOM.

In the event of network congestion, the FCP on the 3-Port Channelized DS3/1 IMA IOM may, under certain circumstances, adjust the rates for active circuits evenly among the available bandwidth, as opposed to their fair bandwidth value. The fair bandwidth value determines the amount of available non-real time (NRT) bandwidth assigned to a particular circuit based on the minimum cell rate (MCR) and, for variable bit rate-non-real time (VBR-NRT) circuits, the sustained cell rate (SCR).

When congestion occurs at a DS1/T1 channel on the 3-Port Channelized DS3/1 IMA IOM, the FCP alleviates the congestion by throttling back (also known as *back pressuring*) the rates of all active NRT circuits that it manages by setting one or more throttle bits.

The following issues affect the operation of the FCP on the 3-Port Channelized DS3/1 IMA IOM:

- The time required to poll each of the 84 DS1/T1 channels on the 3-Port Channelized DS3/1 IMA IOM

  By contrast, FCP-enabled IOM1 modules have a maximum of only eight channels or ports to poll.

- The effects of the increased delay required to poll each of the 84 DS1/T1 channels on the 3-Port Channelized DS3/1 IMA IOM

  If this delay is long enough, the FCP would continue to forward traffic to the egress port. In the absence of any other flow control mechanisms, such as received resource management (RM) cells, the FCP cannot determine whether downstream congestion is present. If this continues, the non-FCP buffers will overflow, resulting in “silent” cell drops.

To minimize the likelihood of “silent” cell drops, the FCP includes a peripheral component known as the Port Congestion Monitor (PCM). The PCM monitors the state of the queue on each of the 84 DS1/T1 channels and sets the throttle bits as appropriate.

To enable a quick response when momentary network congestion is detected, the FCP throttles back each active circuit instantaneously so that the available NRT bandwidth is equally shared, regardless of the Quality of Service (QoS) class or traffic parameters configured on the circuit. When the congestion passes, the FCP immediately returns the circuits to their previous rates. If the congestion persists for an extended period (16K RM processing intervals - 100 msec), the PCM sets a throttle bit that signals the FCP to adjust the circuit rates to their fair bandwidth values.

Why does the Early Packet Discard (EPD) option only work when enabled for all circuit connections?

A virtual circuit (VC) will enter into an Early Packet Discard (EPD) state only if both local and global buffering resources have been utilized. The buffer space between the Global Discard and Global CLP0+1 thresholds allows the VCs on a port to continue to queue cells after the Global Discard threshold is exceeded. Cells are queued according to the following principles:

- If the VC has the EPD discard option enabled, every other frame is discarded, and cells from the current packet are queued. No further increase in the global queue length takes place.
- If the VC has the CLP1 discard option enabled, queuing continues until the Global CLP0+1 threshold is reached, and further cells are discarded. Since the CLP0+1 check is performed first, all cells from active congested circuits are discarded when the threshold is reached.

Lucent recommends that all VCs be set to either the EPD or CLP0+1 discard options, but not both. See "ATM FCP Queues" on page 5-16 for more information about the FCP queuing mechanism.

7

Configuring Trunks

A trunk enables two Lucent switches to pass data to each other and exchange internal control messages such as OSPF, Simple Network Management Protocol (SNMP), and others.

This chapter describes how to configure a Lucent trunk. In addition, the following sections describe how you can manage trunk traffic:

- "About Administrative Cost" on page 7-2 describes how to configure trunk parameters to route circuits over the trunk which has the lowest administrative cost.
- "About Link Trunk Protocol" on page 7-3 describes how to configure keep alive (KA) control frames.
- "About Automatic Protection Switching" on page 7-5 describes how to use the CBX 500 and GX 550 optical cards to provide automated trunk backup in cases of equipment failure. These cards include:
  - OC-3c/STM-1 (CBX 500 and GX 550)
  - OC-12c/STM-4 (CBX 500 and GX 550)
  - OC-48/STM-16 (GX 550)
- "About Trunk Backup for the B-STDX 8000/9000" on page 7-12 describes how to configure *manual* trunk backup for the B-STDX 8000/9000 switch.
- "About Layer2 VPN" on page 11-2 describes how to dedicate trunks to specific customers to guarantee performance and security.

About Administrative Cost

You can manage trunk traffic by defining the trunk's administrative cost. Circuits that route data based on administrative cost are created on the path with the lowest administrative cost. You can assign an administrative cost value from 1-65534. The lower the administrative cost of the path, the more likely the path will be chosen when a PVC or SVC routed on administrative cost needs to be created.

Note – The CBX 500 and GX 550 switches route circuits based on the routing metric you select for the ATM UNI or NNI logical port endpoint: Admin Cost, CDV (cell delay variation), or end-to-end delay. See "ATM Direct Trunk" on page 2-9 for more information.

The switch manages circuits as follows:

- When you first define a circuit, the circuit looks for a path that has enough available virtual bandwidth to handle the circuit's effective bandwidth.
- If the circuit finds more than one path with enough available virtual bandwidth, the circuit chooses the path with the lowest administrative cost. This assumes that administrative cost is the designated routing metric. For the UNI or NNI logical port endpoint, if you designate CDV or end-to-end delay as the routing metric, the circuit chooses the trunk(s) with the lowest CDV or end-to-end delay.

The switch automatically reroutes circuits around a failed trunk or switch. If a circuit cannot find a path with sufficient bandwidth, the circuit remains in an inactive state until the bandwidth becomes available.

For more information on the rules used by the switch to establish PVC endpoints, see "PVC Endpoint Rules" on page 8-4.

About Link Trunk Protocol

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

Trunk Delay

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

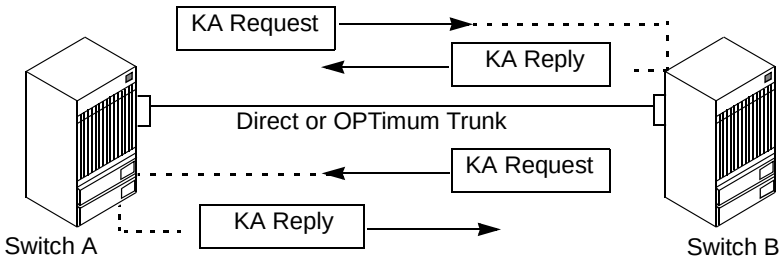


Figure 7-1. Trunk Delay - OSPF Metric and Keep Alive Messaging

Keep Alive Threshold

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

Static and Dynamic Delay

The Static Delay and Dynamic Delay fields on the Set All Trunks dialog box represent the measured one-way delay in units of 100 microseconds. The static delay is measured upon trunk initialization and is updated only when the trunk state changes from Down to Up. The static delay value is used in conjunction with the end-to-end delay routing metric as a means of allowing users to route circuits over trunks with the lowest end-to-end delay.

The Dynamic Delay field is a read-only field where the dynamic delay is measured continually on operational trunks. Under most conditions, the dynamic delay value will match the static delay value. However, if some characteristics of the underlying transmission media for the trunk changes, such that the dynamic delay changes, this value may differ from the static delay.

If you use the Set All Trunks dialog box (Figure 7-2 on page 7-14) to view attributes for a selected trunk, and you notice that the static and dynamic delay values do not match, you can modify the static delay value to match the dynamic delay. To do this, perform the following steps:

1. From the Set All Trunks dialog box (Figure 7-2 on page 7-14), choose Modify. A dialog box similar to Figure 7-4 on page 7-22 appears.
2. Edit the static delay value.
3. Choose OK to accept the change.

If the trunk reinitializes for any reason, the static delay value you entered when you modified the trunk is automatically replaced by the static delay value measured when the trunk reinitializes.

About Automatic Protection Switching

The Automatic Protection Switching (APS) feature is available on all types of CBX and GX optical interfaces. APS allows you to protect optical interfaces by provisioning a backup (protection) port that automatically takes over for the primary (working) port when a physical layer fault or module failure occurs.

Note – Bellcore GR-253-CORE, ITU G.841, Annex B (formerly ITU G.783, Annex B), and ITU G.841 section 7.1 (formerly ITU G.783, Annex A) standards form the basis of the Lucent APS implementation. Review these specifications and standards for further information on how you can use APS in a network environment.

You can use APS functions to backup ATM direct trunk ports on CBX 500 or GX 550 switches. The Fast Inter-card APS 1+1 option is also available for PNNI links configured between GX 550 switches and PSAX 4500 devices. If an equipment failure occurs, APS provides line backup. Automatic Protection Switching eliminates bandwidth reservation for the backup trunk.

APS Options

Different APS options are available depending on the type of Lucent switch module and logical port in use. These options include:

- Intra-card APS 1+1
- APS Trunk Backup
- APS Resilient UNI
- Fast Inter-card APS 1+1

Each of these APS options comply with relevant industry standards and use the same criteria for switching between the working and protection port.

See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for a listing of the minimum software and hardware versions that support the various APS options.

The following sections summarize these options.

Intra-card APS 1+1

The Intra-card APS 1+1 option is available on CBX OC-12c/STM-4 and CBX OC-3c/STM-1 modules. Using Intra-card APS 1+1, traffic can be switched between the working and protection ports in less than 50 ms.

You configure both the working and protection ports on the *same* module. Intra-card APS 1+1 supports ATM UNI/NNI, direct trunk, and ATM OPTimum cell trunk logical ports. You only have to configure one logical port on the working port. This logical port is then internally shared with the protection port.

Note – Since the working and protection port are on the *same* module, Intra-card APS 1+1 can protect against the failure of an individual port or physical link, but not the failure of the entire module.

APS Trunk Backup

The APS Trunk Backup option is available for all CBX and GX optical modules. You can use the APS Trunk Backup option to protect against module failure by provisioning the working port and the protection port on two different switch modules.

This option can be used in conjunction with Lucent ATM direct cell trunk logical ports. When configuring APS Trunk Backup, you have to provision a separate logical port and a separate trunk on each working and protection port. For more information, see "Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks" on page 7-34.

Note – As traffic is rerouted from a working trunk to a protection trunk during a failure, the switchover speed may be less than that provided by Intra-card APS 1+1.

Only one trunk is active at any given moment. If the primary trunk fails (times out), the APS manager detects the link down message and performs an APS switchover to the backup port. APS Trunk Backup provides both facility failure and equipment failure protection.

Special Considerations

APS Trunk Backup on a CBX 500 — Configure the working and protection port on *different* IOMs. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.

APS Trunk Backup on a GX 550 — Configure the working and protection ports on either the same module (BIO or Phy) or a different module (BIO or Phy). See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.

APS Resilient UNI

The APS Resilient UNI option is available for all CBX and GX optical modules. When configuring APS Resilient UNI, you can provision the working port and the protection port on two *different* switch modules, protecting against module failure. You can use this option in conjunction with Lucent UNI logical ports.

When configuring APS Resilient UNI, you have to provision a separate logical port on each working and protection port, and then configure a fault tolerant PVC/resilient UNI between the two working ports. For more information, see "Using APS with Resilient UNI" on page 12-8.

Note – As traffic is rerouted from a working trunk to a protection trunk during a failure, the switchover speed may be less than that provided by Intra-card APS 1+1.

Special Considerations

APS Resilient UNI on a CBX 500 — Configure the working and protection port on *different* IOMs. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.

APS Resilient UNI on a GX 550 — Configure the working and protection port on either the *same* module (BIO or Phy) or a *different* module (BIO or Phy). See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.

APS Resilient UNI Over PNNI

You can use the APS Resilient UNI feature to configure fault-tolerant ATM PVCs across a Private Network-to-Network Interface (PNNI) or combined Virtual Network Navigator/PNNI (VNN/PNNI) domain. You configure APS Resilient UNI over PNNI links using the same procedure as you would for ATM VNN OSPF networks.

For details, see "Resilient UNI and APS Resilient UNI Over PNNI" on page 20-25.

Fast Inter-card APS 1+1

The Fast Inter-card APS 1+1 option (Fast APS 1+1) is available for the modules shown in Table 7-1. You can use the Fast APS 1+1 option with Lucent ATM direct cell trunks or to provide protection switching for SVCs and SPVCs on PNNI links between a GX 550 switch and a PSAX 4500 device. Fast APS 1+1 provides switchover times that are within 50 ms.

Table 7-1. Fast APS 1+1 Options

Option	CBX 500		GX 550		
	4-port OC-3c/ STM-1	1-port OC-12c/ STM-4	4-port OC-3c/ STM-1	1-port OC-12c/ STM-4	1-port OC-48/ STM-16
ATM direct trunks (True APS VNN))	X	X	X	X	X
UNI ports (True APS UNI)	X	X	X	X	X
PNNI links (bidirectional APS, SVCs and SPVCs only)	X	X	X	X	X
PNNI links[1] (unidirectional APS, SVCs and SPVCs only)			X	X	

[1] Unidirectional APS over PNNI links are supported on GX 550 PNNI trunks using the BIO1 module only. BIO2 is not supported.

Note – See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for a listing of the minimum software and hardware versions that support these Fast APS 1+1 options.

As traffic is rerouted from a working trunk to a protection trunk during a failure, the switchover speed may be less than that provided by Intra-card APS 1+1.

Note – Point-to-multipoint circuits are not supported by The Fast APS 1+1 option.

Unidirectional APS Over PNNI

There are two directional switching modes in APS 1+1 architecture: unidirectional mode and bidirectional mode. In unidirectional mode the head end makes a decision on the selector position without regard to the K1/K2 bytes received from the tail end. In bidirectional mode, the head end will consider the K1/K2 bytes received from the tail end in deciding the selector position. Unidirectional APS is less disruptive and is the default mode for the Bellcore GR-253-CORE standard.

APS over PNNI in unidirectional mode is supported for the 4-port OC-3c/STM-1 and 1-port OC-12c/STM-4 modules on the GX 550 BIO1 module.

Special Considerations

Fast APS 1+1 on a CBX 500 — Configure the working and protection physical ports on *different* IOMs. (See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.) Configure an APS trunk between ports on *different* IOMs in a CBX 500 switch.

Fast APS 1+1 on a GX 550 — Configure the working and protection physical ports on *different* modules. (See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.) Configure an APS ATM direct cell trunk between ports on *different* modules in a GX 550 switch.

Only PNNI links are supported between the GX 550 switch and the PSAX 4500. Configure a PNNI link connection between ports on a GX 550 module and an APS-capable module on a PSAX 4500 device.

Physical Port Provisioning

You provision Fast APS 1+1 on the physical port as follows:

- Configure the physical port attributes on the working port. (The protection port is automatically configured with the corresponding values.)
- See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information on configuring Fast APS 1+1 on CBX 500 and GX 550 switches.

Note – For information on configuring Fast APS on the PSAX 4500 device, see the customer documentation provided with your PSAX 4500 product.

Logical Port Provisioning

You provision Fast APS 1+1 on the logical port as follows:

- **Direct Trunks** — Configure a direct trunk logical port at *each* trunk endpoint (for a total of 2 logical ports). (The protection logical ports are automatically configured.)
- **PNNI Links** — Configure one ATM NNI logical port (including PNNI parameters) on the GX 550 Multiservice WAN switch. (The protection logical port is automatically configured.)

Note – If you are using Fast APS 1+1 on a PNNI link to a PSAX 4500 device, you must configure a second NNI logical port on the PSAX 4500 working physical port. For more information, see the customer documentation provided with your PSAX 4500 product.

- See Chapter 3, "Configuring CBX 500 or GX 550 Logical Ports" for more information about configuring these logical port types on CBX 500 and GX 550 switches.

Trunk Provisioning

You provision Fast APS 1+1 on the trunk as follows:

- **Direct Trunks** — Select the working endpoints from the Set All Trunks dialog box. The Fast APS 1+1 trunk is created between these two endpoints. (The protection endpoints are automatically configured with the appropriate values.)

  See "Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks" on page 7-34 for more information.
- **PNNI Links** — PNNI links are automatically activated when you create an ATM NNI logical Port and configure PNNI parameters at either end of the link connection. (You do not need to manually select connection endpoints.) When the working link is activated, the protection endpoints are automatically configured with the appropriate values.

  See "Configuring Fast APS 1+1 for PNNI Links (GX 550 to PSAX 4500 Only)" on page 7-39 for more information.

Note – When an APS-enabled Pport is forced down by using the Admin Down command, all APS switchover requests will be deferred until an Admin Up command is issued on that Pport. Before using Admin Down, force a switchover to the working or protection port, using the APS Command function. Following the maintenance on the port, use the Admin Up command to bring the Pport back up. Finally, clear the issued APS Command to remove the forced switchover condition.

For more information on the APS Command, see "Chapter 11, Configuring Automatic Protection Switching (CBX and GX)" in the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

About Trunk Backup for the B-STDX 8000/9000

The B-STDX 8000/9000 switch platform also provides a *manual* trunk backup option. This feature enables you to set up one or more backup trunks to replace a primary trunk. If a trunk line fails or requires maintenance, you can reroute PVCs from the primary trunk to the backup trunk. You can define primary and backup trunks on any B-STDX 8000/9000 I/O module.

Using the Add Trunk dialog box (Figure 7-4 on page 7-22), you can configure the trunk type as either primary or backup. A backup trunk can have a total bandwidth that is less than that of the primary trunk. To avoid congestion, you can configure multiple backup trunks to back up a single primary trunk. The switch allows you to define up to eight backup trunks for a single primary trunk. Once you configure the primary and backup trunk(s), you configure the primary trunk to automatically back up upon failure. If a trunk line requires maintenance, you can manually initiate and terminate a trunk backup.

Configuring B-STDX Trunk Backup

To configure B-STDX trunk backup:

1. Access the Add Trunk dialog box (see Figure 7-4 on page 7-22).
2. In the Trunk Type field, select Primary.
3. Specify all of the primary trunk field values shown in Table 7-5 on page 7-25. Select Yes in the Initiate Backup Call Setup field on the Add Trunk dialog box.
4. Select Enabled in the Backup on Trunk Failure field on the Add Trunk dialog box.
5. Define from one to eight trunks that have a Trunk Type of Backup.
6. For each trunk with a Trunk Type of Backup, in the Primary Trunk of the backup field, select the name of the primary trunk specified in step 2.

Process for Switching Over to a Backup Trunk

In the event of trunk failure, the system uses the following process to automatically switch over to a defined backup trunk if you have enabled Automatic Trunk Backup (see step 4 on page 7-13).

1. The system switches over to the backup trunk after the trunk is out of service for the amount of time specified for the primary trunk in the Trunk failure thresh.(sec) field (see Table 7-4 on page 7-22).
2. The system resumes using the primary trunk after it is in service for the period of time specified in the Trunk restoration thresh. (sec) field (see Table 7-5 on page 7-25).

Defining the Manual Trunk Backup Feature

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

Accessing Trunk Functions

To access the Set All Trunks dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Trunks.

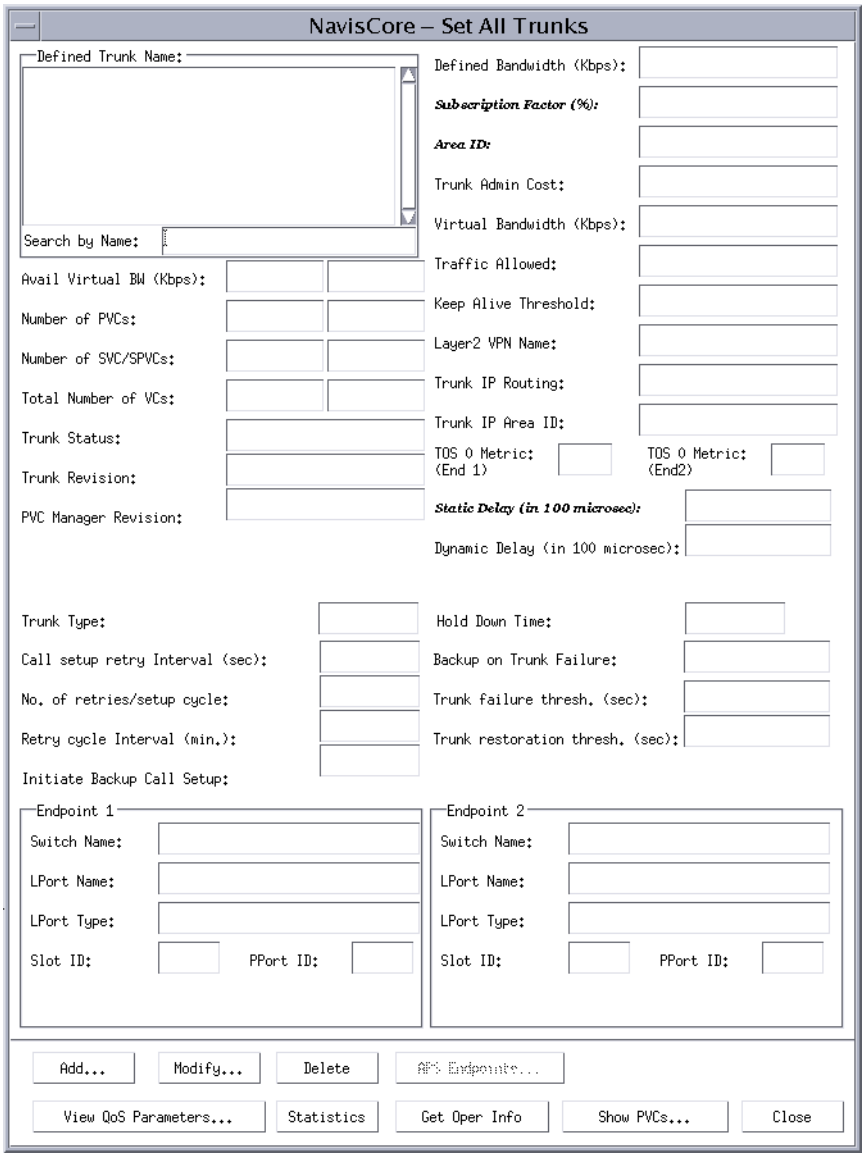


Figure 7-2. Set All Trunks Dialog Box

- To view a list of configured trunks, position the cursor in the Search by Name field and press Return.
- To learn more about the Set All Trunks dialog box, continue with the following section.
- To begin defining a trunk, proceed to page 7-20.

About the Set All Trunks Dialog Box

The Set All Trunks dialog box displays information about the configured options for the trunk you select in the Defined Trunk Name list box. Use any of the following wildcard searches to find a specific circuit name or alias:

- Use an * to match any number of characters
- Use a ? to match a single character
- To match the * character, type *****
- To match the ? character, type **\?**
- To match the \ character, type \\

Table 7-3 and Table 7-2 describe Set All Trunks the dialog box buttons and fields.

Table 7-2. Set All Trunks Dialog Box Buttons

Button	Action/Description
Add	Defines a new trunk.
Modify	Modifies a trunk definition.
Delete	Deletes the selected trunk.
APS Endpoints	If a trunk configured for Fast APS 1+1 is selected in the Defined Trunk Name list box, a dialog box displays showing the status of the working and protection endpoints of the trunk. The APS Endpoints button is enabled only for trunks configured for the Fast APS 1+1 option; it is disabled for trunks configured for the Intra-card APS 1+1 and APS Trunk Backup options.
View QoS Parameters	Displays the Show Logical Port QoS Parameters dialog box for each logical port endpoint of the trunk.
Statistics	Displays the summary statistics for the selected trunk.
Get Oper Info	Displays the status of the selected trunk. A message appears in the Trunk Status field. See page 7-19 for a description of these messages.
Show PVCs	Displays a dialog box that contains a list of the PVCs that traverse the selected trunk. This dialog box also provides logical port descriptions for each PVC endpoint. ***Note**: This function only works when both switches at either end of the trunk are running one of the following minimum switch software versions (or greater):* *B-STDX switch software 06.00.00.00* *CBX 500 switch software 03.00.00.00* *GX 550 switch software 01.00.00.00.*
Close	Exits the Set All Trunks dialog box.

Table 7-3. Set All Trunks Dialog Box Fields

Field	Action/Description
Defined Trunk Name	Displays the names of the trunks configured for the current network map.
Defined Bandwidth (Kbps)	Displays the bandwidth in Kbps for the selected trunk line.
Subscription Factor	The amount of PVCs, SVCs, or SPVCs on a given logical port that can be supported by the physical bandwidth. ***Note:*** *Modifying the value for this attribute does not bring down the trunk or its associated logical port.*
Area ID	Areas are collections of networks, hosts, and routers used for IP routing. The area ID identifies the area. The range of available values is from 0.0.0.0 to 255.255. 255.255. Area 0.0.0.0 is the network backbone area. Area 0.0.0.1 is Area 1. If a trunk is in Area 1 and the OSPF Backwards Compatibility option (which is set through IP) is set to Yes, external routes are not advertised across the link. For a detailed description of OSPF areas, and how to use IP to configure multiple OSPF areas, see the *B-STDX and CBX IP Services Configuration Guide.* ***Note:*** *Modifying the value for this attribute does not bring down the trunk or its associated logical port.*
Trunk Admin Cost	Displays a value that defines the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch. For more information, see "About Administrative Cost" on page 7-2. ***Note:*** *Modifying the value for this attribute does not bring down the trunk or its associated logical port.*
Virtual Bandwidth (Kbps)	Displays the amount of virtual bandwidth in Kbps.

Table 7-3. Set All Trunks Dialog Box Fields (Continued)

Field	Action/Description
Traffic Allowed	Displays one of the following options, which designates the type of traffic allowed on this trunk: *All* – Trunk can carry SVC, PVC, and network management traffic. *Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & Address Restricted* – Trunk can carry PVCs and network management traffic. This trunk option does not support SVC addressing information. If this is the only trunk between two nodes and you configure this option for it, then you effectively prevent SVC traffic from traversing this trunk.
Keep Alive Threshold	Displays the number of seconds the trunk protocol will continue to exchange keep alive (KA) control frames without getting a response from the remote node, before bringing the trunk down.
Layer2 VPN Name	Displays the Layer2 virtual private network (VPN) name.
Trunk IP Routing	Enables or disables IP routing for the trunk. If disabled, the trunk is reserved for use by VNN. See the *B-STDX and CBX IP Services Configuration Guide* for more information.
Trunk IP Area ID	The Open Shortest Path First (OSPF) Area ID used by IP. See the *B-STDX and CBX IP Services Configuration Guide* for more information.
TOS 0 Metric (End 1)	Displays the type of service cost for Endpoint 1 of the trunk. The lowest TOS 0 has the highest priority for routing. Any value between 1 and 65535 is valid.
TOS 0 Metric (End 2)	Displays the type of service cost for Endpoint 2 of the trunk. The lowest TOS 0 has the highest priority for routing. Any value between 1 and 65535 is valid.
Static Delay (in 100 microsec)	Represents the measured one-way delay in units of 100 microseconds. This measurement is taken when the trunk initializes and it is only updated when the trunk state changes from down to up. The static delay value is used in conjunction with the end-to-end delay routing metric to enable you to route circuits over trunks with the lowest end-to-end delay. To modify the Static Delay value, see page 7-4. ***Note:*** *Modifying the value for this attribute does not bring down the trunk or its associated logical port.*

Table 7-3. Set All Trunks Dialog Box Fields (Continued)

Field	Action/Description
Dynamic Delay (in 100 microsec)	Represents the measured one-way delay in units of 100 microseconds. This measurement is made continually on operational trunks. Under most conditions, the dynamic delay value will match the static delay value. However, if some characteristics of the underlying transmission media for the trunk change such that the dynamic delay changes, this value may differ from the static delay.
Hold Down Time	Displays the time delay (in seconds) before link state advertisements (LSAs) are generated when a trunk recovery takes effect on the network. The time delay is not used when a trunk is brought up for the first time, when a trunk's OSPF area ID changes, and when a trunk goes down. This feature reduces the number of LSAs caused by rapid changes in trunk status. The range of values is between 0 (default) and 65535 seconds.
Backup on Trunk Failure	Displays *Enabled* or *Disabled* to indicate that the primary trunk will be automatically backed up upon failure.
Trunk failure thresh. (sec)	Displays the configured trunk failure threshold. The default value is 5 seconds. If the primary trunk remains down for a period of time greater than the configured threshold value, and the value for the Backup on Trunk Failure field is set to Enabled, the switch enters into a call setup retry cycle to enable the backup trunk(s).
Trunk restoration thresh. (sec)	Displays the configured trunk restoration threshold.
Number of PVCs	The total number of PVCs traversing the trunk logical port endpoint.
Number of SVC/SPVCs	The total number of SVCs and SPVCs traversing the trunk logical port endpoint.
Total Number of VCs	The total number of PVCs, SVCs, SPVCs, LSPs, and any other type of VC traversing the trunk.

Table 7-3. Set All Trunks Dialog Box Fields (Continued)

Field	Action/Description
Trunk Status	Displays the current status of the selected trunk. Options include: *Unknown* – The NMS cannot communicate with one or both switch endpoints that make up this trunk. *Down* – The switches cannot establish a communication link. *Attempt* – A switch is attempting to contact another switch but has not yet received a response. *Init* – One-way communication exists between the two switches. *Two-way* – Bidirectional communication exists between the two switches. *Exchange Start* – The two switches are about to exchange the network topology. *Exchange* – The two switches are exchanging network topology. *Loading* – The two switches are requesting the most recent link state information. *Up* – The trunk is up and operational between the two switches.
Trunk Revision	Displays the revision of link trunk protocol software at each endpoint.
PVC Manager Revision	Displays the PVC manager software revision.
Trunk Type	Displays the type of trunk backup services this trunk provides. Options include: *Normal* – Indicates that this trunk offers no backup service. *Primary* – Indicates that this trunk will act as the main trunk connection in a backup service. *Backup* – Indicates that this is the trunk to which traffic will be diverted in the event of primary trunk failure.
Call setup retry Interval (sec)	Displays the lapse of time between each retry during a given retry cycle. The default is 15 seconds.
No. of retries/setup cycle	Displays the number of retries that the system performs during a retry cycle. The default is 20 retries.
Retry cycle Interval (min.)	Displays the lapse of time between retry cycles (in minutes). The default is 10 minutes.
Initiate Backup Call Setup	Displays the name of the switch that performs the backup call setup for the trunk.

Table 7-3. Set All Trunks Dialog Box Fields (Continued)

Field	Action/Description
Endpoint 1 and Endpoint 2 Fields	
Switch Name	Displays the switch name on either side of the trunk line.
LPort Name	Displays the logical port name at each endpoint of the trunk.
Lport Type	Displays the configured logical port type.
Slot ID	Displays the slot number where the I/O module containing the selected port is installed.
PPort ID	Displays the physical port ID number on which the logical port is configured.

Defining a Trunk

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

Defining a trunk is a three-step sequence:

Step 1. Configure a trunk logical port type.

For a CBX 500 or GX 550, see "Defining a Logical Port" on page 3-9.

For a B-STDX 8000/9000, see one of the following sections:

- "Defining ATM Direct Trunk and OPTimum Cell Trunk Logical Ports" on page 4-27
- "Defining ATM OPTimum Frame Trunk Logical Ports" on page 4-37

Step 2. Define a trunk configuration between the two switches. Begin with step 1 on page 7-21.

Step 3. Create a trunk line connection on the network map to represent the trunk. See "Creating a Trunk Line Connection" on page 7-27.

To define a trunk between two Lucent switches:

1. See "Accessing Trunk Functions" on page 7-14 for instructions on accessing the Set All Trunks dialog box (Figure 7-2 on page 7-14).
2. Choose Add. The following dialog box appears.

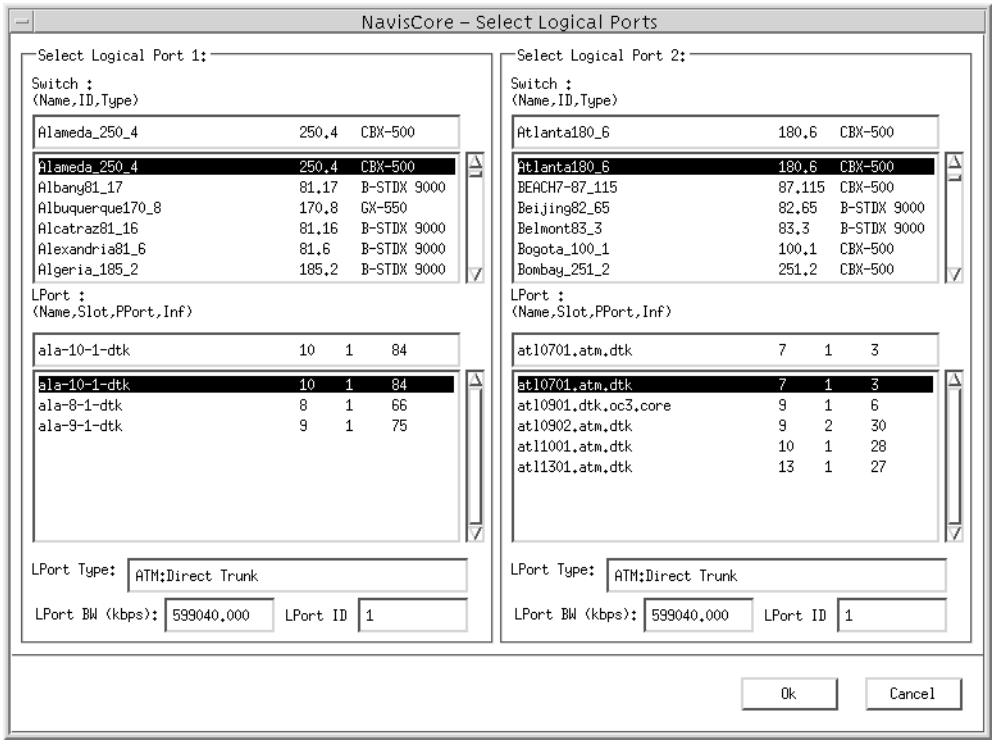


Figure 7-3. Select Logical Ports Dialog Box

3. Provide the following information for both Select Logical Port 1 and Select Logical Port 2 fields:
   a. Select the name of the switch where logical port 1 resides, then select the name of the switch where logical port 2 resides.
   b. Select the name of logical port 1, then select the name of logical port 2.
   c. Review the LPort Type field. Both endpoints must use the same logical port type (either ATM:Direct Trunk or ATM:OPTimum Cell Trunk configurations).

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

d. Review the LPort BW (Kbps) field. The bandwidth for each logical port endpoint must be the same.

4. Choose Ok. The Add Trunk dialog box appears, displaying the parameters for both logical ports in the trunk configuration.

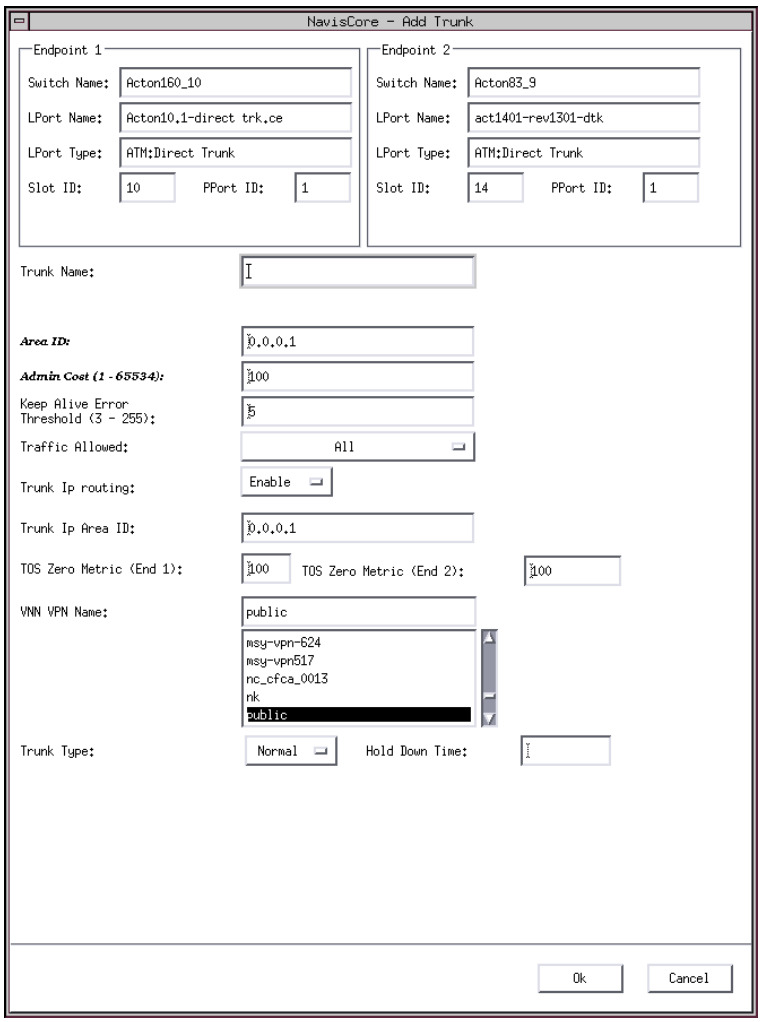


Figure 7-4. Add Trunk Dialog Box

5. Use Table 7-4 on page 7-23 to complete the Add Trunk dialog box fields.

Table 7-4. Add Trunk Dialog Box Fields

Field	Action/Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk.
Area ID	Areas are collections of networks, hosts, and routers used for IP routing. The area ID identifies the area. Enter the area ID (x.x.x.x) for the destination area for this endpoint. The range of available values is from 0.0.0.0 to 255.255.255.255. Area 0.0.0.0 is the network backbone area. Area 0.0.0.1 is Area 1. If a trunk is in Area 1 and the OSPF Backwards Compatibility option (which is set through IP services) is set to Yes, external routes are not advertised across that link. For a detailed description of OSPF areas, and how to use IP to configure multiple OSPF areas, see the *B-STDX and CBX IP Services Configuration Guide.* ***Note:*** *Modifying the value for this attribute does not bring down the trunk or the associated logical port.*
Admin Cost (1- 65534)	Enter a value (from 1 - 65534) that defines the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch. For guidelines, see "About Administrative Cost" on page 7-2. ***Note:*** *Modifying the value for this attribute does not bring down the trunk or the associated logical port.*
Keep Alive Error Threshold (3 - 225)	Enter a value between 3 and 255 seconds to define the KA error threshold. The default is 5 seconds. Service is disrupted if you modify this value once the trunk is online. For more information about this parameter, see page 7-3.
Traffic Allowed	Specify one of the following options to designate the type of traffic allowed on this trunk: *All* – Trunk can carry SVC, PVC, and network management traffic. *Mgmt Only* – Trunk can carry only network management traffic, such as SNMP communication between a switch and the NMS. *Mgmt & User Data* – Trunk can carry PVCs and network management traffic. This trunk option does not support SVC addressing information. If this is the only trunk between two nodes and you configure this option for it, then you effectively prevent SVC traffic from traversing this trunk.
Trunk IP Routing	Enables or disables IP routing for the trunk. If disabled, the trunk is reserved for use by VNN. See the *B-STDX and CBX IP Services Configuration Guide* for more information.
Trunk IP Area ID	The OSPF Area ID used by IP. See the *B-STDX and CBX IP Services Configuration Guide* for more information.

Table 7-4. Add Trunk Dialog Box Fields (Continued)

Field	Action/Description
TOS Zero Metric (End 1)	Enter a value between 1 and 65535. This value specifies the type of service cost for Endpoint 1 of the trunk. The lowest ToS zero has the highest priority for routing.
TOS Zero Metric (End 2)	Enter a value between 1 and 65535. This value specifies the type of service cost for Endpoint 2 of the trunk. The lowest ToS zero has the highest priority for routing.
Layer2 VPN Name	Select a Layer2 VPN name. The default is Public. For more information about Layer2 VPNs, see Chapter 11, "Configuring Layer2 VPNs."
Trunk Type	If you are configuring APS trunk backup for a CBX 500 or GX 550 switch, follow the instructions in "Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks" on page 7-34. To configure Trunk Backup for the B-STDX 8000/9000, select one of the following trunk types: *Normal* – Indicates that this trunk offers no backup service. *Primary* – Indicates that this trunk will act as the main trunk connection. To configure trunk backup features, you must first configure the Primary trunk. Continue with the instructions on page 7-25. *Backup* – Indicates that this is the trunk to which traffic will be diverted in the event of primary trunk failure. Once you configure a Primary trunk, continue with the instructions on page 7-26 to designate a Backup trunk.
Hold Down Time	Accept the default value 0 (zero), or enter a value between 0 and 65535 (seconds). Hold down time allows you to configure the time delay (in seconds) before link state advertisements (LSAs) are generated when a trunk recovery takes effect on the network. The time delay is not used when a trunk is brought up for the first time, when a trunk's Open Shortest Path First (OSPF) area ID changes, and when a trunk goes down. This setting can reduce the number of LSAs caused by rapid changes in trunk status.

6. (*Optional*) If you plan to use the B-STDX 8000/9000 trunk backup feature, continue with the instructions in "Using B-STDX 8000/9000 Trunk Backup."
7. When you finish defining the trunk attributes, choose Ok to complete the trunk configuration.
8. Choose Close to return to the network map.
9. Continue with "Creating a Trunk Line Connection" on page 7-27.

Using B-STDX 8000/9000 Trunk Backup

Complete the steps in one of the following sections depending on the trunk type. Keep in mind that you must first configure a Primary trunk before you designate a backup trunk.

- For specific details on implementing the CBX 500/GX 550 switch platform's APS trunk backup options, see "Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks" on page 7-34.
- For an overview of B-STDX 8000/9000 trunk backup, see "About Trunk Backup for the B-STDX 8000/9000" on page 7-12.

Configuring the Primary Trunk for Trunk Backup

1. If you selected Primary as the Trunk Type, the system displays the fields shown in Figure 7-5.

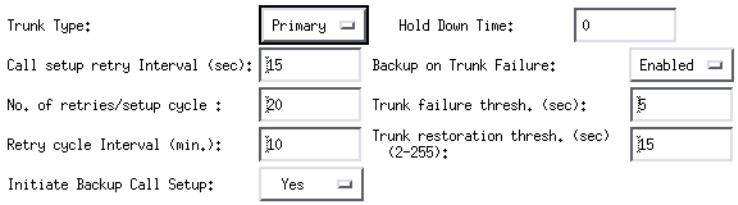


Figure 7-5. Primary Trunk Type Menu Fields

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

Table 7-5. Primary Trunk Type Menu Fields

Field	Action/Description
Call setup retry Interval (sec)	Specify the number of seconds between initiating a call. The default is 15 seconds.
No. of retries/setup cycle	Specify the number of retries per interval. The default is 20 retries.
Retry cycle Interval (min.)	Specify a retry interval in minutes. The default is 10 minutes.
Initiate Backup Call Setup	Choose Yes (default) to initiate a backup call.
Backup on Trunk Failure	Choose Enabled to use trunk backup.

Table 7-5. Primary Trunk Type Menu Fields (Continued)

Field	Action/Description
Trunk failure thresh. (sec)	Specify the number of seconds. The default is 5 seconds. If you enabled trunk backup, this field specifies the number of seconds the system will wait before switching over to the backup trunk.
Trunk Restoration thresh. (sec) (2-255)	Specify the number of seconds that the system will wait for the primary trunk to become functional before resuming use of the primary trunk. The default is 15 seconds. If the primary trunk is out of service and the backup trunk is in use, the system will not resume use of the primary trunk until it has been restored for the period of time you specify. This field prevents a switch-over to a primary trunk that has only been temporarily restored.

3. Choose Ok to complete the configuration.
4. Choose Close to return to the network map.

Configuring the Backup Trunk for Trunk Backup

1. Once you select a Backup trunk type of primary, the Add Trunk dialog box displays the *Primary Trunk of the backup* field. Select the name of the primary trunk. For a B-STDX 8000/9000, you configure up to eight different backup trunks for each primary trunk.
2. Select the name of the switch that initiates the backup call setup for the trunk.
3. Choose Ok to complete the configuration.
4. Choose Close to return to the network map.

Creating a Trunk Line Connection

You must define the trunk configuration between two switches (see "Defining a Trunk" on page 7-20) before you can create the trunk line connection on the network map. The Add Connection dialog box enables you to draw a line to connect the two switches on the network map.

To add a trunk line connection:

1. From the Edit menu, select Add Connection. The Add Connection dialog box appears (Figure 7-6).

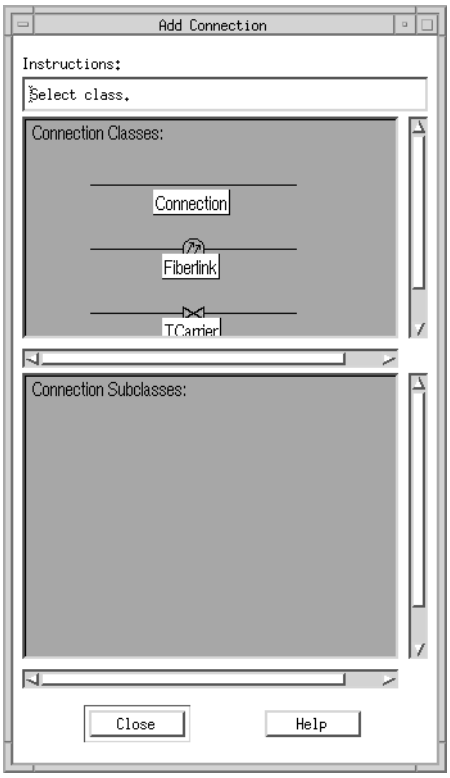


Figure 7-6. Add Connection Dialog Box

2. Select a connection class from the Connection Classes list box. The Add Connection dialog box displays the subclasses for the connection class you select (Figure 7-8).

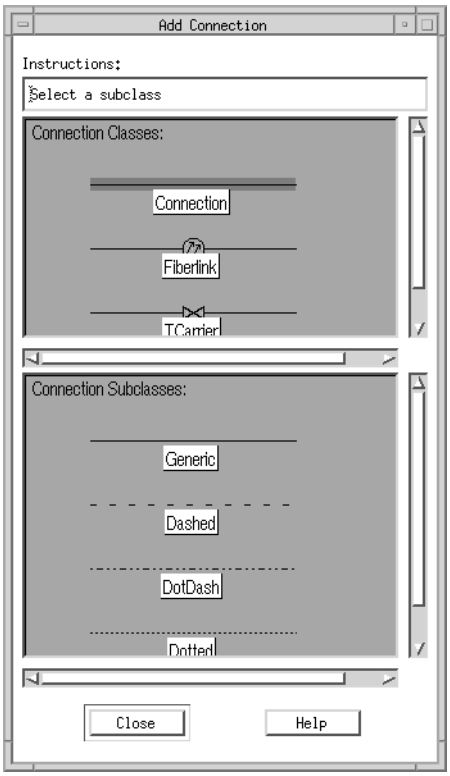


Figure 7-7. Add Connection Dialog Box With Connection Class Selected

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

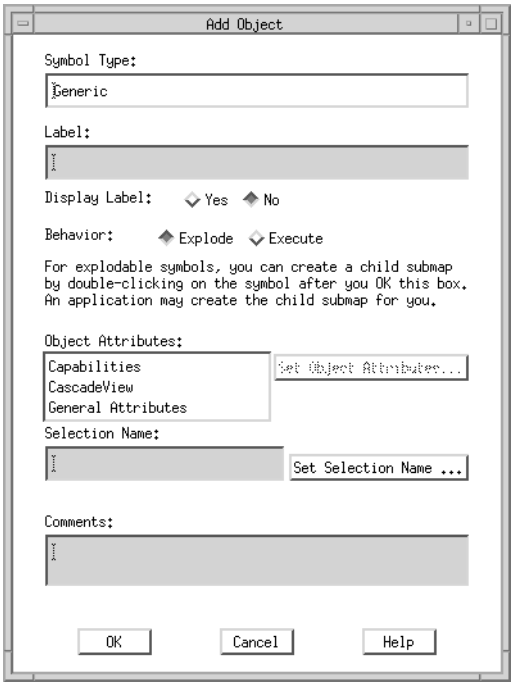


Figure 7-8. Add Object Dialog Box

5. Complete the Add Object dialog box fields described in Table 7-6.

Table 7-6. Add Object Dialog Box Fields

Field	Action/Description
Symbol Type	Displays the type of connection you are adding to the network map.
Label	Enter the trunk name you specified on the Add Trunk dialog box (Figure 7-4 on page 7-22).
Display Label	Select Yes to have the label (name) appear beneath the switch object on the network map. Select No if you do not want the label to appear on the map.
Behavior	Select Explode to create the basic NavisCore network configuration. See your third-party HP OpenView documentation for more information about the Execute function.
Selection Name	Automatically defaults to the value entered in the Label field. The selection name must be unique throughout all HP OpenView objects. Lucent recommends that you leave the selection name as it appears.

6. Select Cascade View from the Object Attributes list box and then choose Set Object Attributes. The Add Object - Set Attributes dialog box appears (Figure 7-9).

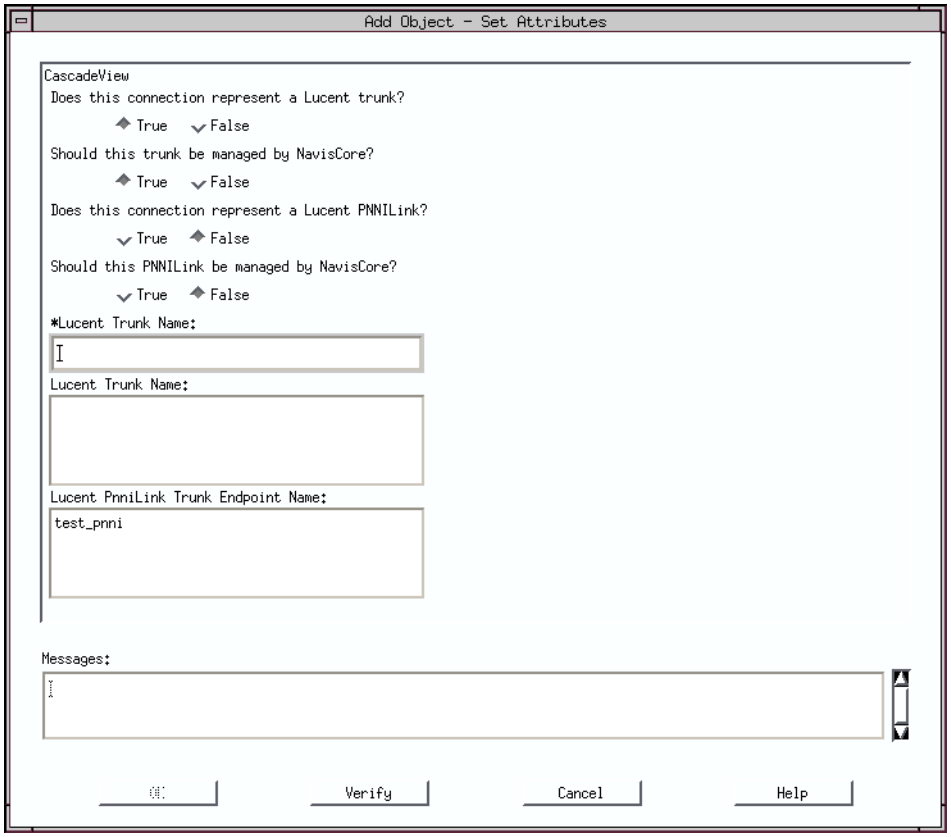


Figure 7-9. Add Object – Set Attributes Dialog Box

7. Complete the Add Object – Set Attributes dialog box fields as described in Table 7-7.

Table 7-7. Add Object – Set Attributes Dialog Box

Field	Action/Description
Does this connection represent a Lucent trunk?	Select True if this is a Lucent trunk. Otherwise, select False.
Should this trunk be managed by NavisCore?	Select True if you want NavisCore to manage this trunk. Otherwise, select False.
Does the connection represent a Lucent PNNI Link?	Select True if this is a Lucent Private Network-to-Network Interface (PNNI) link trunk endpoint. Otherwise, select False. See the "Creating a PNNI Link Line Connection" on page 20-48 for more information on PNNI links.
Should this PNNI Link be managed by NavisCore?	Select True if you want NavisCore to manage this PNNI link. Otherwise, select False. See the "Creating a PNNI Link Line Connection" on page 20-48 for details about managing PNNI links.
*Lucent Trunk Name	Select the name assigned to this trunk from the Lucent Trunk Name list box or from the Lucent PnniLink Trunk Endpoint Name list box. The name you select appears in the *Lucent Trunk Name field.

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

Displaying Multiple Trunks Between Switches

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

To display all trunk connections between two switches:

1. Double-click the left mouse button on the solid line between the switches. The system displays a trunk submap window similar to the one shown in Figure 7-10.

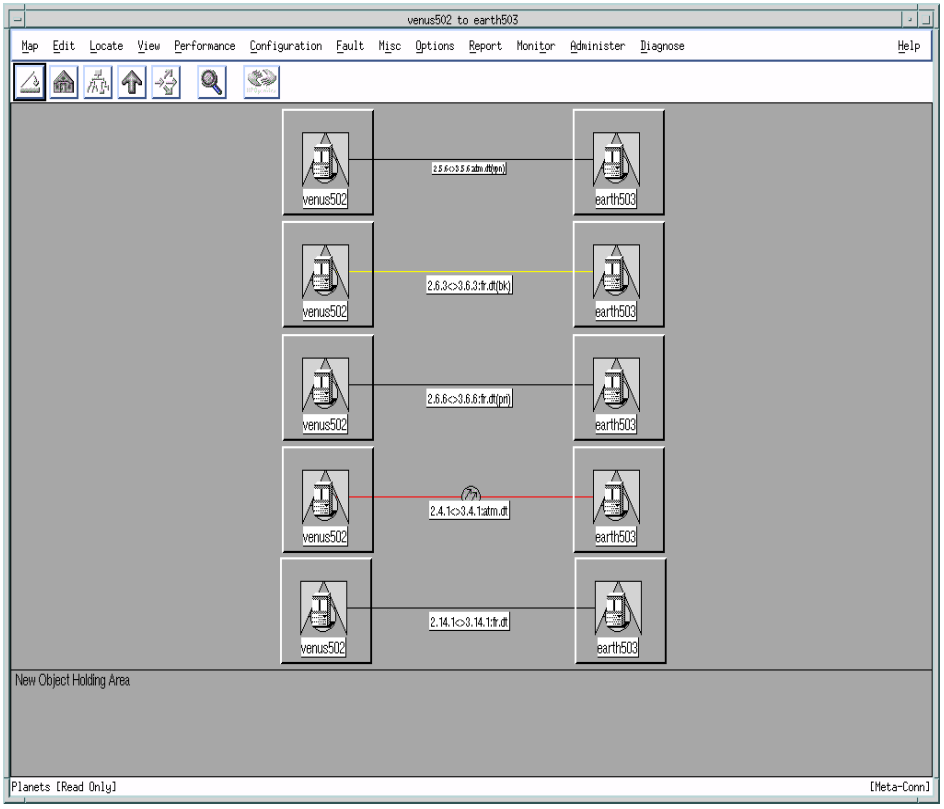


Figure 7-10. Trunk Submap Window

2. From the Map menu, select Submap ⇒ Close to return to the network map.

Understanding Trunk-Line Coloring

All associated trunks are polled for status according to the trunk poll timer. The trunk lines on the network map change color. These colors indicate trunk status according to the polled status and the traps received by the Lucent Alarms Browser. Table 7-8 describes the color scheme that identifies the status of a trunk connection on the network map.

Table 7-8. Trunk Line Color Status Indicators

Color	Status
Black	Either the line connection has not been defined as a trunk, or the environment variable $XUSERFILESEARCHPATH does not point to: **/opt/CascadeView/app-defaults**. [1]
Red	Trunk is down.
Blue	Trunk status is Unknown or Unmanaged.
Yellow	More than half the trunk connections are down.
Green	Trunk connection is Up.
Orange	Only one trunk connection, out of many connections, is Up.
Cyan	More than half the trunk connections are Up.

[1] If the Trunk graphic is black, set the following environment variable in .profile:
$ XUSERFILESEARCHPATH =/opt/CascadeView/app-defaults/%N
$ export XUSERFILESEARCHPATH

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

If you define more than one trunk connection between the same two switches, HP OpenView combines the status to display an orange, yellow, or cyan trunk line. To display a view of the individual connections, double-click on the trunk line and see Table 7-8 to interpret the trunk line color.

For details about trunk line coloring for PNNI links, see "Understanding PNNI Link Line Coloring" on page 20-50.

When you finish defining your trunk configuration(s) and trunk-line connection(s), proceed to Chapter 8, "Configuring ATM PVCs," to complete the network configuration.

Configuring APS Trunk Backup and Fast APS 1+1 for ATM Direct Trunks

This section describes the prerequisite tasks you must perform before you configure ATM direct trunk logical ports for APS trunk backup or Fast APS 1+1. This section also describes the following configuration procedures:

- Defining ATM direct trunk logical ports for APS and Fast APS 1+1
- Configuring the primary and backup trunk for APS trunk backup
- Configuring the primary trunk for Fast APS 1+1

Before You Begin

Before you define APS trunk backup or Fast APS 1+1, verify that you have completed the following configurations described in the *B-STDX, CBX, and GX Switch Module Configuration Guide*:

- Selected APS Trunk Backup or Fast APS 1+1 as the physical port redundancy option. For more information about these options, see "APS Options" on page 7-5.
- Configured two working ports (which are on two different switches) and their APS Trunk Backup/Fast APS 1+1 attributes.
- Configured two protection ports (which are on the same switches as the working ports) and their APS Trunk Backup/Fast APS 1+1 attributes.

Defining ATM Direct Trunk Logical Ports

The steps in this section describe how to configure direct trunk logical ports for APS trunk backup or Fast APS 1+1. For APS Trunk Backup, you must configure each of the physical ports (working and protection) with a direct trunk logical port. For Fast APS 1+1, you configure a direct trunk logical port on each working physical port only. (The protection port is automatically configured with the logical port settings that you define on the working port.) If a working port fails, trunk traffic is diverted to the protection port. See "About Automatic Protection Switching" on page 7-5 for more information.

To create a direct trunk logical port for each working and protection port:

1. Select the switch on which the first working/protection port pair resides.
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. (ATM Trunk Backup only) Select the working port (of the APS pair) and choose Attrs. The Set Physical Port Attributes dialog box appears.
   a. Choose APS.

b. Select Direction and choose Bidirectional.

Note – Unidirectional APS is the default directional mode and is supported only by Fast APS 1+1 over PNNI on either a GX OC-3c/STM-1 or a GX OC-12c/STM-4 module connected to a BIO1 module. Bidirectional mode must be selected so ATM Direct Trunk may be selected as the logical port time.

c. Choose Close to return to the Set Physical Port Attributes dialog.

d. Choose Close to return to the Switch Back Panel dialog box.

4. Select the working port (of the APS pair) and press the third (right) mouse button to display a pop-up menu. Select Logical Port. The Set All Logical Ports in PPort dialog box appears.
5. Choose Add to display the Add Logical Port dialog box (Figure 3-3 on page 3-11).
6. Select ATM Direct Trunk as the logical port type.
7. Choose OK. The Add Logical Port dialog box reappears (Figure 3-3 on page 3-11).
8. Use the instructions in Table 3-4 on page 3-14 to set the Administrative Attributes fields.
9. (*Optional*) Select Set Traffic Descriptors Attributes to configure Node and Card traffic descriptors. The fields in Figure 7-11 appear.

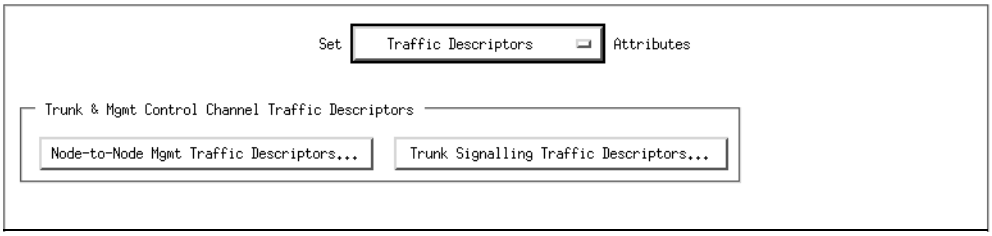


Figure 7-11. Set Traffic Descriptors Attributes Fields

a. Choose Node-to-Node Mgmt Traffic Descriptors. The Set Logical Port Node-to-Node Management Traffic Descriptor dialog box appears.

b. See "Defining Traffic Descriptor Attributes" on page 10-12 to complete the fields on this dialog box.

Note – To use the Add Traffic Descriptor field to define a new traffic descriptor, see "Defining Network-wide Traffic Descriptors" on page 10-9.

c. Choose OK to return to the Add Logical Port dialog box.

d. Choose Trunk Signaling Traffic Descriptors.

e. Repeat step b and step c to configure trunk signaling traffic descriptors.

10. When you finish, choose OK to return to the Set All Logical Ports in PPort dialog box.

11. Choose Close to return to the Set Physical Port Attributes dialog box.

12. Choose Close to return to the Switch Back Panel dialog box.

13. (APS Trunk Backup only) To configure an ATM Direct Trunk logical port for the protection port, repeat step 4 through step 12.

14. Choose Close to return to the network map.

15. Select the switch on which the second working/protection port pair resides and perform one of the following steps:

a. For APS Trunk Backup, complete step 2 though step 13 (beginning on page 7-34) to define ATM Direct Trunk logical ports for the second APS pair.

b. For Fast APS 1+1, complete step 2 though step 12 (beginning on page 7-34) to define an ATM Direct Trunk logical port for the second APS working physical port.

16. Continue with the following section to define the trunks for APS trunk backup or Fast APS 1+1.

Defining ATM Direct Trunks for APS Trunk Backup and Fast APS 1+1

See one of the following sections to configure trunks for APS trunk backup or Fast APS 1+1:

For APS trunk backup – Define the primary and backup trunks as described in:

- "Configuring the Primary Trunk for APS Trunk Backup" on page 7-36
- "Configuring the Backup Trunk for APS Trunk Backup" on page 7-37

For Fast APS 1+1 – Define the primary trunk as described in:

- "Configuring the Primary Trunk for Fast APS 1+1" on page 7-37

Configuring the Primary Trunk for APS Trunk Backup

1. From the Administer menu, select Lucent Parameters ⇒ Set All Trunks. The Set All Trunks dialog box (Figure 7-2 on page 7-14) appears.

2. Choose Add. The Select Logical Ports dialog box appears (Figure 7-3 on page 7-21).

3. Select the name of the switch where the first working port resides, then select the name of the switch where the second working port resides.

4. For each switch endpoint, select the ATM direct trunk logical port that resides on the working port.

5. Choose OK.
6. Complete the fields described in Table 7-4 on page 7-23. Be sure to select the Trunk Type *Primary.*
7. Use the instructions in Table 7-5 on page 7-25 to complete the additional fields that appear for a Primary Trunk.
8. Choose OK to complete this configuration.
9. Choose Close to return to the network map.

Configuring the Backup Trunk for APS Trunk Backup

1. From the Administer menu, select Lucent Parameters ⇒ Set All Trunks. The Set All Trunks dialog box (Figure 7-2 on page 7-14) appears.
2. Choose Add. The Select Logical Ports dialog box appears (Figure 7-3 on page 7-21).
3. Select the name of the switch where the first protection port resides, then select the name of the switch where the second protection port resides.
4. For each switch endpoint, select the ATM direct trunk logical port that resides on the protection port.

Note – Logical port endpoints 1 and 2 *must* reside on the same switch for both the primary and the backup trunks.

5. Choose OK.
6. Complete the fields described in Table 7-4 on page 7-23. Be sure to select the Trunk Type *Backup*.
7. When you select a Trunk Type of Backup, the dialog box displays the *Primary Trunk of the backup* field. Select the name of the primary trunk you configured using the corresponding APS working ports.
8. Choose OK to complete this configuration.
9. Choose Close to return to the network map.

Configuring the Primary Trunk for Fast APS 1+1

1. From the Administer menu, select Lucent Parameters ⇒ Set All Trunks. The Set All Trunks dialog box (Figure 7-2 on page 7-14) appears.
2. Choose Add. The Select Logical Ports dialog box appears (Figure 7-3 on page 7-21).
3. Select the name of the switch where the first working port resides, then select the name of the switch where the second working port resides.
4. For each switch endpoint, select the ATM direct trunk logical port that resides on the working port.

5. Choose OK.
6. Choose OK to complete this configuration.
7. Choose Close to return to the network map.

Configuring Fast APS 1+1 for PNNI Links (GX 550 to PSAX 4500 Only)

This section describes the prerequisite tasks you must perform before you configure GX 550 PNNI link connections for Fast APS 1+1 interworking with the PSAX 4500. This section also describes how to define GX 550 ATM NNI logical ports for Fast APS 1+1.

Note – This section describes procedures for configuring Fast APS 1+1 for GX 550 PNNI links only. This feature enables Fast APS 1+1 PNNI interworking with PSAX 4500 devices. For information on configuring Fast APS on the PSAX 4500 device, see the customer documentation provided with your PSAX 4500 product.

Before You Begin

In order to use Fast APS 1+1 on a GX 550 PNNI link to a PSAX 4500, you need to configure PNNI node parameters for each switch that supports PNNI in the network. See Chapter 20, "Configuring PNNI Routing" for more information on enabling the PNNI routing protocol.

In addition, verify that you have completed the following configurations described in the *B-STDX, CBX, and GX Switch Module Configuration Guide*:

- Selected Fast APS 1+1 as the physical port redundancy option. For more information about this option, see "APS Options" on page 7-5.
- Configured one working port on the GX 550 Multiservice WAN switch and one working port on the PSAX 4500 device.
- Configured one protection port on the GX 550 Multiservice WAN switch and one protection port on the PSAX 4500 device.

Defining ATM NNI Logical Ports for PNNI Links

The steps in this section describe how to configure ATM NNI logical ports on GX 550 switches defined as PNNI links for Fast APS 1+1. You must configure each working physical port on the GX 550 with an ATM NNI logical port (including PNNI parameters). (The protection port is automatically configured with the logical port settings that you define on the working port.) If a working port fails, SVCs and SPVCs traversing the link are preserved and diverted to the protection port. See "About Automatic Protection Switching" on page 7-5 for more information.

To create an NNI logical port for each GX 550 working and protection port:

1. Select the GX 550 switch on which the first working/protection port pair resides. (You will define an NNI logical port for the working physical port.)
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the working port (of the APS pair) and press the third (right) mouse button to display a pop-up menu. Select Logical Port. The Set All Logical Ports in PPort dialog box appears.
4. Choose Add to display the Add Logical Port dialog box (Figure 3-3 on page 3-11).
5. Select ATM NNI as the logical port type.
6. Choose OK. The Add Logical Port dialog box reappears (Figure 3-3 on page 3-11).
7. Use the instructions in Table 7-9 to set the logical port attributes.

Table 7-9. Configuring an ATM NNI Logical Port

Use the instructions on	To set the
page 3-14	Administrative Attributes to enter a logical port name
page 3-22	ATM Attributes to select the ATM Protocol, PNNI 1.0
page 3-28	ILMI/Signaling/OAM Attributes to enable signaling. For PNNI logical ports, signaling is enabled by default and ILMI is disabled.
page 3-36	ATM FCP Attributes (*optional*)
page 3-50	SVC attributes: • SVC Connection ID Parameters • SVC Parameters • SVC Priorities • SVC TD Limits • ATM SVC Parameters

8. Select Set PNNI Parameters Attributes to display the following fields:

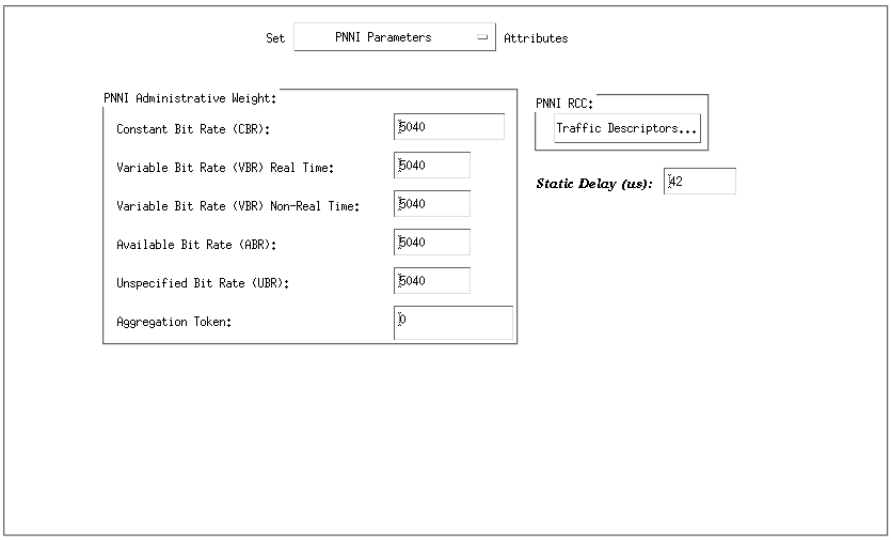


Figure 7-12. Set PNNI Parameters Attributes Fields

The Set PNNI Parameter Attributes menu enables you to configure the PNNI administrative weight status by assigning an administrative weight to each QoS category field. This weight allows you to configure the network to favor one path over another path for a given category. The weights of all the network interfaces along a path are added up, and switches choose the path with the lowest cumulative weight when making routing decisions. For example, suppose that VBR-RT traffic has two available paths for reaching a given destination: one path has a weight of 1000 and the other path has a weight of 4000. If the call requests VBR-RT QoS and administrative weight as a metric and if the path has sufficient bandwidth and other metric resources, the switch will choose the path with the weight of 1000.

In a network that supports, for example, both CBR and UBR calls, you can configure PNNI Administrative Weight values so that the switch will choose one path for the CBR calls and a different path for the UBR calls.

9. Complete the fields described in Table 7-10.

Table 7-10. PNNI Parameters Attributes Fields

Field	Action/Description
Constant Bit Rate (CBR)	Indicates the administrative weight to assign to the CBR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Variable Bit Rate (VBR) Real Time	Indicates the administrative weight to assign to the VBR-RT QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Variable Bit Rate (VBR) Non-Real Time	Indicates the administrative weight to assign to the VBR-NRT QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Available Bit Rate (ABR)	Indicates the administrative weight to assign to the ABR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Unspecified Bit Rate (UBR)	Indicates the administrative weight to assign to the UBR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Aggregation Token	Enter a value in this 4-byte field to identify a PNNI outside link that interconnects two separate peer groups. The default value is 0 (zero). The aggregation token determines how this link is aggregated at the next higher level in the hierarchy. Outside links connecting the same two peer groups are aggregated if they have the same aggregation token or if one link has an aggregation token value of 0 (zero). If the aggregation tokens of different outside links are not equal and nonzero, each will be advertised in a separate horizontal link PTSE by the associated parent LGN nodes. ***Note:*** *The aggregation token value is important only for outside links where the neighboring nodes belong in different peer groups.*
PNNI RCC	Allows you to configure the traffic descriptor values for PNNI routing control channels (RCCs). The RCC is a virtual channel connection (VCC) used between neighboring nodes for the exchange of PNNI routing protocol messages. Choose the Traffic Descriptors button to display the Set Logical Port PNNI RCC Traffic Descriptors dialog box (see Figure 10-3 on page 10-12 to view the dialog box fields). Use step 2 through step 4 beginning on page 10-12 to configure PNNI RCC traffic descriptor values.

Table 7-10. PNNI Parameters Attributes Fields (Continued)

Field	Action/Description
Static Delay (µs)	Static delay for PNNI links in a path is summed to determine the end-to-end delay of the path. Higher values represent slower links. The valid range for this field is 0 (zero) to 167777214 µsec. Default values (in microseconds) are: DS1 – 522 DS3 – 42 OC-3c/STM-1 – 22 E1 – 370 E3 – 41 OC-12c/STM-4 – 10 ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

10. Use the instructions on page 3-43 to complete the logical port configuration.

11. Repeat step 2 through step 9 beginning on page 7-40 for each ATM NNI logical port you need to configure.

Note – For information about configuring Virtual NNI logical ports, see "Virtual UNI/NNI" on page 2-10. Virtual logical ports allow you to configure more than one logical port on the same physical port. Each logical port that you configure uses a portion of the total physical port bandwidth.

12. When you finish, choose OK to return to the Set All Logical Ports in PPort dialog box.

13. Choose Close to return to the Switch Back Panel dialog box.

14. Choose Close to return to the network map.

Note – To complete the configuration, you must configure an ATM NNI logical port for the PSAX 4500 working/protection port pair. For more information, see the customer documentation provided with your PSAX 4500 product.

Note – If PNNI routing is configured on the switch (see "Before You Begin" on page 7-39), Fast APS 1+1 will be enabled once you have created an ATM NNI logical port (including PNNI parameters) on each end of the PNNI link connection.

For more information on using the PNNI routing protocol in your Lucent network, see Chapter 20, "Configuring PNNI Routing."

Configuring External Trunks

An external trunk provides a connection between two nodes on a NavisCore map. You can configure this trunk type to connect a Lucent switch (B-STDX 8000/9000, CBX, or GX) to some other network device. You can configure the endpoints as either ATM or Frame Relay.

An external trunk has two endpoints. The endpoints can be either a logical port (Lucent switch) or an external interface. The external interface resides on an external network device. You define this device as an *external device object*.

Use the following sequence to add a device object to the NavisCore map and connect this device to a Lucent switch object:

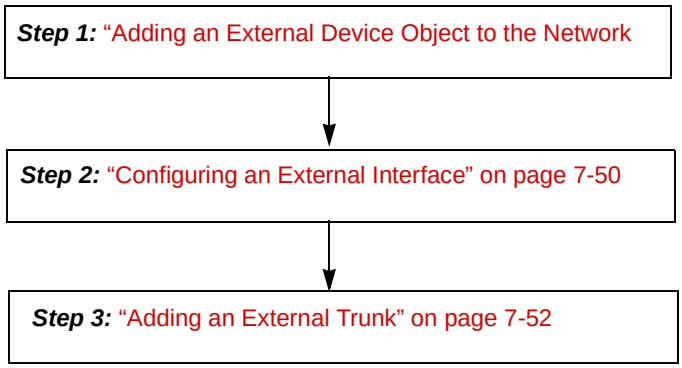


Figure 7-13. External Trunk Configuration Sequence

Adding an External Device Object to the Network Map

The NavisCore network map provides a graphical representation of your network. As you design the network map, you add a variety of device objects (such as an external device) to represent the various elements in your network.

The external device object on the NavisCore network map represents a network device other than a Lucent switch. Once you add this device object to the network map, you can then create an external trunk to connect the device to a Lucent switch.

To add an object to the map:

1. From the Edit menu, select Add Object. The Add Object Palette dialog box appears.

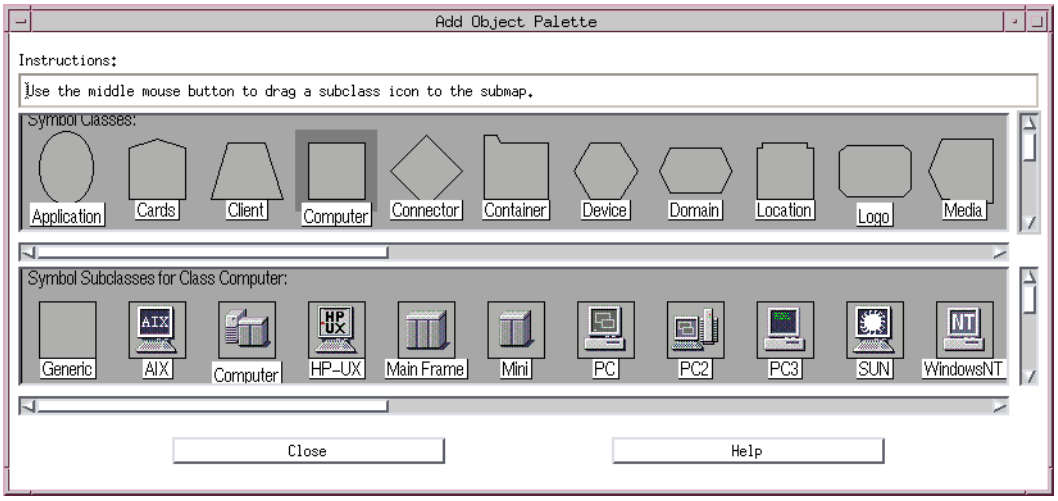


Figure 7-14. Add Object Palette

2. In the Symbol Classes list box, select the device object (for example, Computer). The Symbol Subclasses box displays additional object types.
3. Select the desired object type (for example, Workstation).
4. To add this object to the Network map, select the desired external device object icon. Using the middle mouse button, select, drag, and release the object to the map. The Add Object dialog box appears.

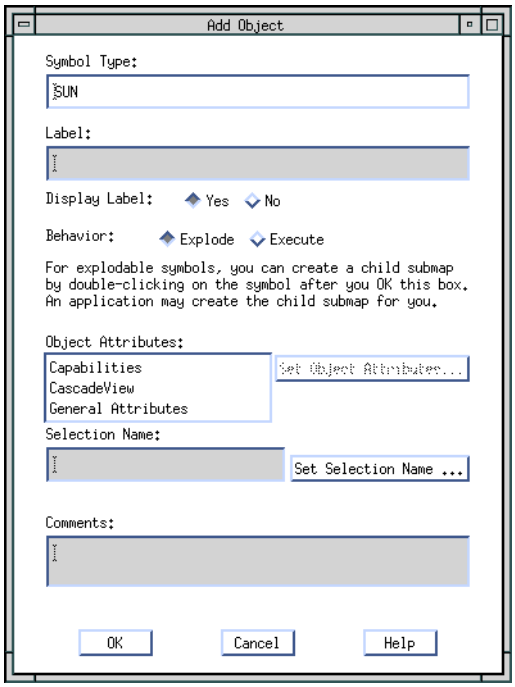


Figure 7-15. Add Object Dialog Box (External Device)

5. Complete the fields described in Table 7-11.

Table 7-11. Add Object Dialog Box Fields (External Device)

Field	Action/Description
Symbol Type	Displays the selected object type to add to the network map.
Label	Enter a label to describe 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 your third-party HP OpenView documentation for more information about using the Execute function.
Object Attributes	Select CascadeView. Then choose Set Object Attributes. The Add Object - Set Attributes dialog box (see Figure 7-9) appears.
Selection Name	Automatically defaults to the value entered in the Label field. The selection name must be unique throughout all HP OpenView objects. Lucent recommends that you leave the selection name as it appears.
Comments	Enter any additional information pertaining to this object.

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

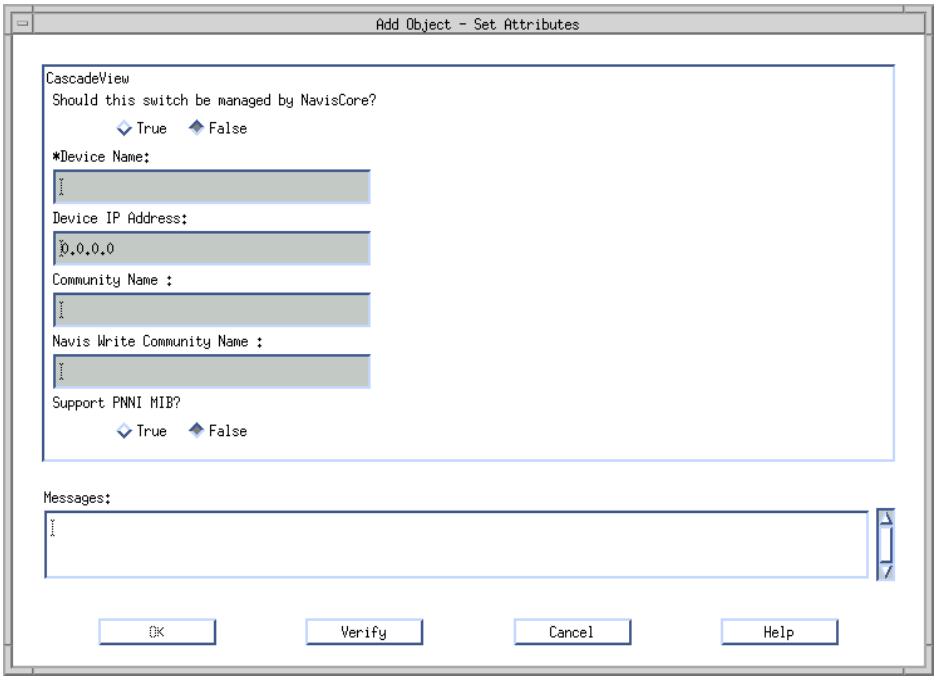


Figure 7-16. Add Object – Set Attributes Dialog Box (External Device)

7. Complete the fields described in Table 7-12.

Table 7-12. Add Object – Set Attributes Fields (External Device)

Field	Action/Description
Should this switch be managed by NavisCore?	Select True to enable NavisCore to manage this device.
* Device Name	Enter a unique name for the device.
Device IP Address	Enter the IP address for this device.
Community Name	Enter the name of the SNMP community to which this device belongs (for example, public).
Navis Write Community Name	Enter the name of the read-write SNMP community to which this device belongs (for example, public).
Support PNNI MIB?	If this device needs to support PNNI services, select Yes to enable this device to support the PNNI MIB.

8. Choose Verify to configure your settings. The following message appears in the Message field:

```
Verification has completed
```

Note – 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 Log on from the Misc menu. Enter the default operator login, *cascade*.

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

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

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

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

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

Configuring an External Interface

The external device contains an external interface. This interface is similar to a logical port in that it represents the interface point to which you can connect the external device to the Lucent switch via an external trunk.

To configure the external interface:

1. From the Administer menu, select Lucent External Parameters ⇒ Set All External Interfaces. The Set All External Interfaces dialog box appears.

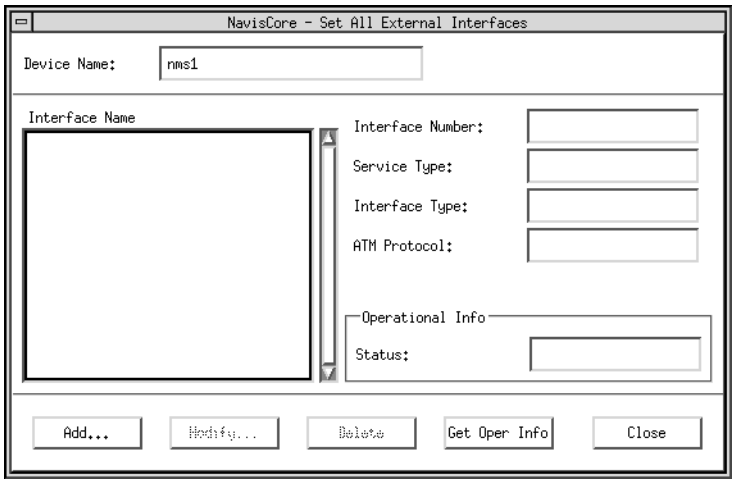


Figure 7-17. Set All External Interfaces Dialog Box

The Set All External Interfaces dialog box lists the names and attributes of any existing external interfaces.

2. Choose Add. The Add External Interface dialog box appears.

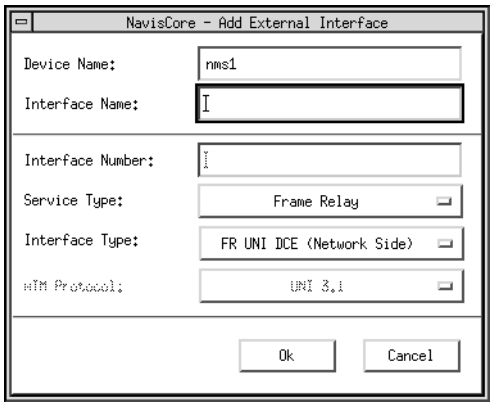


Figure 7-18. Add External Interface Dialog Box

3. Complete the fields described in Table 7-13.

Table 7-13. Add External Interface Dialog Box Fields

Field	Action/Description
Device Name	Displays the name of the external device or SA device on which you are configuring the external interface.
Interface Name	Enter a unique 32-character name for this interface.
Interface Number	Enter a unique number to identify this interface.
Service Type	Select the type of service, either Frame Relay or ATM, that this interface will support.
Interface Type	Select one of the following interface types to correspond with the type of service this interface connection will provide: **Frame Relay**: FR UNI DCE (Network Side) FR UNI DTE (User Side) FR NNI **ATM**: ATM UNI DCE ATM UNI DTE ATM NNI
ATM Protocol	(*ATM only*) The equipment to which you connect this port must support the protocol you select. Lucent logical ports support the following protocols: UNI 4.0 UNI 3.1 UNI 3.0 IISP 3.1 IISP 3.0 ITU UNI BICI 1.1 (*NNI only*) PNNI 1.0 (*NNI only*)

4. Choose Ok to complete this configuration and return to the Set All External Interfaces dialog box (Figure 7-17 on page 7-50).

5. Choose Close to return to the network map.

Adding an External Trunk

The external trunk represents the connection between the Lucent switch object's logical port and the device's external interface.

To add an external trunk:

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

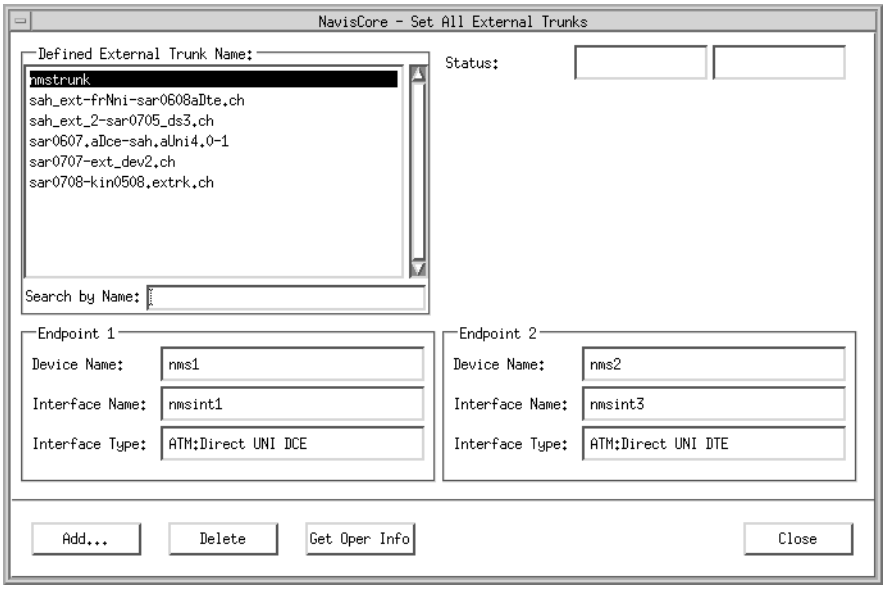


Figure 7-19. Set All External Trunks Dialog Box

The Set All External Trunks dialog box lists the names and attributes of any existing external trunks.

2. Choose Add. The Select Interfaces dialog box appears.

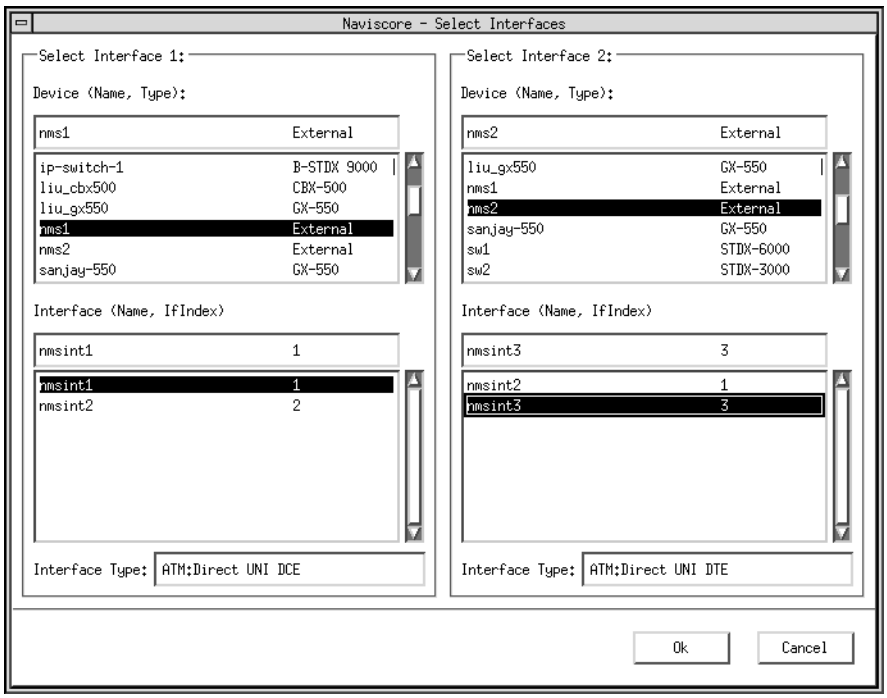


Figure 7-20. Select Interfaces Dialog Box

3. Provide the following information for both Select Interface 1 and Select Interface 2 fields:

a. Select the name of the Lucent switch or device where the first endpoint resides, then select the name of the switch or device where the second endpoint resides.

b. Select the name of Interface 1, then select the name of Interface 2. Remember that for an external device, the logical port represents the external interface for this endpoint.

4. Choose Ok. The Add External Trunk dialog box appears.

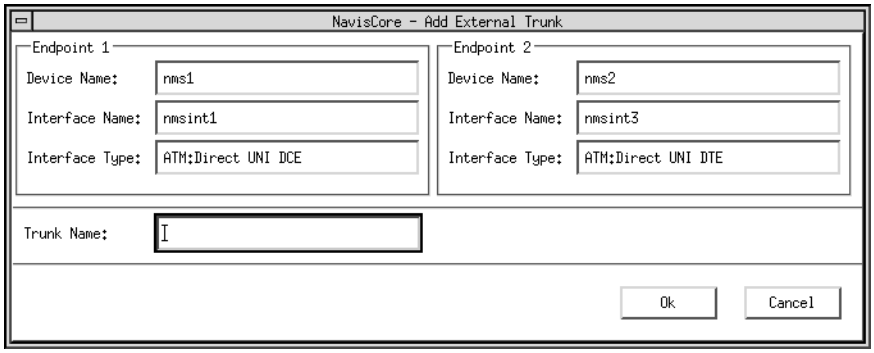


Figure 7-21. Add External Trunk Dialog Box

The Add External Trunk dialog box displays the names and logical port types for both endpoints. It also displays information to identify the physical location of the endpoints inside their respective devices (Slot ID, PPort ID).

5. Complete the fields described in Table 7-14.

Table 7-14. Add External Trunk Dialog Box Fields

Field	Action/Description
Device Name	Displays the name of the external device or SA device on which you are configuring the external interface.
Interface Name	Enter a unique 32-character name for this interface.
Interface Type	Select one of the following interface types to correspond with the type of service this interface connection will provide: **Frame Relay**: FR UNI DCE (Network Side) FR UNI DTE (User Side) FR NNI **ATM**: ATM UNI DCE ATM UNI DTE ATM NNI
Trunk Name	Enter a unique alphanumeric name to identify the trunk.

6. In the Interface Name field, enter a unique alphanumeric name up to 32 characters long to identify this trunk.
7. Choose Ok to return to the Set All External Trunks dialog box (Figure 7-19 on page 7-52).
8. Choose Close to return to the network map.
9. Draw the trunk line connection. See "Creating a Trunk Line Connection" on page 7-27 for more information.

Configuring VNN OSPF

Lucent switches can perform routing tasks using IP and Virtual Network Navigator (VNN) routing software. Both IP and VNN support the Open Shortest Path First (OSPF) routing protocol. In previous releases of Lucent switch software, VNN and IP shared the same OSPF software component to perform their OSPF routing tasks. However, VNN and IP now have their own OSPF software components, or *instances*. These instances are called *VNN OSPF* and *IP OSPF*.

VNN OSPF is supported in Lucent switches that are configured as Autonomous System boundary routers (ASBRs). In an Autonomous System (AS) each switch belongs to an area. Switches configured as ASBRs exchange routing information with other ASs via external gateway routing protocols, such as BGP. The external route information collected through these protocols is then aggregated and flooded through the AS.

VNN OSPF is typically configured over Lucent trunks. This section describes how to configure loopback addresses, area aggregates, external route aggregates, and virtual links for VNN OSPF. It also describes how to configure VNN OSPF optimized flooding and VNN OSPF Name LSA suppression, which enhance VNN OSPF performance.

For details about how IP OSPF and VNN OSPF interoperate, as well as step-by-step configuration procedures for IP OSPF, see the *B-STDX and CBX IP Services Configuration Guide*.

Configuring VNN OSPF Loopback Addresses

To configure loopback addresses for VNN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN Loopbacks. The Set All VNN Loopback Addresses dialog box appears (see Figure 7-22).

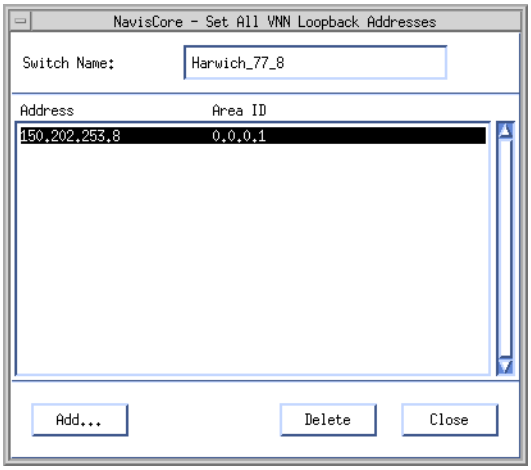


Figure 7-22. Set All VNN Loopback Addresses Dialog Box

2. Choose Add. The Add VNN Loopback Address dialog box appears (Figure 7-23).

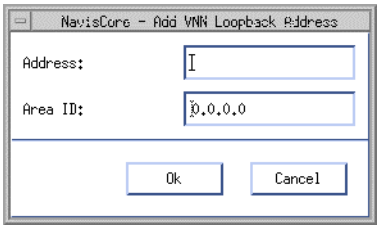


Figure 7-23. Add VNN Loopback Address Dialog Box

3. Enter the loopback IP address (for example, 152.148.30.5).
4. Enter the Area ID (for example, 0.0.0.2).
5. Choose OK. The Set All VNN Loopback Addresses dialog box appears, displaying the new loopback address.

Configuring VNN Area Aggregates

To configure area aggregates for VNN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN Area Aggregates. The Set All VNN Area Aggregates dialog box appears (Figure 7-24).

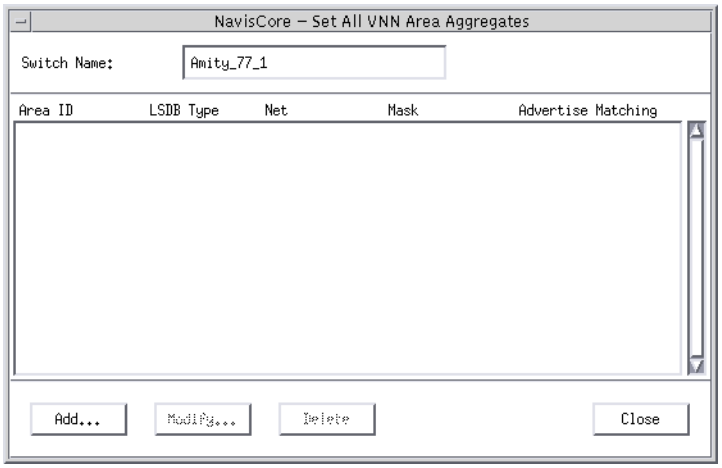


Figure 7-24. Set All VNN Area Aggregates Dialog Box

2. Choose Add. The Add VNN Area Aggregate dialog box appears (Figure 7-25).

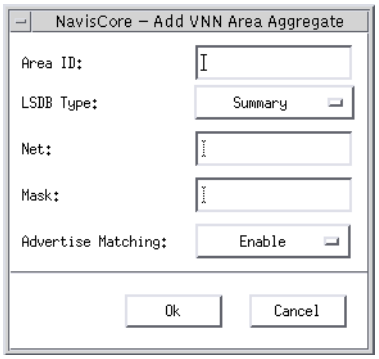


Figure 7-25. Add VNN Area Aggregate Dialog Box

3. Complete the fields described in Table 7-15.

Table 7-15. Add VNN Area Aggregate Dialog Box Fields

Field	Action/Description
Area ID	Enter the ID (x.x.x.x) of the area in which the IP address range is located. Area 0.0.0.0 is the network backbone. Areas are collections of networks, hosts, and routers. The area ID identifies the area.
LSDB Type	Specify the link state database type to which this address aggregate applies. The only option is as follows: *Summary* – (default) Area border routers generate summary link advertisements, which describe inter-area routes (routes between areas) to networks. ***Note:*** *NSSA External is not a supported option for VNN OSPF area aggregates. It is only supported for IP OSPF area aggregates.*
Net	Enter the IP address of the network or subnetwork that encompasses the range of addresses you want to advertise.
Mask	Enter the subnet mask that pertains to the net or subnet.
Advertise Matching	Select one of the following options: *Enable* – (default) If you enable this parameter, you "leak" the net/mask you specified for the given area, making it available to the rest of the network. *Disable* – If you disable this parameter, you hide the net/mask you specified for the given area.

4. When you are done setting parameters, choose OK.

Configuring VNN OSPF Virtual Links

To configure virtual links for VNN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN Virtual Links. The Set All VNN Virtual Links dialog box appears (Figure 7-26).

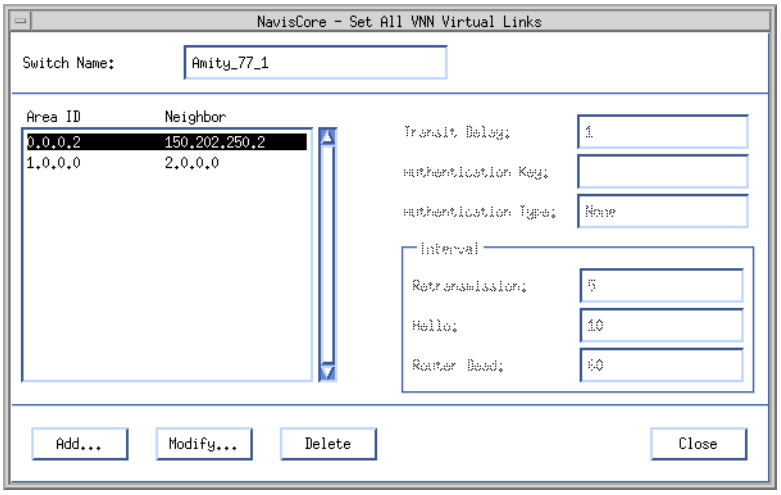


Figure 7-26. Set All VNN Virtual Links Dialog Box

2. Choose Add. The Add VNN Virtual Link dialog box appears (see Figure 7-27).

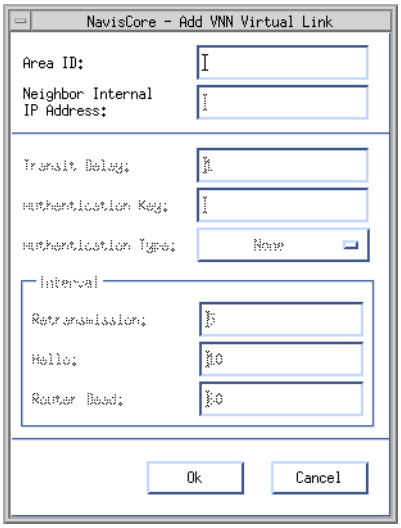


Figure 7-27. Add VNN Virtual Link Dialog Box

3. Complete the fields described in Table 7-16.

Table 7-16. VNN OSPF Virtual Link Fields

Field	Action/Description
Area ID	Enter the area ID (x.x.x.x) of the transit area, which is the non-backbone area that the virtual link traverses to connect to the backbone area. This ID cannot be 0.0.0.0 (the Area ID of the backbone area). Areas are collections of networks, hosts, and routers. The area ID identifies the area. ***Note:*** *VNN OSPF virtual links require a loopback address configured in both area border routers, where the area is equal to the area ID. For instance, if the area ID is 0.0.0.99, then the loopback address must also be 0.0.0.99.*
Neighbor Internal IP Address	Enter the internal IP address of the switch (that is, the neighbor) on the other end of the virtual link. The internal IP address is configured when the switch is installed. To determine the internal IP address, access the switch console and issue the `show system` command. In the command output, the internal IP address appears in the Internal IP Addr field. For example: `Internal IP Addr: 150.202.77.2` In this example, the internal IP address is 150.202.77.2.

4. Choose OK.
5. At the Set All VNN Virtual Links dialog box, choose Close.

Configuring VNN/OSPF External Route Aggregates

Configuring VNN/OSPF external route aggregates allows the VNN/OSPF on a Lucent switch to aggregate Autonomous System External Link State Advertisements (ASE LSAs) for routes learned from another autonomous system via another routing protocol, such as BGP. This can reduce the number of ASE LSAs that need to be installed in the VNN/OSPF database, thereby minimizing memory and CPU usage.

Note – To configure VNN/OSPF external route aggregates, you must be running one of the following *minimum* switch software releases:

- CBX 500 switch software Release 08.01.00.00
- GX 550 switch software Release 08.01.00.00

Configuring VNN External Route Aggregates

This section describes how to configure VNN external route aggregates in a Lucent network.

To configure external route aggregates for VNN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN External Route Aggregates. The Set All VNN External Routes Aggregates dialog box appears (Figure 7-24).

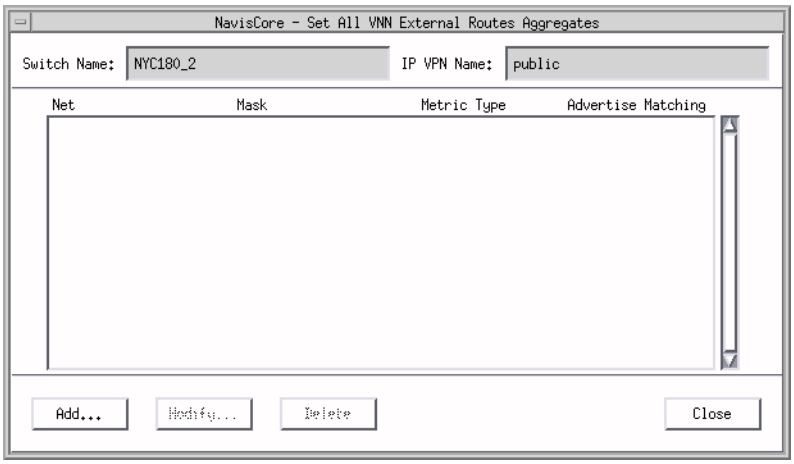


Figure 7-28. Set All VNN External Routes Aggregates Dialog Box

2. Choose Add. The Add VNN External Routes Aggregate dialog box appears (Figure 7-25).

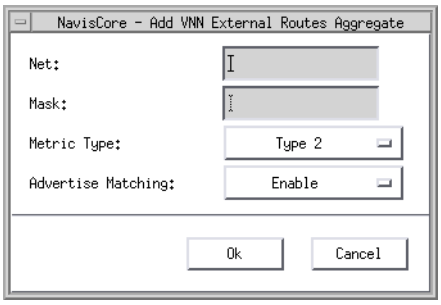


Figure 7-29. Add VNN External Routes Aggregate Dialog Box

3. Complete the fields described in Table 7-15.

Table 7-17. Add VNN/OSPF External Routes Aggregate Dialog Box Fields

Field	Action/Description
Net	Enter the IP address of the network or subnetwork that encompasses the range of addresses you want to advertise.
Mask	Enter the subnet mask that pertains to the net or subnet.
Metric Type	Select one of the following options to calculate the administrative cost for the external network: *Type 1* - The total cost is equal to the cost specified by the preferred routing table entry for the Autonomous System Border Router (ASBR) or forwarding address *plus* the cost specified in the LSA. If IC = the cost specified by routing table for ASBR and EC = the cost specified in the LSA, then the Type 1 cost = IC + EC. *Type 2* - (default) The total cost is equal to the cost specified by the LSA only, regardless of internal cost to ASBR. If IC = the cost specified by routing table entry for ASBR and EC = the cost specified in the LSA, then the Type 2 cost = EC. ***Note:*** *Type 1 routes are typically preferred over Type 2 routes. The Type 2 metric assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal metrics.*
Advertise Matching	Select one of the following options: *Enable* – (default) If you enable this parameter, you "leak" the net/mask you specified for the given area, making it available to the rest of the network. Enabling this option allows the switch to advertise the aggregate routes as well as the individual routes. *Disable* – If you disable this parameter, you hide the net/mask you specified for the given area. Disabling this option causes only the aggregate routes to be advertised, while the individual routes will be suppressed.

Note – VNN/OSPF external aggregation will aggregate only those type-5 routing entries that match the Type configured in external aggregation. For example, if routes are configured as:

- 10.10.1.1. and 10.10.1.2 as Type 1 and
- 10.10.1.4 as Type 2

then aggregation configured with Net of 10.10.0.0, Mask of 255.255.0.0, Type 1, and Advertising Matching disabled, then only 10.10.1.1 and 10.1.1.2 will aggregate as 10.10.0.0. The route of 10.10.1.4 will not be affected since the Type does not match the configured aggregate.

4. When you are done setting parameters, choose OK.

Modifying VNN External Route Aggregates

To modify an existing VNN external route aggregate:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN External Route Aggregates. The Set All VNN External Routes Aggregates dialog box appears (see Figure 7-28 on page 7-61).
2. Select the VNN external route aggregate to modify.
3. Choose Modify. The Modify VNN External Route Aggregate dialog box appears. Only Metric Type and Advertise Matching fields may be modified.
4. Make changes to the VNN external route aggregate, then choose Ok to accept the changes.

Deleting VNN External Route Aggregates

To delete an existing VNN external route aggregate:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN External Route Aggregates. The Set All VNN External Routes Aggregates dialog box appears (see Figure 7-28 on page 7-61).
2. Select the VNN external route aggregate to be deleted.
3. Choose Delete.
4. When prompted with a delete confirmation message, choose OK to delete the VNN external route aggregate.

Configuring OSPF External Route Aggregates

This section explains how to configure OSPF external route aggregates in a Lucent switch network.

To configure external route aggregates for OSPF:

1. From the Administer menu, select Lucent IP Parameters ⇒ Set All OSPF ⇒ Set All OSPF External Routes Aggregates. The Set All OSPF External Routes Aggregates dialog box appears (Figure 7-30).

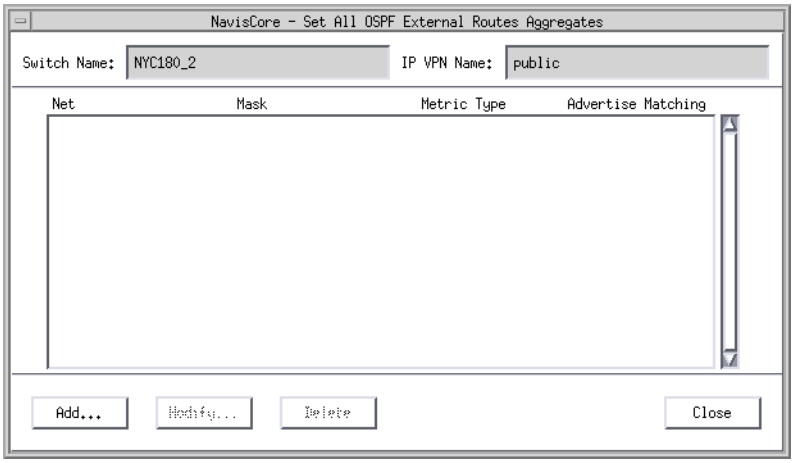


Figure 7-30. Set All OSPF External Routes Aggregates Dialog Box

2. Choose Add. The Add OSPF External Routes Aggregate dialog box appears (Figure 7-25).

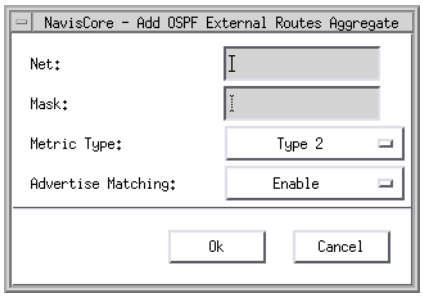


Figure 7-31. Add OSPF External Routes Aggregate Dialog Box

3. Complete the fields described in Table 7-17 on page 7-62.
4. When you are done setting parameters, choose OK.

Modifying OSPF External Route Aggregates

To modify an existing OSPF external route aggregate:

1. From the Administer menu, select Lucent IP Parameters ⇒ Set All OSPF ⇒ Set All OSPF External Routes Aggregates. The Set All OSPF External Routes Aggregates dialog box appears (see Figure 7-30 on page 7-64).
2. Select the OSPF external route aggregate to modify.
3. Choose Modify. The Modify OSPF External Route Aggregate dialog box appears. Only Metric Type and Advertise Matching fields may be modified.
4. Make changes to the OSPF external route aggregate, then choose Ok to accept the changes.

Deleting OSPF External Route Aggregates

To delete an existing OSPF external route aggregate:

1. From the Administer menu, select Lucent IP Parameters ⇒ Set All OSPF ⇒ Set All OSPF External Routes Aggregates. The Set All OSPF External Routes Aggregates dialog box appears (see Figure 7-30 on page 7-64).
2. Select the OSPF external route aggregate to be deleted.
3. Choose Delete.
4. When prompted with a delete confirmation message, choose OK to delete the VNN external route aggregate.

Configuring VNN OSPF Optimized Flooding

This section describes VNN OSPF optimized flooding and explains how to configure it in a Lucent switch network.

Note – To configure VNN OSPF optimized flooding, you must be running one of the following *minimum* switch software releases:

- CBX 500 switch software Release 08.00.03.00
- GX 550 switch software Release 08.00.03.00

About VNN OSPF Optimized Flooding

VNN OSPF, like IP OSPF, uses *flooding* as a reliable way to send link-state advertisements (LSAs) to ensure that all switches within the same OSPF area have identical link-state databases. Because multiple copies of each LSA travel through the network, standard OSPF flooding causes significant network traffic and increases CPU utilization on the switch. Configuring VNN OSPF optimized flooding enables you to reduce the number of identical LSAs that are flooded, received, and processed between Lucent switches in the same area connected by multiple parallel trunks.

To understand the benefits of VNN OSPF optimized flooding, it is helpful to compare it with how standard OSPF flooding works between switches in the same area connected by multiple parallel trunks.

Standard OSPF flooding — With standard OSPF flooding, one switch floods an LSA on all of its parallel trunk interfaces and the other switch receives this LSA on all of these interfaces. The receiving switch, in turn, floods the same LSA on all of its parallel trunk interfaces, with the exception of the interface on which it received the LSA.

As a result, the two switches flood, receive, process, and retransmit multiple copies of the same LSA throughout the network, while only the original LSA is stored in the receiving switch's link-state database. This repeated flooding of identical LSAs generates significant network traffic, consumes valuable CPU utilization and bandwidth, and increases the VNN and OSPF database sizes without distributing any additional topology information.

VNN OSPF optimized flooding — When you enable VNN OSPF optimized flooding on a Lucent switch connected to another switch in the same area by multiple parallel trunks, the switch establishes a single *neighbor-switch adjacency* in that area. The neighbor-switch adjacency identifies a neighbor at the switch level, and not at the trunk interface level (as is the case with standard OSPF). Each additional trunk that interconnects the two switches in the same area becomes part of the trunk interface list.

The switch then selects the first interface in the trunk interface list that has a fully adjacent neighbor relationship to serve as the *flooding interface* for LSAs. Once the flooding interface (also known as the *flooding trunk*) is selected, all subsequent LSAs are flooded, received, processed, and retransmitted only on this trunk interface and not on all parallel trunk interfaces between the two switches, as occurs with standard OSPF flooding. These LSAs are added to the neighbor-switch retransmission list, and not to the OSPF neighbor retransmission list on that trunk.

If the flooding trunk fails, the switch selects a new flooding trunk that inherits the neighbor-switch retransmission list from the original flooding trunk. This ensures that LSAs will be retransmitted on the new flooding trunk if the original flooding trunk fails before receiving acknowledgement for the LSAs.

Enabling this optimized VNN OSPF flooding mechanism has the following benefits in a Lucent switch network:

- Reduces the volume of network traffic caused by repeated flooding of identical LSAs on multiple parallel trunks
- Reduces CPU utilization and bandwidth consumption on the switch processor modules of both switches in a neighbor-switch adjacency; one switch floods fewer LSAs, and the other switch receives fewer LSAs to process
- Improves performance by reducing the sizes of the VNN and OSPF databases in the network

Note – To ensure that these benefits apply to both switches in the neighbor-switch adjacency, you should enable VNN OSPF optimized flooding on *both* switches interconnected by multiple parallel trunks.

Interoperability in Lucent Switch Networks

Switches with VNN OSPF optimized flooding enabled can interoperate in Lucent switch networks with either or both of the following:

- Lucent CBX 500 and GX 550 switches running Release 08.00.03.00 or greater on which VNN OSPF optimized flooding is disabled (the default setting)
- Lucent switches running releases *prior* to 08.00.03.00 that do not support the VNN OSPF optimized flooding feature

Switches on which VNN OSPF optimized flooding is disabled or unsupported will use standard OSPF flooding mechanisms to flood the LSAs on all multiple parallel trunk interfaces. The switch receiving the LSA will still acknowledge the LSA on the interface on which it was received, regardless of whether VNN OSPF optimized flooding is supported on that switch.

Enabling and Disabling VNN OSPF Optimized Flooding

To enable or disable VNN OSPF optimized flooding on a CBX 500 or GX 550 switch:

1. From the network map, select the appropriate switch object. (If you are not already logged on, select NavisCore ⇒ Logon from the Misc menu, and enter your operator password.)
2. From the Administer menu, select Lucent Parameters ⇒ Set All VNN ⇒ Set All VNN Optimized Flooding.The Set All VNN Optimized Flooding dialog box appears for the selected switch.

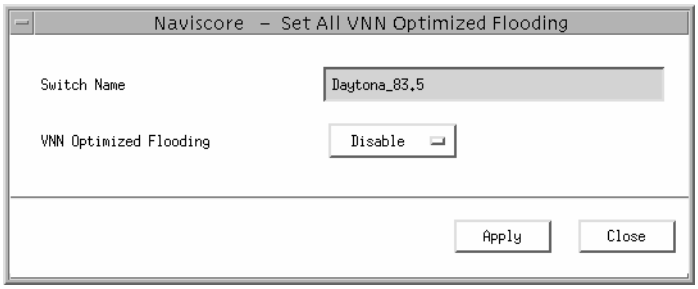


Figure 7-32. Set All VNN Optimized Flooding Dialog Box

3. In the VNN Optimized Flooding field, select one of the following options:
   - *Disable* — (default) Disables VNN OSPF optimized flooding on the switch.
   - *Enable* — Enables VNN OSPF optimized flooding on the switch.
4. Choose Apply to save your changes and close the dialog box.

Note – Lucent recommends that you enable VNN OSPF optimized flooding on *both* switches interconnected by multiple parallel trunks.

Monitoring VNN OSPF Optimized Flooding

You can access the Show All VNN Optimized Flooding dialog box from the Monitor menu to display the status (enabled or disabled) of VNN OSPF optimized flooding on your switch. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.

You can also run the command line interface (CLI) console commands listed in Table 7-18 to monitor the operation of VNN OSPF optimized flooding on your switch. For detailed information about using each command, see the *Console Command Reference*.

Table 7-18. VNN OSPF Optimized Flooding Console Commands

Console Command	Description
show vnn optflooding	Displays details about the status of each neighbor-switch adjacency and trunk interface established by the switch in one or more OSPF areas, including the state of the current flooding trunk in each area. You can also display these details for a specified neighbor switch in a specified area.
show vnn optflooding area	Displays results similar to the show vnn optflooding command for a specified OSPF area.
show vnn optflooding floodactive	Displays details about the currently active flooding trunks on the switch in each OSPF area, or for a specified neighbor switch.

Configuring VNN OSPF Name LSA Suppression

This section describes VNN OSPF Name LSA suppression and explains how to configure it in a Lucent switch network.

Note – To configure VNN OSPF Name LSA suppression, you must be running one of the following *minimum* switch software releases:

- CBX 500 switch software Release 08.00.03.00
- GX 550 switch software Release 08.00.03.00

About VNN Name LSA Suppression

For Lucent switches that use the Private Network-to-Network Interface (PNNI) protocol or require PNNI-VNN interoperability, a Lucent VNN switch floods NAME(3) and SUMM_NM(3) type LSAs over the VNN trunk interfaces. These LSAs bind the VNN switch IP address to an ATM address so the PNNI and VNN switches can communicate. However, generating these LSAs increases network traffic and consumes valuable CPU utilization and bandwidth, which imposes unnecessary overhead on switches that do not require PNNI-VNN interoperability.

You can suppress (disable) or enable the flooding of NAME(3) and SUMM_NM(3) LSAs for a Lucent switch, depending on whether that switch interoperates with PNNI switches in the network. If these LSAs are suppressed, they are not installed in the VNN database nor flooded over VNN trunk interfaces. However, this suppresses only the default VNN-Network Service Access Point (NSAP) address binding. Any other node prefixes or port prefixes that you configure will still generate NAME(3) and SUMM_NM(3) LSAs.

Enabling and Disabling VNN Name LSAs

To enable or disable Name LSA flooding on a CBX 500 or GX 550 switch:

1. From the network map, select the appropriate switch object. (If you are not already logged on, select NavisCore ⇒ Logon from the Misc menu, and enter your operator password.)
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel for the selected switch appears.

3. Choose Attrs. The Set Switch Attributes dialog box appears. Figure 7-33 shows an example of the Set Switch Attributes dialog box for a CBX 500 switch.

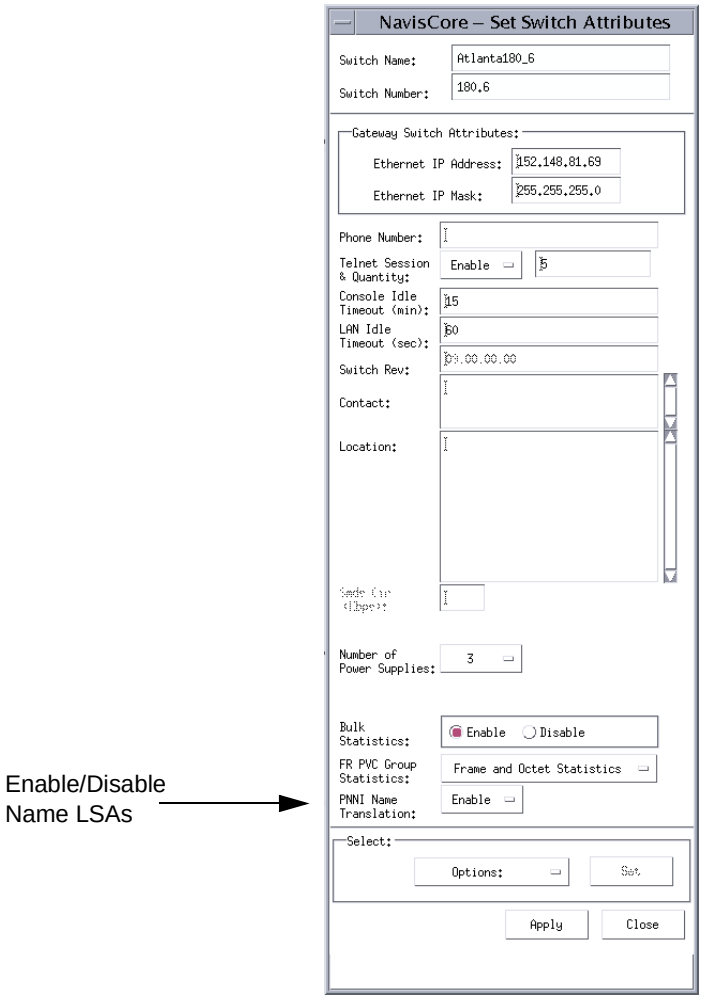


Figure 7-33. Set Switch Attributes Dialog Box (CBX 500)

4. In the PNNI Name Translation field, select one of the following options:
   - *Disable* — (default) Disables (suppresses) flooding of NAME(3) and SUMM_NM(3) LSAs for the specified switch. Use this option if the switch does not need to interoperate with PNNI switches in your network.
   - *Enable* — Enables flooding of NAME(3) and SUMM_NM(3) LSAs for the specified switch. Use this option if the switch must interoperate with PNNI switches in your network.
5. Choose Apply to save your changes and close the dialog box.

Monitoring VNN Name LSA Suppression

You can access the Show Switch Attributes dialog box from the Monitor menu to display the status (enabled or disabled) of NAME(3) LSA flooding on your switch. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.

8

Configuring ATM PVCs

This chapter describes how to configure the following types of Lucent ATM permanent virtual circuits (PVCs):

- Point-to-Point (page 8-22)
- Frame Relay-to-ATM Service Interworking (page 8-41)
- Redirect (page 8-62)
- Point-to-Multipoint (page 8-75)

In addition, this chapter explains how to manually define PVCs and use the Move Circuit function.

See Chapter 9, "Configuring Management Paths" for information about management PVCs, management SPVCs, and management redirect PVCs.

Note – For information about the virtual circuit capacity for various elements on a B-STDX, CBX, or GX switch, see the appropriate Switch SRN.

GX 550 VC Provisioning Guidelines

Base Input/Output (BIO) modules support the following number of VC connection entries, depending on type:

- BIO2 modules support a maximum of 32K connection entries per phy card (a total of 128K per BIO).
- 256-MB BIO1 modules support a maximum of 16K (16,348) connection entries per phy card (a total of 64K per BIO).
- 128-MB BIO1 modules support a maximum of 8K (8,156) connection entries per phy card (a total of 32K per BIO).

n

Note – For information on the BIO-C module, see the *GX BIO-C, OC-48c/STM-16c, and SF2 Modules User's Guide*.

To determine the type of BIO module you have, access the View Card Attributes dialog box in NavisCore. To determine your BIO size, access the View Card Attributes/Actual/Total Memory Size dialog box.

See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information on accessing the View Card Attributes dialog box.

BIO modules can store the following number of PVC endpoints in PRAM, depending on type:

- BIO2 modules can store 64,000 PVC endpoints.
- 256-MB BIO1 modules can store 16,000 PVC endpoints.
- 128-MB BIO1 modules can store 8,000 PVC endpoints.

The remainder of the BIO VC capacity is used by SVCs and/or VCs that traverse trunks on the BIO module.

Note – Keep the following VPI/VCI assignment guidelines in mind to maximize connection entry resource use. Failure to follow these guidelines may result in SNMP SET failures when provisioning PVCs.

- When you provision VCCs on a logical port and choose a VPI that is not currently in use on that logical port, a 1K block of connection entry resource is reserved for that VPI on that particular logical port (that is, VCIs 0-1023 are reserved for this VPI; VCIs 32 – 1023 are usable for PVC establishment). The size of the block reserved depends on the logical port VPI/VCI bit setting. The 1K block size applies if the default VPI/VCI bit setting of VPI bits = 4 and VCI bits = 10 is used.

  This means that if you provision VCCs of VPI/VCI = 1/100, 2/100, 3/100, 4/100 on a particular logical port, you would reserve 4K of connection entry resources just for those 4 VCCs. If you provision the VCCs with a VPI/VCI of 1/100, 1/101, 1/102, and 1/103 instead, you would reserve only the 1K block needed for VPI =1.

  Connection entry resources are reserved for each VCC VPI on a per-port basis. This means that if you configure a phy card with Port 1 having a VCC using a VPI/VCI of 1/100 and Port 2 also having a VCC with a VPI/VCI of 1/100, you reserve 1K for each of the ports (meaning 2K is consumed in total).

- When you provision VPCs on a logical port, the switch uses a different connection entry resource reservation process. For the first VPI associated with a VPC, 64 connection entries are reserved. Subsequent VPCs on the same phy card consume the remaining 63 connection entries. Once you provision 64 VPCs on the phy card, adding one more VPC reserves another 64 connection entries.

  When you provision VPCs, you still have the ability to use the full VCI range of 0-65535 within the VPC for VCCs. The connection entry reservation process does not limit the quantity of VCCs within the VPC.

  The `show ckt slot.port` console command provides details on the connection entry allocation for VCCs and VPCs on a per slot and per port basis. See the *Console Command Reference* for more information.

PVC Endpoint Rules

Table 8-1 can help you determine the following when PVCs are created:

- calling and called endpoints on the switch
- endpoint 1 and endpoint 2 in the NMS.

Table 8-1. PVC Endpoint Rules

PVC Type	Switch	NMS	Task
Both circuit endpoints are fixed[a] (Point-to-point PVC)	1. Higher switch IP address is always the caller. 2. If both endpoints are on same switch, the higher interface number is the caller.	1. Higher IP address is always endpoint 1 on NMS. 2. If both endpoints are on the same switch then higher interface number is always endpoint 2 on NMS.	1. See the Attributes for Object dialog box. 2. Use the **`show ospf names`** command to find the interface number. For more information, see the *B-STDX, CBX, and GX Switch Troubleshooting Guide*.
First endpoint is fixed[a] while second endpoint is variable[b] and primary[c]	Fixed endpoint is always the caller.	Fixed endpoint is always designated endpoint 2 in NMS.	See the Set All PVCs on Map dialog box (Figure 8-1 on page 8-10) in NavisCore.
First endpoint is variable and primary while second endpoint is fixed	Fixed endpoint is always the caller.	Fixed endpoint is always designated endpoint 2 in NMS.	See the Set All PVCs on Map dialog box (Figure 8-1 on page 8-10) in NavisCore.
Both endpoints are variable and primary	Higher Service Name Binding (SNB) ID is always the caller.	Higher SNB ID is designated as endpoint 2 in NMS.	Use the **`Cvlistcontained`** command in Provisioning Server to find the SNB ID. For more information, see the *B-STDX, CBX, and GX Switch Troubleshooting Guide*.
First endpoint is variable and primary while second endpoint is backed up[d]	Higher variable (SNB) is always the caller (even if backed up).	Backed up endpoint is always designated endpoint 1 in NMS.	For the switch, use the **`Cvlistcontained`** command in Provisioning Server to find the SNB ID. For more information, see the *B-STDX, CBX, and GX Switch Troubleshooting Guide*. For the NMS, see the Set All PVCs on Map dialog box (Figure 8-1 on page 8-10).
First endpoint is backed up while second endpoint is variable and primary	Sets whatever configuration is given from NavisCore.	Backed up endpoint is always designated endpoint 1 in NMS.	See the Set All PVCs on Map dialog box in NavisCore (Figure 8-1 on page 8-10).

[a] Fixed refers to endpoints that do not have an SNB configured.

[b] Variable refers to an endpoint with a SNB on the primary interface.

[c] Primary refers to an endpoint that is the primary logical port for a SNB.

[d] Backed up refers to endpoints where a backup logical port is active for a SNB.

Note – For more information on using the **`show ospf names`** and **`Cvlistcontained`** commands, see the *B-STDX, CBX, and GX Switch Troubleshooting Guide*.

PVC Establishment Rate Control

The PVC Establishment Rate Control feature dynamically adjusts the PVC retry rate of the I/O card where the calling endpoint resides.

PVC Establishment Rate Control works with the VC Overload Control feature in the call initiating switch, and reacts to changing conditions in the network by monitoring the PVC establishment success rate and adjusting the retry rate appropriately.

You can trace events related to the PVC Establishment Rate Control feature using the Event Log.

For more information on the VC Overload Control feature, "VC Overload Control" on page 8-6.

VC Overload Control and PVC Establishment Rate Control

This section describes the differences in how the PVC Establishment Rate Control feature works when the VC Overload Control feature is enabled or disabled.

PVC Establishment Rate Control When VC Overload Control Is Enabled

When the VC Overload Control feature is enabled, the PVC Establishment Rate Control feature varies the rate between a minimum of 20 calls/sec and the maximum allowed by the card without going into overload. Having VC Overload Control enabled on the call initiating switch sets the upper limit for the PVC re-establishment rate.

PVC Establishment Rate Control When VC Overload Control Is Disabled

When the VC Overload Control feature is disabled, PVC Establishment Rate Control reacts to changing conditions in the network by adjusting the rate from a minimum of 20 calls/sec to a maximum of 120 calls/sec.

VC Overload Control

This section describes the VC Overload Control feature, and includes the following topics:

- About VC Overload Control
- About Overload Severity Levels

About VC Overload Control

The VC Overload Control feature detects overload conditions and allows application load to be shed during high CPU utilization. Overload control prevents the sustained level of CPU utilization from exceeding 90% by directing switch applications to shed new service requests.

A CPU utilization rate of 90% provides administrative controls and diagnostic software with a sufficient amount of real-time bandwidth to maintain the integrity of the software.

In addition, VC Overload control affects system performance in the following ways:

- the number of successful completions during extended periods of high SVC setup and tear down requests increases up to 70% when this feature is enabled.
- PVC reroute rates are greater than the current fixed maximum rate up to the point that the CPU utilization rate reaches 90% or the reroute success rate is below 90%.
- maximum SVC setup and setup/tear down rates are approximately 10-15% lower when this feature is enabled.

VC Overload Control is supported for PVC, SVC, and SPVC processing.

You enable VC Overload Control on the Set Switch Attributes dialog box. For more information on this dialog box, and instructions for enabling VC Overload Control, see the *B-STDX, CBX, and GX Getting Started User's Guide*.

About Overload Severity Levels

The overload severity level for a card is displayed on the View Card Attributes dialog box. Overload severity levels are different on the CBX 500 and GX 550 switches and vary depending on the service requests currently running on the switch. At each severity level, a certain percentage of the following service requests are shed:

- SVC originations
- PVC originations
- PVC routing
- SVC routing
- PVC reroutes
- Circuit tear downs

The highest overload severity level is 10, where the card is in the highest overload condition and an application must shed all new service requests. The lowest overload severity level is 1.

An overload severity level of 0 indicates that there is currently no overload condition on the card.

For more information on viewing the Overload Control Setting and the Overload Security Level, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*

Reliable Scalable Circuit

The NavisCore Reliable Scalable Circuit feature (set to On by default) improves PVC configuration reliability. The NMS verifies that the card states for all standard PVC or redirect PVC endpoints are up before sending the `SNMP set` command to the corresponding cards in the end-point switches. If the card status of an endpoint is not up, the system displays an error message indicating where the failure occurred. The error message includes an abort option that allows you to cancel the PVC or redirect PVC configuration and prevent an out-of-sync card condition.

When enabled, the Reliable Scalable Circuit feature enables you to add, modify, or delete standard or redirect PVCs in the following scenarios:

Standard PVC	Redirect PVC
• Both switches are unmanaged.	• All three switches are unmanaged.
• Both switches are managed. Both cards (endpoints) have a status of Up.	• All three switches are managed. All three cards (endpoints) have a status of Up.
• One switch is unmanaged and one switch is managed. Both cards have a status of Up.	• One or two switches are unmanaged or one or two switches are managed. All cards have a status of Up.

For information on Reliable Scalable Circuit reported error types, see Appendix F.

Disabling the Reliable Scalable Circuit Feature

To disable this feature, edit the `cascadeview.cfg` file and remove the # sign from the following line:

```
#CV_CARD_STATS=DISABLE
#EXPORT CV_CARD_STATS
```

Setting the VPI/VCI Values for PVCs

For each PVC you configure, you must specify a value from 0-*nnnn* to represent the virtual path identifier (VPI) for the PVC (see page 8-25). The maximum value that you can specify is based on the Valid Bits in VPI that is configured for the logical port, as follows:

Maximum value = $2^P - 1$

where *P* is the value in the Valid Bits in VPI field. For example, if you entered 5 in the Valid Bits in VPI field, the maximum value is 31 ($2^5 - 1 = 31$), which would give you up to 32 virtual paths (numbered 0-31). See page 2-11 for details on setting the number of Valid Bits in VPI.

If you are defining a virtual channel connection (VCC), you must also specify a value to represent the virtual channel identifier (VCI) for an ATM circuit (see page 8-25). The maximum value that you can specify is based on the Valid Bits in VCI value that is configured for the logical port, as follows:

Maximum value = $2^C - 1$

where C is the value in the Valid Bits in VCI field. For example, if you entered 6 in the Valid Bits in VCI field, the maximum VCI value you can enter is 63 (which would give you 32 virtual channels, numbered 32 to 63).

Note – These VPI/VCI range restrictions only apply to VCCs. You can provision a virtual path connection (VPC) to any value in the VPI = 0-255 range. In addition, if the logical port uses the NNI cell header format, you can provision VPCs over the 0 - 4095 range. For more information on the Valid Bits in VPI/VCI fields, see page 2-11.

The VPI/VCI combination must be unique at each circuit endpoint (including multipoint circuits). As a result, since a VPC has access to all valid VCIs, a VCC or multipoint circuit that uses a VPI that is already assigned to a VPC cannot be established, nor can a VPC be established if the selected VPI is already assigned to a VCC or multipoint circuit.

Accessing the Set All PVCs On Map Dialog Box

The Set All PVCs On Map dialog box (Figure 8-1) displays status information for the circuit you select from the Defined Circuit Name (Circuit Alias Name) list box.

To access this dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Point-to-Point.

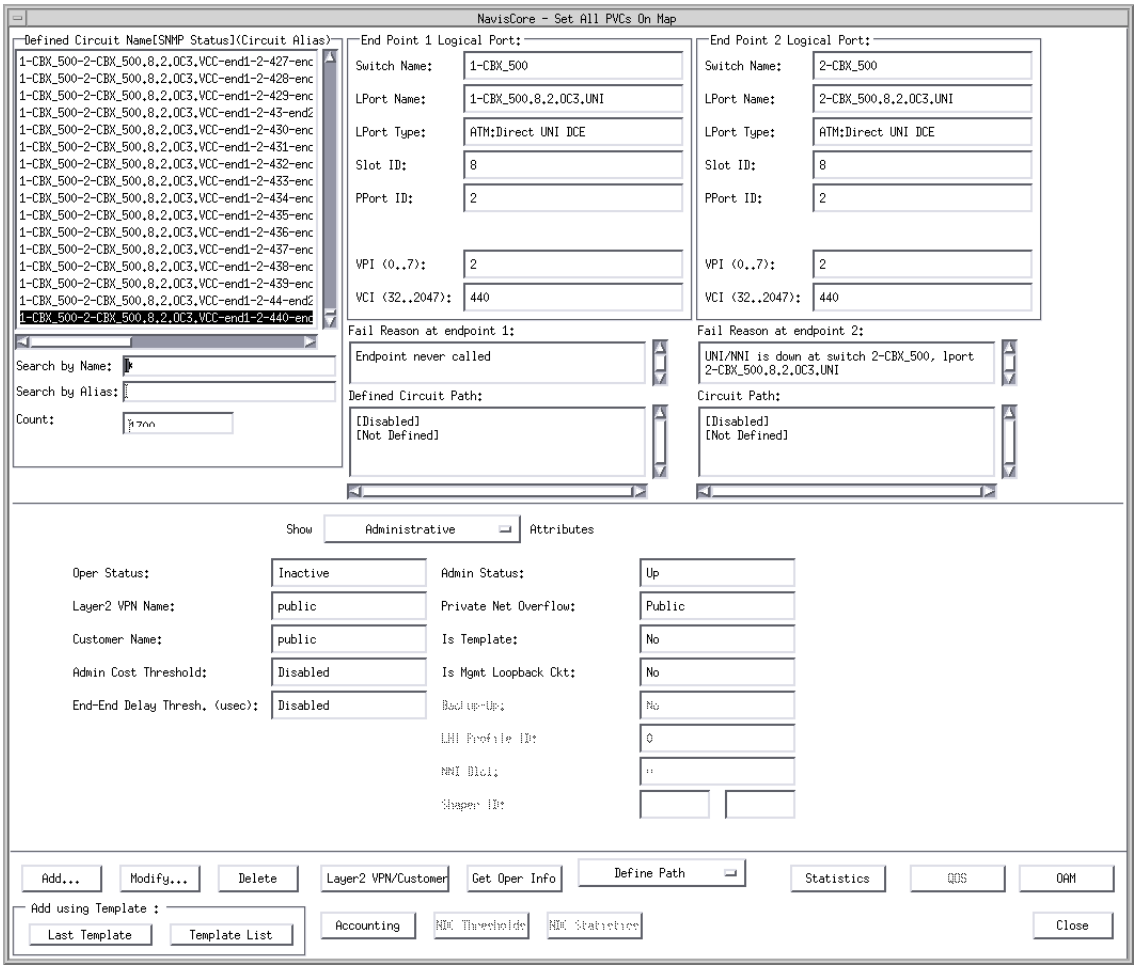


Figure 8-1. Set All PVCs On Map Dialog Box

- To view a list of configured circuits, position the cursor in the Search by Name field and press Return.
- To learn more about the Set All PVCs On Map dialog box, continue with the following section.
- To begin defining a PVC connection, proceed to page 8-22.

About the Set All PVCs On Map Dialog Box

The Set All PVCs On Map dialog box displays configured option information for the circuit name/circuit alias you select. Use any of the following wildcard searches in the Search by Name or Search by Alias field to find a specific circuit name or alias:

- Use an * to match any number of characters
- Use a ? to match a single character
- To match the * character, type *****
- To match the ? character, type **\?**
- To match the \ character, type \\

Table 8-2 describes the Set All PVCs On Map dialog box buttons.

Table 8-2. Set All PVCs On Map Dialog Box Buttons

Button	Action/Description
Add	Adds a new PVC.
Modify	Modifies the selected circuit. The Modify button displays dialog boxes that are similar to those displayed for Add circuit; however, you cannot modify the circuit name, logical port endpoints, circuit type, or VPI/VCI values from this dialog box.
Delete	Deletes the selected circuit.
Layer2 VPN/ Customer	Assigns the selected circuit to a specific Layer2 VPN and customer name.
Get Oper Info	Displays the selected circuit's current operational status in the Oper Status field. See Oper Status on page 8-14 for an explanation of these status messages.
Define Path	Manually defines a circuit path (see page 8-69).
Statistics	Displays the summary statistics for the selected circuit.
OAM	Runs the Operations, Administration, and Management loopback diagnostics for the selected circuit.
Add using Template	If you have already defined a circuit configuration and saved it as a template, use this command to define a new circuit using similar parameters. • Choose Last Template to apply the last template you used to establish a circuit in this NMS session. • Choose Template List to display a list of previously defined templates for this map.
Accounting	Accesses the NavisXtend Accounting server functions for a PVC.

Table 8-2. Set All PVCs On Map Dialog Box Buttons (Continued)

Button	Action/Description
NDC Thresholds (*CBX 500 and GX 550 only*)	Displays the configured Network Data Collection (NDC) thresholds for the selected circuit. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
NDC Statistics (*CBX 500 and GX 550 only*)	Displays the NDC statistics for the selected circuit. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
Close	Exits this dialog box and returns to the network map.

Table 8-3 describes the Set All PVCs On Map dialog box fields.

Table 8-3. Set All PVCs On Map Dialog Box Fields

Field	Action/Description
Defined Circuit Name (Circuit Alias Name)	Displays a listing of the circuits configured in the network. Use a wildcard search to find a specific circuit name. If applicable, this field also lists the configured circuit alias.
Count	Displays the number of circuits found depending on the criteria used in the Search by Name field.
End Point 1 Logical Port and End Point 2 Logical Port	The dialog box displays the following logical port information for each circuit endpoint: *Switch Name* – Displays the name of the switch at each circuit endpoint. *LPort Name* – Displays the name of the logical port at each circuit endpoint. *LPort Type* – Displays the configured logical port type at each circuit endpoint. *Slot ID* – Indicates the physical slot number where the I/O module containing the selected port is installed. *PPort ID* – Displays the ID number of the physical port on which the selected logical port is configured. *VCI (1..nnnn)* – Displays the VCI for the selected circuit endpoint. For more information on the Valid Bits in VPI/VCI fields, see page 2-11.
Fail Reason at endpoint 1 and Fail Reason at endpoint 2	Displays the reason a selected circuit failed (if any) for a given endpoint. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for a description of these failure reasons.
Defined Circuit Path	Displays the configured circuit path.

Table 8-3. Set All PVCs On Map Dialog Box Fields (Continued)

Field	Action/Description
Circuit Path	Displays the actual path that OSPF and/or PNNI selected for this circuit to use to get to its destination.
Show [Administrative] Attributes	Displays the appropriate attributes configured for the selected option. See one of the following sections for more information: *For ATM PVCs:* "Administrative Attributes" on page 8-27 "Traffic Type Attributes" on page 8-30 "User Preference Attributes" on page 8-32 "Frame Discard Attributes" on page 8-36 "Extended QoS Parameters Attributes" on page 8-37 "Selectable Statistics Attribute" on page 8-39 *For Interworking PVCs:* "Administrative Attributes" on page 8-27 "Traffic Type Attributes" on page 8-52 "User Preference Attributes" on page 8-57 ***Note:*** *See the* B-STDX, CBX, and GX Switch Diagnostics User's Guide *for more information about NDC configuration and functions.*
Admin Status	Displays whether the selected circuit is online (Up) or offline (Down).
Layer2 VPN Name	Assigns the selected circuit to a specific Layer2 VPN and customer name.
Private Net Overflow	Displays how PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Displays one of the following values: *Public* – (default) PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Customer Name	Displays the customer name for the selected PVC (if applicable).

Table 8-3. Set All PVCs On Map Dialog Box Fields (Continued)

Field	Action/Description
Oper Status	Displays the current operational status of the selected circuit. Messages include: *Active* – The circuit is operational through the network end-to-end. *Inactive* – The circuit is not operational. Check the Fail Reason at endpoint fields for possible explanations. *Unknown* – The NMS cannot reach the higher-numbered node for status. (If the circuit is an intra-switch PVC, then the NMS cannot reach the highest-numbered logical port.) *Invalid* – The circuit definition is not found in the higher-numbered node. You may need to save the circuit definition; it may also be necessary to PRAM synch the host card.
Is Template	Displays Yes if you can use this circuit as a template to create other circuits using similar parameters.
Admin Cost Threshold	If you enable this option, the PVC will not be routed over a path whose total administrative cost exceeds the entered value. This means that if you enable this field and enter a value of 1000, the PVC will not be routed over a path whose total administrative cost exceeds 1000. The total administrative cost for a path is calculated by summing the administrative cost for each trunk in the path. The valid range of values for this field is 1 - 4294967295. ***Note**: Do not enable this option if you use End-End Delay routing.*
Is Mgmt Loopback Ckt	Display the current state of this PVC configuration in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity. This option is especially useful in some management configurations.
Backup-up	Indicates whether the selected circuit has a backup circuit. Options include: *No* – (default) This circuit does not have a backup circuit. *Yes* – This circuit has a backup circuit.
End-End Delay Thresh. (µsec) (cell transfer delay)	Displays the maximum acceptable delay for traffic using this PVC to traverse the network. The valid range of values is 1 - 16777214.

About Redirect PVCs

This section describes how to configure redirect permanent virtual circuits (PVCs) for ATM UNI and NNI logical ports. Redirecting PVCs provides PVC backup recovery in the event of data terminal equipment (DTE) state changes.

Redirecting PVCs enables you to configure a PVC with the following three end points:

- Pivot
- Primary
- Secondary

Each end point has its own port and VPI/VCI combination. Typically, traffic follows the path between the pivot and primary end points. When the primary end point goes down, a redirection (or switchover) of PVC traffic is triggered, either manually or automatically. The traffic then follows a path between the pivot and secondary end points. Redirecting PVCs takes place only if the called end point is down. Redirecting PVCs does not take place if the PVC segment within the Lucent network becomes inactive (for example, if there is no route to the primary end point, or the trunk is down).

Note – You cannot configure PVC redirection on a Point-to-Point (PPP) logical port or a GX 250 extender.

Note – The product formerly called the GX 250 Multiservice Extender is now referred to as the GX 550 ES (Extender Shelf) in the NavisCore NMS interface.

The NavisCore NMS may display features that are not available in this release. For a complete list and explanation of each of the features that are supported in this release, see the NavisCore Software Release Notice.

Accessing the Set All Redirect PVCs On Map Dialog Box

The Set All Redirect PVCs On Map dialog box (Figure 8-2) displays status information for the circuit you select from the Defined Circuit Name (Circuit Alias Name) list box.

To access this dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Redirect. The Set All Redirect PVCs on Map dialog box appears.

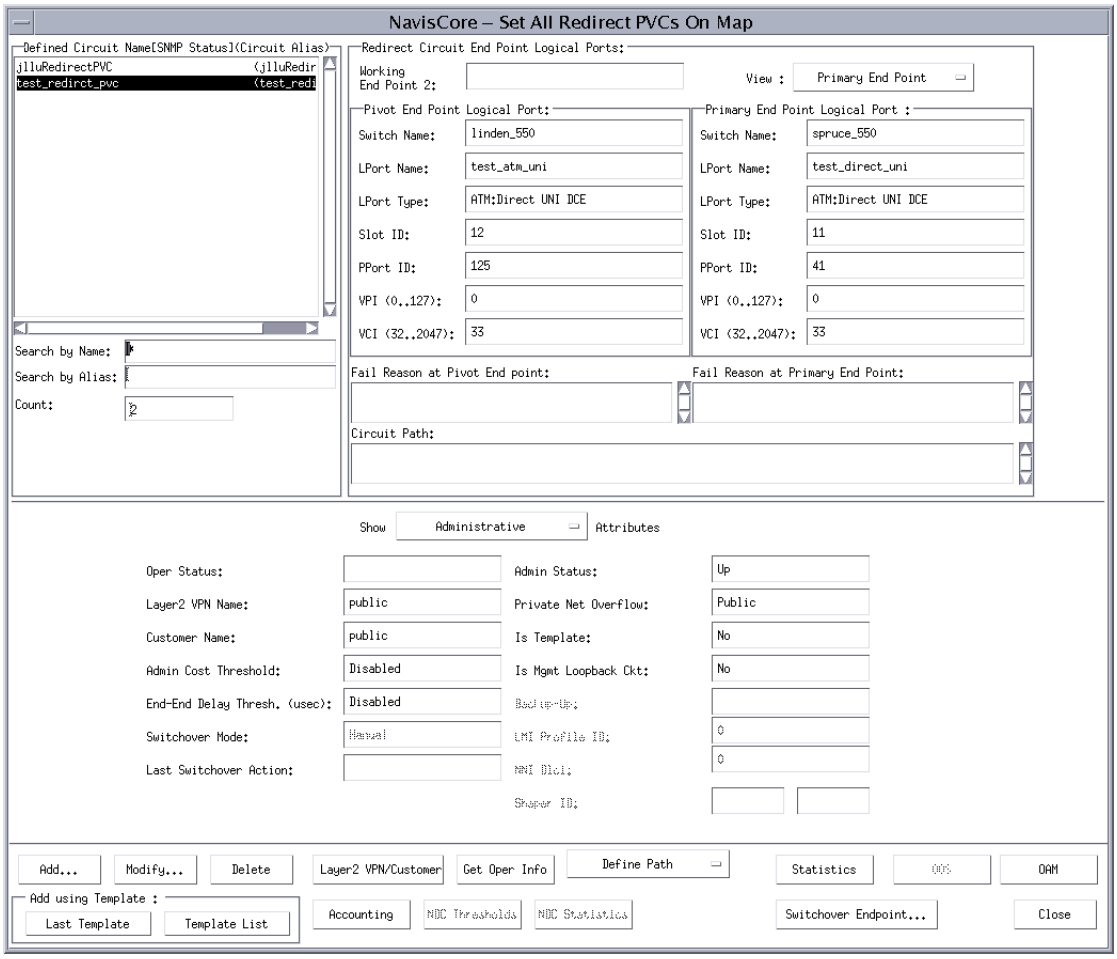


Figure 8-2. Set All Redirect PVCs On Map Dialog Box

- To view a list of configured circuits, position the cursor in the Search by Name field and press Return.
- To learn more about the Set All Redirect PVCs On Map dialog box, continue with the following section.
- To configure a Redirect PVC connection, proceed to page 8-62.

About the Set All Redirect PVCs On Map Dialog Box

Table 8-4 describes the Set All Redirect PVCs dialog box buttons.

Table 8-4. Set All Redirect PVCs On Map Dialog Box Buttons

Button	Description
Add/Modify/Delete	Enables you to add a new redirect PVC or modify or delete an existing redirect PVC.
Layer2 VPN/Customer	Assigns the selected circuit to a specific VPN and customer name.
Get Oper Info	Displays a status message in the Oper Status field for the selected circuit. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
Statistics	Displays the summary statistics for the selected circuit. For more information about summary statistics, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*. ***Note:*** *If you switch endpoint views from primary to secondary on the Set All Redirect PVCs dialog box without first closing the statistics display, the statistics display does not refresh automatically. To see statistical information for the new view, you must close and then reopen the Circuit Summary Statistics dialog box.*
QoS	Displays the Quality of Service values for the selected circuit. For more information about QoS, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*. For a description of the QoS classes, see "Setting Quality of Service Parameters" on page 3-44.
Add Using Template	If you have already defined a redirect circuit configuration and saved it as a template, you can use this option to define a new redirect circuit. ***Note:*** *You create templates for redirect PVCs the same way that you do for standard PVCs. However, the template lists for redirect and traditional PVCs are maintained separately.*
Accounting	Accesses the NavisXtend accounting server functions for a PVC. For information about the accounting server functions, see the *NavisXtend Accounting Server Administrator's Guide*.

Table 8-4. Set All Redirect PVCs On Map Dialog Box Buttons (Continued)

Button	Description
Switchover Endpoint	Displays the Switchover End Point dialog box, which enables you to reconfigure redirect circuit traffic for end point 2 to primary or secondary when the DTE state of the primary or secondary end point fails. Switchover End Point is available/unavailable depending on the following *switchover mode* configurations: • You can switch end points in either direction when you configure *manual* switchover mode. • You can only switch end points backward (from the working secondary to the primary end point) when you configure *non-revertive* switchover mode. • You cannot switch end points manually when you configure *revertive* switchover mode. See the Switchover Mode field description in this table for mode definitions. See Table 8-19 on page 8-65 for information about configuring switchover mode.
Close	Exits the dialog box and returns to the network map.

Table 8-5 describes the Set All Redirect PVCs on Map dialog box fields.

Table 8-5. Set All Redirect PVCs On Map Dialog Box Fields

Field	Description
Defined Circuit Name (Circuit Alias Name)	Displays a list of the Redirect PVCs configured in the network. Use a wildcard search to find a specific Redirect PVC name. If applicable, this field also lists the configured Redirect PVC alias.
Count	Displays the number of Redirect PVCs found depending on the criteria used in the Search by Name field.
Redirect Circuit End Point Logical Ports	Displays the following logical port information for the redirect circuit's pivot, primary, and secondary end points: *Working End Point 2* – The end point to which the PVC is currently established from the pivot end point (end point 1). The working end point can be either the primary or the secondary end point. *View* – Enables you to view logical port information for either the primary or the secondary end points. This information displays in the second column.

Table 8-5. Set All Redirect PVCs On Map Dialog Box Fields (Continued)

Field	Description
Pivot End Point Logical Port	*Switch Name* – The name of the switch at the pivot end point. *LPort Name* – The name of the logical port for the switch at the pivot end point. *LPort Type* – The configured type of the selected logical port. *Slot ID* – The physical slot number where the I/O module containing the selected port is installed. *PPort ID* – The number of the physical port for which the selected logical port is configured. *VPI Number* – The VPI number chosen for the circuit. *VCI Number* – The VCI number chosen for the circuit.
Primary/Secondary End Point Logical Port	*Switch Name* – The name of the switch at the primary or secondary end point. *LPort Name* – The name of the logical port for the switch at the primary or secondary end point. *LPort Type* – The configured type of the selected logical port. The primary and secondary end points must have the same LPort type (for example, ATM: UNI DCE). *Slot ID* – The physical slot number where the I/O module containing the selected port is installed. *VPI Number* – The VPI number chosen for the circuit. *VCI Number* – The VCI number chosen for the circuit.
Fail Reason at Pivot End Point	Displays the reason a selected circuit failed (if any) for a given pivot end point. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for a description of reasons for circuit failures.
Fail Reason at Primary/Secondary End Point	Displays the reason a selected circuit failed (if any) for a given primary end point. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for a description of reasons for circuit failures.
Circuit Path	Displays the actual path that OSPF and/or PNNI selected for this circuit to use to get to its destination. ***Note:*** *The Defined Circuit Path field and Define Path button (see the Set All PVCs on Map dialog box (Figure 8-1 on page 8-10) are unavailable on the Set All Redirect PVCs dialog box. You cannot manually define a circuit path for a redirect PVC.*

Table 8-5. Set All Redirect PVCs On Map Dialog Box Fields (Continued)

Field	Description
Show [Administrative] Attributes	Displays the appropriate attributes configured for the selected option. See one of the following sections for more information: "Administrative Attributes" on page 8-27 "Traffic Type Attributes" on page 8-30 "User Preference Attributes" on page 8-32 "Frame Discard Attributes" on page 8-36 "Extended QoS Parameters Attributes" on page 8-37 ***Notes:*** *The Set Traffic Type Attributes information displayed in the Reverse column applies to both primary and secondary end points.* *See the* B-STDX, CBX, and GX Switch Diagnostics User's Guide *for more information about NDC configuration and functions.*
Oper Status	Displays the current operational status of the selected circuit. Messages include: *Active* – The circuit is operational through the network end-to-end. *Inactive* – The circuit is not operational. Check the Fail Reason at Pivot End Point and Fail Reason at Primary End Point fields for possible reasons. *Unknown* – The NMS cannot reach the higher-numbered node for status. (If the circuit is an intra-switch redirect PVC, then the NMS cannot reach the highest-numbered LPort.) *Invalid* – The circuit definition is not found in the higher-numbered node. You may need to save the circuit definition; it may also be necessary to PRAM synch the host card.
Admin Status	Displays whether the selected circuit is online (*Up*) or offline (*Down*).
Layer2 VPN Name	Assigns the selected circuit to a specific VPN and customer name.
Customer Name	Displays the customer name for the selected redirect PVC (if applicable).
Is Template	Displays Yes if you can use this circuit as a template to create other circuits using similar parameters.
Admin Cost Threshold	If you enable this option, the redirect PVC will not be routed over a path whose total administrative cost exceeds the entered value. This means that if you enable this field and enter a value of 1000, the PVC will not be routed over a path whose total administrative cost exceeds 1000. The total administrative cost for a path is calculated by summing the administrative cost for each trunk in the path. The valid range of values for this field is 1 - 4294967295. (Do not enable this option if you use End-End Delay routing.)

Table 8-5. Set All Redirect PVCs On Map Dialog Box Fields (Continued)

Field	Description
Is Mgmt Loopback Ckt	Display the current state of this redirect PVC configuration in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download this file to the switch, this redirect PVC can be used to establish NMS-to-switch connectivity. This option is especially useful in some management configurations.
End-End Delay Thresh. (µsec) (cell transfer delay)	Displays the maximum acceptable delay for traffic using this redirect PVC to traverse the network. The valid range of values is 1 - 16777214.
Backup-up	Indicates whether the selected redirect circuit has a backup circuit. Options include: *No* – (default) This redirect circuit does not have a backup circuit. *Yes* – This redirect circuit has a backup circuit.
Switchover Mode	Displays one of the following configurations: *Manual* – Enables you to switch the circuit connection between the pivot end point and the primary *or* secondary end point. *Non-Revertive* – Triggers an automatic forward switchover to establish the connection between the pivot and secondary end points in case of primary end point failure. If the secondary end point goes down and the primary end point recovers, no automatic switchover is triggered. The administrator must manually switch the circuit connection from the working secondary end point backward to the primary end point. *Revertive* – Triggers an automatic forward switchover to establish the connection between the pivot and secondary end points in case of primary end point failure. If the primary end point recovers, the backward switchover is triggered automatically to re-establish the connection between the pivot and primary end points. ***Note:*** *To implement redirect PVC with Revertive mode, the entire network must be upgraded to the current network management and switch software release.*
Last Switchover Action	Describes the action taken at the most recent switchover. This diagnostic information can include the following resolutions: • *gopri-manual* – switched over to primary endpoint, manually • *gopri-ondemand* – switched over to primary endpoint, automatically • *gosec-manual* – switched over to secondary endpoint, manually • *gosec-ondemand* – switched over to secondary endpoint, automatically

Defining a PVC Connection

To set up a PVC connection between two UNI or NNI logical ports:

1. See page 8-10 for instructions on accessing the Set All PVCs On Map dialog box (Figure 8-1 on page 8-10).
2. From the Set All PVCs On Map dialog box, choose Add. The Select End Logical Ports dialog box appears.

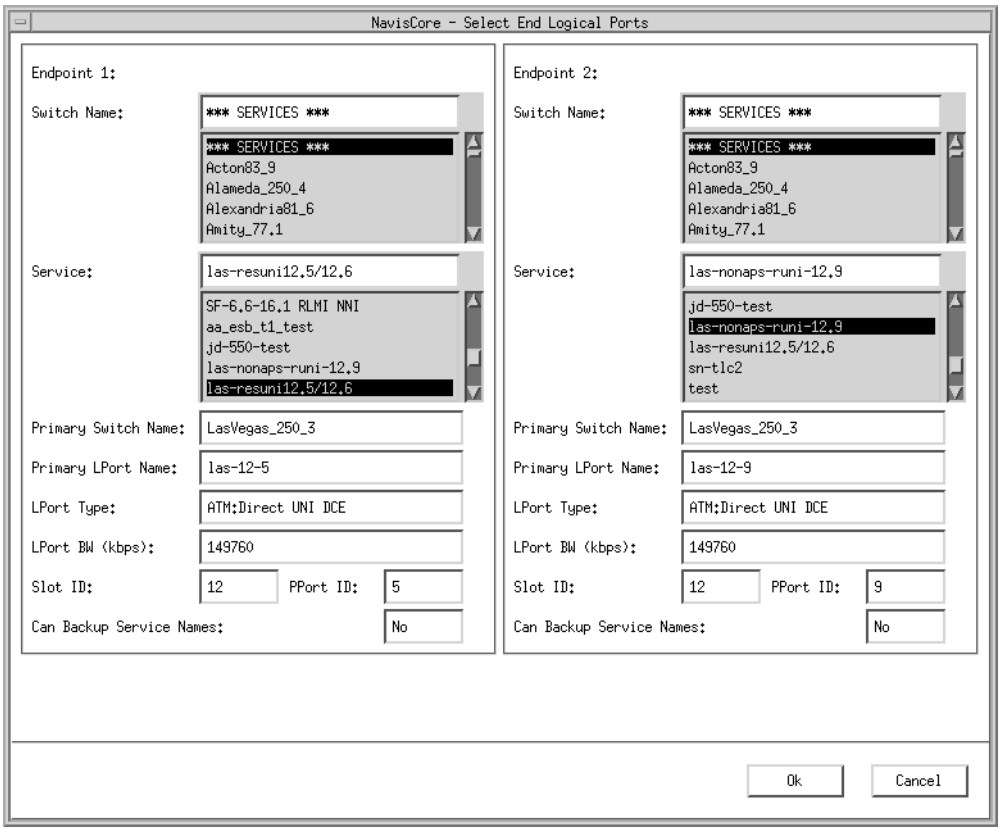


Figure 8-3. Select End Logical Ports Dialog Box

3. Configure Endpoint 1 and Endpoint 2 as follows:

For a Standard Circuit Configuration

a. Select the name of the switch where Endpoint 1 resides, then select the name of the switch where Endpoint 2 resides.

b. Select the name of the logical port for Endpoint 1, then select the name of the logical port for Endpoint 2. Note that if you enable the Select Layer2 VPN Customer View feature (see page 11-8), only logical ports that belong to the VPN or customer you select appear in this list.

c. Continue with step 5.

For a fault-tolerant PVC Connection

For more information about fault-tolerant PVCs, see Chapter 12, "Configuring Fault-Tolerant PVCs."

a. Choose *** SERVICES *** to configure a fault-tolerant PVC.

b. Select a service name from the list.

c. Continue with step 5.

For a Resilient LMI PVC Connection

For more information about resilient LMI (RLMI), see Chapter 13, "Configuring Resilient LMI."

a. Choose *** SERVICES *** to configure an RLMI PVC.

b. Select a service name from the list. You can configure an RLMI PVC only for the following logical port types:

- UNI DCE, UNI DTE, NNI (see the *B-STDX and CBX Frame Relay Services Configuration Guide*)
- ATM Network Interworking for Frame Relay NNI

c. Continue with step 5.

4. Review the information displayed in the Select End Logical Ports dialog box (Figure 8-3 on page 8-22) for endpoint 1 and endpoint 2. Table 8-6 describes the fields in the Select End Logical Ports dialog box.

Table 8-6. Select End Logical Ports Dialog Box Fields

Field	Description
Switch Name	Displays the name of the switch on which the logical port at this endpoint resides.
LPort Name	Displays the name defined for each logical port (LPort) in the circuit configuration.
LPort Type	Displays the logical port type for each logical port in the circuit configuration.
LPort BW (kbps)	Displays the bandwidth for each logical port in the circuit configuration.
Slot ID	Displays the number of the physical slot where the I/O module containing the selected logical port is installed.
PPort ID	Displays the number of the physical port on which the logical port is configured.

Table 8-6. Select End Logical Ports Dialog Box Fields (Continued)

Field	Description
IMA Group ID *(3-Port Channelized DS3/1 IMA IOM only)*	Displays the identification number of the IMA group for which the logical port is configured.
Can Backup Service Names	Indicates whether this logical port can be backed up to a service name binding. Options include: *Yes* – The logical port is used to implement Automatic Protection Switching (APS) Resilient UNI. (For details, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.) *No* – The logical port does not implement APS Resilient UNI.

5. Choose OK. The Add PVC dialog box appears.

Figure 8-4. Add PVC Dialog Box

The Add PVC dialog box displays the information for the End Point 1 and End Point 2 Logical Ports that you selected on the Select End Logical Ports dialog box (Figure 8-3 on page 8-22).

Continue with one of the following sections, according to the ATM service you are configuring:

- If both endpoints provide ATM services, continue with the following section, "Configuring an ATM Service PVC."
- If one endpoint provides Frame Relay services, continue with "Configuring Frame Relay-to-ATM Interworking Circuits" on page 8-41.

Configuring an ATM Service PVC

To configure attributes for this type of PVC, define the following parameters for each of the circuit's two endpoints. If you are configuring a circuit with an ATM CE endpoint(s), the VPI value defaults to 0 (zero) and the VCI value defaults to 256.

VPI (0..nnn) — Enter a value from 0-*nnnn* to represent the VPI for the PVC. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. Note that 0 (zero) is not a valid value for a management PVC. See page 8-9 for information about setting this value.

VCI (1..nnnn) — (*for VCCs only*) Depending on the circuit configuration, enter a value to represent the VCI for an ATM PVC. Although you can configure VCIs in the 1 – 31 range (with the exception of VCI = 3 and 4), the ATM Forum reserves VCIs in this range for various purposes. You should only use a VCI in the 1–31 range if you are certain that compatibility issues will not arise with any attached non-Lucent equipment. See page 8-9 for information about setting this value.

About the Set Attributes Menu

When you configure a PVC, the dialog box provides detailed parameters that you need to specify for each endpoint. During this procedure, you use the Set Attributes menu on the Add PVC dialog box.

Administrative — Defines administrative information, such as circuit name, administrative status, and circuit type.

Traffic Type — Defines the traffic descriptor settings for forward and reverse traffic.

User Preference — Defines PVC features that deal with port congestion and traffic policing.

NDC — Defines CBX 500 and GX 550 Network Data Collection (NDC) functions, which can detect any violation of PVC service subscription parameters and establish trends in network traffic patterns and loads. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for information about NDC functions.

Frame Discard — Defines UNI 4.0 signaling frame discard features for the forward and/or backward direction. The method of achieving frame discard depends on the implementation of early packet discard/partial packet discard (EPD/PPD) in your network. Your equipment must support frame discard.

Extended QoS Parameters — Defines the ATM Forum TM 4.0 Extended QoS Parameters. This selection enables you to define cell delay variation (CDV) and cell loss ratio (CLR) in the forward and reverse direction.

Selectable Statistics — Defines the Selectable Statistics function, which allows you to enable/disable PVC bulk statistics collection. This option is available with the NavisXtend Statistics Server.

Continue with the following sections to configure these parameters.

Administrative Attributes

From the Add PVC dialog box (Figure 8-4 on page 8-24), select Set [Administrative] Attributes and complete the fields described in (Table 8-7).

Table 8-7. Set Administrative Attributes Fields

Field	Action/Description
Circuit Name	Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Circuit Alias Name	(*Optional*) The circuit alias is used by service providers to identify the circuit in a way that is meaningful to their customers. This option is often used in conjunction with NavisXtend Report Generator. Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the circuit at switch startup, or Down if you do not want to activate the circuit at switch startup.
Circuit Type	Specify whether the circuit is a virtual path connection (VPC) or virtual channel connection (VCC, the default). If you select VPC, the VCI field is set to 0 (zero) and cannot be changed. A VPC enables a network that interfaces with an OPTimum trunk to accept circuits with this VPI and any of its valid VCIs.
Private Net Overflow	Determines how PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Select one of the following options: *Public* – (default) PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template *(Optional)*	You can save these settings as a template to configure another PVC with similar options. To create a template, choose Yes in the Template field. The default value is No. See "Using Templates" on page 8-87 for more information.

Table 8-7. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Mgmt Loopback Ckt	If you choose Yes, this PVC configuration will be included in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download the configuration file to the switch, the PVC can be used to establish NMS-to-switch connectivity. The Mgmt Loopback Ckt field is especially useful in some Management configurations. The default value is No.
Admin Cost Threshold	This field is disabled by default. If you enable this option, the PVC will not be routed over a path whose total administrative cost exceeds the entered value. This means that if you enable this field and enter a value of 1000, the PVC will not be routed over a path whose total admin cost exceeds 1000. The NMS calculates the total admin cost for a path by using the sum of the admin cost for each trunk in the path. The valid range for this field is 1 – 4294967295. ***Note**: For more information, see the next section "How PVC Routing Thresholds Interact With LPort Routing Metrics."*
End-End Delay Threshold (cell transfer delay)	This field is disabled by default. If you enable this option, the PVC will not be routed over a path whose total end-to-end delay exceeds the entered value. This means that if you enable this field and enter a value of 500 µsec., the PVC will not be routed over a path whose total end-to-end delay exceeds 500 µsec. The NMS calculates the total end-to-end delay for a path by using the sum of the end-to-end delays for each trunk in the path. The valid range for this field is 0 – 16777214 µsec. The value you enter should reflect your network topology. If a PVC typically traverses high speed trunks, set the delay rate lower. You need to increase the delay if the PVC uses low-speed trunks. ***Note**: For more information, see the next section "How PVC Routing Thresholds Interact With LPort Routing Metrics."*

How PVC Routing Thresholds Interact With LPort Routing Metrics

If you enable the PVC Admin Cost and/or End-End Delay (CTD or cell transfer delay) Thresholds, you should be aware of the following interactions with the UNI/NNI logical port routing metrics (see "Setting Quality of Service Parameters" on page 3-44). These interactions also apply to the PVC cell delay variation (CDV) and cell loss ratio (CLR) thresholds described in "Extended QoS Parameters Attributes" on page 8-37.

Admin Cost Threshold Enabled — If you enable the Admin Cost Threshold field (Table 8-7 on page 8-27), the system does not override the originating node logical port routing metric. Instead, OSPF and VNN use the routing metric to route the circuit (provided that the selected path has an admin cost less than the configured threshold).

CDV Enabled — In most cases, the system uses the routing metric associated with the originating node logical port. However, if you enable the CDV (or CTD) threshold (Table 8-11 on page 8-38), the system overrides the lport routing metric with the enabled CVD (or CTD) threshold. This means that if you choose the default admin cost routing metric on the logical port and enable the CDV (or CTD) threshold, OSPF and VNN route the circuit on a path with the lowest CDV (or CTD), even if the circuit has a higher admin cost than other network paths.

CLR Enabled — If you enable the CLR threshold (Table 8-11 on page 8-38), the system does not override the originating node logical port routing metric. Instead, OSPF and VNN use the routing metric to route the circuit (provided that each trunk in the path has a larger CLR than the configured threshold).

Traffic Type Attributes

Select Set [Traffic Type] Attributes from the Add PVC dialog box (Figure 8-5) to specify Traffic Descriptor settings for forward and reverse traffic. For more information about using ATM traffic descriptors, see Chapter 10, "Configuring ATM Traffic Descriptors."

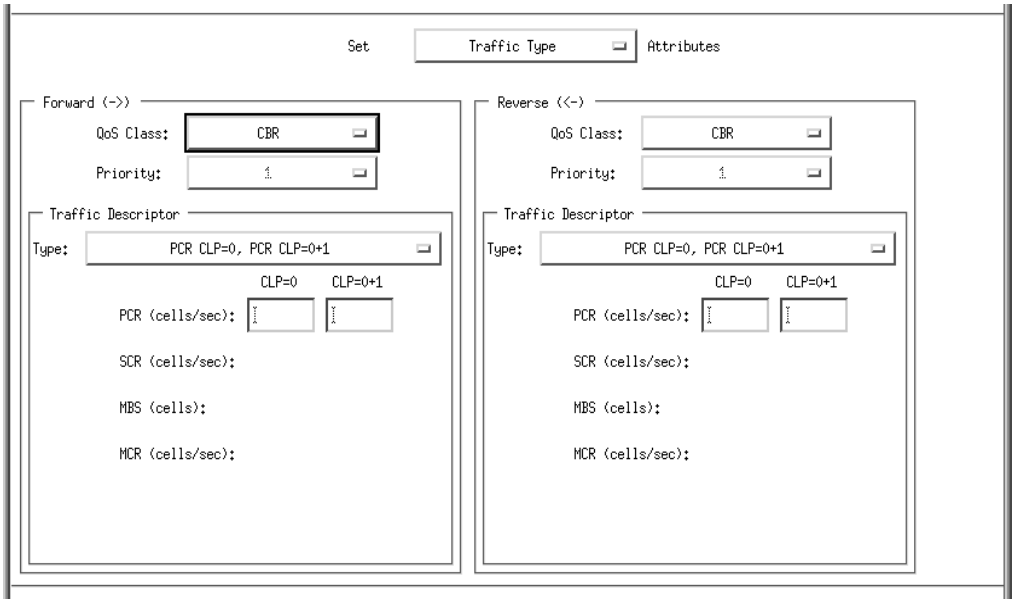


Figure 8-5. Set Traffic Type Attributes Fields

Forward traffic is traffic from Endpoint 1 to Endpoint 2, and reverse traffic is traffic from Endpoint 2 to Endpoint 1. Complete the fields described in Table 8-8 to set traffic type attributes in each direction.

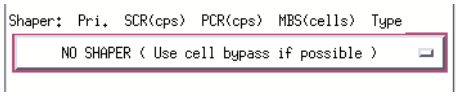
Table 8-8. Set Traffic Type Attributes Fields

Field	Action/Description
QoS Class (Fwd/Rev)	Select the Quality of Service class for forward and reverse traffic. The forward and reverse QoS classes do not have to match. The QoS class determines which traffic descriptors you can select. For more information on QoS classes, see Table 10-1 on page 10-4. ***Notes**: For a CBX 500 that uses the flow control processor, RM cells are sent in the backward direction. As a result, they assume the QoS class of the other direction.* *Due to hardware restrictions, you cannot dynamically modify the configured QoS class for ATM circuits with endpoints residing on BIO2 modules. The NMS will not allow changes to the configured QoS for established BIO2 circuits. To modify the QoS class for a BIO2 circuit endpoint, delete the existing circuit and re-configure it using the new QoS class.*

Table 8-8. Set Traffic Type Attributes Fields (Continued)

Field	Action/Description
Priority (Fwd/Rev) (*VBR-NRT and VBR-RT QoS classes on CBX/GX only*)	Select both the forward and reverse circuit priority, where 1 is high priority, 2 is medium priority, 3 is low priority, and 4 is lowest priority. (Note that for a B-STDX endpoint the priority range is from 1 – 3 only.) The forward and reverse circuit priority values do not have to match. CBR QoS class priority is set to 1.
Traffic Descriptor Type	Select from the following traffic descriptor options: *PCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (that is, the CLP=0 cell stream). *PCR CLP=0+1 (cells/sec)* – Specify the PCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (that is, the CLP=0 cell stream). *SCR CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *MBS CLP=0 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). *MBS CLP=0+1 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (that is, the CLP=0+1 cell stream). *MCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MCR CLP=0. If so, specify the MCR (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). Although the MCR traffic descriptor is only applicable to a CBX 500 with an FCP, this attribute is offered as a selection on non-CBX endpoints. This is because even though one or both endpoints may not be on a CBX with FCP, the PVC might traverse a CBX 500 FCP trunk. In this case, the provisioned attribute is used. ***Note**: On ATM CE endpoint(s), the PCR, SCR, and MCR cells/sec values default to 118980 and cannot be changed.*

Table 8-8. Set Traffic Type Attributes Fields (Continued)

Field	Action/Description
Shaper (*B-STDX ATM CS/IWU endpoint only*)	If this circuit carries ATM cell traffic, use the default of NO SHAPER. If this circuit carries frame relay traffic, select one of the configured shapers in the following pull-down menu.  These shapers correspond to the traffic shapers configured for the physical port on which this logical port resides. For information about physical port traffic shaping, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

User Preference Attributes

Select Set [User Preference] Attributes from the Add PVC dialog box and complete the Set User Preference Attributes fields (Figure 8-6) described in Table 8-9.

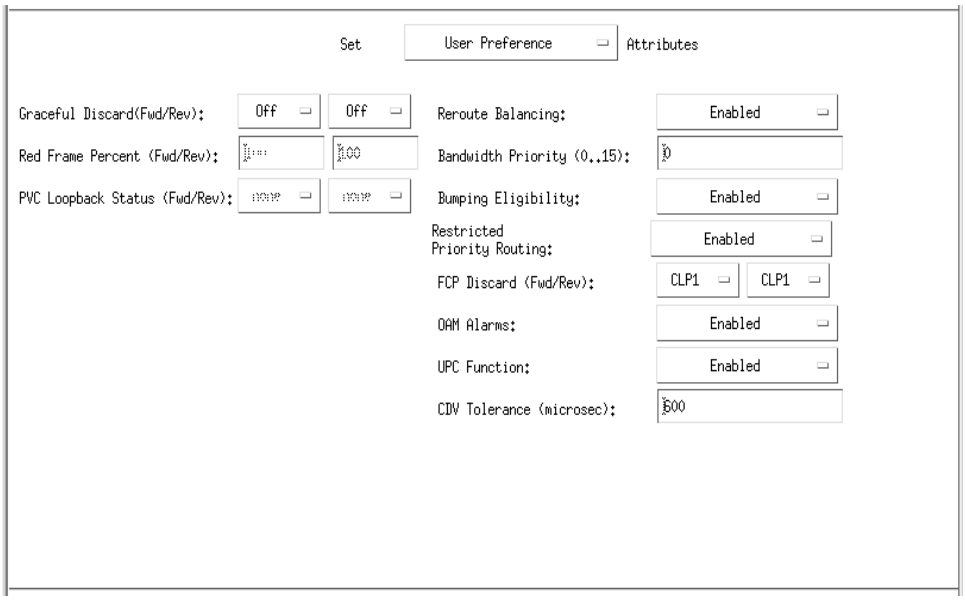


Figure 8-6. Set User Preference Attributes Fields

Table 8-9. Set User Preference Attributes Fields

Field	Action/Description
Reroute Balancing	When enabled (default), the PVC conforms to the configured reroute tuning parameters. This means that when the PVC reroutes during trunk failure, it will migrate back to its original trunk at a rate and time determined by the configured reroute tuning parameters. When disabled, the PVC ignores the switch tuning parameters. For more information, see the *B-STDX, CBX, and GX Getting Started User's Guide*.
Bandwidth Priority (0..15)	Specify a value from 0 (zero) through 15, where 0 (zero) is the default and indicates the highest priority. See Appendix E, "Priority Routing," for more information.
Bumping Eligibility	If restricted priority routing is disabled, specify Enabled (default) for the non-real time circuit to become active whether or not sufficient bandwidth exists. Specify Disabled to keep the non-real time circuit in retry mode until sufficient bandwidth is available. If restricted priority is enabled, a non-real time circuit that has been bumped remains in retry mode until sufficient bandwidth is available, regardless of the bumping eligibility setting (Disabled or Enabled). See Appendix E, "Priority Routing," for more information.
Restricted Priority Routing	Set to Enabled (default) to provision new circuits at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings. Set to Disabled if you want to use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits. See Appendix E, "Priority Routing," for more information.

Table 8-9. Set User Preference Attributes Fields (Continued)

Field	Action/Description
FCP Discard (Fwd/Rev)	Displays only if you selected a QoS class that supports FCP Discard. Select one of the following options: *CLP1* – (default) You can provision selective CLP1 discard for UBR, ABR, and VBR-NRT PVCs. If the current cell causes the queue for a PVC to exceed the discard thresholds, and the cell has CLP set to 1, the cell is discarded. Note that EPD is not performed in this case. *EPD* – Early Packet Discard. The ATM Flow Control Processor (FCP) can perform EPD for UBR, ABR, and VBR-NRT PVCs. If you select this option, when a cell causes the queue for a PVC to exceed the discard thresholds, the VC enters the EPD state. The cells in the current packet of the VC are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded for that PVC. See "ATM Flow-Control Discard Mechanisms" on page 5-18 for more information. Although the frame discard attribute is only applicable to a CBX 500 with an FCP, this attribute is offered as a selection on non-CBX endpoints. This is because even though one or both endpoints may not be on a CBX with FCP, the PVC might traverse a CBX 500 FCP trunk. In this case, the provisioned attribute is used. ***Note**: On ATM CE endpoint(s), the FCP Discard (Fwd/Rev) option is not available.*
OAM Alarms (*CBX/GX and ATM CS/IWU modules only*)	Set to Enabled (default) to use OAM alarms on this circuit. Set to Disabled to disable OAM alarms on this circuit. When enabled, the switch sends OAM F5 or F4 alarm indicator signal (AIS) cells out of each UNI logical port endpoint to indicate that the circuit is down. ***Note:** For a management PVC, this field is set to disabled and cannot be changed.*

Table 8-9. Set User Preference Attributes Fields (Continued)

Field	Action/Description
UPC Function (*PVCs with CBX/GX endpoints only*)	Enables (default) or disables the usage parameter control (UPC) function. When you enable UPC, the circuit tags or drops cells as they come into the port that do not conform to the configured traffic descriptors. When you disable UPC, the circuit allows all traffic, including non-conforming traffic, into the port. As a result, when you disable UPC, quality of service is no longer guaranteed for circuits in the network due to the potential for increasing the cell loss ratio because of port congestion. For this reason, *Lucent recommends that you enable the UPC function on all circuits.* For information about UPC traffic parameters, see Chapter 10, "Configuring ATM Traffic Descriptors." To use the UPC function for individual circuits, verify that the UPC function is enabled for both logical port endpoints on which you will define the circuit. Enabling UPC at the circuit level has no effect if you did not enable UPC at the logical port level. UPC is enabled by default (without the ABR option) for both logical ports and circuits. ***Note**: If both endpoints are configured as ATM CE endpoints, the UPC Function is not available.*
CDV Tolerance (*PVCs with CBX/GX endpoints only*)	Configure the cell delay variation tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. Valid values are between 1 - 65535 µs. The default is 600 µs. ***Note:** If you are using the 3-Port Channelized DS3/1 IMA IOM, the recommended minimum CDV Tolerance value is 1000 microseconds.*
Graceful Discard (Fwd/Rev) (*ATM UNI endpoint on Frame-based card*)	Select either On or Off to define how this circuit handles "red" packets. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (BC) and excess burst size (BE) thresholds, including the current frame. The discard eligible (DE) bit for a red packet is set to 1, meaning the network can discard this packet unless Graceful Discard is set to On. *On* – (default) Forwards some red packets if there is no congestion. *Off* – Immediately discards red packets. ***Note:** For the ATM UNI DS3/E3, if you set this value for shaping purposes, the switch code ignores the PCR, SCR, and MBS values calculated from Set Traffic Type Attributes menu (Figure 8-11 on page 8-52); the switch instead picks the highest PCR queue available and sets the SCR to that PCR.*

Table 8-9. Set User Preference Attributes Fields (Continued)

Field	Action/Description
Red Frame Percent (Fwd/Rev) (*ATM UNI endpoint on Frame-based card*)	Set this value only if Graceful Discard is set to On. The default is 100. See "Graceful Discard" on page 8-46 for more information. The Red Frame Percent limits the number of red frames the network is responsible to deliver.
PVC Loopback Status (Fwd/Rev) (*ATM UNI endpoint on Frame-based card*)	Displays the current loopback state. If None is not displayed in the PVC Loopback Status field, do not attempt to modify or delete the selected circuit. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information about loopback testing.

If both ATM endpoints reside on a CBX 500 or GX 550 switch, proceed to the following section, "Frame Discard Attributes." Otherwise, continue with "Selectable Statistics Attribute" on page 8-39.

Frame Discard Attributes

The Set Frame Discard menu (see Figure 8-7) only appears if both endpoints reside on either a CBX 500 or GX 550 switch. If you enable FCP on a CBX 500 IOM (see the *B-STDX, CBX, and GX Switch Module Configuration Guide*), the FCP based EPD/PPD function (see Table 8-17 on page 8-58) takes precedence over the IOM output buffer EPD/PPD function. Select Set [Frame Discard] Attributes from the Add PVC dialog box and complete the fields described in Table 8-10.

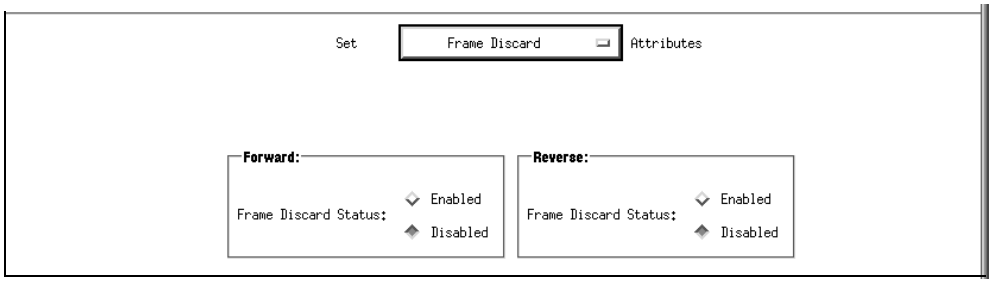


Figure 8-7. Set Frame Discard Attributes Fields

Note – You should only enable frame discard if the traffic traversing the VC is encapsulated using AAL5. If frame discard is enabled on VCs that are not using AAL5 encapsulation, all traffic traversing the VC may be discarded.

Note – Due to hardware restrictions, you cannot dynamically modify (enable or disable) the configured Frame Discard mode for ATM circuits with endpoints residing on BIO2 modules. The NMS will not allow changes to the configured Frame Discard mode for established BIO2 circuits. To modify the Frame Discard mode for a BIO2 circuit endpoint, delete the existing circuit and re-configure it using the new Frame Discard mode.

Table 8-10. Set Frame Discard Attributes Fields

Field	Action/Description
Forward Frame Discard Status	These parameters are set to Disabled by default. Select Enabled to turn on the physical port output buffer early packet discard/partial packet discard (EPD/PPD) function for this particular PVC. When enabled, AAL5 traffic that is traversing the PVC will be subject to EPD/PPD when physical port congestion is experienced.
Reverse Frame Discard Status	

Extended QoS Parameters Attributes

The Set Extended QoS Parameters Attributes menu (see Figure 8-8) only appears if both endpoints reside on either a CBX 500 or GX 550 switch. Select Set [Extended QoS Parameters] Attributes from the Add PVC dialog box and complete the fields described in Table 8-11.

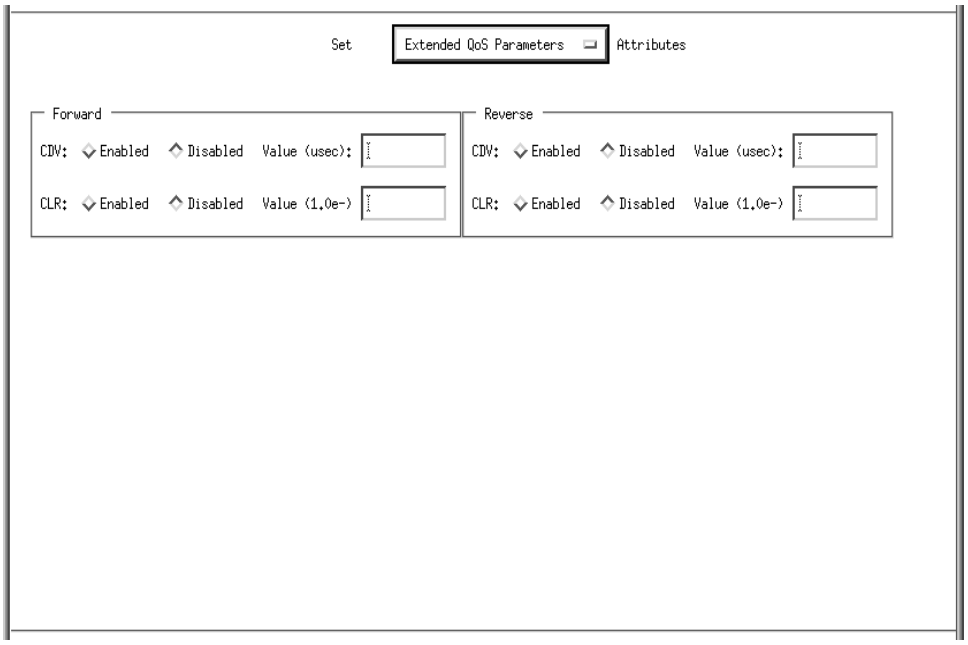


Figure 8-8. Set Extended QoS Parameters Attributes Fields

Table 8-11. Set Extended QoS Parameters Attributes Fields

Field	Action/Description
Forward/ Reverse CDV	If you enable this option, the PVC will not be routed over a path whose total cell delay variation (CDV) exceeds the entered value. If you enable this field and enter a value of 1000 µsec, the PVC will not be routed over a path whose total CDV exceeds 1000 µsec. The total CDV for a path is calculated by summing the CDV for each trunk in the route. The valid range for this field is 1 – 1777214 µsec. ***Note**: If you enable this option, see "How PVC Routing Thresholds Interact With LPort Routing Metrics" on page 8-28 for more information.*
Forward/ Reverse CLR	If you enable this option, the PVC will not be routed over a path if the cell loss ratio (CLR) of one of the trunks exceeds the entered value. If you enable this field and enter a value of 10, the PVC will not be routed over a path that has one or more trunks with a CLR worse than 1.0 e^{-10}. The CLR for a trunk is based on the CAC objective for the host switches. The valid range for this field is $1.0e^{-1}$ to $1.0e^{-12}$. Enter a value between 1 and 12. ***Note**: If you enable this option, see "How PVC Routing Thresholds Interact With LPort Routing Metrics" on page 8-28 for more information.*

Selectable Statistics Attribute

The option is available with the NavisXtend Statistics Server. This feature allows you to enable and disable PVC bulk statistics collection. Select Set [Selectable Statistics] Attributes from the Add PVC dialog box, and enable or disable (default) the Bulk Statistics option.

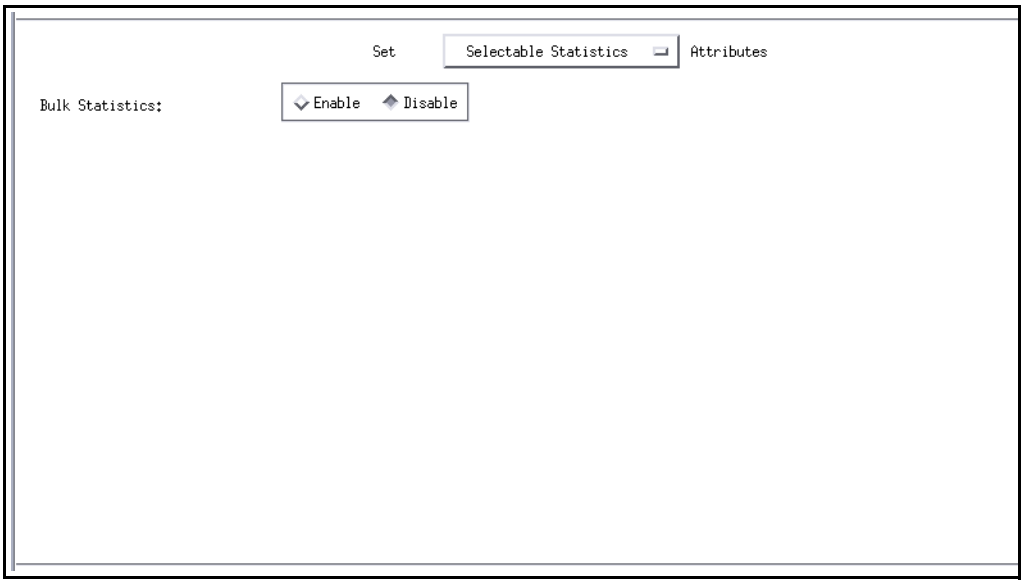


Figure 8-9. Set Selectable Statistics Attributes Field

Bulk statistics for the logical port must be enabled before enabling bulk statistics for PVCs. For more information, see "Selectable Statistics Attributes" on page 3-42.

For information about using the feature, see the *NavisXtend Statistics Server User's* Guide.

Completing the PVC Configuration

Use the following steps to complete the circuit configuration.

1. (*Optional*) To configure CBX 500 or GX 550 Network Data Collection (NDC) parameters for this circuit, select Set [NDC] Attributes. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
2. (*Optional*) To configure NavisXtend Accounting Server parameters for this circuit, choose the Accounting button. For more information, see the *NavisXtend Accounting Server Administrator's Guide*.
3. Choose OK to define the circuit parameters. The Set All PVCs on Map dialog box reappears (Figure 8-1 on page 8-10).

Note – If enabled, the Reliable Scalable Circuit feature verifies the card state of each PVC endpoint before sending the `SNMP Set` command. If the card status at either endpoint is not up, the NMS displays an error message indicating where the failure occurred. If you receive such a message, see Appendix F, "Reliable Scalable Circuit," for more information.

4. (*Optional*) To configure this PVC for a specific Layer2 VPN and customer, see page 11-10.
5. To add more PVCs, repeat the steps in "Defining a PVC Connection" on page 8-22.
6. When you finish, choose Close to return to the network map.

Configuring Frame Relay-to-ATM Interworking Circuits

Frame Relay-to-ATM Interworking provides a means of transparently integrating Frame Relay and ATM networks. This section describes how to configure Frame Relay-to-ATM Service and Network Interworking circuits.

Frame Relay-to-ATM Service Interworking

You can configure the following circuits for ATM services:

Frame Relay-to-ATM Service Interworking — Frame Relay-to-ATM Service Interworking (FRF.8) enables a Frame Relay device to connect to an ATM user device over a common wide area network (WAN) backbone. Frame Relay to ATM Service Interworking provides a seamless communication between ATM and Frame Relay networks or end-user devices.

This service uses a circuit with a Frame Relay logical port at one endpoint and an ATM logical port at the other endpoint. The circuit uses a 10-bit address called a Data Link Connection Identifier (DLCI). DLCIs identify the logical endpoints of a virtual circuit and have local significance only.

ATM Data Exchange Interface/Frame User-to-Network Interface (DXI/FUNI) — This service uses a circuit with an ATM logical port defined on a Frame-based I/O module, such as the 8-port Universal I/O module. The circuit is identified by a 4-bit virtual path identifier (VPI) and a 6-bit virtual channel identifier (VCI). Circuits on the ATM DS3/E3 module use an 8-bit VCI.

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

A virtual channel (VC) is a connection between two communicating ATM devices. A VC may consist of a group of several ATM links, customer premise equipment (CPE) to central-office switch, switch-to-switch, and switch-to-user equipment.

Note – ATM DXI/FUNI is *not supported* on the 32-Port Channelized T1/E1 FR/IP I/O module or the 8-Port Subrate DS3 FR/IP I/O module.

Frame Relay-to-ATM Network Interworking

Frame Relay-to-ATM Network Interworking (FRF.5) allows you to connect two Frame Relay end nodes, for example Frame Relay Access Devices (FRADs) or routers, which are attached to a Frame Relay network over an ATM backbone. The FRADs have no knowledge of the ATM backbone because the network equipment, particularly ATM WAN switches, provide the interworking function. The ATM backbone can support multiple Frame Relay networks, providing a scalable, high-speed option that does not require changes to customer premise equipment.

Lucent's CBX 500 implementation of FRF.5 enables a single Frame Relay PVC to tunnel through an ATM network via an ATM PVC. The ATM PVC is located in the core of the ATM network and is treated as a virtual Network-to-Network Interface (NNI) running Link Management Interface (LMI) with the far-end entity.

Note – This implementation of the FRF.5 ATM Forum implementation agreement is available only for the following CBX 500 Frame cards:

- 6-Port DS3 FR/IP IOM
- 4-Port Channelized DS3/1 FR/IP IOM
- 4-Port Channelized DS3/1/0 FR/IP IOM
- 8-Port Subrate DS3 FR/IP IOM
- 32-Port Channelized T1/E1 FR/IP IOM

In the CBX switch that contains the Frame Relay user interface, the card configured as the FR UNI endpoint must be one of the CBX 500 Frame cards listed above. The card that contains the other circuit endpoint may be a CBX or GX ATM card. The interworking function is always performed on the CBX Frame card.

Configuring Link Management for the Frame Relay Logical Port

When you configure the Frame Relay logical port endpoint for this circuit, the Link Management Protocol can be set to any of the following protocols: Disable, LMI Rev1, ANSI T1.617 Annex D, CCITT Q.933 Annex A, or Auto Detect. This attribute appears on the Add Logical Port - Set Link Management Attributes dialog box. For information about configuring a logical port to set this attribute, see the *B-STDX and CBX Frame Relay Services Configuration Guide*.

Special Network Interworking PVC Configuration Parameters

You configure a network interworking PVC (FRF.5) the same way as a service interworking PVC (FRF.8). The only difference is that you select an LMI profile and specify a Network-to-Network Interface (NNI) Data Link Connection Identifier (DLCI) for the network interworking PVC.

The following list summarizes the special configuration parameters that are required for network interworking PVCs:

LMI Profile ID — Enables the selected LMI profile. Selecting Disable, the default value, disables FRF.5.

You enable the LMI profile on a per PVC basis instead of on a logical port basis. The LMI profile is a temporary instance of LMI that runs across the ATM network interworking PVC, and it defines the LMI state for the *circuit*. The LMI profile is required *in addition* to the LMIs that are defined for the Frame Relay UNI DCE *logical port* endpoints (see "Configuring Link Management for the Frame Relay Logical Port" on page 8-42).

Note – This release supports one predefined LMI profile, which does not contain any user-configurable parameters.

The default LMI profile contains the following hard-coded parameters:

Counters

N391	1
N392	3
N393	4

Timers

T391	180
T392	200

LMI Protocol

Q.933 Annex A

Note – The parameters listed above are hard-coded for the LMI running on the NNI (Network Interworking) PVC.

The LMIs at both FR UNI DCE endpoints, however, do not have to be set to Q.933 Annex A. They can be set to any of the following protocols: Disable, LMI Rev1, ANSI T1.617 Annex D, CCITT Q.933 Annex A, or Auto Detect.

For information about configuring the LMI Profile ID field, see Table 8-15 on page 8-50.

NNI DLCI — If you select an LMI profile, you must specify the NNI DLCI for the network interworking PVC. This DLCI can differ from the DLCI configured at the UNI port. The LMI that the NNI runs will use this DLCI to identify the PVC.

The NNI DLCI value should be a valid DLCI value (in the range of 16 - 991, and 1022).

Note – Review the Restrictions and Special Considerations section of the *Software Release Notice for CBX Switch Software* that comes with your release for specific PVC capacities. The information about PVC capacities describes the use of NNI DLCI with VPI/VCI values.

For information about configuring the NNI DLCI, see Table 8-15 on page 8-50.

CLP/DE Mapping Parameters — At the Frame Relay UNI endpoint, configure the following cell loss priority (CLP)/discard eligibility (DE) parameters, which apply to *both* ATM-to-Frame Relay Interworking PVCs *and* Frame Relay-to-ATM Interworking PVCs:

- Map DE to CLP
- Set CLP to 0 Always
- Set CLP to 1 Always

Note – For ATM-to-Frame Relay Interworking PVCs, the Set CLP to 0 Always and Set CLP to 1 Always CLP/DE parameters are relevant *only* to Frame Relay-to-ATM Service Interworking (FRF.8) configurations. For Frame Relay-to-ATM Network Interworking (FRF.5) configurations, these parameters are interpreted as No Mapping.

For information about configuring CLP/DE mapping parameters, see Table 8-17 on page 8-58.

EFCI/FECN Mapping Parameters — There are no user-configurable parameters for EFCI and FECN mapping. For ATM to Frame Relay Interworking PVCs, EFCI is always mapped to FECN; for Frame Relay to ATM Interworking PVCs, EFCI is set to 0 (zero). For information about configuring EFCI/FECN mapping, see Table 8-17 on page 8-58.

Rate Enforcement

Rate enforcement prevents network congestion and allocates network resources to ensure the commitment of service contracts. Rate enforcement measures the actual traffic flow across a connection and compares it to the configured traffic flow parameters for that connection. Traffic outside the acceptable committed information rate (CIR) is tagged and discarded if congestion develops.

Rate enforcement is implemented on a per-DLCI basis on all circuits on ingress switches. When the switch receives data over time interval *Tc* (Tc=Bc/CIR), it classifies the frame as follows:

- Under the committed burst size (Bc)
- Over the committed burst size but under the excess burst size (Be)
- Over the excess burst rate

Color designators (green, amber, and red) identify packets travelling through the network. Congested nodes use the designators to determine which frames to discard first under various congested states or congestion conditions. Table 8-12 describes the designators (traffic colors) and discard policy.

Table 8-12. Rate Enforcement and Discard Policy

Traffic Color	Description	Discard Eligible (De)
Green	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, less than Bc.	No
Amber	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, greater than Bc but less than Be.	Frame is eligible for discard if it passes through a congested node.
Red	Accumulated number of bits received up to any time during the current time interval, excluding the current frame, greater than Be.	All red frames are discarded.

Graceful Discard

The *graceful discard* feature enables you to control network behavior and user traffic. You can set the graceful discard parameters as follows:

On — The switch allows some red frames to be transmitted. This maximizes network usage, but may overload the network.

Off — This option avoids potential congestion. This allows strict control of user traffic, but may waste network resources.

When graceful discard is set to On, you can configure the red-frame percent. The red-frame percent is used to limit the number of red frames the network is responsible for delivering. The red-frame percent (Pr) is determined as follows:

$$Pr = \frac{\text{Allowed red frame bits}}{\text{Bc + Be + allowed red frame bits}}$$

Rate Enforcement Schemes

Rate enforcement schemes provide more flexibility, increased rate enforcement accuracy, and improved switch performance. You configure the rate enforcement scheme in the Add PVC dialog box by completing the Set Traffic Type Attributes fields (see Table 8-16 on page 8-53).

Table 8-13 compares the accuracy and switch performance of the Jump and Simple rate enforcement schemes. Number 1 specifies the more accurate scheme and better switch performance, while 2 specifies a less-accurate scheme and slightly degraded switch performance.

Table 8-13. Rate Enforcement Schemes

Scheme	Rate Enforcement Accuracy	Switch Performance
Jump	1	2
Simple	2	1

Frame Relay-to-ATM Parameters Conversion Formula

When you configure Frame Relay traffic parameters on the Frame Relay endpoint, the NMS automatically converts the Frame Relay CIR, Bc, and Be fields to the ATM PCR, SCR, and MBS fields and displays these ATM parameters on the screen. You should use these values as a guideline in order to provision a PVC with roughly symmetric traffic parameters. *Optionally*, you can enter these converted values into the appropriate fields on the ATM endpoint, or enter new ATM parameter values for the ATM endpoint.

The NMS uses the following formula to convert the entered Frame Relay traffic parameters:

PCR = (CIR + EIR) * IOH / 8

SCR = CIR * IOH / 8

MBS = Bc * IOH / 8

EIR = Be * CIR /Bc

IOH = .0234375

IOH represents the Interworking Overhead factor; it is a fixed number based on an average frame size of 256 bytes with additional factors for the AAL5 trailer size and the cell padding overhead.

Defining Service or Network Interworking PVC Connections

To define a circuit for Frame Relay-to-ATM service or network interworking:

1. Follow step 1 through step 5 beginning on page 8-22 to select the PVC endpoints for Frame Relay-to-ATM service or network interworking.
2. The Add PVC dialog box appears (Figure 8-10). In this example, the dialog box defines Frame Relay and ATM endpoints.

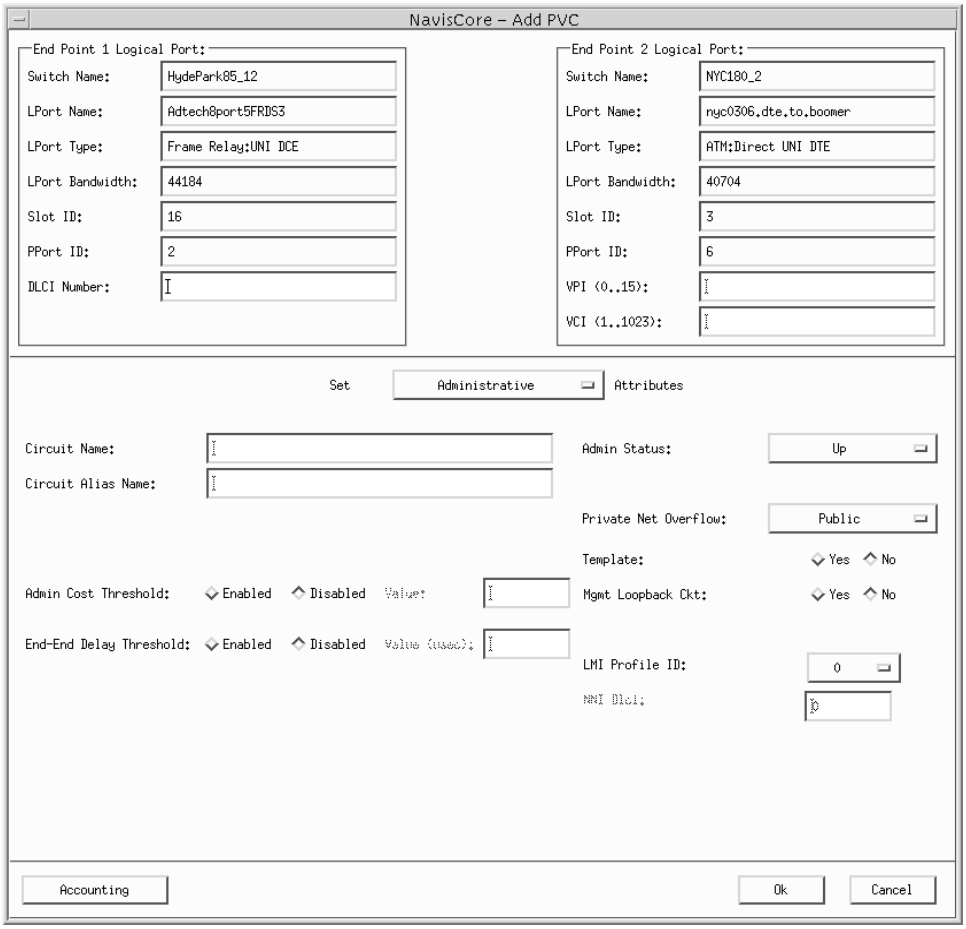


Figure 8-10. Add PVC Dialog Box (FR-ATM)

3. Complete the Add PVC dialog box fields described in Table 8-14.

Table 8-14. Add PVC Dialog Box Fields (FR-ATM)

Field	Action/Description
DLCI Number *(Frame Relay endpoint)*	Enter a unique DLCI for this logical port.
VPI (0..nnnn)	Enter a value from 0 (zero) to *nnnn* to represent the virtual path identifier (VPI) for an ATM circuit. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. Note that 0 (zero) is not a valid value for a management PVC. See page 8-9 for information about setting this value. • For a 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 module, the VPI range depends on the number of VPI bits selected on the physical port. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information. • For an ATM UNI DS3/E3 module, the number of VPI bits is set to 4; the VPI range is 0 – 15.
VCI (1..nnnn) *(ATM endpoint only, VCCs only)*	Enter a value to represent the virtual channel identifier (VCI) for an ATM circuit. See page 8-9 for information about setting this value. When you configure the ATM circuit: • On a Frame-based I/O module, enter a value from 32 to 63. • On an ATM-based I/O module (such as the ATM DS3 module), enter a value from 32 to 255. • On a 1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 module, the total number of bits available for the VPI and VCI is 12 bits. For example, if the VPI is set to 1, there are 11 bits available for the VCI. If the VPI is set to 2, there are 10 bits available for the VCI. ***Note:*** *If you are configuring the VCI on a 1-port ATM CS DS3/E3 or 1-port ATM IWU OC-3c/STM-1 module, the VCI range depends on the number of VPI bits selected on the physical port. See the* B-STDX, CBX, and GX Switch Module Configuration Guide *for more information.* • For FRF.5 network interworking, enter a value from 1 to *nnn* to represent the VCI for an ATM circuit.

4. Complete the Set Administrative Attributes fields described in Table 8-15.

Table 8-15. Set Administrative Attributes Fields

Field	Action/Description
Circuit Name	Enter any unique, continuous, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. You can use hyphens.
Circuit Alias Name	(*Optional*) The circuit alias is used by service providers to identify the circuit in a way that is meaningful to their customers. This option is often used in conjunction with NavisXtend Report Generator. See the *NavisXtend Report Generator* for more information. Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the circuit at switch startup, or Down if you do not want to activate the circuit at switch startup.
Private Net Overflow	Determines how PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Select one of the following options: *Public* – (default) PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template (*Optional*)	You can save these settings as a template to configure another PVC with similar options. To create a template, choose Yes in the Template field. The default value is No. See "Using Templates" on page 8-87 for more information.
Mgmt Loopback Ckt	If you choose Yes, this PVC configuration will be included in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity. This option is especially useful in some management configurations. The default value is No.

Table 8-15. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Admin Cost Threshold	If you enable this option, the PVC will not be routed over a path whose total administrative cost exceeds the entered value. This means that if you enable this field and enter a value of 1000, the PVC will not be routed over a path whose total admin cost exceeds 1000. The total admin cost for a path is calculated by summing the admin cost for each trunk in the path. The valid range for this field is 1 – 4294967295.
End-End Delay Threshold (cell transfer delay)	If you enable this option, the PVC will not be routed over a path whose total end-to-end delay exceeds the entered value. This means that if you enable this field and enter a value of 500 µsec., the PVC will not be routed over a path whose total end-to-end delay exceeds 500 µsec. The total end-to-end delay for a path is calculated by summing end-to-end delay for each trunk in the path. The valid range for this field is 0 – 16777214 µsec. ***Note:*** *The value you enter should reflect your network topology. If a PVC will typically traverse high-speed trunks, set the delay rate lower; increase the delay if the PVC must use low-speed trunks.*
LMI Profile ID	For a service interworking PVC (FRF.8), accept the default value (0), which disables FRF.5. For a network interworking PVC (FRF.5), select 1 to enable the LMI profile for the circuit, and then enter the NNI DLCI value. ***Note:*** *The LMI profile for the network interworking PVC is configured on a* per-PVC *basis using Q.933 Annex A as the LMI protocol. However, when you configure the Frame Relay* logical port *endpoint for this circuit, the Link Management Protocol can be set to any of the following protocols: Disable, LMI, Rev1, ANSI T1.617 Annex D, CCITT Q.933 Annex A, or Auto Detect. See the* B-STDX and CBX Frame Relay Services Configuration Guide *for details about setting the Link Management Protocol attribute for a logical port.*
NNI DLCI	If you enable an LMI profile ID, you *must* specify the NNI DLCI for the network interworking PVC. The NNI DLCI can differ from the DLCI configured at the UNI port. The LMI that the NNI runs will use the NNI DLCI to identify the network interworking PVC. Enter the NNI DLCI. The valid range of values for this field is 16 - 991, and 1022. ***Note:*** *Review the Restrictions and Special Considerations section of the* Software Release Notice for CBX Switch Software *that comes with your release for information about setting the NNI DLCI and VPI/VCI values.*

5. Using the Set Attributes menu, complete the following sections:
   - "Traffic Type Attributes" on page 8-52
   - "User Preference Attributes" on page 8-57

Traffic Type Attributes

Select Set [Traffic Type] Attributes from the Add PVC dialog box to specify Traffic Descriptor settings for forward and reverse traffic. In the example shown in Figure 8-11, configure the fields beneath Forward (–>); then configure the fields beneath Reverse (<–). The attributes that appear depend upon the endpoint type, either Frame Relay or ATM.

Note – You *must* configure Traffic Type attributes before choosing Ok in the Add PVC dialog box to save the circuit configuration. Otherwise, the default values for committed information rate (CIR), committed burst size (Bc), and excess burst size (Be) will generate an error message.

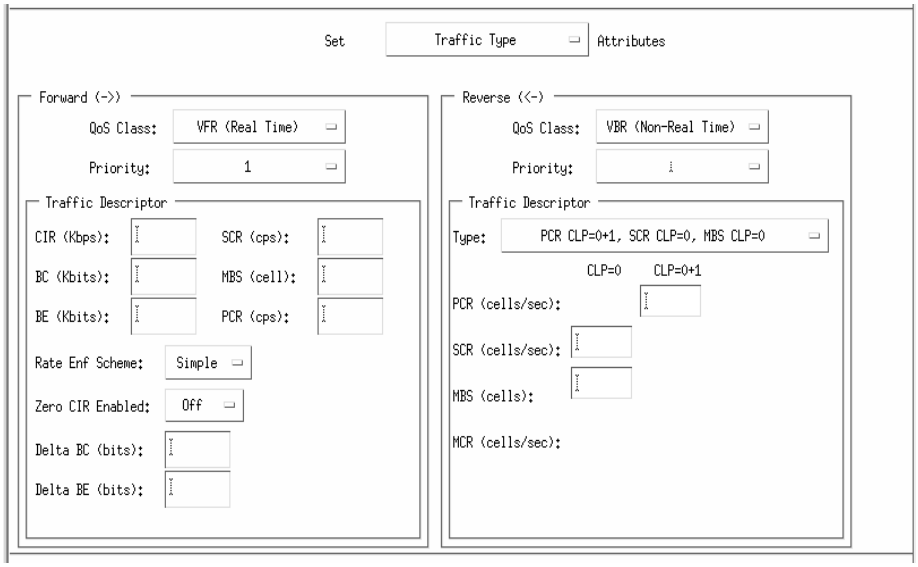


Figure 8-11. Set Traffic Type Attributes Fields (FR-ATM)

Complete the Set Traffic Type Attributes fields in Table 8-16.

Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters)

Field	Action/Description
Frame Relay Endpoint Traffic Parameters	
QoS Class (Fwd/Rev)	Select one of the following Frame Relay class of service (CoS) values: *VFR (Real-Time)* – Variable frame rate-real time (VFR-RT). Used for packaging special delay-sensitive applications, such as packet video, which require low cell-delay variation between endpoints. *VFR (Non-Real Time)* – Variable frame rate-non real time (VFR-NRT) Handles packaging for transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of VFR-NRT. *UFR* – Unspecified frame rate. Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic. *ABR* – Available bit rate. Primarily used for LAN traffic. The CPE compensates for any delay or lost cell traffic. Select this option if the PVC will traverse a CBX 500 cloud that uses an FCP.
Priority (Fwd/Rev)	Select both the forward and reverse circuit priority, where 1 is high priority, 2 is medium priority, and 3 is low priority. The forward and reverse circuit priority values do not have to match.
CIR (Kbps)	Enter the committed information (CIR) rate in Kbps at which the network transfers data under normal conditions. Normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the committed rate measurement interval (Tc).
SCR (cps)	Displays the sustainable cell rate (SCR) that is calculated from the CIR value you enter.
BC (Kbits)	Committed Burst Size. Enter the maximum amount of data, in Kbits, that the network attempts to transfer under normal conditions during a specified time interval (Tc, calculated as BC/CIR). This value must be greater than 0 (zero) and is typically set to the same value as CIR.
MBS (cell)	Displays the maximum burst size (MBS) that is calculated from the Bc value you enter.

Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
BE (Kbits)	Excess Burst Size. Enter the maximum amount of uncommitted data, in Kbits, the network will attempt to deliver during a specified time interval, Tc. Tc is calculated Bc/CIR. The network treats this data as discard eligible (DE) data. ***Note:*** *For ATM UNI DS3/E3 modules, if the sum of Bc + Be is greater than the value of MBS, you will get an error. If you set Bc = CIR and Be to 0 (zero), traffic shaping is disabled on the ATM side of the circuit and MBS is forced to equal 32.*
PCR (cps)	Displays the peak cell rate (PCR) that is calculated from the Be value you enter.
Rate Enf Scheme	Select Simple (default) or Jump. The configurable rate enforcement scheme provides more flexibility, increased rate enforcement accuracy, and improved switch performance. See "Rate Enforcement Schemes" on page 8-46 for more information.
Zero CIR Enabled (Fwd/Rev)	Set the CIR parameter to On or Off. *On* – Indicates that the PVC has an assigned CIR value of 0 (zero) and is a best-effort delivery service. Customer data that is subscribed to Zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on Zero CIR PVCs have DE set to 1. *Off* (default) – Disables Zero CIR. ***Note:*** *If you set Zero CIR Enabled to On, you can not set the CIR, Bc, and Be values.*
Delta BC (bits)	The maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval provided there are positive committed bit (Bc) credits before receiving the frame, but negative Bc credits after accepting the frame. Set the number of Delta Bc bits for this circuit between 0 - 65528 (default 65528).
Delta BE (bits)	The maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval provided there are positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame. Set the number of Delta Be bits for this circuit between 0 - 65528 (default 65528).

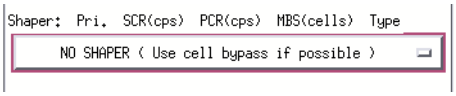
Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
ATM Endpoint Traffic Parameters	
QoS Class (Fwd/Rev)	Select the Quality of Service Class for forward and reverse traffic. The forward and reverse QoS classes do not have to match. The QoS Class determines which traffic descriptors you can select. For more information on QoS, see Table 10-1 on page 10-4. ***Note:*** *For a CBX 500 that uses the flow control processor, RM cells are sent in the backward direction. As a result, they assume the QoS class of the other direction.*
Priority (Fwd/Rev) (*VBR-NRT and VBR-RT QoS classes on CBX/GX only*)	Select both the forward and reverse circuit priority, where 1 is high priority and 4 is lowest priority. The forward and reverse circuit priority values do not have to match.

Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
Traffic Descriptor Type	Select from the following traffic descriptor options: *PCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (that is, the CLP=0 cell stream). *PCR CLP=0+1 (cells/sec)* – Specify the PCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (that is, the CLP=0 cell stream). *SCR CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *MBS CLP=0 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). *MBS CLP=0+1 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (that is, the CLP=0+1 cell stream). *MCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MCR CLP=0. If so, specify the MCR (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). ***Note:*** *While the MCR traffic descriptor is only applicable to a CBX 500 with an FCP, this attribute is offered as a selection on non-CBX endpoints. This is because even though one or both endpoints may not be on a CBX with FCP, the PVC might traverse a CBX 500 FCP trunk. In this case, the provisioned attribute is used.*

Table 8-16. Set Traffic Type Attributes Fields (Traffic Parameters) (Continued)

Field	Action/Description
Shaper (*B-STDX CS/IWU endpoint only*)	If this circuit carries ATM cell traffic, use the default of NO SHAPER. If this circuit carries frame relay traffic, select one of the configured shapers in this pull-down menu.  These shapers correspond to the traffic shapers configured for the physical port on which this logical port resides. For information about physical port traffic shaping, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

User Preference Attributes

Select Set [User Preference] Attributes and complete the fields described in Table 8-17.

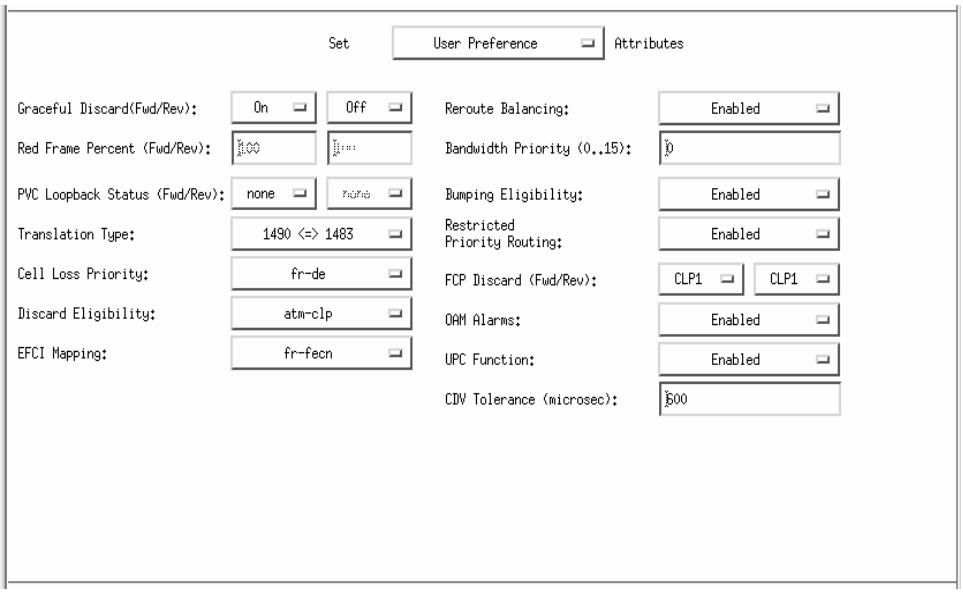


Figure 8-12. Set User Preference Attributes Fields (FR-ATM)

Table 8-17. Set User Preference Attributes Fields

Field	Action/Description
Graceful Discard (Fwd/Rev) (*PVCs with frame relay UNI endpoints only*)	Select either On or Off to define how this circuit handles "red" packets. Red packets are designated as those bits received during the current time interval that exceed the committed burst size (Bc) and excess burst size (Be) thresholds, including the current frame. The Discard Eligible (DE) bit for a red packet is set to 1, meaning the network cannot discard this packet unless Graceful Discard is set to On. *On* – (default) Forwards some red packets if there is no congestion. *Off* – Immediately discards red packets. ***Note:*** *For the ATM UNI DS3/E3, if you set this value for shaping purposes, the switch software ignores the PCR, SCR, and MBS values calculated from the Set Traffic Descriptor Attributes menu (Figure 8-11 on page 8-52); the switch instead picks the highest PCR queue available and sets the SCR to that PCR.*
Red Frame Percent (Fwd/Rev) (*PVCs with frame relay UNI endpoints only*)	Set this value only if Graceful Discard is set to On. See "Graceful Discard" on page 8-46 for more information. The Red Frame Percent limits the number of red frames the network is responsible to deliver.
PVC Loopback Status (Fwd/Rev)	Displays the current loopback state. If None is not displayed in the PVC Loopback Status field, do not attempt to modify or delete the selected circuit. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information about loopback testing.
Translation Type	*(ATM endpoint only)* Select the ATM Translation Type protocol. Options include: *None* – Each end of the circuit uses the 1490 protocol. *RFC 1490 ⇔ 1483* – This value is the default if you have a Frame Relay logical port on Endpoint 1 and an ATM logical port on endpoint 2. *RFC 1483 ⇔ 1490* – This option is the default if you have an ATM logical port on Endpoint 1 and a Frame Relay logical port on Endpoint 2.

Table 8-17. Set User Preference Attributes Fields (Continued)

Field	Action/Description
Cell Loss Priority	Specify the cell loss priority (CLP) setting. The CLP bit is in each cell's cell header. Options include: *0* – Sets the CLP bit to 0 (zero). *1* – Sets the CLP bit to 1. *fr-de* (1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 modules only) – Sets the CLP bit to the same value as the Frame Relay frame discard eligible (DE) bit on all ATM cells. This maps the DE bit to CLP. For more information about configuring this parameter for FRF.5, see "Special Network Interworking PVC Configuration Parameters" on page 8-42.
Discard Eligibility	Select one of the following settings: *0* – Sets the DE to 0 (zero). *1* – Sets the DE to 1. *atm-clp* (1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 modules only) – Sets the CLP bit received in last cell of the frame to Frame Relay frame DE bit. For more information about configuring this parameter for FRF.5, see "Special Network Interworking PVC Configuration Parameters" on page 8-42.
EFCI Mapping	Select one of the following settings: *fr-fecn* – (default) Maps the EFCI bit on the ATM endpoint to the frame relay FECN bit. *0* – Ignores EFCI to FECN bit mapping. ***Note:*** *For FRF.5, EFCI is always mapped to FECN for ATM-to-Frame Relay Interworking PVCs; EFCI is set to 0 (zero) for Frame Relay-to-ATM Interworking PVCs.*
Reroute Balancing	When enabled (default), the PVC conforms to the configured reroute tuning parameters. This means that when the PVC reroutes during trunk failure, it will migrate back to its original trunk at a rate and time determined by the configured reroute tuning parameters. When disabled, the PVC ignores the switch tuning parameters. For more information, see the *B-STDX, CBX, and GX Getting Started User's Guide*.
Bandwidth Priority (0..15)	Specify a value from 0 (zero) through 15, where 0 (zero) is the default and indicates the highest priority. See Appendix E, "Priority Routing," for more information.

Table 8-17. Set User Preference Attributes Fields (Continued)

Field	Action/Description
Bumping Eligibility	If restricted priority routing is disabled, specify Enabled (default) for the non-real time circuit to become active whether or not sufficient bandwidth exists. Specify Disabled to keep the non-real time circuit in retry mode until sufficient bandwidth is available. If restricted priority is enabled, a non-real time circuit that has been bumped remains in retry mode until sufficient bandwidth is available, regardless of the bumping eligibility setting (Disabled or Enabled). See Appendix E, "Priority Routing," for more information.
Restricted Priority Routing	Set to Enabled (default) to provision new circuits at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings. Set to Disabled if you want to use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits. See Appendix E, "Priority Routing," for more information.
FCP Discard (Fwd/Rev)	Displays only if you selected a QoS class that supports FCP Discard. Select one of the following options: *CLP1* – (default) You can provision selective CLP1 discard for UBR, ABR, and VBR-NRT PVCs. If the current cell causes the queue for a PVC to exceed the discard thresholds, and the cell has CLP set to 1, the cell is discarded. Note that EPD is not performed in this case. *EPD* – Early packet discard. The ATM Flow Control Processor can perform EPD for UBR, ABR, and VBR-NRT PVCs. If you select this option, when a cell causes the queue for a PVC to exceed the discard thresholds, the VC enters the EPD state. The cells in the current packet of the VC are admitted to the queue. However, when the end of the current packet is detected, all of the cells in the next packet are discarded for that PVC. See "ATM Flow-Control Discard Mechanisms" on page 5-18 for details. ***Note:*** *While the frame discard attribute is only applicable to a CBX 500 with an FCP, this attribute is offered as a selection on non-CBX endpoints. This is because even though one or both endpoints may not be on a CBX with FCP, the PVC might traverse a CBX 500 FCP trunk. In this case, the provisioned attribute is used.*

Table 8-17. Set User Preference Attributes Fields (Continued)

Field	Action/Description
OAM Alarms (*CBX/GX and 1-port ATM CS DS3/E3, 1-port ATM IWU OC-3c/STM-1, and 12-port T1/E1 module endpoints only*)	Choose Enable to allow this circuit to generate OAM alarms to indicate whether the circuit is up or down. These alarms send a signal to the logical port whenever the circuit goes down or comes back up.
UPC Function *(PVCs with CBX/GX endpoints only)*	Enables (default) or disables the usage parameter control (UPC) function. When you enable UPC, the circuit tags or drops cells as they come into the port that do not conform to the configured traffic descriptors. When you disable UPC, the circuit allows all traffic, including non-conforming traffic, into the port. As a result, when you disable UPC, quality of service is no longer guaranteed for circuits in the network due to the potential for increasing the cell loss ratio because of port congestion. For this reason, *Lucent recommends that you enable the UPC function on all circuits.* For information about UPC traffic parameters, see Chapter 10, "Configuring ATM Traffic Descriptors." ***Note:*** *To use the UPC function for individual circuits, verify that the UPC function is enabled for both logical port endpoints on which you will define the circuit. Enabling UPC at the circuit level has no effect if you did not enable UPC at the logical port level. UPC is enabled by default for both logical ports and circuits.*
CDV Tolerance (microsec) *(PVCs with CBX/GX and 1-port ATM CS DS3/E3, 1-port ATM IWU OC-3c/STM-1, and 12-port T1/E1 module endpoints only)*	Enter a value between 1 - 65535 µsec. to define the cell delay variation Tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. A lower CDVT value results in a more stringent enforcement of the traffic descriptor, while a larger CDVT results in a less stringent enforcement. The default is 600 µsec. For more information, see the *ATM Forum User-Network Interface (UNI) Specification* (section 3).

6. Choose OK to accept the circuit parameters and send the configuration information to the switch (provided the switch is communicating with the NMS).
7. The Set All PVCs dialog box reappears.
8. (*Optional*) To configure this PVC for a specific VPN and customer, see page 11-10.
9. Choose Close to return to the network map.

Defining a Redirect PVC Connection

To define a Redirect PVC connection between two UNI or NNI logical ports:

Note – Redirect PVCs are not supported on PPP connections.

1. From the Set All Redirect PVCs On Map dialog box (Figure 8-2 on page 8-16), select the circuit you want to view from the Defined Circuit Name list box.
2. Choose Add. The Select Redirect Circuit End Logical Ports dialog box appears (Figure 8-13).

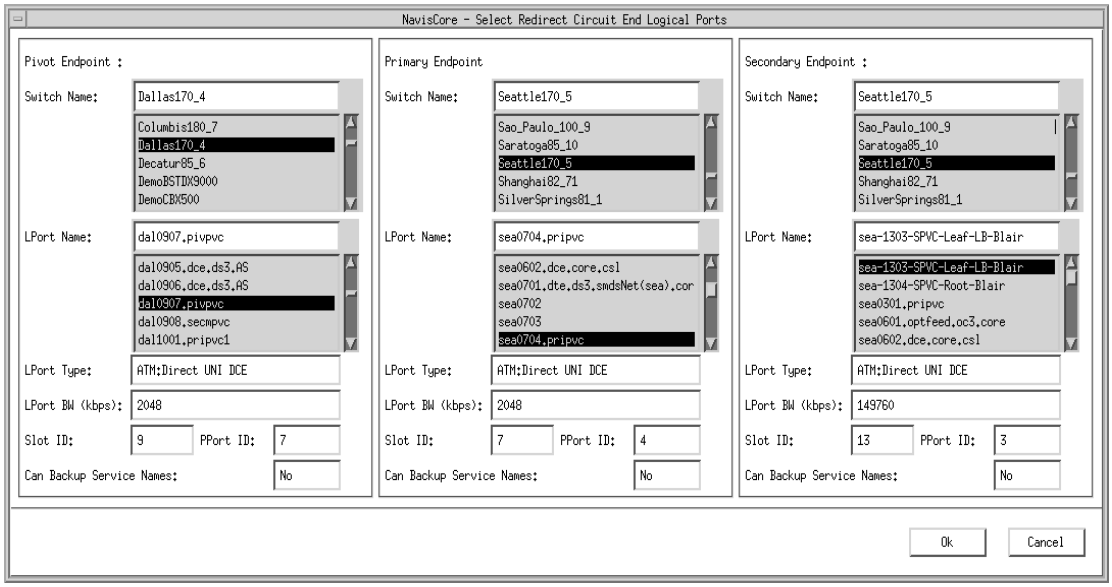


Figure 8-13. Select Redirect Circuit End Logical Ports Dialog Box

3. Select the appropriate switch and LPort names. Table 8-18 describes each of the fields on the Select Redirect Circuit End Logical Ports dialog box.

Table 8-18. Select Redirect Circuit End Logical Ports Dialog Box Fields

Field	Action/Description
Pivot Endpoint – Displays data for the switch, logical port (LPort), slot, physical port (PPort), and if Backup Service Names is available. Pivot is one of three end points having its own port/DLCI (VPI/VCI for ATM PVCs) combination.	
Switch Name	Select the appropriate switch name for the pivot end point.
LPort Name	Select the appropriate LPort name to display on the switch.

Table 8-18. Select Redirect Circuit End Logical Ports Dialog Box Fields (Continued)

Field	Action/Description
LPort Type	Displays the LPort type for the chosen LPort name.
LPort BW (kbps)	Displays the LPort bandwidth (BW) measurement in kpbs.
Slot ID	Displays the card's slot ID.
PPort ID	Displays the PPort's ID.
Can Backup Service Names	Displays Yes if LPort is configured for Backup Service Names; otherwise, displays No.
Primary Endpoint – Displays data for the switch, logical port (LPort), slot, physical port (PPort), and if Backup Service Names is available. Primary is one of three end points having its own port/DLCI combination.	
Switch Name	Select the appropriate switch name for the primary end point.
LPort Name	Select the appropriate LPort name to display on the switch.
LPort Type	Displays the type of LPort for the chosen LPort name. ***Note:*** *The Primary Endpoint's LPort Type field must display the same data as the Secondary Endpoint's LPort Type field.*
LPort BW (kbps)	Displays the LPort's BW measurement in Kpbs.
Slot ID	Displays the card's slot ID.
PPort ID	Displays the PPort's ID.
Can Backup Service Names	Displays Yes if LPort is configured for backup service names; otherwise, displays No.
Secondary Endpoint – Displays data for the switch, logical port (LPort), slot, physical port (PPort), and if Backup Service Names is available. Secondary is one of three end points having its own port/DLCI combination.	
Switch Name	Select the appropriate switch name for the secondary end point.
LPort Name	Select the appropriate LPort name to display on the switch.
LPort Type	Displays the type of LPort for the chosen LPort name ***Note:*** *The Secondary Endpoint's LPort Type field must display the same data as the Primary Endpoint's LPort Type field.*
LPort BW (kbps)	Displays the LPort BW measurement in Kpbs.
Slot ID	Displays the card's slot ID.
PPort ID	Displays the PPort's ID.

Table 8-18. Select Redirect Circuit End Logical Ports Dialog Box Fields (Continued)

Field	Action/Description
Can Backup Service Names	Displays Yes if LPort is configured for backup service names; otherwise, displays No.
OK (Button)	Displays the Add Redirect PVC dialog box.

4. Choose OK. The Add Redirect PVC dialog box (Figure 8-14) appears, displaying the current fields.

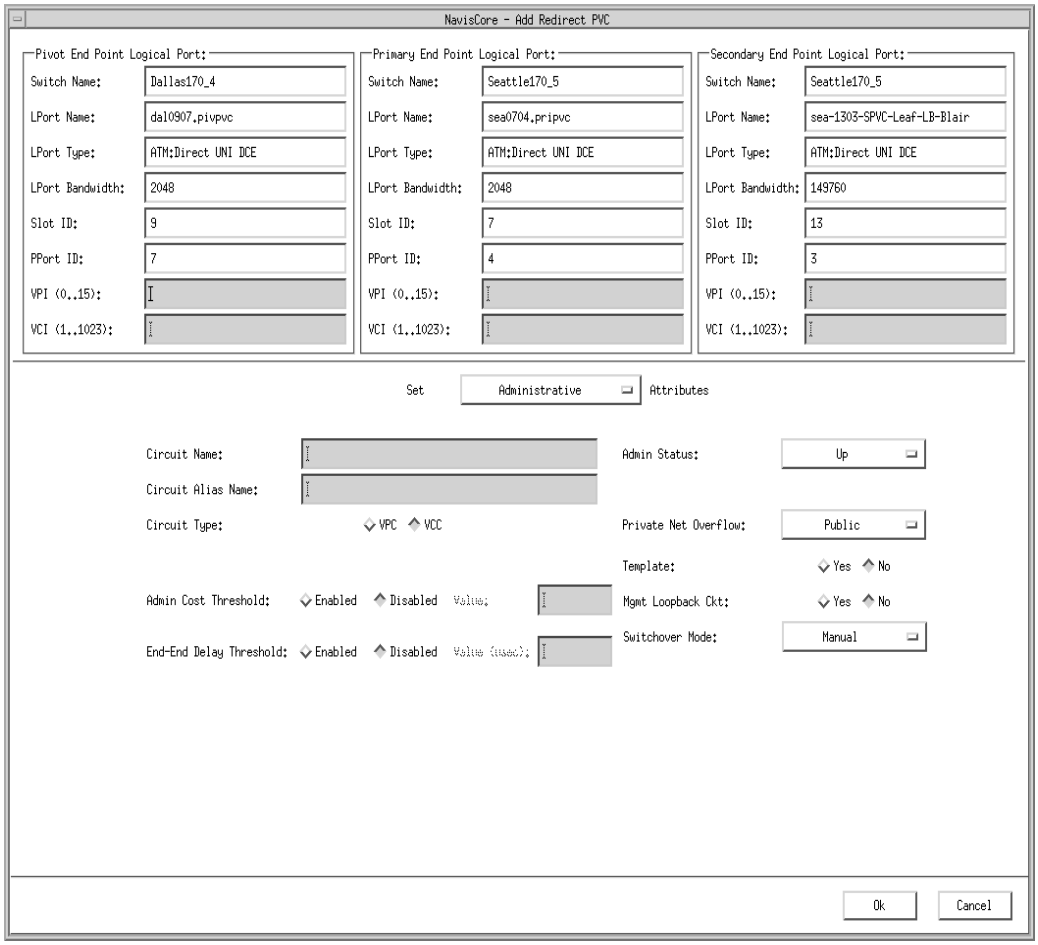


Figure 8-14. Add Redirect PVC Dialog Box

5. Complete the Add Redirect PVC dialog box fields in Table 8-19.

Table 8-19. Add Redirect PVC Dialog Box Fields

Field	Action/Description
VPI (0..15)	Enter a value from 0-*nnnn* to represent the VPI for the PVC. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. See page 8-9 for information about setting this value.
VCI (1..1023)	Depending on the circuit configuration, enter a value to represent the VCI for an ATM PVC. Although you can configure VCIs in the 1 – 31 range (with the exception of VCI=4), the ATM Forum reserves VCIs in this range for various purposes. You should only use a VCI in the 1 – 31 range if you are certain that compatibility issues will not arise with any attached non-Lucent equipment. See page 8-9 for information about setting this value.
Set Attributes (menu)	Displays the attributes that you can configure for the selected option. ***Note:*** *The Set Traffic Type Attributes information displayed in the Reverse column applies to both primary and secondary end points.*
Circuit Name	Enter any unique, continuous, alphanumeric name to identify the redirect circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Circuit Alias Name	(*Optional*) The circuit alias is used by service providers to identify the circuit in a way that is meaningful to their customers. This option is often used in conjunction with NavisXtend Report Generator. Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Circuit Type	Specify whether the circuit is a virtual path connection (VPC) or virtual channel connection (VCC, the default). If you select VPC, the VCI field is set to 0 (zero) and cannot be changed.
Admin Status	Select either Up or Down to define whether the redirect circuit is to be activated. *Up* (default) – Activates the circuit. *Down* – Takes the circuit offline to run diagnostics such as PVC loopback.

Table 8-19. Add Redirect PVC Dialog Box Fields (Continued)

Field	Action/Description
Private Net Overflow	Determines how redirect PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Select one of the following options: *Public* – (default) Redirect PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – Redirect PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template	(*Optional*) Save these settings as a template to use again to configure another PVC with similar options. The default parameter is No. To create a template, choose Yes in the Template field. See "Using Templates" on page 8-87 for more information.
Mgmt Loopback Ckt	Choose Yes to include this redirect PVC configuration in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download this file to the switch, this redirect PVC can be used to establish NMS-to-switch connectivity. This option is especially useful in some management configurations. The default value is No. (For more information about management PVCs, see Chapter 9.)
Admin Cost Threshold	This option is disabled by default. If you enable this option, the redirect PVC will not be routed over a path whose total administrative cost exceeds the entered value. This means that if you enable this field and enter a value of 1000, the redirect PVC will not be routed over a path whose total administrative cost exceeds 1000. The total administrative cost for a path is calculated by summing the administrative cost for each trunk in the path. The valid range of values for this field is 1 - 4294967295. (Do not enable this option if you use End-End Delay routing.)

Table 8-19. Add Redirect PVC Dialog Box Fields (Continued)

Field	Action/Description
End-End Delay Threshold (cell transfer delay)	This option is disabled by default. If you enable this option, the redirect PVC will not be routed over a path whose total end-to-end delay exceeds the entered value. This means that if you enable this field and enter a value of 500 µsec., the redirect PVC will not be routed over a path whose total end-to-end delay exceeds 500 µsec. The total end-to-end delay for a path is calculated by summing end-to-end delay for each trunk in the path. The valid range for this field is 0 - 16777214 µsec. ***Note:*** *The value you enter should reflect your network topology. If a redirect PVC typically traverses high speed trunks, set the delay rate lower; if the redirect PVC uses low-speed trunks, set the delay rate higher.*
Switchover Mode	Configure one of the following options: *Manual* – (default) Enables you to switch the circuit connection between the pivot end point and the primary *or* secondary end point. *Non-Revertive* – Triggers an automatic forward switchover to establish the connection between the pivot and secondary end points in case of primary end point failure. If the secondary end point goes down and the primary end point recovers, no automatic switchover is triggered. The administrator must manually switch the circuit connection from the working secondary end point backward to the primary end point. *Revertive* – Triggers an automatic forward switchover to establish the connection between the pivot and secondary end points in case of primary end point failure. If the primary end point recovers, the backward switchover is triggered automatically to re-establish the connection between the pivot and primary end points. ***Note:*** *To implement Redirect PVC with Revertive mode, the entire network must be upgraded to the current network management and switch software release.*

6. See the following sections to configure the remaining attributes for this Redirect PVC:
   - "Traffic Type Attributes" on page 8-30
   - "User Preference Attributes" on page 8-32
   - "Frame Discard Attributes" on page 8-36
   - "Extended QoS Parameters Attributes" on page 8-37
   - "Selectable Statistics Attribute" on page 8-39

Completing the Redirect PVC Configuration

To complete the redirect circuit configuration:

1. (*Optional*) To configure NavisXtend Accounting Server parameters for this circuit, choose the Accounting button. For more information, see the *NavisXtend Accounting Server Administrator's Guide*.
2. (*Optional*) To configure CBX 500 or GX 550 Network Data Collection (NDC) parameters for this circuit, select Set [NDC] Attributes. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
3. To add more Redirect PVCs, repeat the steps in "Defining a Redirect PVC Connection" on page 8-62.
4. Choose OK. The Set All Redirect PVCs On Map dialog box reappears (Figure 8-2 on page 8-16) displaying the new Redirect PVC in the Defined Circuit Name (Circuit Alias Name) list box.
5. When you finish, choose Close to return to the network map.

Setting the Redirect PVC Delay Time

You configure the Redirect PVC Delay Time on the Add Logical Port dialog box (Table 3-4 on page 3-14 or Table 4-7 on page 4-15) for ATM UNI and NNI logical port types. This option enables you to set the number of seconds to wait before the network initiates call clearing after a circuit goes down.

You configure the Redirect PVC Delay Time only for the primary end point.You can reset this field at any time; the range is 0 – 255 seconds. Entering 0 (default) in this field causes the network to immediately initiate call clearing, which can trigger the switchover between a working redirect PVC end point and its primary or secondary end point. Increasing the value can minimize the Redirecting PVCs as a result of temporary data terminal equipment (DTE) state changes.

Manually Defining the Circuit Path

The Define Circuit Path dialog box enables you to manually define a circuit path and the OSPF algorithm's circuit routing decisions. You cannot manually route a circuit that is configured with both endpoints in the same switch.

The circuit may cross PNNI peer groups, PNNI-VNN boundaries, VNN Areas, and Non-Lucent Networks (PNNI). If the alternate path option is defined, and a circuit failure occurs in the manually defined circuit path, the circuit can be routed based on VNN or PNNI information provided.

To manually define the circuit path:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs on Map dialog box (Figure 8-1 on page 8-10) appears.
2. Select the circuit for which you want to manually define the circuit path and choose Define Path.
3. Select Pure VNN Path or VNN/PNNI Mixed Path.
   - Selecting Pure VNN Path will cause the Pure VNN Define Circuit Path dialog box to display (see Figure 8-15 on page 8-70). This will list only VNN links of the switch in the network map.
   - Selecting VNN/PNNI Mixed Path will cause the VNN/PNNI Mixed Define Circuit Path dialog box to display (see Figure 8-16 on page 8-70). This will list both PNNI and VNN links of the switch in the network map.

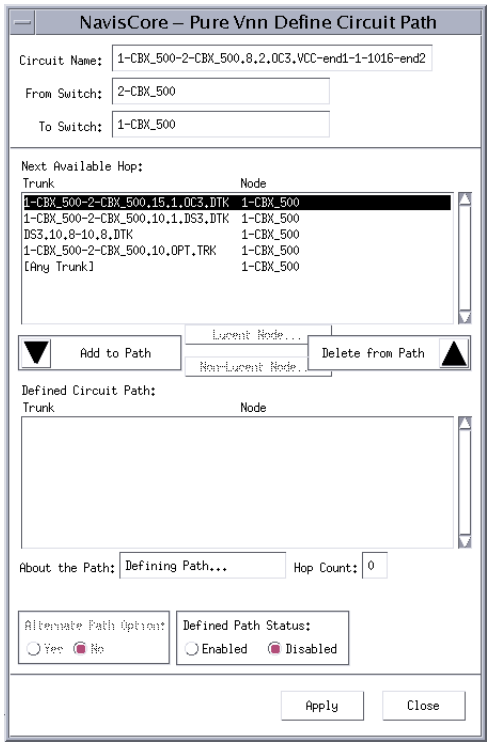


Figure 8-15. Pure VNN Define Circuit Path Dialog Box

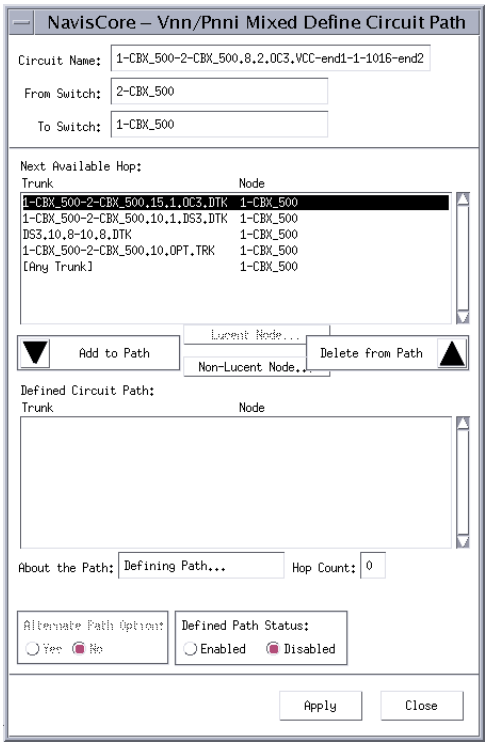


Figure 8-16. VNN/PNNI Mixed Define Circuit Path Dialog Box

4. Complete the fields described in Table 8-20.

Table 8-20. Define Circuit Path Dialog Box Fields

Field	Action/Description
Next Available Hop	Displays a listing of the available hops (for example, trunk-node pairs or PNNI links). • Select the trunk-node pair through which you want to route the circuit. When there are multiple trunks between two nodes, select Any Trunks to cause OSPF to decide which is the best path to use at any given time. • Choose Add to Path. The trunk-node selection is added to the Defined Circuit Path field, which displays all selected hops.
Alternate Path Option	Select either Yes or No to define whether OSPF should route the circuit if the manual route fails. • Select Yes to enable OSPF to route the circuit based on the best available path. • Select No to disable the circuit from being rerouted; the circuit remains down until the defined path becomes available.
Defined Path Status	Select Enabled to route the circuit based on the manual route defined. Select Disabled to route the circuit based on the network's OSPF algorithm.

5. To define the next hop to a non-Lucent node:

   a. Select Non-Lucent Node. The PNNI Node ATM Address dialog box will display.

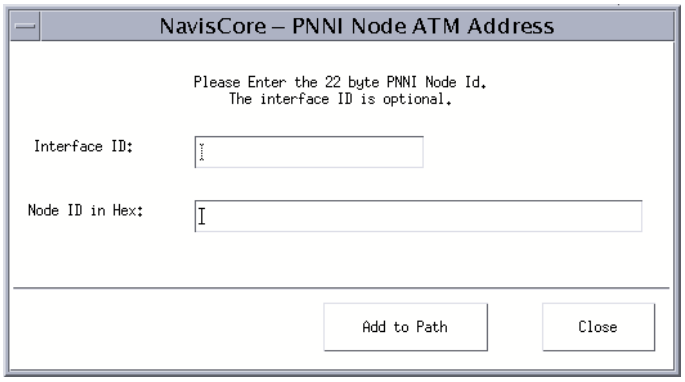


Figure 8-17. PNNI Node ATM Address Dialog Box

   b. (*Optional*) Enter the logical port Interface ID.

   c. Enter the 22-byte PNNI Node ID of the non-Lucent node.

   d. Choose Add to Path. The Define Path dialog box will reappear.

6. After defining all the non-Lucent nodes, define the next hop to a Lucent switch:
   a. Select Lucent Node. The Lucent Node IP Address dialog box will display.

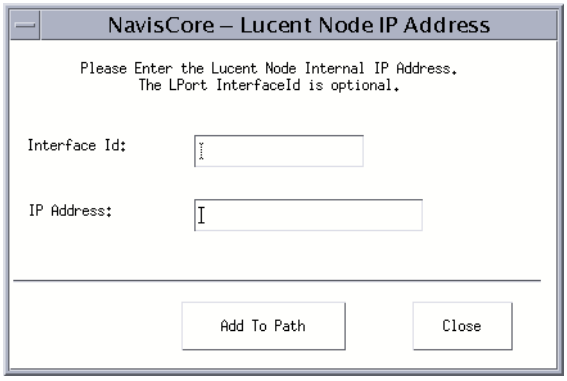


Figure 8-18. Lucent Node IP Address Dialog Box

   b. (*Optional*) Enter the logical port Interface ID.
   c. Enter the internal IP Address of the next Lucent switch node.
   d. Choose Add to Path. The Define Path dialog box will reappear.
7. Choose Apply and then choose Ok.

Moving Circuits

The Move Circuit function enables you to move a circuit endpoint defined for one logical port (the source) to another logical port (the destination). If you are upgrading a switch or replacing an I/O card and do not want to lose PVC connections, you can use this function to move circuits to another switch or I/O card.

This function has the following restrictions:

- You should not move a circuit that is currently in use, because it may lose traffic.
- You cannot move a circuit for which you have manually defined a circuit path.
- The VPI/VCI must be unique to the destination logical port.
- The Move Circuit function fails if the number of circuits moved exceeds the maximum allowed for the I/O card.
- You can not move a circuit with one endpoint defined with Service Name Binding (SNB). NavisCore will display the error message “Cannot move circuit with one endpoint defined on service name.”

To move a circuit:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Move Circuit Endpoint. The Select Source & Destination LPorts dialog box appears.

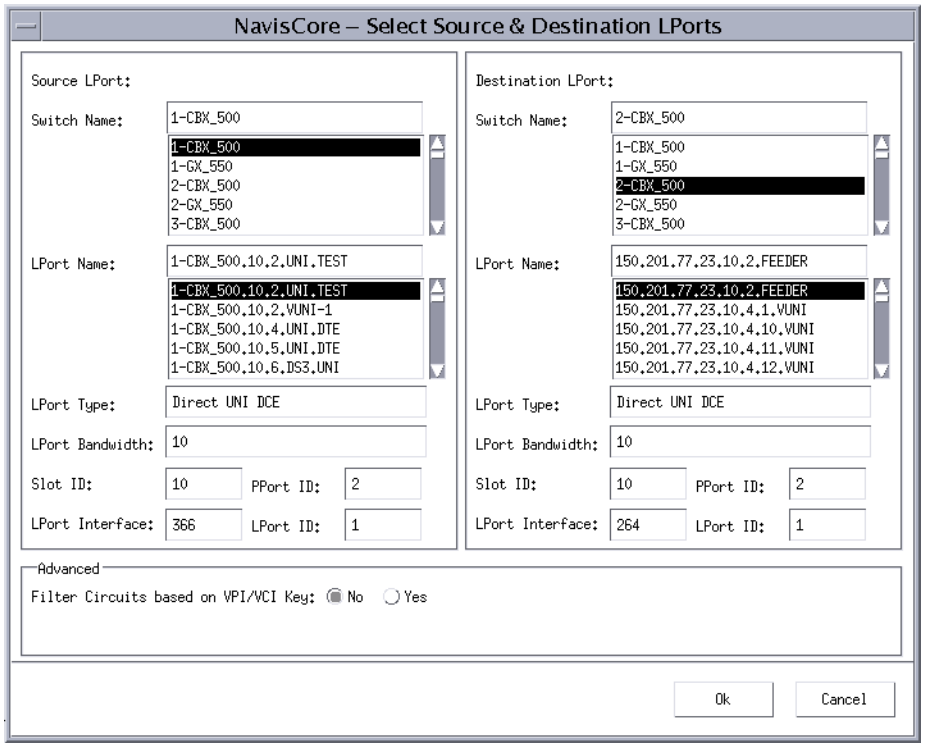


Figure 8-19. Select Source & Destination LPorts Dialog Box

2. To select the Source LPort that contains the circuit you want to move:
   a. Select the Switch Name.
   b. Select the LPort Name.
3. To select the Destination LPort to which you want to move the circuit:
   a. Select the Switch Name.
   b. Select the LPort Name.
4. Choose OK. The Move Circuit Endpoint dialog box appears. This dialog box displays the circuits that have the source logical port as an endpoint.

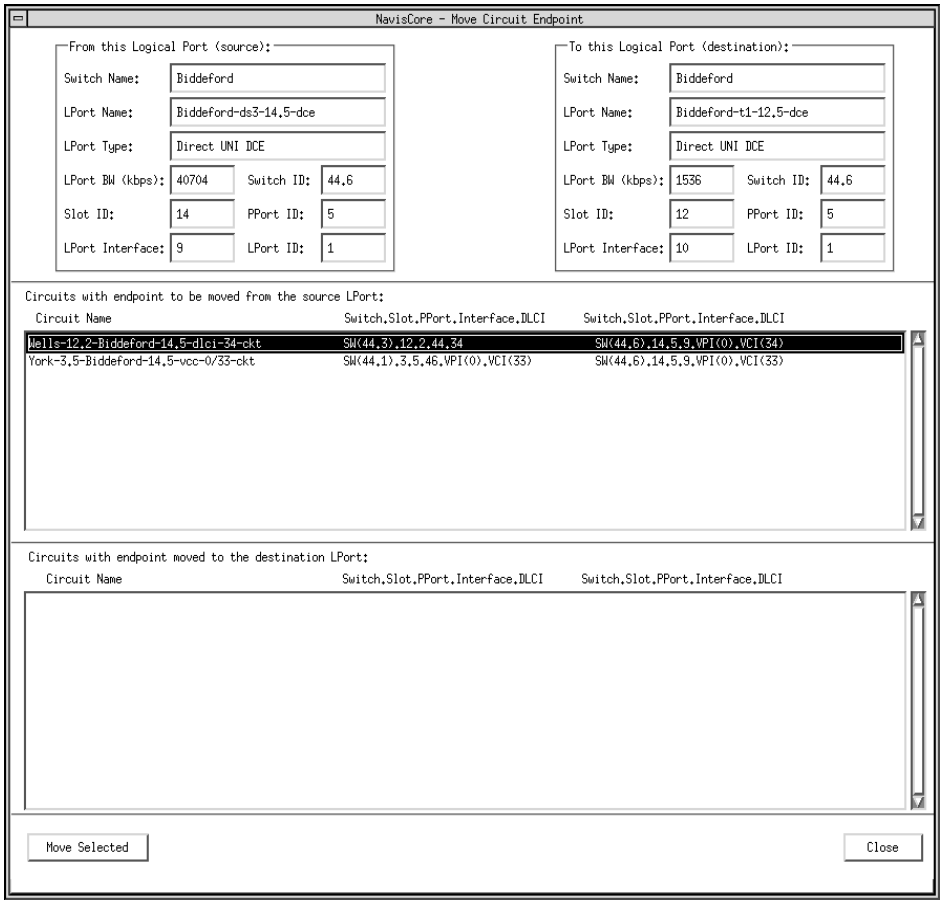


Figure 8-20. Move Circuit Endpoint Dialog Box

5. From the *Circuits with endpoint to be moved from the source LPort* list box, select the circuit(s) you want to move.
6. Choose Move Selected. The selected circuit appears in the *Circuits with endpoint moved to the destination LPort* list box.
7. When you finish, choose Close.

Configuring Point-to-Multipoint Circuits

A point-to-multipoint (PMP) circuit consists of the originating point (circuit root), and endpoints (circuit leafs). The endpoints of a given PMP circuit can be on any switch in the network map, and on any number of switches (that is, the endpoints do not have to terminate on the same switch).

To access the Set All Point-to-Multiple-Point Circuit Roots dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Point-to-Multipoint Circuits. Place the cursor in the Search Circuit Root by Name field and press Enter to display the list of circuit root names. The following dialog box appears.

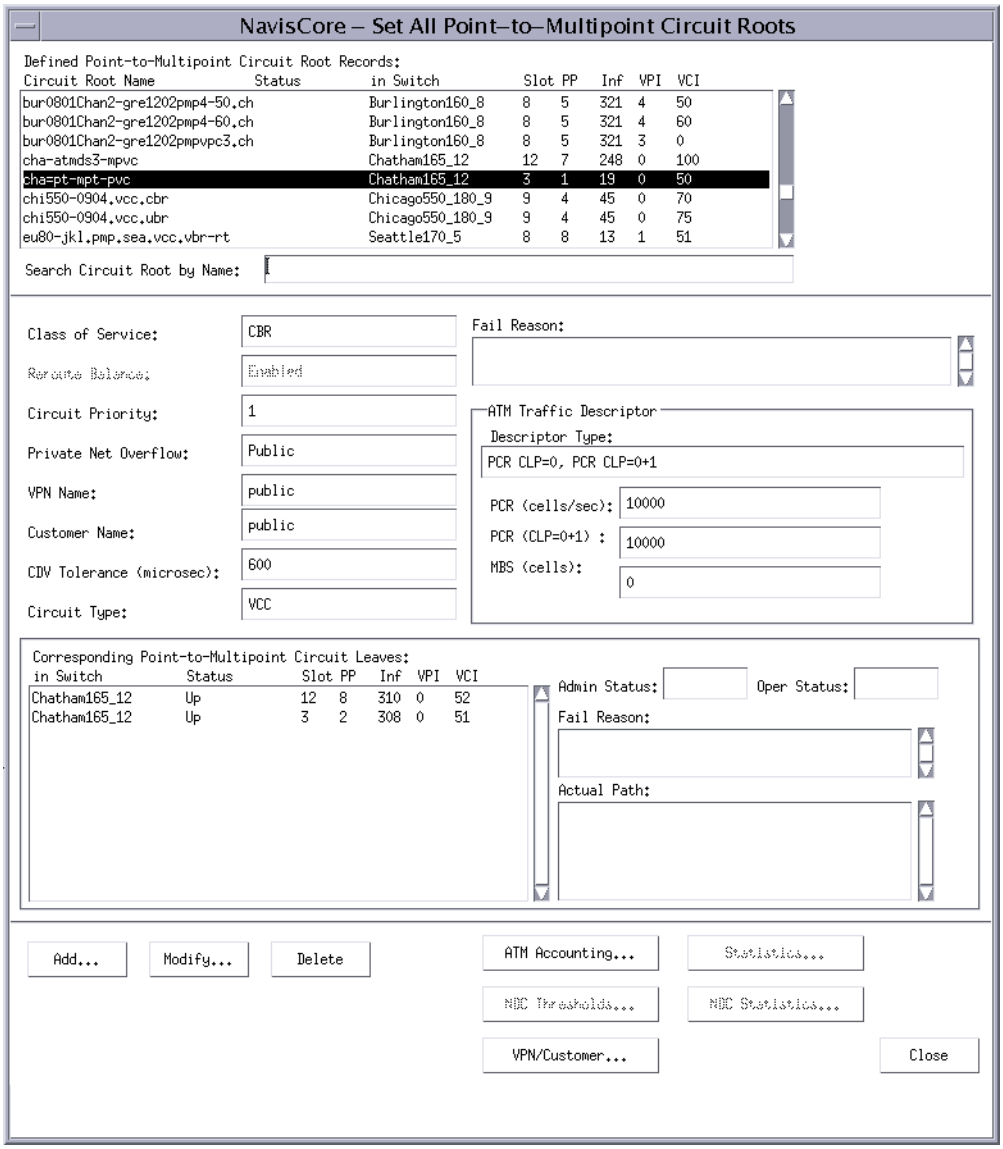


Figure 8-21. Set All Point-to-Multiple-Point Circuit Roots Dialog Box

The *Defined Point-to-Multiple-Point Circuit Root Records list* box at the top of the screen lists any existing PMP circuit roots. The *Corresponding Point-to-Multiple-Point Circuit Leafs list* box at the bottom of the screen lists any existing circuit leafs (endpoints) for the selected circuit root.

Table 8-21 describes the buttons on the Set All Point-to-Multiple Point Circuit Root dialog box.

Table 8-21. Set All Point-to-Multiple-Point Circuit Root Dialog Box Buttons

Button	Description
Add	Adds a new point-to-multiple-point circuit.
Modify	Modifies the selected point-to-multipoint circuit root. The Modify button displays dialog boxes that are similar to those displayed for Add point-to-multipoint; however, you cannot modify the circuit name, logical port endpoints, circuit type, or VPI/VCI values from this dialog box.
Delete	Deletes the selected point-to-multipoint circuit root.
ATM Accounting	Accesses the NavisXtend Accounting Server functions for a PVC.
Statistics	Displays the summary statistics for the selected point-to-multipoint circuit.
NDC Thresholds (*CBX 500 and GX 550 only*)	Displays the configured Network Data Collection (NDC) thresholds for the selected circuit. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
NDC Statistics (*CBX 500 and GX 550 only*)	Displays the NDC statistics for the selected circuit. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
VPN/Customer	Assigns the selected point-to-multipoint circuit root to a specific Layer2 VPN and customer name. You must do this before you create PMP circuit leafs.

Table 8-22 describes the fields on the Set All Point-to-Multiple Point Circuit Root dialog box.

Table 8-22. Set All Point-to-Multiple-Point Circuit Root Dialog Box Fields

Field	Description
in Switch	The switch ID and switch name on which the root or leaf resides.
Slot	The physical slot for the IOM on which the root or leaf was created.
PP	The number of the physical port on which the root or leaf was created.
Inf	The MIB interface number for the logical port on which the root or leaf was created.
VPI	The virtual path identifier of the logical port assigned to the root or leaf.
VCI	The virtual channel identifier of the logical port assigned to the root or leaf.
Class of Service	Displays the QoS class (CBR, VBR-RT, VBR-NRT, or UBR) for the PMP circuit.
Reroute Balance	Shows whether reroute balancing is Enabled (default) or Disabled for this PMP circuit. See page 8-33 for information about the Reroute Balancing field.
Circuit Priority	Displays the priority of the circuit: 1 (High), 2 (Medium), 3 (Low), or 4 (Lowest).
Private Net Overflow	Displays how circuit traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Displays one of the following values: *Public* – (default) Circuits are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – Circuits can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
VPN Name	Assigns the selected circuit to a specific Layer2 VPN and customer name.
Customer Name	Displays the customer name for the selected circuit (if applicable).

Table 8-22. Set All Point-to-Multiple-Point Circuit Root Dialog Box Fields (Continued)

Field	Description
CDV Tolerance (circuits *with CBX/GX endpoints only*)	Displays the configured cell delay variation tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor.
Circuit Type	Displays whether the circuit is a VCC or VPC.
Fail Reason	Displays the reason for the logical port failure if an SNMP request was not sent successfully. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information.
ATM Traffic Descriptor	Displays the circuit's traffic descriptor(s) settings. The number of values displayed depends on the traffic descriptor combination that was selected for the circuit. For example, if you selected the combination PCR CLP = 0+1, SCR CLP = 0, and MBS CLP = 0, three values are displayed: • The first value (PCR) is the PCR for CLP = 0+1 • The second value (SCR) is the SCR for CLP = 0 • The third value (MBS) is the MBS for CLP = 0 If, however, you selected the PCR CLP = 0+1 combination, only one value is displayed: the PCR for CLP = 0+1.
Actual Path	Displays the actual path that OSPF and/or PNNI selected for this circuit to use to reach its destination.

Defining a Point-to-Multipoint Circuit Root

To configure the originating point (circuit root) for a point-to-multipoint circuit:

1. From the Set All Point-to-Multiple-Point Circuit Roots dialog box, choose Add. The following dialog box appears.

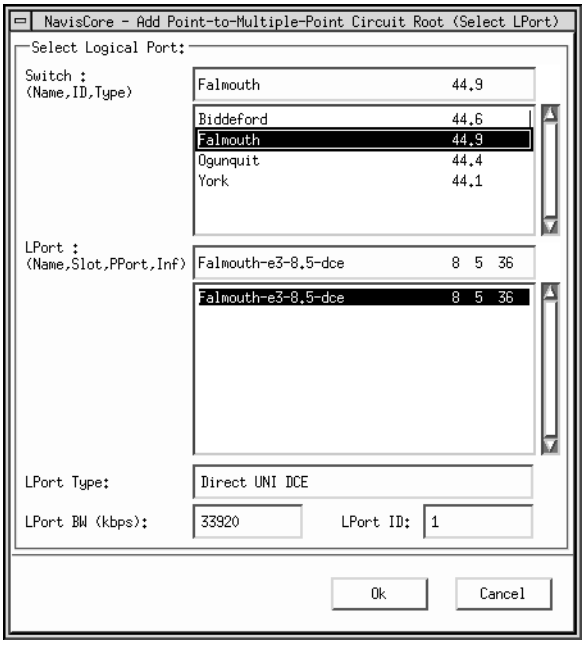


Figure 8-22. Add Point-to-Multiple-Point Circuit Root (Select LPort) Dialog Box

2. In the Switch list box, select the switch on which the originating point of the circuit will reside. The list contains the switch name, switch ID and switch type for all switches the NMS can currently access. The selected switch name appears in the text box above the list.
3. In the LPort list box, select the logical port on which the originating point of the circuit will reside. The selected logical port appears in the text box above the list. The list box displays the logical port name, slot ID, physical port number, and MIB interface number (Inf) for all logical ports on the selected switch.

   The LPort list box displays the following information for the selected port:

   LPort Type — Displays the type of logical port.

   LPort BW (Kbps) — Displays the total logical port bandwidth for the selected logical port, in kilobits per second (Kbps).

   LPort ID — Displays the logical port ID for the selected logical port.

4. Choose OK to display the Add Point-to-Multiple-Point Circuit Root dialog box.

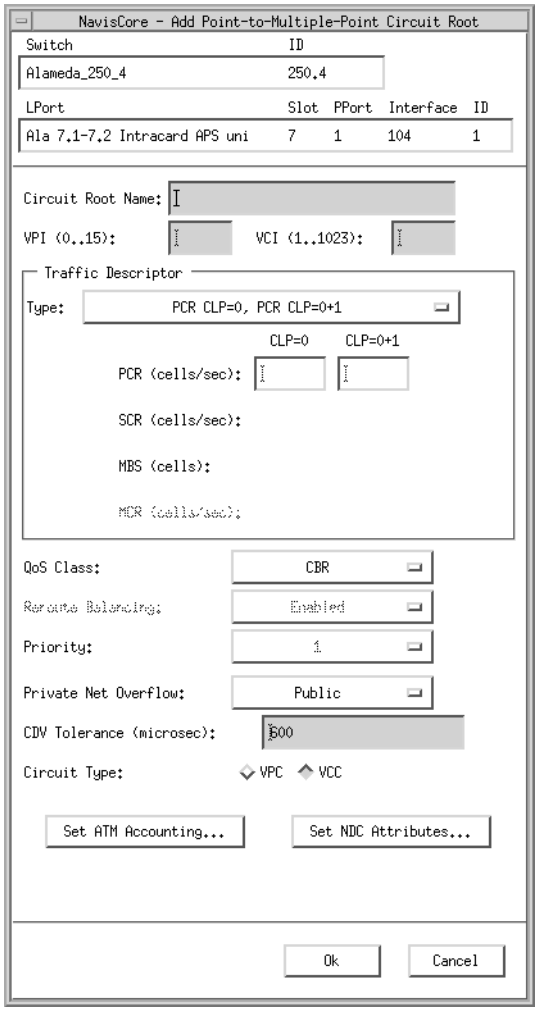


Figure 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box

5. Complete the fields described in Table 8-23.

Table 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box Fields

Field	Action/Description
Circuit Root Name	Enter an alphanumeric name for the circuit root.
VPI (0..15)	Enter a value from 0-15 to represent the VPI for the PVC. The maximum value you can enter is based on the valid bits in VPI that are configured for the logical port. See page 8-9 for information about setting this value.

Table 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box Fields (Continued)

Field	Action/Description
VCI (1..1023) (*For VCCs only*)	Depending on the circuit configuration, enter a value from 1-1023 to represent the VCI for an ATM PVC. Although you can configure VCIs in the 1 – 31 range (with the exception of VCI=4), the ATM Forum reserves VCIs in this range for various purposes. You should only use a VCI in the 1 – 31 range if you are certain that compatibility issues will not arise with any attached non-Lucent equipment. See page 8-9 for information about setting this value.
Traffic Descriptor Type	Select from the following traffic descriptor options: *PCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (that is, the CLP=0 cell stream). *PCR CLP=0+1 (cells/sec)* – Specify the PCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *SCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for the combined high-priority traffic (that is, the CLP=0 cell stream). *SCR CLP=0+1 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream). *MBS CLP=0 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). *MBS CLP=0+1 (cells)* – Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for the combined high- and low-priority traffic (that is, the CLP=0+1 cell stream). *MCR CLP=0 (cells/sec)* – Displays only if you selected a traffic descriptor combination that includes MCR CLP=0. If so, specify the MCR (in cells per second) for the combined high-priority traffic (that is, the CLP=0 cell stream). ***Note:*** *While the MCR traffic descriptor is only applicable to a CBX 500 with an FCP, this attribute is offered as a selection on non-CBX endpoints. This is because even though one or both endpoints may not be on a CBX with FCP, the PVC might traverse a CBX 500 FCP trunk. In this case, the provisioned attribute is used.*

Table 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box Fields (Continued)

Field	Action/Description
QoS Class	Select one of the following Quality of Service (QoS) options: *CBR* – (default) Constant Bit Rate *VBR-rt* – Variable Bit Rate Real Time *VBR-nrt* – Variable Bit Rate Non-Real Time *UBR* – Unspecified Bit Rate
FCP Discard *(CBX 500 with FCP only)*	Appears only if you select a QoS class that supports FCP Discard. Select either the *CLP1* or *EPD* option. (See "ATM Flow-Control Discard Mechanisms" on page 5-18 for more information.)
Reroute Balancing	When enabled, circuits use the tuning parameters you defined for the switch. When disabled, switch tuning parameters are ignored for the circuit. For more information, see the *B-STDX, CBX, and GX Getting Started User's Guide*.
Priority (*VBR-NRT and VBR-RT QoS classes only*)	Select circuit priority, where 1 is high priority, 2 is medium priority, 3 is low priority, and 4 is lowest priority.
Private Net Overflow	Determines whether this PVC is restricted to trunks of its own Layer2 VPN or can use public (shared) trunks during overflow conditions. To configure this circuit for a specific Layer2 VPN and customer, see page 11-10. For more information about Layer2 VPNs, see page 11-2. Select one of the following options: *Public* – (default) PVCs are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – PVCs can only use dedicated Layer2 VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
CDV Tolerance (microsec)	Enter a value between 1 - 65535 µsec to define the cell delay variation tolerance (CDVT). The UPC uses this value to police the requested traffic descriptor. The default is 600 µsec. ***Note:*** *If you are using the 3-Port Channelized DS3/1 IMA IOM, the recommended minimum CDV Tolerance value is 1000 microseconds.*

Table 8-23. Add Point-to-Multiple-Point Circuit Root Dialog Box Fields (Continued)

Field	Action/Description
Circuit Type	Specify whether the circuit is a virtual path connection (*VPC*) or virtual channel connection (*VCC*, the default). If you select VPC, the VCI field is set to 0 (zero) and cannot be changed.

6. (*Optional - CBX 500 and GX 550*) Choose the Set [NDC] Attributes option. See the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for configuration information. When you finish, continue with step 7.
7. Choose OK to return to the Set All Point-to-Multiple-Point Circuit Roots dialog box (Figure 8-21 on page 8-75).

Note – For information about the Set ATM Accounting button (Figure 8-23 on page 8-80), see the *NavisXtend Accounting Server Administrator's Guide*.

8. To assign this PMP Circuit to a Layer2 VPN or customer, choose the VPN/Customer button and see page 11-10.
9. Continue with "Defining Point-to-Multipoint Circuit Leafs" on page 8-84.

Defining Point-to-Multipoint Circuit Leafs

To add endpoints to the root circuit:

1. To configure the multiple endpoints of the point-to-multipoint circuit, from the Set All Point-to-Multiple-Point Circuit Roots dialog box (Figure 8-21 on page 8-75) choose Modify. The Modify Point-to-Multiple-Point dialog box appears.

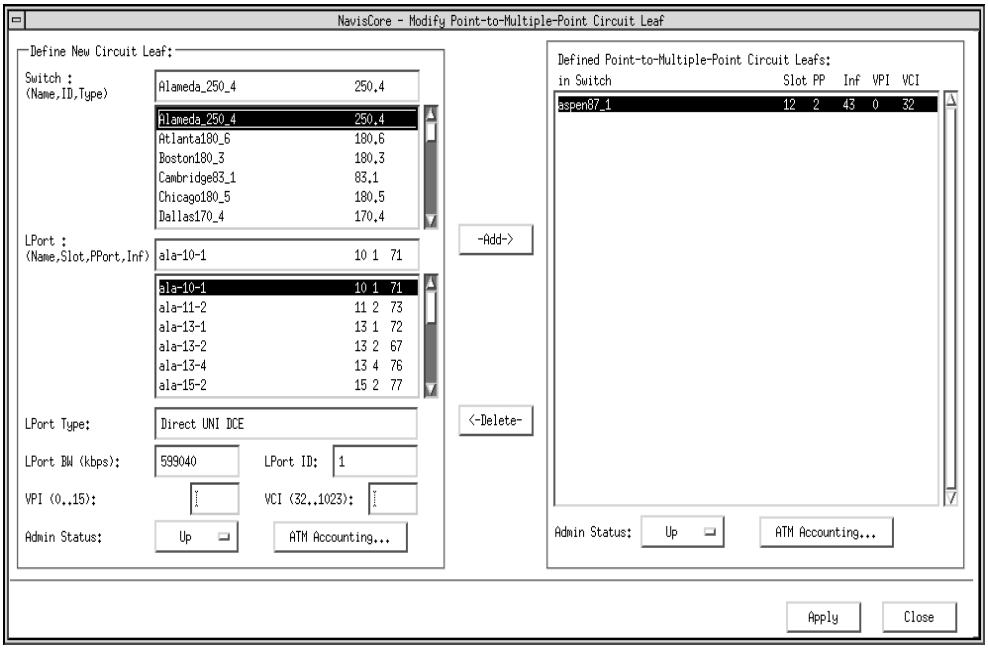


Figure 8-24. Modify Point-to-Multiple-Point Circuit Leaf Dialog Box

The list box on the left enables you to define the endpoints of the new circuit leaf. The list box on the right shows the endpoints that have already been defined for the point-to-multipoint circuit leaf.

2. To add a new endpoint:

   a. From the Switch list box, select the switch on which to configure the new endpoint. The LPort list box changes to show the logical ports that are configured on the selected switch.

   b. In the LPort list box, select the logical port for the new endpoint.

   c. In the VPI (0..15) and VCI (32..1023) fields, enter the virtual path identifier and virtual channel identifier for the point-to-multiple-point circuit as appropriate (that is, VPCs do not require a VCI).

   d. Set the Admin Status to Up if you want to activate this circuit when the switch comes online. Set the Admin Status to Down if you do not want to activate this circuit when the switch comes online.

e. Choose -Add-> to add the circuit to the Defined Point-to-Multiple-Point Circuit Leafs list box.

f. Repeat step 2 for each endpoint you want to create for this PMP circuit. When you finish, go to step 3.

3. Choose Apply, then choose Close to return to the Set All Point-to-Multiple Point Circuit Root dialog box.

To define additional PMP circuits and endpoints, repeat step 1 through step 3. When you are done adding PMP circuits and endpoints, choose Close to return to the network map.

Restrictions on Multiple Leafs on the Same Physical Port

On the GX 550 and certain releases of CBX 500 (prior to version 03.02.00.00), logical multicasting is not supported. In this situation, you should not configure more than one point-to-multipoint leaf on a physical port. Do not configure more than one circuit leaf for a given root on the same physical port. If you configure more than one OPTimum trunk on a physical port, only one OPTimum trunk can be used for routing one of the leafs for a given root.

Figure 8-25 illustrates invalid and valid configuration examples that show how multiplexing cannot and can occur at the port level.

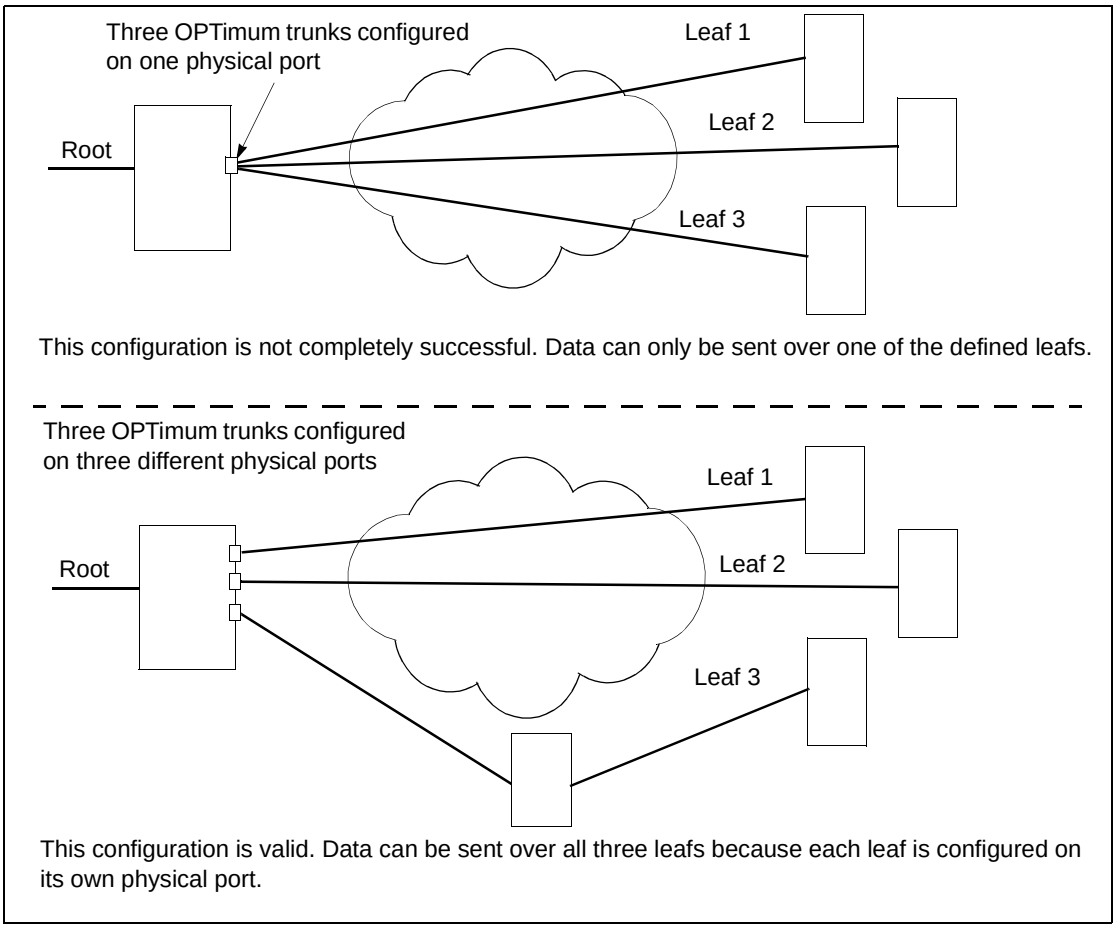


Figure 8-25. Point-to-Multipoint Circuit Example

Deleting a Point-to-Multipoint Circuit Root and Leafs

Before you delete a circuit root, you must delete all of the circuit's leafs.

To delete a PMP circuit root and/or one or more of the circuit's leafs, as well as the entire circuit:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Point-to- Multipoint Circuits. The Set All Point-to-Multiple-Point Circuit Roots dialog box appears (Figure 8-21 on page 8-75).
2. From the Circuit Root Name list, select the PMP circuit root you want to delete.
3. Choose Modify. The Modify PMP Circuit Leaf screen appears.
4. From the Defined PMP Circuit Leafs list, select the leaf you want to delete.
5. Choose Delete. When the confirmation box appears, choose OK to continue.

6. Repeat step 4 and step 5 for each circuit leaf you want to remove from the PMP circuit. If you are deleting the circuit, delete all leafs.
7. When done, choose Apply and then Close.
8. In the Circuit Root Name list, verify that the circuit you want to delete is selected. Also, in the Corresponding Point-to-Multiple-Point Circuit Leafs list box, verify that no leafs are listed (that is, they have all been deleted).
9. Choose Delete. A confirmation box appears.
10. Choose OK to delete the circuit root. The circuit is now deleted from the network.
11. Choose Close to return to the network map.

Using Templates

If you defined a circuit configuration and saved it as a template (see the Template field in Table 8-7 on page 8-27), you can define a new circuit using the same parameters.

To define a circuit from a template:

1. Choose one of the buttons in the Add Using Template section on the Set All PVCs on Map dialog box (see Figure 8-1 on page 8-10).
2. Choose one of the following in the Add Using Template field:
   - Choose Last Template to use the last template you defined for this switch.
   - Choose Template List to display a list of templates defined for this map. Select a template and choose Ok.

Deleting Circuits

To delete a circuit:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits. The Set All PVCs On Map dialog box appears (see Figure 8-1 on page 8-10).
2. To view the list of circuits, select the Search by Name field and press Return. If necessary, select each circuit and review each logical-port endpoint.
3. Select the circuit to delete.
4. Choose Delete.

9

Configuring Management Paths

This chapter explains how to configure a management path between a Lucent switch and the Network Management Station (NMS) or IP host. This management path can then be used to access the switch for either configuration or Telnet purposes. The term *NMS* describes the workstation that is used to host NMS applications. You can use this same procedure to establish communications between the switch and any IP host (that is, NavisXtend Accounting Server).

The management path options described in this chapter are available when the NMS or IP host connects to the switch via an ATM router or Network Interface Card (NIC). Unless otherwise noted, these options are available on all Lucent switch platforms (B-STDX and CBX switches, and GX Multiservice WAN switch).

The connection between the NMS and the switch network is called the *NMS Path.* This connection sets up the link to send and receive management protocol requests and responses. To make this connection, you must know the IP address of the NMS. The NMS path configuration is node-specific and describes each NMS that attaches via the switch.

You only need to define an NMS path for the switch that contains one of the following management connection elements:

Management PVC (MPVC) — 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 or NNI logical port (to which the NMS or IP host connects), and the remote switch CP/SP/NP module, the switch that connects the NMS or IP host is not burdened by the traffic traversing the management PVC.

You can also use *redirect* MPVC to create a management path for a connection that has *three* endpoints: pivot, primary, and secondary.

Management VPI/VCI — This is the preferred method if you only use the attached NMS or IP host to transfer information between the host and the local switch. Even though you can use a management VPI/VCI connection to transfer information between the host and remote switch(es), using this method to transfer large amounts of information can have a negative impact on the local switch. This is because the CP/SP/NP at the local switch would have to act as the gateway interface between the host and the remote switches.

You can also configure *Subnet Routing for Management VPI/VCI* to manage multiple devices over one VPI/VCI connection. You configure an autonomous system external (ASE) Mask to connect to an external device, or an IP network of external devices to enable management VCs to traverse Virtual Network Navigator (VNN) areas.

Management SPVC (MSPVC) — (CBX and GX only) You can use this type of connection to connect the switch management port to an SVC terminating address located on an adjacent switch. This management connection is used as the NMS path which enables the NMS to manage the switch.

MSPVCs are particularly useful for providing the management connectivity needed in a PNNI environment as shown in Figure 9-1. See "Using Management SPVCs in a PNNI Environment" on page 9-11 for more information.

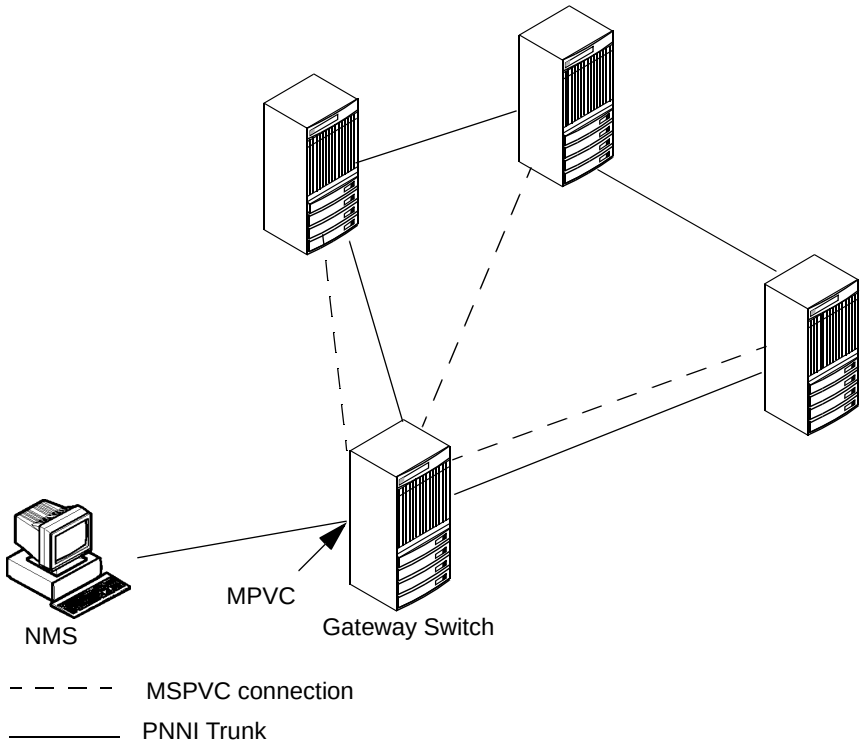


Figure 9-1. Connecting a PNNI Network

Using Management PVCs

A management PVC (MPVC) provides the connection from the NMS (or other workstation) to the gateway switch, while the remaining switches in your PNNI network are connected using management SPVCs (MSPVCs). Figure 9-1 on page 9-2 illustrates this concept.

A management PVC (MPVC) provides an access point to the switching network's management plane (which is IP-based). MPVCs offer an efficient, high-performance data path capable of transferring large amounts of management data, such as NavisXtend Accounting or Statistics Server files. This feature is available on B-STDX, CBX, and GX switch platforms.

MPVCs originate at the switch I/O interface: IOP (B-STDX), IOM (CBX), and BIO (GX 550). They terminate at an internal logical port located on the switch processor module (either CP, SP, or NP, respectively). MPVCs provide a data path that accesses internal network management functions. This enables you to use any physical port as a network management port.

The MPVC internal logical port is designated as MgmtLPort.SW<*switchname*>. It uses an interface number (ifnum) of 4093. To form the circuit, connect the MgmtLPort. SW<*switchname*> endpoint to any UNI logical port type. You can configure MPVCs across different switch platforms; for example, B-STDX Frame Relay UNI to CBX MPVC. Configure the remaining PVC attributes as you would for a standard PVC. Note that you can use the internal management port to terminate more than one MPVC.

Note – When you configure a redirect MPVC, the pivot endpoint must be the management logical port (MgmtLPort) on the CP/SP/NP.

The CBR QoS class is not available on MPVCs.

MPVCs enable you to configure a management path to an Autonomous System External (ASE). Once you define the management path, the IP process on the switch's processor module can send (and receive) IP packets over the MPVC to (and from) the ASE. The management path is described in the switch's arp cache and routing table.

Note – Lucent 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. See the *B-STDX, CBX, and GX Getting Started User's Guide* for information about downloading the initialization-script file.

Configuring a Management PVC

The following section describes how to define an MPVC connection and configure an NMS path using a standard or redirect management PVC. To define a standard MPVC connection, follow the instructions in the next section. To define a redirect MPVC connection, follow the instructions on page 9-6.

Before you configure an MPVC, do the following:

1. Select the switch for which you want to configure the ATM UNI or NNI logical port endpoint and define the physical port attributes. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.
2. Define an ATM UNI or NNI logical port. See page 3-7 for more information.

Defining a Standard MPVC Connection

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Point-to-Point. The Set All PVCs on Map dialog box appears (Figure 8-1 on page 8-10).
2. Choose Add. The Select End Logical Ports dialog box appears (Figure 8-3 on page 8-22).
3. Select the name of the switch where the management port (Endpoint 1) resides.
4. Select the logical port name "MgmtLPort.SW<*switchname*>" for Endpoint 1. The <*switchname*> should correspond to the name of the switch on which the management port endpoint resides. The LPort Type field should display Others:Multi Hop MPVC.
5. Select the name of the switch where Endpoint 2 resides.
6. Select the name of the logical port for Endpoint 2.
7. Choose OK. The Add PVC dialog box appears (Figure 8-4 on page 8-24).

8. Enter the VPI/VCI or DLCI values as follows:
   - For an ATM UNI endpoint, enter a VPI and VCI value. Use the instructions on page 8-25 for CBX/GX ATM endpoints; see page 8-50 for B-STDX endpoints.
   - For a Frame Relay UNI endpoint, use the instructions on page 8-50 to enter a DLCI value.
9. Enter a Circuit Name for the MPVC. You will select this name when you configure the NMS path.
10. Set the remaining PVC attributes as shown in Table 9-1.

Table 9-1. Configuring Standard MPVC Attributes

For ATM Service PVCs	For Interworking PVCs
Table 8-7 on page 8-27 to set the Administrative Attributes	Table 8-15 on page 8-50 to set the Administrative Attributes
Table 8-8 on page 8-30 to set the Traffic Type Attributes	Table 8-16 on page 8-53 to set the Traffic Type Attributes
Table 8-9 on page 8-33 to set the User Preference Attributes	Table 8-17 on page 8-58 to set the User Preference Attributes
Table 8-10 on page 8-37 to set the Frame Discard Attributes	

11. (*Optional*) To configure CBX 500 or GX 550 Network Data Collection parameters for this circuit, select Set [NDC] Attributes. For more information, see the *B-STDX, Cabstand GX Switch Diagnostics User's Guide*.
12. (*Optional*) To configure NavisXtend Accounting Server parameters for this circuit, choose the Accounting button. For more information, see the *NavisXtend Accounting Server Administrator's Guide*.
13. Choose OK to define the circuit parameters. The Set All PVCs on Map dialog box reappears.
14. Choose Close to return to the network map.
15. Continue with "Completing the Management Configuration" on page 9-15 to define the NMS path and static route.

Defining a Redirect MPVC Connection

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Redirect. The Set All Redirect PVCs on Map dialog box appears (Figure 8-5 on page 8-18).
2. Choose Add. The Select Redirect Circuit End Logical Ports dialog box appears (Figure 8-13 on page 8-62).
3. Select the name of the switch where the management port (Pivot Endpoint) resides.
4. Select the logical port name MgmtLPort.SW<*switchname*> for the Pivot Endpoint. The <*switchname*> should correspond to the name of the switch on which the management port Pivot Endpoint resides. The LPort Type field should display Others:Multi Hop MPVC.
5. Select the name of the switch where the Primary Endpoint resides.
6. Select the name of the logical port for the Primary Endpoint.
7. Select the name of the switch where the Secondary Endpoint resides.
8. Select the name of the logical port for the Secondary Endpoint.
9. Choose OK. The Add Redirect PVC dialog box appears (Figure 8-14 on page 8-64).
10. Enter the VPI/VCI or DLCI values as follows:
    - For an ATM UNI endpoint, enter a VPI and VCI value. Use the instructions on page 8-25 for CBX/GX ATM endpoints; see page 8-50 for B-STDX endpoints.
    - For a Frame Relay UNI endpoint, use the instructions on page 8-50 to enter a DLCI value.
11. Enter a Circuit Name for the redirect MPVC. You will select this name when you configure the NMS path.
12. Set the remaining PVC attributes as shown in Table 9-2.

Table 9-2. Configuring Redirect MPVC Attributes

For an ATM Service PVC see...	For an Interworking PVC see...
Table 8-7 on page 8-27 to set the Administrative Attributes	Table 8-15 on page 8-50 to set the Administrative Attributes
Table 8-8 on page 8-30 to set the Traffic Type Attributes	Table 8-16 on page 8-53 to set the Traffic Type Attributes
Table 8-9 on page 8-33 to set the User Preference Attributes	Table 8-17 on page 8-58 to set the User Preference Attributes
Table 8-10 on page 8-37 to set the Frame Discard Attributes	

13. (*Optional*) To configure CBX 500 or GX 550 Network Data Collection parameters for this circuit, select Set [NDC] Attributes. For more information, see the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
14. (*Optional*) To configure NavisXtend Accounting Server parameters for this circuit, choose the Accounting button. For more information, see the *NavisXtend Accounting Server Administrator's Guide*.
15. Choose OK to define the circuit parameters. The Set All Redirect PVCs on Map dialog box reappears (Figure 8-2 on page 8-16).
16. Choose Close to return to the network map.
17. Continue with "Completing the Management Configuration" on page 9-15 to define the NMS path and static route.

Using Management VPI/VCI

You use a management VPI/VCI when the NMS connects to the gateway switch via an ATM router or ATM network interface card (NIC). The NMS accesses the gateway switch through this connection. This method of access enables you to monitor the network without the use of an Ethernet module in the switch.

Before you configure a management PVC, do the following:

1. Select the switch for which you want to configure the ATM UNI or NNI logical port endpoint and define the physical port attributes. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.
2. Define an ATM UNI or NNI logical port. See page 3-7 for more information.

Defining the Management VPI/VCI Connection

1. From the Administer menu, select Lucent Parameters ⇒ Set All Management VPI/VCIs. The Set All Management VPI/VCIs dialog box appears.

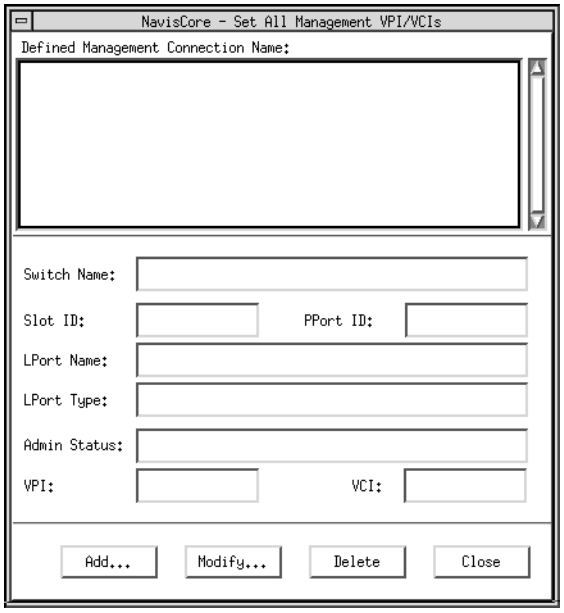


Figure 9-2. Set All Management VPI/VCIs Dialog Box

If you have already configured a management VPI/VCI, the Set All Management VPI/VCIs dialog box displays the defined management connection names and configured parameters. From the Set All Management VPI/VCIs dialog box, use the Modify or Delete buttons to modify or delete management VPI/VCI configurations.

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

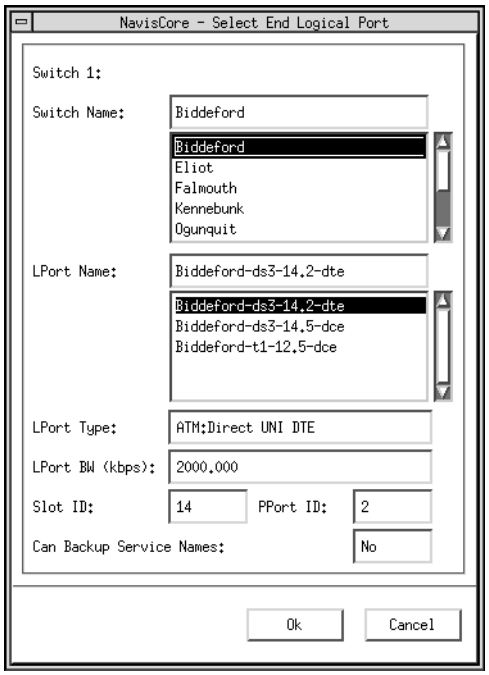


Figure 9-3. Select End Logical Port Dialog Box

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

Table 9-3. Select End Logical Port Dialog Box Fields

Field	Action/Description
Switch Name	Select the name of the switch that connects to the router or NIC that serves as the interface for the Network Management VPI/VCI.
LPort Name	Select the name of the logical port configured to access the router or NIC.
LPort Type	Displays the logical port type.
LPort BW (kbps)	Displays the logical port bandwidth.
Slot ID	Displays the I/O slot number in which the I/O card resides.
PPort ID	Displays the port number for the port you are configuring.

4. Choose OK. The Add Management VPI/VCI dialog box appears.

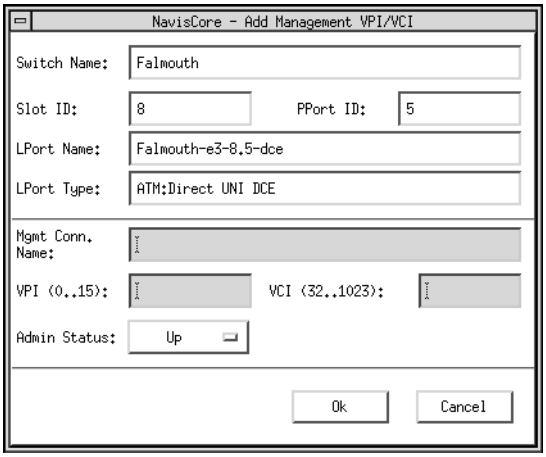


Figure 9-4. Add Management VPI/VCI Dialog Box

5. Complete the Add Management VPI/VCI dialog box fields (Table 9-4).

Table 9-4. Add Management VPI/VCI Dialog Box Fields

Field	Action/Description
Switch Name	Displays the name of the switch that connects to the router that serves as the interface for the Network Management VPI/VCI.
Slot ID	Displays the I/O slot (number) in which the I/O card resides.
PPort ID	Displays the port number for the physical port.
LPort Name	Displays the name of the logical port configured for the router.
LPort Type	Displays the logical port type.
Mgmt Conn. Name	Enter a unique, continuous, alphanumeric name to identify the connection. Do not use hyphens, parentheses, or asterisks.
VPI (0..15)	Enter the VPI that is used for the connection. ***Note**: On a B-STDX switch, the VPI value defaults to 0 (zero) and can not be modified.*
VCI (32..1023)	Enter the VCI that is used for the connection.
Admin Status	Select either Up or Down to define whether the management VPI/VCI connection is activated when the switch or port comes online.

6. Choose OK to return to the network map. Continue with "Completing the Management Configuration" on page 9-15 to define the NMS path and static route.

Using Management SPVCs

A management SPVC (MSPVC) connects the switch management port to an SVC terminating address located on an adjacent switch. This management connection is used as the NMS path which enables the NMS to manage the switch.

MSPVCs originate at an internal logical port located on the switch's processor module (either SP or NP, respectively). They terminate at the switch's I/O interface: IOM for a CBX, and BIO for the GX 550. MSPVCs are not supported on the B-STDX.

MSPVCs provide a data path that accesses internal network management functions. The MSPVC internal logical port is designated as MgmtLPort.SW<*switch name*>. It uses an interface number (ifnum) of 4093. To form the MSPVC, connect the MgmtLPort. SW<*switch name*> endpoint to any target AESA address configured on an ATM UNI logical port.

Using Management SPVCs in a PNNI Environment

When using a backbone of PNNI links, it is not possible to manage Lucent switches using the traditional methods of inband management over Lucent direct or OPTimum trunks. For this reason, you must use an alternate means of communicating between the Lucent switches and the NMS and other types of management stations. Due to the fact that MSPVCs are signaled connections that can be established over any PNNI link (including those PNNI links to other vendor equipment), MSPVCs are ideal for meeting the connectivity needs between the NMS and the Lucent switches.

When you use MSPVCs, the connection between the management logical port on the SP/NP and the UNI/NNI logical port where the management station is located is a standard SPVC. This means the VC can traverse any combination of Lucent CBX and GX switches and other vendor equipment that is capable of supporting PNNI SPVCs.

Configuring Management SPVCs

The following section describes how to define an SVC port address and configure the management SPVC connection.

Before you configure a management SPVC, do the following:

1. Select the switch for which you want to configure the ATM UNI or NNI logical port endpoint and define the physical port attributes. See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for more information.
2. Define an ATM UNI or NNI logical port. See page 3-7 for more information.

Defining SVC Port Addresses

If the device attached to a given physical port does not support ILMI address registration, or to fully specify an address:

1. Define SVC port addresses for all logical ports on a given physical port (see "Configuring SVC Port Addresses" on page 15-26).
2. Configure the PVP Termination, Connection ID, and VPI/VCI parameters (see "Configuring PVP Termination" on page 15-37).

Defining the Management SPVC Connection

To configure the MSPVC connection:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Soft PVC Parameters ⇒ Point-to-Point. The Set All Point-to-Point SPVCs dialog box appears. (See page 17-5 for a description of the fields.)
2. Choose Add. The Select SPVC Endpoints dialog box appears.

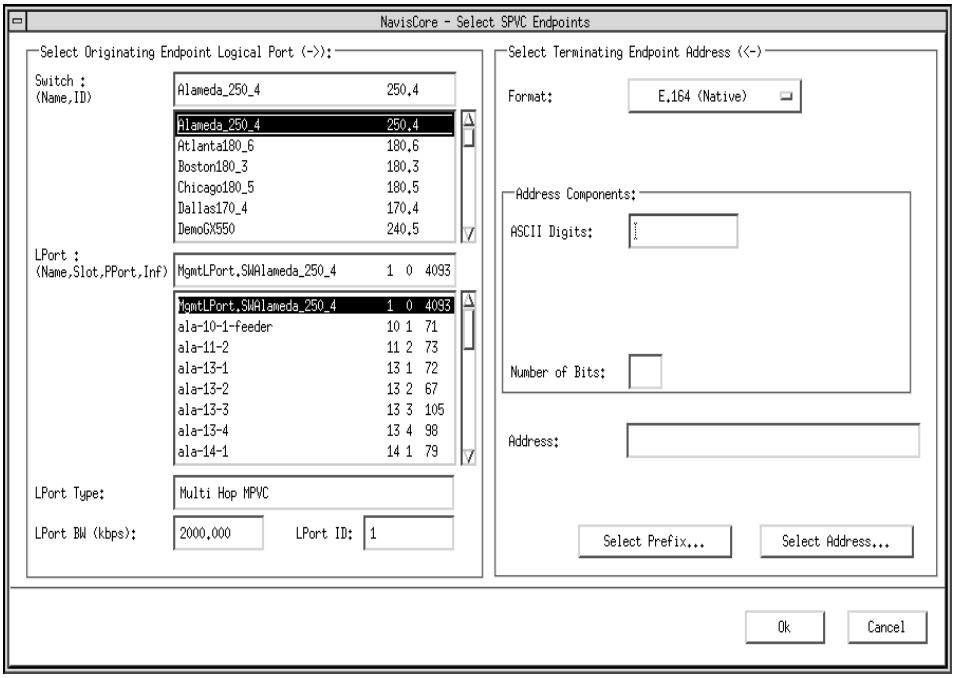


Figure 9-5. Select SPVC Endpoints Dialog Box

3. Perform the following steps to configure the originating endpoint logical port:
   a. Select the name of the switch on which the MSPVC endpoint will reside.
   b. Select the MgmtLPort.SW<*switch name*> endpoint.
4. To complete this configuration:
   - If you know the SVC terminating endpoint address, use Table 17-4 on page 17-9 to select the address format and configure the terminating endpoint address. For more information on AESA address formats, see page 14-2.
   - If you do not know this address, or if you need to configure the terminating endpoint address, see page 17-13 for instructions on using the Select Prefix and Select Address buttons to configure this address.
5. Choose OK. The Add Soft PVC dialog box appears.

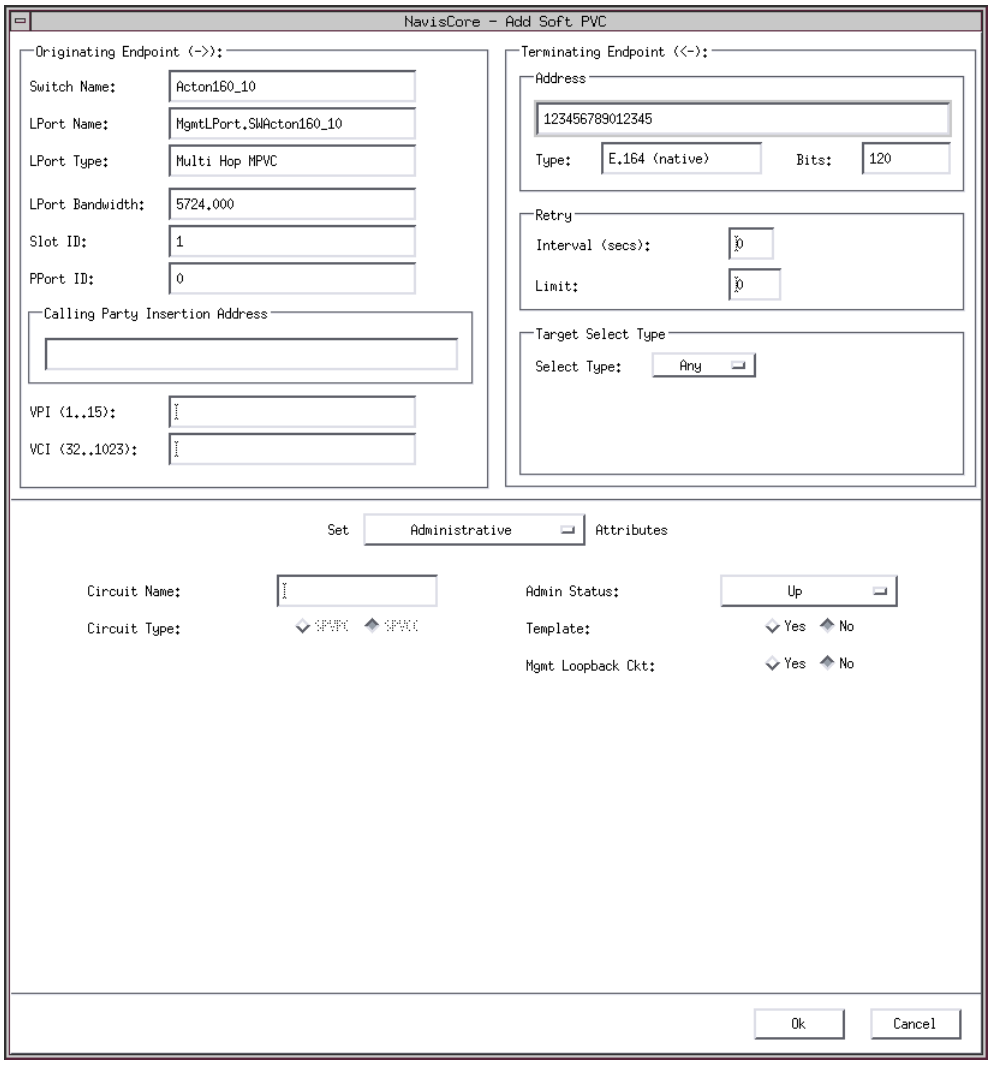


Figure 9-6. Add Soft PVC Dialog Box

6. Use the information in Table 17-5 on page 17-11 to configure these fields.

7. Choose Set [Traffic Type] Attributes to select the traffic descriptors for this SPVC. The Set Traffic Type Attributes fields appear (Figure 17-4 on page 17-12).
8. See "Defining Traffic Descriptor Attributes" on page 10-12 for instructions on configuring these attributes.
9. Choose OK to create the new SPVC and return to the Set All Point-to-Point SPVCs dialog box (Figure 17-1 on page 17-5).
10. Choose Close to return to the network map.
11. Continue with the next section, "Completing the Management Configuration" to define the NMS path and static route.

Completing the Management Configuration

To complete the management configuration, you must define the NMS path and configure the attached device.

Defining the NMS Path

To define an NMS path:

1. On the network map, select the switch to connect to the NMS.
2. From the Administer menu, select Lucent Parameters ⇒ Set All Management Paths. The Set All Management Paths dialog box appears.

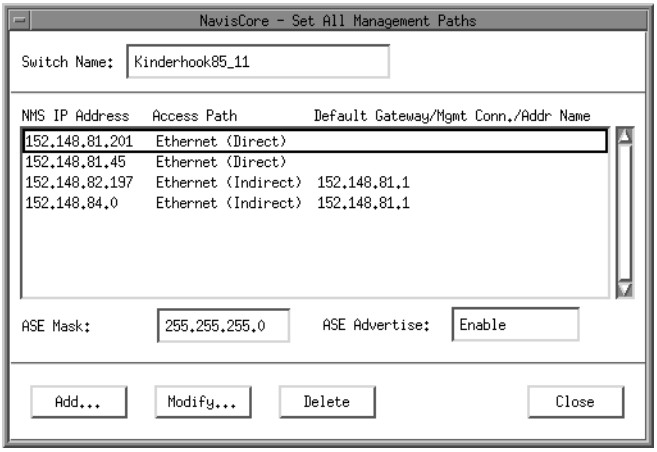


Figure 9-7. Set All Management Paths Dialog Box

3. Choose Add. The Add Management Path dialog box appears (see Figure 9-8). Figure 9-8 shows an example of a Management PVC connection.

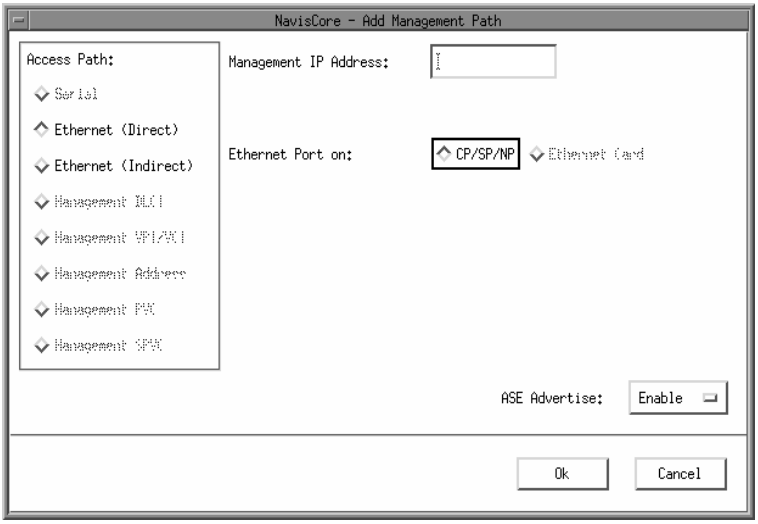


Figure 9-8. Add Management Path Dialog Box

4. Complete the steps in one of the following sections and continue with step 5 on page 9-17.

For Standard or Redirect MPVCs

a. Select Management PVC as the Access Path.

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

c. Select the Management PVC Name you entered in step 9 on page 9-5 (or in step 11 on page 9-6 for a redirect MPVC).

For Management VPI/VCIs

a. Select Management VPI/VCI as the Access Path.

b. In the Management IP Address field, enter the IP address of the external device to which this switch connects.

c. Select the Management VPI/VCI Name (Mgmt Conn. Name) you entered when completing the fields in Table 9-4 on page 9-10.

d. Enter the Autonomous System External (ASE) Mask of the device connected to this management VPI/VCI. The default is 255.255.255.255.

This mask should be the IP network mask for the network to which this switch connects. For example, if the devices to be managed are on IP network 10.1.2.3, you should enter 10.255.255.255 for the ASE Mask.

For Management SPVCs

a. Select Management SPVC as the Access Path.

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

c. Select the Management SPVC Name as entered in Table 17-5 on page 17-11.

5. Enable (default) or disable the ASE Advertise option to indicate whether or not to advertise the new NMS management path on the network.

Disable this option if you do not want to advertise the switch's management path as a gateway to the Network Management Station.

Using ASE Advertise to select switches that function as gateway switches to the NMS can provide greater control of OSPF database size, network control traffic, and CPU usage.

6. Choose OK.

7. Choose Close to return to the network map.

Configuring the Attached Device

To complete the management configuration and configure the attached device:

1. Enter a static route in the router or NMS workstation to access the internal IP network. (See the *Network Management Station Installation Guide* for more information.)

2. Configure a PVC at the ATM interface of the router using the VPI/VCI values used by the terminating PVC endpoint and the IP address of the switch.

10

Configuring ATM Traffic Descriptors

This chapter describes basic information you need for configuring traffic descriptors. Both the CBX 500 switch and the GX 550 Multiservice WAN switch can use traffic descriptors to define a service contract, which guarantees that a specified amount of data is delivered. While the network can still deliver data that exceeds the limits of this traffic contract, this data may be delayed or lost if network resources are unavailable.

Note – The B-STDX switch, CBX 500 Frame-based models, and 4-port Ethernet modules do not support ATM traffic descriptors.

When you configure a PVC, you select the desired ATM traffic descriptor and enter the appropriate parameter value based on those items provided in the menu selection list. When you configure an SPVC, you first configure the specific traffic descriptor and then assign this traffic descriptor to the SPVC. Alternatively, for SPVCs, you may also choose one of the preconfigured traffic descriptors.

Overview

Configuring a logical port associates ATM traffic descriptors with the logical port control channels. Depending on the type of logical port, these control channels include ILMI, UNI signaling, PNNI routing, trunk protocol, and management traffic control channels. To simplify the provisioning process, you do not have to explicitly select the ATM traffic descriptor needed for the applicable control channel. A default value is always provided. Table 10-5 (on page 10-14) through Table 10-7 (on page 10-16) describe these default values in more detail.

In most cases, you do not need to change the control channel default traffic descriptors. However, if you wish to have a particular control channel use a different QoS class or a different PCR/SCR/MBS, you have the ability to do so. For example, the default trunk signaling and management control channels that are used on trunks between Lucent switches are assigned to use the CBR QoS class and 5% of the configured logical port bandwidth (2.5% for each of the two channels). If necessary, you can change the QoS class of the trunk signaling channel; you can also change the amount of bandwidth associated with it.

If you plan to change the default values for logical port control channels, keep the following guidelines in mind:

- For control channels between two Lucent switches (which encompasses the trunk signaling control channel and the node-to-node management traffic control channel), the traffic descriptor (TD) values (PCR/SCR/MBS) are only used to calculate the amount of bandwidth reserved by the CAC for this type of traffic. The TD values do not affect traffic shaping on these channels nor do they affect the channel policing (these channels are never policed). You can change the default amount of bandwidth reserved for these control channels if you find the amount unacceptable.
- Starting with Release 03.00.00.00 of CBX 500 switch software, the default amount of control channel bandwidth reserved on OC-3c/STM1 and OC-12c/STM4 trunks has changed. Previously, trunk control channel traffic was reserved at 5% of the logical port bandwidth (regardless of the media type). In some network scenarios for OC-3c/STM1 and OC-12c/STM4 trunks, this value was excessive; see Table 10-7 on page 10-16 for new default reserved bandwidth values.
- For control channels between a Lucent switch and another vendor device (including the ILMI, UNI signaling, and PNNI routing control channels), the TD values calculate both the amount of bandwidth reserved by CAC and the rate at which the control channels are policed.

  Control channels are not policed by default. You enable the UPC/NPC for the particular logical port, and the control channel will be policed at the traffic descriptor rate. Similar to the trunk control channels, the TD values associated with the ILMI, UNI signaling, and PNNI routing control channels do not affect the traffic shaping rate.

About Traffic Descriptors

To define a traffic descriptor, you must select the Quality of Service Class (QoS Class) and traffic descriptor combination to meet your network needs. The following sections describe each of the QoS classes, as well as the various traffic descriptor parameters. For each QoS class, you can select combinations of traffic parameters, which together form a traffic descriptor.

About Quality of Service

ATM supports four service classes to handle the various data types in a network. By selecting the appropriate service class, you can ensure optimal network usage.

Table 10-1 describes each service type class. The numerical value for the QoS Class reflects the ATM Forum definitions.

Table 10-1. Quality of Service Classes

Type	Description	QoS Class
Constant Bit Rate (CBR)	Handles digital information, such as video and digitized voice that is represented by a continuous bit stream. CBR traffic requires guaranteed throughput rates and service levels. ***Note**: The CBR QoS class is not available on Management PVCs (MPVCs).*	1
Variable Bit Rate (VBR) Real Time	For packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.	2
Variable Bit Rate (VBR) Non-Real Time	Handles packaging for transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of a VBR non-real time service class.	3
Available Bit Rate/Unspecified Bit Rate (ABR/UBR)	Primarily used for LAN traffic. The CPE should compensate for any delay or lost cell traffic. This service class is intended for (but not restricted to) use with the ATM Flow Control Processor.	4

Note – If the network equipment connected to the logical port does not support QoS, select the corresponding Unspecified class of service type. This provides a QoS class of 0 (zero).

About Logical Port Quality of Service Parameters

When you configure a logical port, you specify QoS parameters for each class of service (CBR through ABR/UBR). For more information about configuring these parameters, see "Setting Quality of Service Parameters" on page 3-44. The following list summarizes each of these parameters:

Bandwidth Allocation — Configures the amount of bandwidth to allocate on a logical port. You can configure a fixed percentage of bandwidth, or enable the bandwidth to change dynamically according to bandwidth demands.

Routing Metric — Optimizes network resources by routing traffic over the path that best matches the QoS needs of the associated VC. By selecting one of these metrics, you can ensure that a PVC, SVC, or SPVC originating from this logical port follows an efficient routing path to its destination.

Oversubscription Factor — Enables you to provision more PVCs, SVCs, or SPVCs on a given logical port than the amount of supported physical bandwidth. This ability to "oversubscribe" a logical port's bandwidth assumes that not all network resources are in use at the same time. For more information about the oversubscription factor, see page 2-18.

About Traffic Parameters

This section describes network traffic parameters and their associated ATM traffic descriptor combinations. When you create a logical port, PVC, or an SPVC, you can select a traffic descriptor that specifies how the network controls traffic going in the forward and reverse direction on that entity. This traffic descriptor is made up of individual traffic parameters which work together to provide traffic shaping.

Table 10-2 describes the individual traffic parameters.

Table 10-2. Traffic Parameters

Traffic Parameter	Description
CLP=0	Specifies the high-priority cell stream (cells whose cell loss priority bit is set to 0).
CLP=1	Specifies the low-priority cell stream (cells whose cell loss priority bit is set to 1).
CLP=0+1	Specifies the aggregate cell stream (all cells in this circuit whose cell loss priority bit is either 0 or 1).
PCR (peak cell rate)	Peak cell rate is the maximum allowed cell transmission rate (expressed in cells per second). It defines the shortest time period between cells and provides the highest guarantee that network performance objectives (based on cell loss ratio) will be met.
SCR (sustainable cell rate)	Sustainable cell rate is the maximum average cell transmission rate that is allowed over a given period of time on a given circuit. It allows the network to allocate sufficient resources (but fewer resources than would be allocated based on PCR) for guaranteeing that network performance objectives are met. This parameter applies only to VBR traffic; it does not apply to CBR or UBR/ABR traffic.

Table 10-2. Traffic Parameters (Continued)

Traffic Parameter	Description
MBS (maximum burst size)	Maximum burst size is the maximum number of cells that can be received at the PCR. This allows a burst of cells to arrive at a rate higher than the SCR. If the burst is larger than anticipated, the additional cells are either tagged or dropped. This parameter applies only to VBR traffic; it does not apply to the CBR or UBR traffic.
MCR (minimum cell rate) (CBX 500 with FCP support only)	Minimum cell rate is the rate at which the source switch is always allowed to send data. This parameter only applies to ABR traffic. For more information about Flow Control Processor features, see Chapter 5, "About the ATM Flow Control Processor (FCP)."
Tagging	Tagging refers to the method of changing a high-priority cell (CLP=0) to a low-priority cell (CLP=1). This method provides an alternative to simply dropping the cells from the cell stream, when the CLP=0 cell stream is non-conforming.
Best Effort	This option means that the network attempts to deliver traffic that exceeds the limits of the traffic contract. However, there are no guarantees that traffic will be delivered.

The traffic descriptor combination you select determines the number and type of cells that are admitted into a congested queue, and whether or not high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds.

You can configure up to 512 traffic descriptors per switch. Table 10-3 lists the traffic descriptors that are available for each QoS class.

Table 10-3. QoS Class Traffic Descriptors

QoS Class	Traffic Descriptor	Description
Constant bit rate (CBR) (specified/ unspecified)	PCR CLP=0, PCR CLP=0+1, tagging	Traffic conformance is based on the PCR of both the CLP=0 and CLP=0+1 cell streams with Tagging enabled.
	PCR CLP=0, PCR CLP=0+1, no tagging	Traffic conformance is based on the PCR of both the CLP=0 and CLP=0+1 cell streams with no Tagging.
	PCR CLP=0+1	Traffic conformance is based only on the PCR of the CLP=0+1 aggregate cell stream with no Best Effort.
VBR-RT/ VBR-NRT (specified/ unspecified)	PCR CLP=0+1, SCR CLP=0, MBS CLP=0, tagging	Traffic conformance is based on the PCR of the CLP=0+1 aggregate cell stream, as well as the SCR and MBS of the CLP=0 cell stream with Tagging enabled.
	PCR CLP=0+1, SCR CLP=0, MBS CLP=0, no tagging	Traffic conformance is based on the PCR of the CLP=0+1 aggregate cell stream, as well as the SCR and MBS of the CLP=0 cell stream with no Tagging.
	PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1	Traffic conformance is based on the PCR, SCR, and MBS of the CLP=0+1 cell stream with no Tagging.
UBR	PCR CLP=0+1	Traffic conformance is based only on the PCR of the CLP=0+1 aggregate cell stream with no Best Effort.
	Best Effort	No traffic conformance is applied to this cell steam. A Best Effort attempt is made to deliver all traffic, but there is no guarantee the switch will not drop cells due to congestion.
	Best Effort, Tagging	Traffic conformance is only applied to tag all cells as CLP1. A Best Effort attempt is made to deliver all traffic, but there is no guarantee the switch will not drop cells due to congestion.
ABR	PCR CLP=0, MCR CLP=0	No traffic conformance is applied to this cell stream unless the logical port User UPC Function or User NPC Function is set to Enabled with ABR. Traffic conformance is based on PCR of the CLP=0 cell stream. For information about the User UPC Function, see page 3-24. For information about the User NPC Function, see page 3-25.

When you choose the Forward (or Reverse) Traffic Descriptor combination, select the combination that best describes the traffic characteristics. The usage parameter control (UPC) and network parameter control (NPC) functions use the traffic parameters to determine the conforming cells of an ATM connection, based on the threshold values for PCR, SCR, and MBS as specified in the service contract. If a traffic descriptor combination is not valid for the service class specified in the Forward (or Reverse) QoS class field, you cannot select it.

For more information on how each traffic descriptor combination affects the cell streams under different traffic conditions, see Appendix B, “ATM Traffic Descriptors.”

Configuring ATM Traffic Descriptors

NavisCore provides the ability to preconfigure a set of network-wide traffic descriptors. When you need to specify traffic information for a logical port or SPVC, you can select a predefined traffic descriptor definition.

The Configurable Control Channel feature enables you to define traffic descriptors for control circuits. To do this, you configure traffic descriptor information for the logical port's ILMI, UNI, and PNNI signaling or trunk control channels.

To configure ATM traffic descriptors, do the following:

- To define network-wide traffic descriptors, continue with the following section.
- To specify traffic descriptors for an existing logical port or SPVC, see "Defining Traffic Descriptor Attributes" on page 10-12.

Defining Network-wide Traffic Descriptors

To configure a set of traffic descriptors for use in your network:

1. From the Administer menu, choose Lucent Parameters ⇒ Set All ATM Traffic Descriptors. The Set All ATM Traffic Descriptors dialog box appears.

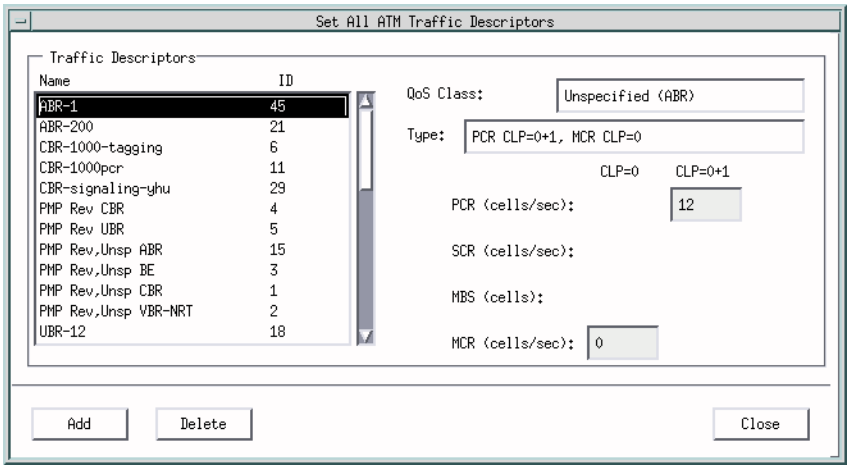


Figure 10-1. Set All ATM Traffic Descriptors Dialog Box

This dialog box displays information about previously configured traffic descriptors. If you need to delete a traffic descriptor, select the name from the list and choose Delete.

2. Choose Add to add a traffic descriptor. The Add Traffic Descriptor dialog box appears.

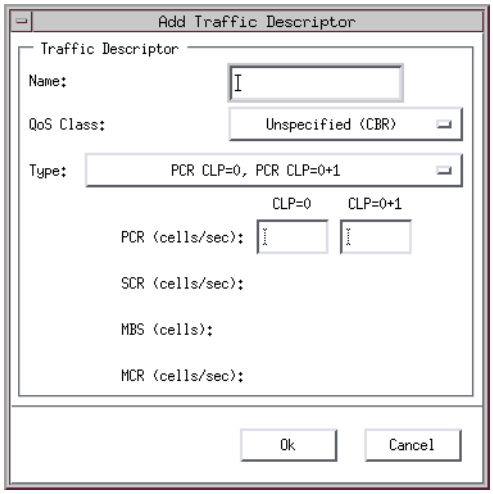


Figure 10-2. Add Traffic Descriptor Dialog Box

3. Enter a name (up to 20 characters) for this character descriptor type.
4. See Table 10-1 on page 10-4 to select the QoS class. Note that your choice of QoS class affects which traffic descriptors are available. If the attached equipment does not support QoS classes other than 0 (zero), select only the unspecified service classes.
5. See Table 10-3 on page 10-7 to select the traffic descriptor type.
6. Use the information in Table 10-4 to specify the required values in cells per second.

Table 10-4. Traffic Descriptor Types

Traffic Descriptor Type	Description
PCR CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes PCR CLP=0. If so, specify the PCR in cells per second for high-priority traffic (that is, the CLP=0 cell stream).
PCR CLP=0+1 (cells/sec)	Specify the PCR in cells per second for combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream).
SCR CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes SCR CLP=0. If so, specify the SCR in cells per second for combined high-priority traffic (that is, the CLP=0 cell stream).
SCR CLP=0+1 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes SCR CLP=0+1. If so, specify the SCR in cells per second for combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream).

Table 10-4. Traffic Descriptor Types (Continued)

Traffic Descriptor Type	Description
MBS CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes MBS CLP=0. If so, specify the MBS (in cells per second) for combined high-priority traffic (that is, the CLP=0 cell stream).
MBS CLP=0+1 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes MBS CLP=0+1. If so, specify the MBS (in cells per second) for combined high- and low-priority traffic (that is, the CLP=0+1 cell stream).
MCR CLP=0 (cells/sec)	Displays only if you selected a traffic descriptor combination that includes MCR CLP=0. If so, specify the MCR (in cells per second) for combined high-priority traffic (that is, the CLP=0 cell stream).

7. Choose OK to set the ATM traffic descriptor. The Set All ATM Traffic Descriptors dialog box appears (Figure 10-1 on page 10-9).
8. Choose Add to repeat these steps to create additional ATM traffic descriptors, or choose Close to return to the network map.

Defining Traffic Descriptor Attributes

To assign a traffic descriptor to a logical port or SPVC:

1. See one of the following sections to access the traffic descriptor attributes:
   - For UNI logical ports, see "ILMI/Signaling/OAM Attributes" on page 3-28.
   - For Direct/OPTimum trunk logical ports, see "Traffic Descriptors Attributes" on page 3-37.
   - For SPVCs, see "Adding a Point-to-Point SPVC" on page 17-8.
   - For PNNI RCC, see "Configuring an ATM NNI Logical Port" on page 20-44.

   Figure 10-3 shows an example of defined traffic descriptors and fields.

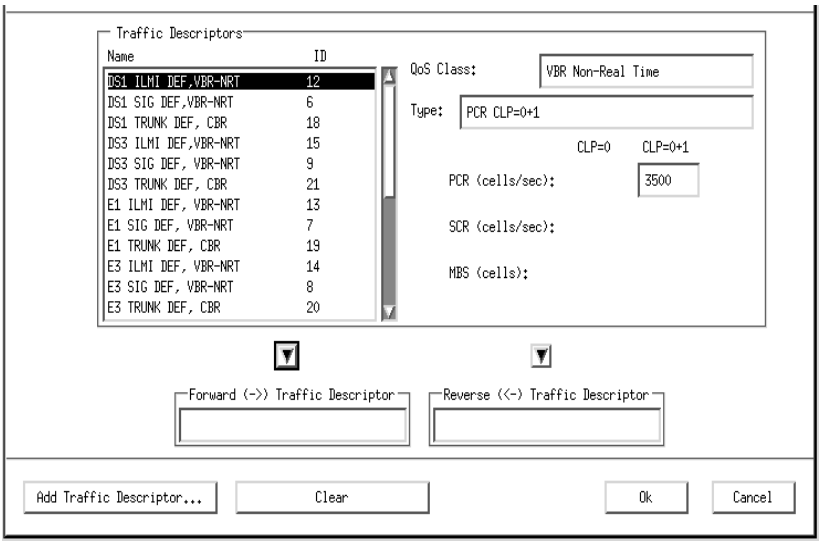


Figure 10-3. Traffic Descriptors Fields

2. Select a traffic descriptor name from the list box and click on the Forward (->)Traffic Descriptor button to assign this as the forward traffic descriptor.
3. Select a traffic descriptor name from the list box and click on the Reverse (<-) Traffic Descriptor button to assign this as the reverse traffic descriptor.

Note – The display-only fields to the right of the traffic descriptor list in Figure 10-3 are configured from the Add Traffic Descriptor dialog box (Figure 10-2 on page 10-10). To create a new traffic descriptor definition, choose the Add Traffic Descriptor button and perform the steps beginning with step 3 on page 10-10.

4. Choose OK to complete this configuration.

Deleting Traffic Descriptor Definitions

To delete a traffic descriptor definition for either a logical port or SPVC:

1. Access the traffic descriptor attributes. A dialog box similar to Figure 10-3 appears.
2. For each direction, select the traffic descriptor you want to remove.
3. Choose Clear.
4. Choose OK.

Control Channel Default Traffic Descriptors

Each type of control channel is initially configured with a set of default traffic descriptors. These defaults specify the QoS class information and cell rate values for each traffic descriptor type. See the following tables to review these defaults:

- Table 10-5, "UNI Signaling Control Channel Traffic Descriptor Defaults," on page 10-14
- Table 10-6, "ILMI Control Channel Traffic Descriptor Defaults," on page 10-15
- Table 10-7, "Trunk Control Channel Traffic Descriptor Defaults," on page 10-16
- Table 10-8, "PNNI Routing Control Channel Traffic Descriptors," on page 10-17

Table 10-5. UNI Signaling Control Channel Traffic Descriptor Defaults

	DS1	E1	E3	DS3	OC-3c/ STM1	OC-12c/ STM4
Type	NoClpScr[a]	NoClpScr	NoClpScr	NoClpScr	NoClpScr	NoClpScr
Class	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT
PCR[b] (cells/sec)	3500	4700	13500	13500	13500 (CBX) 56000 (GX)	13500 (CBX) 56000 (GX)
SCR (cell/sec)	42	42	500	500	2000	8000
MBS (cells)	16	16	16	16	16	16
Approximate EBW[c] (cell/sec)	52	52	617	617	2468	9873

[a] The default Type, NoClpScr, represents the following: PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1.

[b] If the configured logical port bandwidth is less than the physical port bandwidth, then PCR is 100% of logical port bandwidth.

[c] The approximate equivalent bandwidth (EBW) values are based on the use of the default values with the Lucent CAC in absence of user circuits on the logical port. It is provided here only as an aid to determine how much total bandwidth is reserved for the control channel.The amount reserved changes if you modify the traffic descriptor class or value.

Table 10-6. ILMI Control Channel Traffic Descriptor Defaults

	DS1	E1	E3	DS3	OC-3c/ STM1	OC-12c/ STM4
Type	NoClpScr[a]	NoClpScr	NoClpScr	NoClpScr	NoClpScr	NoClpScr
Class	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT	VBR-NRT
PCR[b] (cells/sec)	3500	4700	13500	13500	13500 (CBX) 56000 (GX)	13500 (CBX) 56000 (GX)
SCR (cell/sec)	21	21	250	250	1000	4000
MBS (cells)	16	16	16	16	16	16
Approximate EBW[c] (cell/sec)	26	26	309	309	1236	4944

[a] The default Type, NoClpScr, represents the following: PCR CLP-0+1, SCR CLP=0+1, MBS CLP=0+1.

[b] If the configured logical port bandwidth is less than the physical port bandwidth, then PCR is 100% of logical port bandwidth.

[c] The approximate equivalent bandwidth (EBW) values are based on the use of the default values with the Lucent CAC in absence of user circuits on the logical port. It is provided here only as an aid to determine how much total bandwidth is reserved for the control channel. The amount reserved changes if you modify the traffic descriptor class or value.

Table 10-7. Trunk Control Channel Traffic Descriptor Defaults

	DS1	E1	E3 (with PLCP)	DS3 (with PLCP)	DS3 (with HEC)	OC-3c/ STM1 [a]	OC-12c/ STM4 [b]
Type	NoClpNoScr [c]	NoClpNoScr	NoClpNoScr	NoClpNoScr	NoClpNoScr	NoClpNoScr	NoClpNoScr
Class	CBR	CBR	CBR	CBR	CBR	CBR	CBR
PCR [d, e] (cells/sec)	90	115	2000	2400	2600	CBX 6750 GX 9100	CBX 6750 GX 28000

[a] For OC3/STM1 and OC12/STM4, the default values are associated with the maximum control channel transmission rate the card type supports. For CBX IOMs, this is 13500cps; for GX BIOs this is 56000.

[b] For OC-3c/STM1 and OC-12c/STM4, the default values are associated with the maximum control channel transmission rate the card type supports. For CBX IOMs, this is 13500cps; for GX BIOs this is 56000.

[c] The default Type, NoClpNoScr, represents the following: PCR CLP=0+1.

[d] If the configured logical port bandwidth is less than the physical port bandwidth, then PCR is 2.5% of logical port bandwidth.

[e] Approximate equivalent bandwidth (EBW) values are not provided in this case for CBR circuits, EBW=PCR.

Note – Both a trunk signaling and a node-to-node management control channel are used on a trunk. This means that when you examine the bandwidth reserved on a trunk that uses these default values, the values that are reserved are equal to the values in this table times two.

Table 10-8. PNNI Routing Control Channel Traffic Descriptors

Value	Description
Type	NoClpScr
Class	VBR-NRT
PCR	906 cps
SCR	453 cps
MBS	171 cells
EBW [a]	645

[a] The approximate equivalent bandwidth (EBW) values are based on the use of the default values with the Lucent CAC in absence of user circuits on the logical port. It is provided here only as an aid to determine how much total bandwidth is reserved for the control channel. The amount reserved changes if you modify the traffic descriptor class or value.

Note – PNNI routing control traffic descriptors are the same across all port types.

11

Configuring Layer2 VPNs

Layer2 Virtual Private Network (VPN) is an *optional* software feature that enables network providers to dedicate resources for those customers who require guaranteed performance, reliability, and privacy. This feature is sometimes called Application Specific Routes (ASRs) or Customer Specific Routes (CSRs).

A Layer2 VPN enables you to provide dedicated bandwidth to the customer. When you configure a trunk, you can dedicate it to a specific VPN and, if desired, allow customers to monitor their own networks. However, switch control and configuration stays with you as the network provider.

Layer2 VPNs support PNNI links. See "Layer2 VPNs over PNNI" on page 11-11 for more information.

About Layer2 VPN

The Layer2 VPN feature allows you to create multiple private networks from a single public network. After you create a Layer2 VPN name and ID, you associate one or more customer names and IDs with the VPN. When all VPNs and customers are created in the database, you assign UNI/NNI logical ports to the specific VPN/customer association. In addition, you need to dedicate selected public network trunks to specific VPNs.

You must configure all PVCs that you create on the UNI/NNI logical ports for selected Layer2 VPN/customer associations. SVCs, however, inherit the VPN/customer associations of the host logical port.

When you configure the logical port or PVC, you also set the Net Overflow attribute. This attribute specifies whether PVCs or SVCs are restricted to trunks of their own Layer2 VPN or can use public (shared) trunks during outages. Customers that operate in restrictive mode need to purchase redundant trunks. Figure 11-1 provides a restrictive mode example.

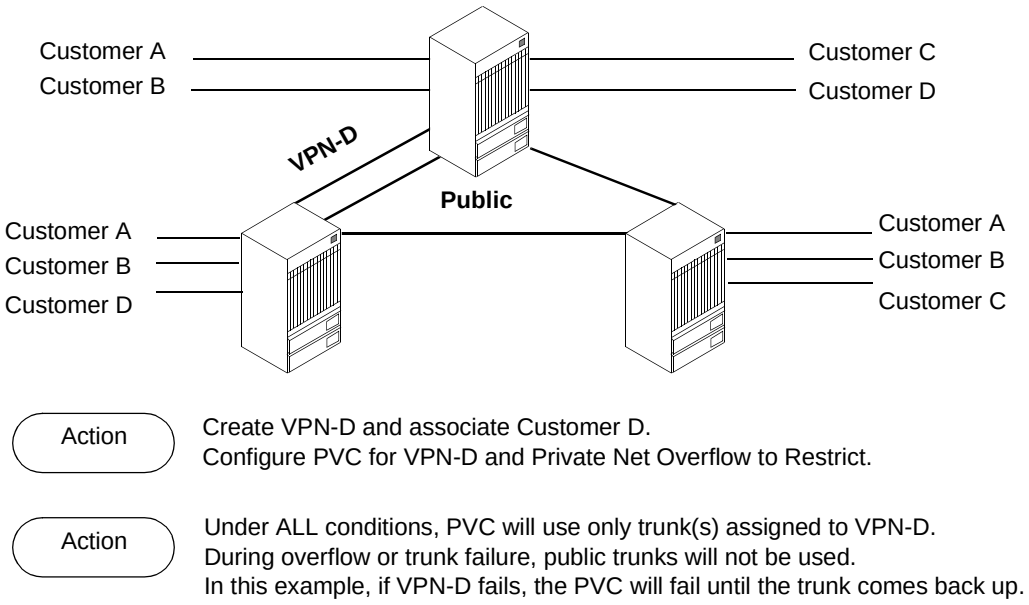


Figure 11-1. Layer2 VPN Restrictive Mode Example

If you set the Net Overflow parameter to shared, a private network can also use public trunks as a backup. This is called inclusive mode (shown in Figure 11-2). The identifier, VPN 0, is reserved to indicate the public part of the network. Trunks that have non-zero VPNs are reserved for data traffic matching that VPN, although they can also carry management traffic for the entire network.

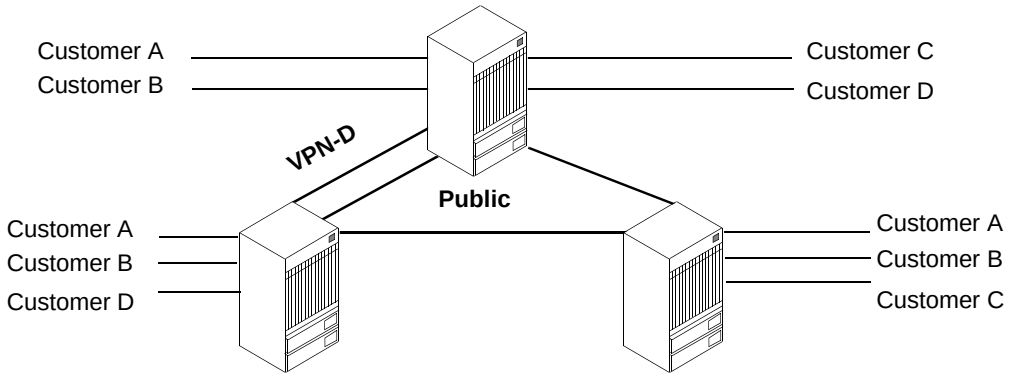


Figure 11-2. Layer2 VPN Inclusive Mode Example

Configuring a Layer2 Virtual Private Network

Use the following sequence to set up a Layer2 VPN:

Step 1. Create the Layer2 VPN (see page 11-4).

Step 2. Add customers to a specific Layer2 VPN (see page 11-5).

Step 3. Dedicate a trunk to a specific Layer2 VPN (see page 7-24).

Step 4. *For SVC traffic*, when you configure the UNI or NNI logical port, specify the Net Overflow field (see page 3-14). Then, dedicate this logical port to a specific VPN and customer (page 11-10).

Step 5. *For PVC traffic*, specify the Private Net Overflow attribute for the circuit (page 8-27). Then, dedicate the circuit to a specific VPN and customer (page 11-10).

Creating a Layer2 VPN

To create a Layer2 VPN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Layer2 Private Networks. The Set All Layer2 VPNs dialog box (Figure 11-3) appears.

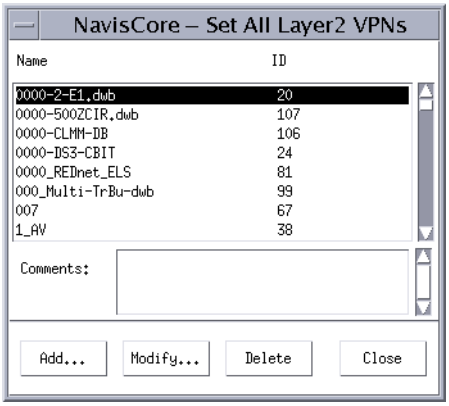


Figure 11-3. Set All Layer2 VPNs Dialog Box

2. Choose Add. The Add Layer2 Virtual Private Network dialog box (Figure 11-4) appears.

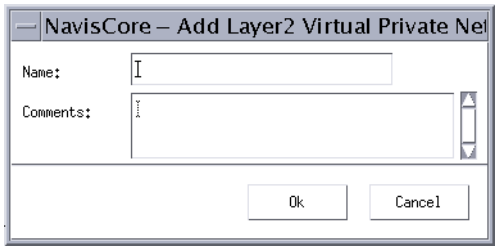


Figure 11-4. Add Layer2 Virtual Private Network Dialog Box

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

Adding Customers to the Layer2 VPN

To add customers to the Layer2 VPN:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN Customers. The Set All Customers dialog box (Figure 11-5) appears.

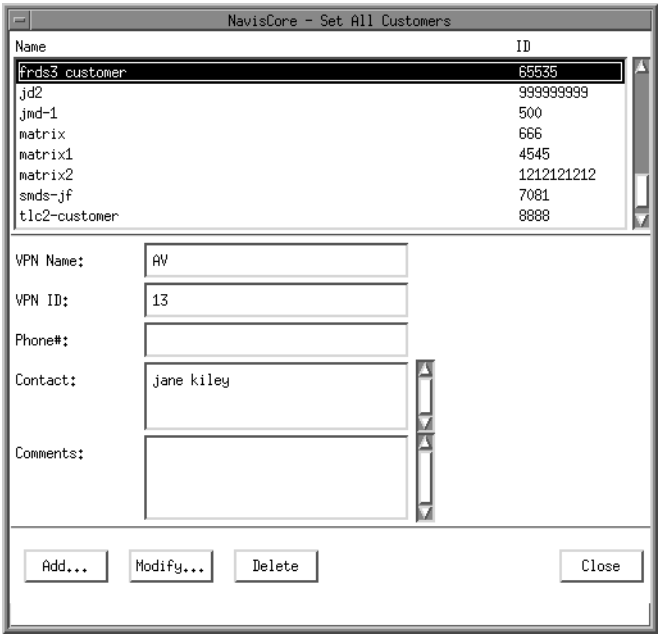


Figure 11-5. Set All Customers Dialog Box

2. Choose Add. The Add Customer dialog box (Figure 11-6) appears.

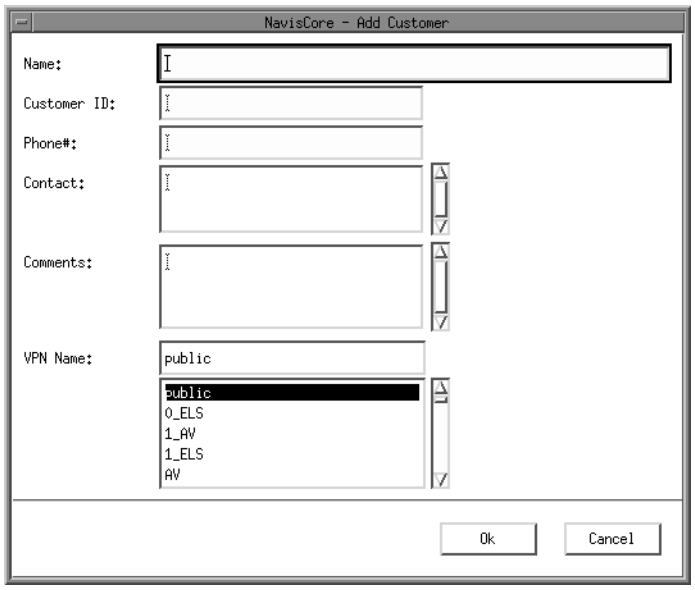


Figure 11-6. Add Customer Dialog Box

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

Configuring a Logical Port for Layer2 VPN

To implement VPN for a network that contains SVCs, specify the net overflow attribute when you configure a UNI logical port (see Table 3-4 on page 3-14). This parameter determines whether SVCs originating from this port are restricted to trunks of their own VPN, or whether SVCs can use public (shared) trunks during overflow conditions.

Once you configure a logical port, use the following steps to dedicate it to a VPN:

1. See page 3-2 to access the Set All Logical Ports in PPort dialog box.
2. From the list of logical port names, select the one you need to dedicate to a VPN.
3. Using the Select:Options button, select Layer2 VPN/Customer Info and choose Set. The Select Customer and Layer2 VPN dialog box (Figure 11-7) appears.

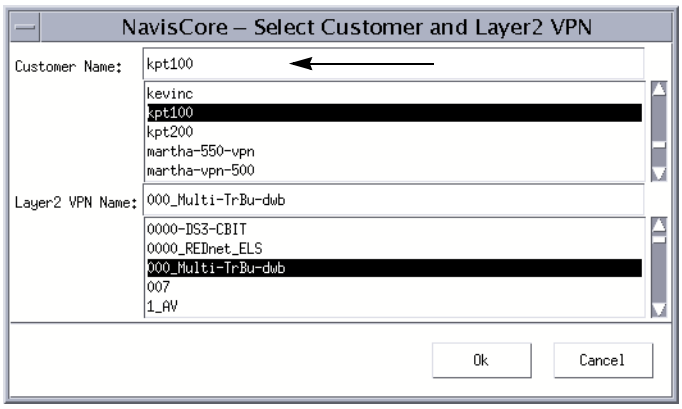


Figure 11-7. Select Customer and Layer2 VPN Dialog Box

4. Select the customer and Layer2 VPN name.
5. Choose Ok.
6. Choose Close to exit.

Using the Layer2 VPN/Customer View Feature

When you need to create PVCs for a specific VPN or customer, use the Select Layer2 VPN/Customer View feature. This feature allows you to enable a network map view for a specific VPN or customer. Layer2 VPN/Customer View makes it easy to identify those logical ports that belong to the VPN for which you need to configure PVCs; with this feature enabled, the Select End Logical Ports dialog box (page 8-22) only displays the logical ports that belong to the VPN or customer you select.

As you configure logical ports, use the instructions in "Configuring a Logical Port for Layer2 VPN" on page 11-7 to assign the port to a VPN or customer.

Note – To give a customer the ability to monitor network resources without the ability to provision, edit either the `.cshrc` or the `.profile` file for an NMS user and add the following lines:

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

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

To use Layer2 VPN/Customer View:

1. From the Administer menu, select Lucent Layer2/IP VPN ⇒ Select Layer2 VPN/VNN Customer. The Select Layer2 Customer/Layer2 VPN View dialog box (Figure 11-8) appears.

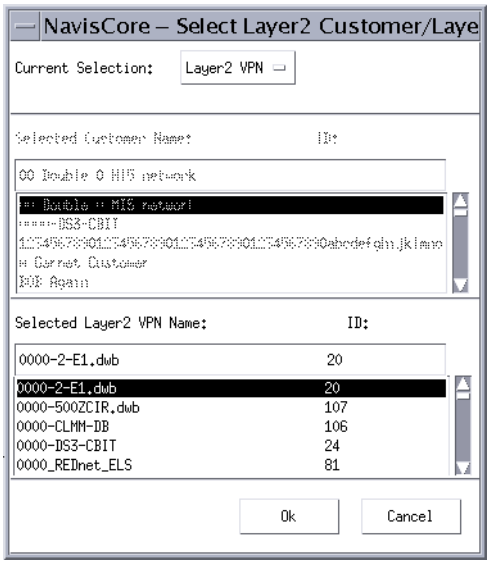


Figure 11-8. Select Layer2 Customer/Layer2 VPN View Dialog Box

2. Complete the Current Selection field to select either VNN Customer or Layer2 VPN.

   Choose None (default) to disable VNN Customer/Layer2 VPN View. (With the VNN Customer/Layer2 VPN view disabled, you can configure PVCs using logical port endpoints that belong to any customer or VPN.)

3. Depending on the option you select, review either the Selected Customer Name or Selected Layer2 VPN Name list.
4. Select the VNN Customer or Layer2 VPN name.
5. Choose Ok.

Configuring a PVC for Layer2 VPN

When you configure a PVC for Layer2 VPN, first specify the private net overflow attribute (see Table 8-7 on page 8-27). This parameter determines whether the PVC is restricted to trunks of its own Layer2 VPN, or can use public (shared) trunks during overflow conditions.

After you configure a PVC, use the following steps to dedicate it to a VPN:

1. See page 8-10 to access the Set All PVCs on Map dialog box.
2. From Defined Circuit Names list box, select the one you need to dedicate to this VPN.
3. Choose Layer2 VPN/Customer. The Select Customer and Layer2 VPN dialog box appears (see Figure 11-7 on page 11-7).
4. Select the Customer Name and the Layer2 VPN Name.
5. Choose Ok.
6. Choose Close to exit.

Layer2 VPNs over PNNI

Layer2 VPNs over PNNI are supported on CBX 500 and GX 550 switches. Supported circuits include PVCs, SVCs, and SPVCs.

The entire PNNI configuration needs to be done on the switches that form part of the PNNI domain. The NNI ports can be configured at egress and ingress cards of the connecting switches by selecting PNNI as the protocol.

By default all PNNI links are part of the public VPN. When a PNNI link is assigned to a VPN other than public, it is no longer available to any other VPN. The endpoints of a PNNI link must be configured to the same VPN.

After VPN IDs have been created, PNNI interfaces and circuits can be assigned to the VPN. Both VNN and PNNI links can be assigned to a particular VPN. Layer2 VPNs over PNNI are supported within peer groups and on border trunks and will function in a multi-level PNNI domain.

If there are multiple border nodes, PNNI routing will give preference to the border node that belongs to a particular VPN, unless no other VPNs exist. In that case, the border nodes in the public VPN will be selected. Similarly, if there are multiple paths that can be used within a peer group, preference will be given to the links that belong to a particular VPN.

To configure a Layer2 VPN over PNNI:

1. Create a Layer2 VPN (see “Configuring a Layer2 Virtual Private Network” on page 11-4).
2. Add customers to the Layer2 VPN (see “Adding Customers to the Layer2 VPN” on page 11-5).
3. Assign the PNNI Lports to the VPN (see “Configuring a Logical Port for Layer2 VPN” on page 11-7).

Layer2 Limitations on PNNI Links

In a network consisting of multiple domains such as PNNI-VNN-PNNI or VNN-PNNI-VNN, a VPN path to a destination beyond a particular gateway can not be defined. Also, usage of VPN trunks beyond the first domain is not ensured.

12

Configuring Fault-Tolerant PVCs

A fault-tolerant PVC configuration enables ATM UNI DCE and DTE logical ports to serve as a backup for any number of active UNI ports. The backup port can be manually activated if a primary port fails or if you need to take a primary port offline. This function is sometimes referred to as *resilient UNI/NNI*.

To automate PVC redundancy functions, you can also configure the CBX 500 switch or GX 550 Multiservice WAN switch physical port on which a UNI logical port resides for automatic protection switching (APS). The APS with resilient UNI configuration protects against facility defects and equipment failure as well as I/O module failure. Keep in mind that this feature requires a circuit reroute. Although you can configure manually activated fault-tolerant PVCs for the B-STDX, the B-STDX switch platform does not support the APS with resilient UNI feature. See "Using APS with Resilient UNI" on page 12-8 for more information.

Note – Resilient NNI is not currently supported on ATM modules, though it is supported on Frame Relay modules.

Configuring Fault-Tolerant PVCs

Use the following sequence to configure fault-tolerant PVCs:

Step 1. Follow the sequence on page 3-9 to define a UNI DCE or UNI DTE logical port as a backup port. Choose Yes for the option "Can Backup Service Names" (see Table 3-4 on page 3-14).

Step 2. Define and specify a Service Name that will be bound to the primary port (see page 12-4).

Step 3. Configure circuits to use the Service Name as an endpoint (see page 8-23). Note that both endpoints can be different Service Names.

Step 4. Define one or more backup logical ports (of the same type as the primary logical port). When defining Administrative Attributes for the backup logical port, make sure to enable the "Can Backup Service Names" option (see Table 3-4 on page 3-14 for more information).

Step 5. (*Optional*) Activate one of the backup logical ports, as needed (see "Activating a Backup Binding Port" on page 12-6).

Note – Lucent recommends that you avoid configuring SVCs on a logical port that is also designated as a backup port in a fault-tolerant PVC configuration.

Note – You cannot use redirect PVCs with Resilient UNI/NNI.

Creating a Primary Port

To create a primary logical port, you assign a Service Name to a UNI logical port. (Do not choose a port that will be used for backup.) When you configure the circuit, choose this assigned Service Name as an endpoint instead of selecting a switch and logical port combination. You can define Service Names for both PVC endpoints, if needed. When you activate the backup port, the fault-tolerant PVC on the primary port is rerouted, preserving VPI/VCIs in the process.

Lucent's fault-tolerant PVC feature is transparent to the end user, meaning that you do not have to configure the CPE to accommodate the new functionality. Therefore, end users can benefit from this feature through the public Lucent-based ATM network, or by combining their private Lucent switches with services provided by their public carrier.

Creating a Backup Port

To create a backup port, first define a UNI DCE or DTE logical port and select Yes for the Can Backup Service Names field (see Table 3-4 on page 3-14). When a backup port is not in use, the port is idle and does not use network resources.

You can create a number of backup ports for later use with the same Service Name. You then select a particular backup port during the backup binding procedure (see "Activating a Backup Binding Port" on page 12-6 for more information).

Caution – When you define the UNI DCE or UNI DTE logical port for use as the backup port, ensure that the virtual path identifier/virtual channel identifier (VPI/VCI) range of the logical port you select is *equal to or greater than* the VPI/VCI range of the logical port you have selected for the primary port. If the VPI/VCI range of the backup port is lower than that of the primary port, the module may crash when service is switched to the backup port.

Creating Service Names

You define the *Service Name* to identify (bind to) the primary port. A circuit recognizes its service endpoint by this name, instead of the logical port name.

To create the Service Name bindings:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Service Name Bindings ⇒ Set All Resilient UNI/NNI. The Set All Service Name Bindings dialog box appears (Figure 12-1), displaying any defined Service Names that have already been configured.

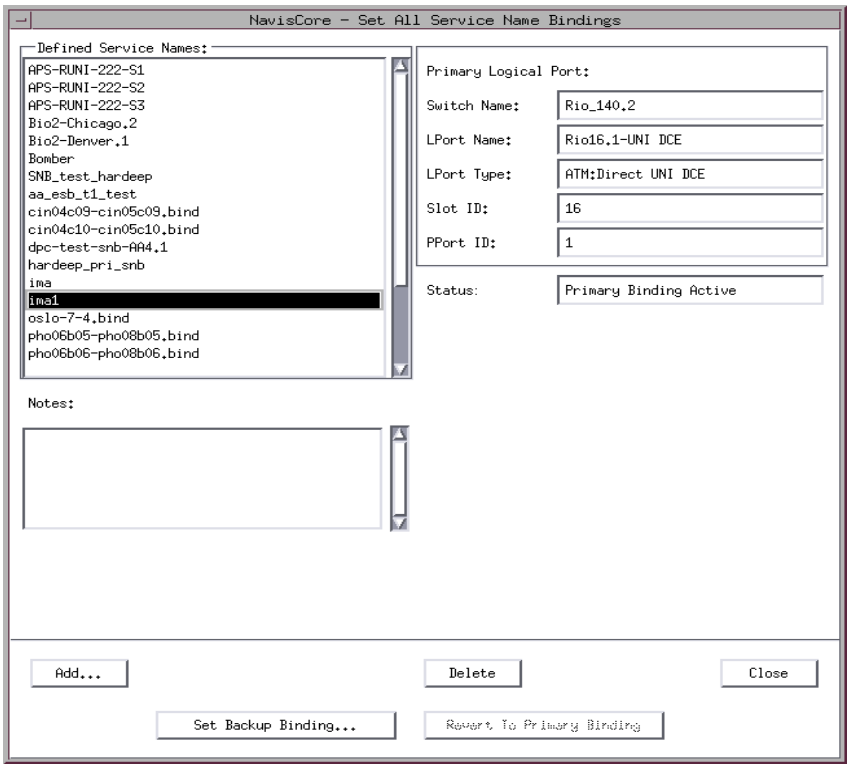


Figure 12-1. Set All Service Name Bindings Dialog Box

You can access the following functions from the Set All Service Name Bindings dialog box:

- To return the primary logical port to service (after the Backup Binding has been set), select the Defined Service Name and choose *Revert to Primary Binding*.
- To delete a Service Name, select the Defined Service Name and choose *Delete*.
- To create or modify a backup binding, choose *Set Backup Binding*.

2. Choose Add. The Select End Logical Port dialog box appears (Figure 12-2).

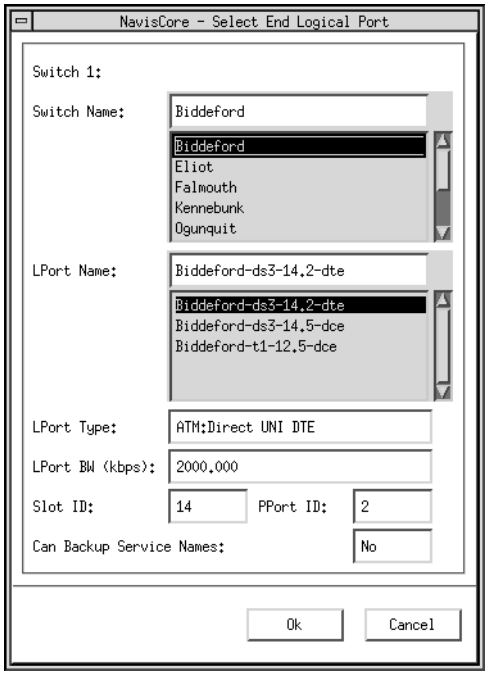


Figure 12-2. Select End Logical Port Dialog Box

3. Select the Switch Name and the primary LPort Name.

Note – Make sure that the Can Backup Service Names field displays No. You cannot configure a Service Name for a logical port designated as a backup.

4. Choose OK. The Add Service Name Binding dialog box appears (Figure 12-3).

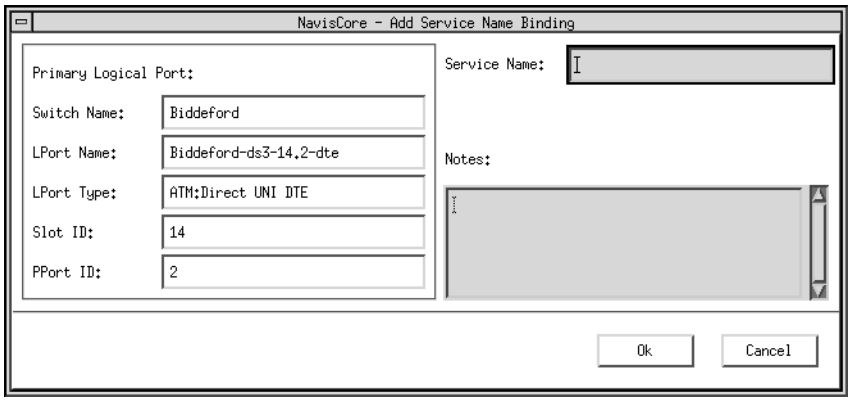


Figure 12-3. Add Service Name Binding Dialog Box

5. Enter a Service Name (up to 32 characters). Optionally, you can enter a brief comment or description of the service in the Notes box.
6. Choose OK.
7. Continue with the instructions in "Defining a PVC Connection" on page 8-22 to configure circuits as fault-tolerant PVCs.

   To reroute the Service Name endpoint of a fault-tolerant PVC, see the next section, "Activating a Backup Binding Port."

Activating a Backup Binding Port

If a primary port fails (or needs administrative maintenance), you reassign the Service Name of the primary port to a backup port. Since fault-tolerant PVCs use the Service Name as an endpoint, circuits configured for the primary port are rerouted to the backup port.

To enable the backup binding:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Service Name Bindings ⇒ Set All Resilient UNI/NNI. The Set All Service Name Bindings dialog box (Figure 12-1 on page 12-4) appears.
2. Choose Set Backup Binding. The Select End Logical Port dialog box appears (Figure 12-4).

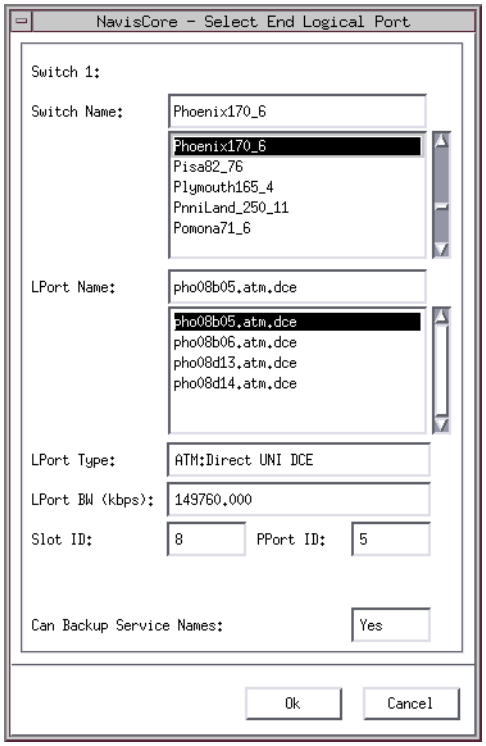


Figure 12-4. Select End Logical Port Dialog Box

3. Select the Switch Name for the backup Service Name binding you want to use.
4. The LPort Name field displays a list of logical ports configured on the selected switch. Select an LPort Name that has the *same* logical port type as the port you need to back up.

Note – Make sure that the Can Backup Service Names field displays Yes. This indicates you can use this logical port as a backup.

5. Choose OK. The Set/Modify Backup Service Name Binding dialog box appears, displaying the Service Name that corresponds to the switch and logical port names you selected.

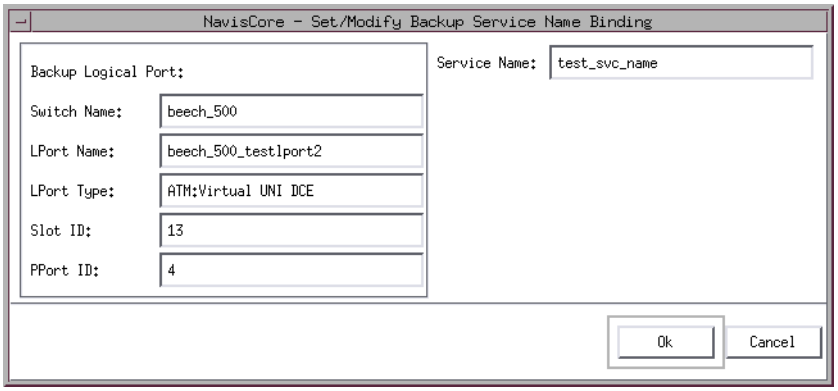


Figure 12-5. Set/Modify Backup Service Name Binding Dialog Box

6. Choose OK. The Set All Service Name Bindings dialog box reappears (Figure 12-1 on page 12-4). The Status field should now display the message “Backup Binding Active.”

Using APS with Resilient UNI

You can use APS functions to automate the basic (manually activated) fault-tolerant PVC/resilient UNI backup feature. If an equipment failure occurs, the APS provides a backup physical port, while Resilient UNI provides a backup logical port.

Note – Resilient NNI cannot be used with APS functions.

The Automatic Protection Switching (APS) feature is available on all types of CBX and GX ATM optical interfaces. (See the *B-STDX, CBX, and GX Switch Module Configuration Guide* for a listing of the minimum software and hardware versions that support the various APS options.) Automatic Protection Switching allows you to protect optical interfaces by provisioning a backup (protection) port that automatically takes over for the primary (working) port when a physical layer fault or module failure occurs.

Note – Bellcore GR-253-CORE, ITU G.841, Annex B (formerly ITU G.783, Annex B), and ITU G.841 section 7.1 (formerly ITU G.783, Annex A) standards form the basis of the Lucent APS implementation. Review these specifications and standards for further information on how you can use APS in a network environment.

You can configure APS Resilient UNI on the following optical modules:

- OC-3c/STM-1 (CBX and GX)
- OC-12c/STM-4 (CBX and GX)
- OC-48/STM-16 (GX)

Note – See the Switch Software Release Notice (SRN) for any module restrictions that apply to APS.

Working Port and Protection Port Configuration Guidelines

With APS Resilient UNI, you can provision the working port and the protection port on two different switch modules, protecting against module failure. You can use this option in conjunction with Lucent UNI logical ports. When you configure APS Resilient UNI, you have to provision a separate logical port on one or both working and protection ports. If a working (primary logical) port fails, the fault-tolerant PVC/APS Resilient UNI software automatically moves circuits to the corresponding protection (backup logical) port.

Note – As traffic is rerouted from a working trunk to a protection trunk during a failure, APS Resilient UNI switchover speed may be less than that provided by Intra-card APS 1+1. For more information, see Chapter 7, "Configuring Trunks."

CBX 500 Considerations

When you select APS Resilient UNI on a CBX 500, you configure the working and protection port on *different* interface modules.

GX 550 Considerations

When you select APS Resilient UNI on a GX 550, you can configure the working and protection ports on either the same module (BIO or Phy) or a different module (BIO or Phy).

APS Resilient UNI Over PNNI

You can use the APS Resilient UNI feature to configure fault-tolerant ATM PVCs across a Private Network-to-Network Interface (PNNI) or combined Virtual Network Navigator/PNNI (VNN/PNNI) domain. You configure APS Resilient UNI over PNNI links using the same procedure as you would for ATM VNN OSPF networks.

For details, see "Resilient UNI and APS Resilient UNI Over PNNI" on page 20-25.

Configuring APS Resilient UNI

This section describes the prerequisite tasks you must perform before you configure UNI logical ports for APS Resilient UNI. This section also describes the following tasks:

- Defining an ATM UNI primary logical port on one or both of the working ports (of the APS pair).
- Defining an ATM UNI backup logical port on one or both of the protection ports (of the APS pair).
- Defining a fault-tolerant PVC/Resilient UNI configuration between the working/protection ports.

Before You Begin

Before you define a UNI logical port for APS Resilient UNI, verify that you have configured the following:

- One or more working ports (which are on two different switches) and their APS Resilient UNI attributes.
- One or more protection ports (which are on the same switches as the working ports) and their APS Resilient UNI attributes.

Note – Both working/protection port pairs are often used for double redundancy. It is also possible to use a regular (non-Service Name) logical port as one PVC endpoint, with APS Resilient UNI set up at the other end.

For more information, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

Defining ATM UNI Logical Ports on the Working Ports

To configure an ATM UNI logical port on an APS working port:

1. Select the switch on which the first working port pair resides. (You will define an ATM UNI logical port for each of these physical ports.)
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the working port (of the APS pair) and press the right mouse button to display a pop-up menu.
4. Select Logical Port. The Set All Logical Ports in PPort dialog box appears (Figure 3-1 on page 3-4).

5. Choose Add to display the Add Logical Port Type dialog box (Figure 3-2 on page 3-10).
6. Select ATM UNI (DCE or DTE) as the LPort Type.
7. Choose OK. The Add Logical Port dialog box reappears (Figure 3-3 on page 3-11).
8. Complete the additional attributes as follows:

To Set	See
Administrative Attributes	Table 3-4 on page 3-14
ATM Attributes	Table 3-6 on page 3-22
ILMI/Signaling/OAM Attributes	Table 3-7 on page 3-29
Opt Trunk VPI Range Attributes	Table 3-9 on page 3-39

9. Choose OK to return to the Set All Logical Ports in PPort dialog box.
10. Choose Close to return to the Set Physical Port Attributes dialog box.
11. Choose Cancel to return to the Switch Back Panel dialog box.
12. Choose Close to return to the network map.

Defining ATM UNI Logical Ports on the Protection Ports

To configure an ATM UNI logical port on an APS protection port:

1. Select the switch on which the first working port pair resides. (You will define an ATM UNI logical port for each of these physical ports.)
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
3. Select the protection port (of the APS pair) and press the right mouse button to display a pop-up menu.
4. Repeat step 4 through step 11 in the previous section, titled "Defining ATM UNI Logical Ports on the Working Ports." When you set the Administrative Attributes for this protection port, be sure to select Yes in the Can Backup Service Names field (Table 3-4 on page 3-14).
5. Choose Close to return to the network map.

Defining the APS Fault-tolerant PVC/Resilient UNI Configuration

If the working port fails, the APS fault-tolerant PVC/resilient UNI software automatically moves the Service Name endpoint to the protection (backup) port. Use the following instructions to define the APS fault-tolerant PVC/resilient UNI configuration between two working ports:

1. Complete the steps described in "Creating Service Names" on page 12-4 to assign a Service Name to one of the working/ATM UNI logical port endpoints. A different Service Name must be used if backing up the working APS port on the other side of a fault-tolerant PVC.
2. Continue with the instructions in "Defining a PVC Connection" on page 8-22 to configure the fault-tolerant PVC.

13

Configuring Resilient LMI

This chapter describes the Frame Relay Resilient Link Management Interface (RLMI) feature and explains how to configure RLMI on ATM Network Interworking for Frame Relay NNI logical ports on 1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 cards. See the *B-STDX and CBX Frame Relay Services Configuration Guide* for more information on configuring RLMI on Frame Relay UNI and NNI logical ports.

Resilient LMI provides resiliency by monitoring Link Management Interface (LMI) link status. RLMI enables a pair of Frame Relay logical ports configured on a B-STDX or CBX switch to serve as preferred and backup ports. If the primary port fails, a switchover to the backup port occurs.

The RLMI feature requires one end of the RLMI pair to be configured as Master (controls the automatic switchover) and the other end to be configured as Slave. Lucent switches can operate as Master or Slave.

RLMI supports the following LMI types:

- LMI Rev. 1
- Q.933 Annex A
- ANSI T1.617 Annex D
- Auto Detect (if the logical port is configured as Slave DCE)

Note – You cannot configure RLMI on a logical port that is configured for fault-tolerant PVCs.

Resilient LMI Terms

Table 13-1 lists the RLMI terms used in this chapter.

Table 13-1. Resilient LMI Terms

Term	Definition
Full Status Enquiry	Status Enquiry Message with Report Type of Full Status.
Full Status Response	Status Response Message with Report Type of Full Status.
Preferred Link	The link configured by the RLMI to activate as the working link.
Backup Link	The link selected by the RLMI to activate as the working link (in case the preferred link is not up or goes down while in an active phase).
Working Link	The active link, which is used for data transfer, LMI polling, and SVC signaling. A working link is either a preferred link or a backup link.
Protection Link	The link selected by the RLMI to activate in case the working link goes down. A protection link is either a preferred link or a backup link.
Full Revertive	If the Master RLMI switch's RLMI mode is configured as Full Revertive, the following occurs: • When the preferred link goes down, the backup link becomes the working link. • If or when the preferred link comes back up, the working link automatically switches back to the preferred link.
Semi Revertive	If the Master RLMI switch's RLMI mode is configured as Semi Revertive, the following occurs: • When the preferred link goes down, the backup link becomes the working link. • If or when the preferred link comes back up, the working link remains on the backup link (unless the backup link is down as well, then the preferred link becomes the working link again).

Table 13-1. Resilient LMI Terms (Continued)

Term	Definition
Manual Switchover Only	If the Master RLMI switch's RLMI mode is configured as Manual Switchover Only, the following occurs: • When the preferred link goes down, the backup link does not automatically become the working link. You must manually apply the switchover through the NMS, at which point the backup link becomes the working link. • When the backup link is down and the preferred link comes back up, the preferred link does not automatically become the working link unless you manually switch over again.

Configuration Guidelines

This section lists the guidelines you should follow when you configure RLMI. NavisCore enforces these guidelines to prevent configuration errors.

Note – SVC FRF.10 (NNI) is not supported in this release.

- You must configure a pair of RLMI ports on the same node. Each of the two RLMI ports can be configured on the same IOP/IOM or on different IOP/IOMs.
- Fault-tolerant PVC (resilient UNI/NNI) ports must not have RLMI enabled. This ensures that fault-tolerant PVCs and RLMI remain mutually exclusive.
- An RLMI preferred/backup pair can be a combination of any two FR UNI/NNI physical links (for example, a preferred Universal Input/Output [UIO] V.35 and a backup T1) or ATM Network Interworking for FR NNI logical ports on the B-STDX 1-port ATM CS DS3/E3 and 1-port ATM IWU OC-3c/STM-1 cards. Each RLMI preferred/backup pair is configured independently from other pairs.
- You must configure the UNI DTE as the Master and the UNI DCE as the Slave. You can configure the NNI as Master or Slave (one side must be Master and the other side must be Slave).
- You must define both preferred and backup logical ports for an RLMI name. You select these ports from a list of Frame Relay ports that have RLMI enabled. You cannot select the same port as both preferred and backup, and the port cannot be in use by any other RLMI service name.
- The preferred port must not have backup capability provisioned. The backup port must have backup capability provisioned.
- A single switch supports a combination of UNI Masters, UNI Slaves, NNI Masters, and NNI Slaves.
- The service name address that identifies an RLMI preferred/backup pair must be unique within the Frame Relay network.
- You can configure a maximum of 128 RLMI pairs (service name addresses) per node.

Resilient LMI Configuration Sequence

Perform the following steps to configure primary and backup RLMI logical ports:

Step 1. Define an ATM Network Interworking for Frame Relay NNI logical port (see "Network Interworking for Frame Relay Network-to-Network Interface" on page 4-4).

Configure the following RLMI options:

- Can Backup Service Names (see Table 4-7 on page 4-15) to specify a backup or a primary port
- RLMI Admin Status and RLMI Max Full Status Attempts (see Table 4-23 on page 4-44)

Step 2. Configure a defined service name for the Preferred Logical Port and Backup Logical Port fields (see "Creating Service Names" on page 13-6).

Step 3. Configure the RLMI Master/Slave Mode field (see Table 13-2 on page 13-8) and RLMI switchover mode (see "Configuring the RLMI Switchover Mode" on page 13-10).

Step 4. Add a circuit connection as described in "Defining a PVC Connection" on page 8-22, and configure the Resilient LMI service names as Endpoint 1 or Endpoint 2 (see "For a Resilient LMI PVC Connection" on page 8-23).

Creating Service Names

The *service name binding* is a name you define to identify the RLMI preferred/backup pair. A circuit recognizes its service endpoint by this name instead of the logical port name.

To create the service name bindings:

1. From the Administer menu, select Lucent Parameters ⇒ Set All Service Name Bindings ⇒ Set All Resilient LMI.

   The Set All RLMI Service Name Bindings dialog box (Figure 13-1) appears, displaying any defined service names you have already configured.

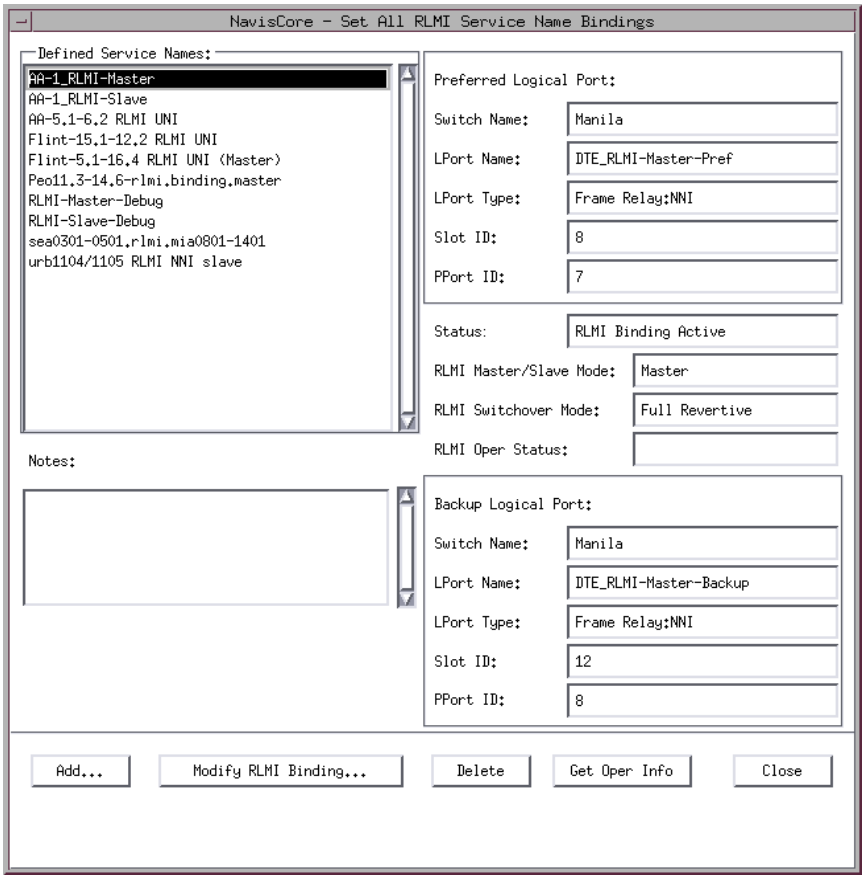


Figure 13-1. Set All RLMI Service Name Bindings Dialog Box

You can access the following functions from The Set All RLMI Service Name Bindings dialog box:

- To modify a service name binding, choose Modify RLMI Binding and see "Configuring the RLMI Switchover Mode" on page 13-10.
- To delete a service name, select the defined service name and choose Delete.

2. Choose Add. The Select End Logical Port dialog box appears. Select the appropriate preferred switch that is configured for RLMI, as shown in Figure 13-2.

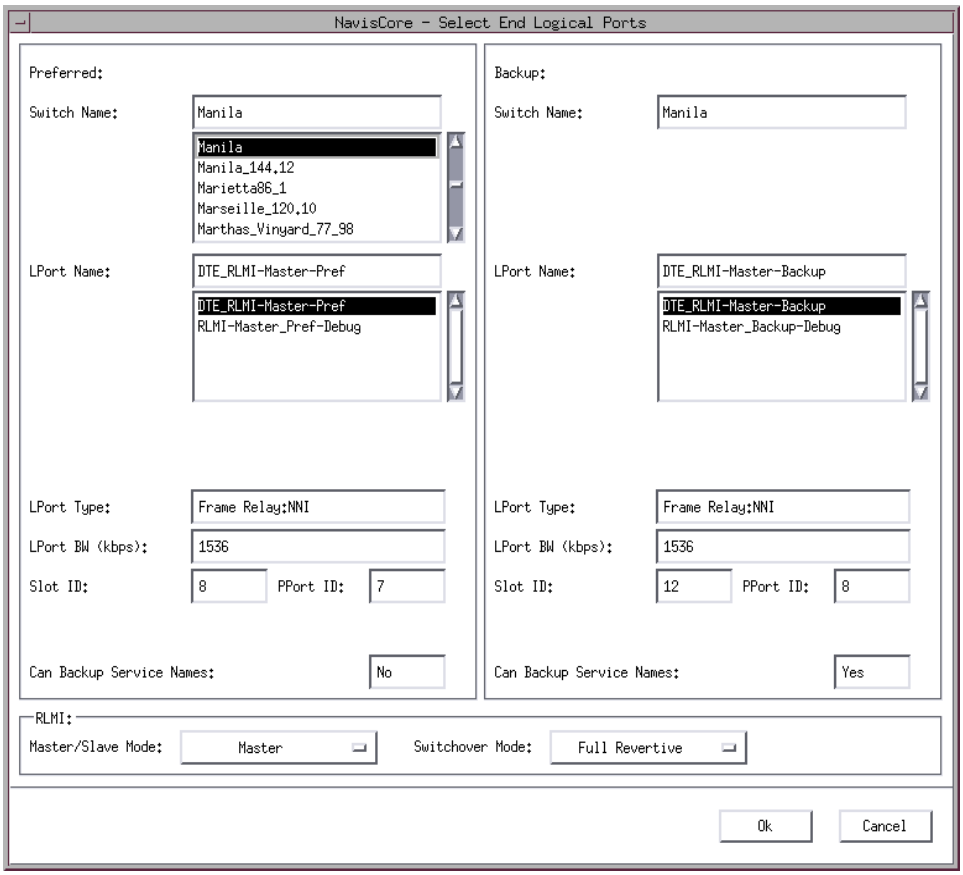


Figure 13-2. Select End Logical Ports Dialog Box

If you configure the RLMI Mode as Master, only Frame Relay UNI DTE or NNI logical ports will appear as preferred and backup ports. If you configure the RLMI Mode as Slave, only Frame Relay UNI DCE or NNI logical ports will appear as preferred and backup ports.

3. In the Preferred window, the system displays only DTE or NNI logical ports configured with RLMI enabled and Can Backup Service Names set to No. Select the preferred logical port name for the selected preferred switch name.

4. In the Backup window, the system displays the selected preferred switch name in the Preferred window. The system displays only DCE or NNI logical ports configured with RLMI enabled and Can Backup Service Names set to Yes. Select the appropriate backup logical port name.

5. Complete the RLMI fields in Table 13-2.

Table 13-2. RLMI Fields

Field	Action/Description
Master/Slave Mode	Select the mode of operation for resilient LMI bindings. The RLMI feature does not detect invalid Master-Master or Slave-Slave configurations. You must configure complementary types (for example, a master-slave connection). You must configure UNI RLMI with the DTE (user side) as the Master and the DCE (network side) as the Slave. You can configure either side of an NNI RLMI as Slave or Master. *Master* – (default) This mode determines which link to activate as the working link. Only Frame Relay UNI DTE or NNI logical ports may be configured as Preferred and Backup ports under this mode. *Slave* – Only Frame Relay UNI DCE or NNI logical ports can be configured as Preferred and Backup ports under this mode.
Switchover Mode	Select the mode of operation for automatic bindings when an interface changes up/down states. You can configure the Switchover Mode only when the Mode parameter is configured as Master. By default, the Switchover Mode is set to Full Revertive. To configure the Switchover Mode, see page 13-10. *Manual Only* – No switchover occurs when a link goes down or up. A switchover can occur only by a manual NMS-forced switchover. *Full Revertive* – (default) Reverts to primary binding when primary is up. *Semi Revertive* – Remains on backup binding when primary is up.

6. Choose OK. The Add Service Name Binding dialog box (Figure 13-3) appears.

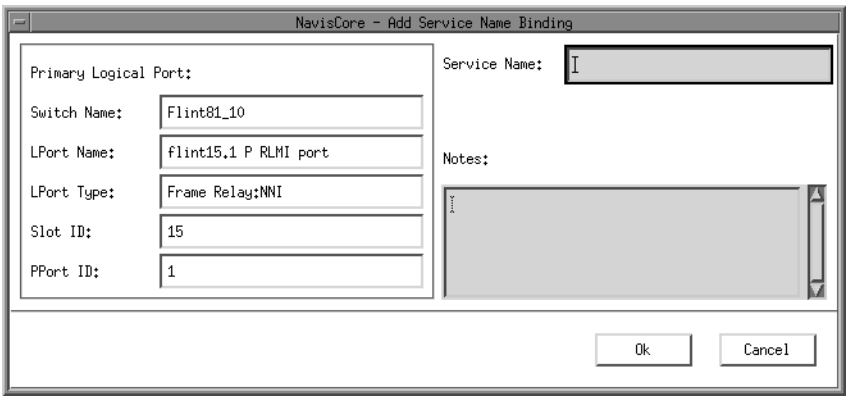


Figure 13-3. Add Service Name Binding Dialog Box

7. Enter a Service Name (up to 32 characters). Optionally, you can enter a brief comment or description of the service in the Notes box.
8. Choose Ok.

Configuring the RLMI Switchover Mode

To modify the RLMI parameters or "force" a preferred/backup switchover:

1. Choose Modify RLMI Binding from the Set All RLMI Service Name Bindings dialog box (Figure 13-1 on page 13-6). The Modify RLMI Service Name dialog box appears.

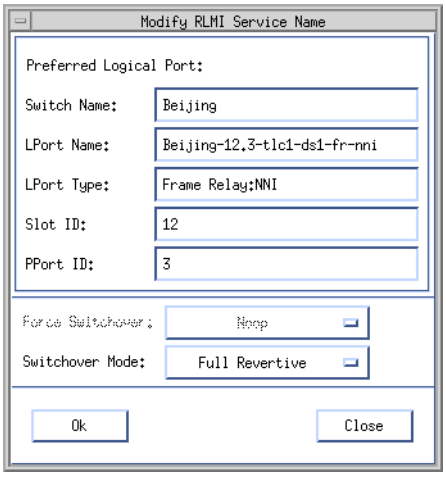


Figure 13-4. Modify RLMI Service Name Dialog Box

2. Complete the fields in Table 13-2.

Table 13-3. Modify RLMI Service Name Dialog Box Fields

Field	Action/Description
Force Switchover	Select the switchover mode. Options include: *Noop* – No switchover occurs. *Switchover* – The current binding is switched to the other binding (for example, primary is switched to backup and backup is switched to primary). ***Note**: The Force Switchover feature is disabled when the RLMI pair's Switchover Mode is set to Full Revertive.*

Table 13-3. Modify RLMI Service Name Dialog Box Fields (Continued)

Field	Action/Description
Switchover Mode	The Switchover Mode indicates the mode of operation for automatic bindings when an interface changes up/down states. You can configure the Switchover Mode only when the Mode parameter is configured as Master. Options include: *Manual Only* – No switchover occurs when a link goes down or up. A switchover can occur only by a manual NMS-forced switchover. *Full Revertive* – (default) Reverts to primary binding when primary is up. *Semi Revertive* – Remains on backup binding when primary is up.

3. Choose Ok.
4. See the following sections to add a circuit connection and configure endpoints for an RLMI PVC connection:
   - "Defining a PVC Connection" on page 8-22
   - "For a Resilient LMI PVC Connection" on page 8-23

14

About SVCs

This chapter describes how to use switched virtual circuits (SVCs). With SVCs, connections are not predefined as they are for permanent virtual circuits (PVCs). Instead, end stations use a signaling protocol to indicate to the ATM network the endpoint to which it should route the SVC request (*called party*). To support SVC services, each user endpoint is assigned a unique address which identifies the endpoint and enables the network to route the SVC request.

Note – You cannot configure ATM SVCs on B-STDX switches or CBX 500 Frame-based modules.

Address Formats

Before you configure your network for SVCs, you must decide which of the following address format types to use:

ATM End System Address (AESA) formats — AESA formats give service providers using a private ATM network the flexibility to develop an addressing scheme that best suits their network needs; for example, you may find that most CPEs in your network only support a specific AESA address format.

AESA Anycast Formats – AESA Anycast formats give service providers "group address" functionality for each of the AESA address formats. Using the Anycast format, a call is placed to the group address and the network selects one of the members to which the call will be routed. This group address could, for example, represent a group of Internet servers which contain the same information and perform identical functions. It does not matter which of these servers handles the call.

Native E.164 address format — E.164 addresses are phone numbers. This address format is simple and familiar; native E.164 addresses are a convenient choice for service providers using a public ATM network (for example, Regional Bell Operating Companies [RBOCs]) that already "own" E.164 address space.

The following sections describe these address formats.

ATM End System Address (AESA) Formats

The GX 550 and CBX 500 support four AESA formats:

Data country code (DCC) — For DCC AESA addresses, the initial domain identifier (IDI) is a two-byte data country code field that identifies the country in which this address is registered. These country codes are standardized and defined in ISO reference 3166. *DCC Anycast AESA* provides a group address function for this address type.

International Code Designator (ICD) — For ICD AESAs, the initial domain identifier (IDI) field contains the International Code Designator that uniquely identifies an international organization. The British Standards Organization administers these values. ICD Anycast AESA provides a group address function for this address type.

Custom — A Custom AESA address enables you to use a customized octet structure and a customized authority and format identifier (AFI).

E.164 — For E.164 AESA addresses, the IDI field contains an eight-byte E.164 address. This E.164 address uses the international format and consists of up to fifteen decimal digits. E.164 Anycast AESA provides a group address function for this address type.

Embedded E.164 AESA format — An embedded E.164 is a specific type of AESA format that requires a specific encoding in the IDI section. As shown in the example below, a Native E.164 address is converted to BCD format. Leading zeros are added to obtain the maximum length of 15 octets and a trailing semi-octet 0xF is added to pad the final semi-octet. The High-Order Domain Specific Part (HO-DSP) and the end system identifier (ESI) must be all zeros. For specific information, see Section 5.1.3.1.1.3 of the *ATM User-Network Interface (UNI) Specification 3.1*.

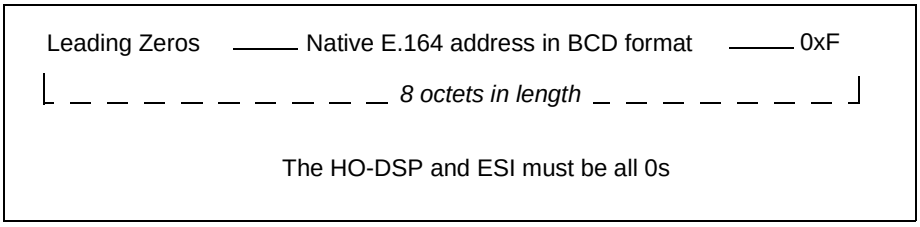


Figure 14-1. Native E.164 Address Converted to BCD Format

An example of an embedded E.164 AESA format is shown below using the Native E.164 address 1508555.

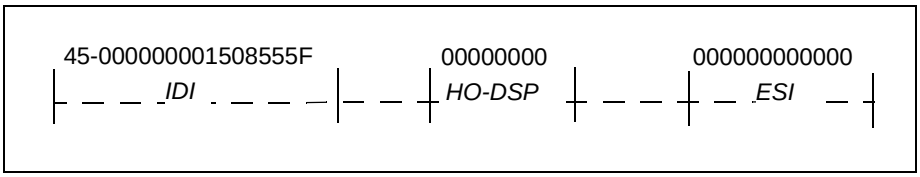


Figure 14-2. Embedded E.164 AESA Format

* HO-DSP = high-order domain-specific part

* ESI = end system identifier

All AESA address formats consist of 20 octets. Each of these address formats contain the following components:

Initial domain part (IDP) — Defines the type of address and the regulatory authority responsible for allocating and assigning the Domain Specific Part. There are two subfields: the AFI and IDI fields.

Authority and Format Identifier (AFI) – The AFI part of the AESA address identifies the authority that allocates the DCC, ICD, or E.164 part of the AESA address, as well as the syntax of the rest of the address. The following are default AFIs:

Table 14-1. AFI Default Values

Address Type	AFI Description
DCC	0x39
DCC Anycast	0xBD
ICD	0x47
ICD Anycast	0xC5
E.164	0x45
E.164 Anycast	0xC3
Custom	A user-specific code for custom prefixes/addresses. (You must know the appropriate code to enter when defining custom prefixes/addresses.)

Initial Domain Identifier (IDI) – A hex code that identifies the sub-authority that has allocated the address. The format depends on the following address types:

Table 14-2. IDI Default Values

Address Type	IDI Description
DCC (including Anycast)	Consists of 2 octets (4 hex digits) that identify the country in which this address is registered. The DCC is generally considered a three digit quantity with a trailing hex “f” semi-octet. For example, the ANSI IDI of 840 is encoded as 0x840f.
ICD (Anycast)	Consists of 2 octets (4 hex digits) that identify an international organization to which this address is registered. The ICD is generally considered a four digit quantity. For example, the US GOSIP IDI of “5” is encoded as 0x0005.

Table 14-2. IDI Default Values (Continued)

Address Type	IDI Description
E.164 (Anycast)	Consists of 8 octets in BCD format. (1-15 hex digits, plus a trailing Fh; if less than 15 digits are entered, type leading zeros to fill the 8 octets.) Represents an international E.164 address. For example, the E.164 address of 978-555-1212 is encoded as 0x000009785551212f.

Domain Specific Part — Consists of the HO-DSP, EDI, and SEL fields.

High Order Domain Specific Part (HO-DSP) – The authority specified in the AFI/IDI octets determines the format of this field. It identifies a segment of address space that is assigned to a particular user or subnetwork. It should be constructed to facilitate routing through interconnected ATM subnetworks. The general format for each address type is as follows:

Table 14-3. HO-DSP Default Values

Address Type	HO-DSP Description
DCC, ICD (including Anycast)	Consists of 10 octets (20 hex digits)
E.164 (Anycast)	Consists of 4 octets (8 hex digits)
Custom	Consists of 12 octets (24 hex digits)

End System Identifier (ESI) – A 6-octet (12 hex digit) field that uniquely identifies the end system within the specified subnetwork. This is typically an IEEE MAC address.

Selector (SEL) – A 1-octet (2 hex digit) field that is not used for ATM routing, but may be used by the end system.

Figure 14-3 shows how the octets are assigned for each AESA address format. Each octet is equivalent to two hex digits.

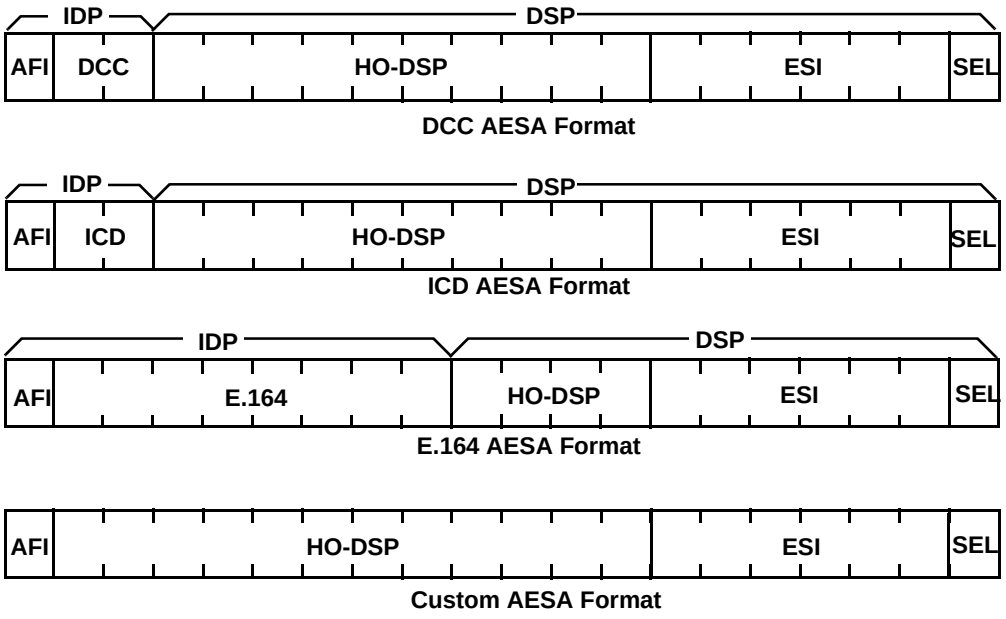


Figure 14-3. AESA Address Formats

Native E.164 Address Format

Native E.164 addresses are the standard Integrated Services Digital Network (ISDN) numbers, including telephone numbers. Native E.164 addresses consist of 1-15 ASCII digits. For example, standard 10-digit United States telephone numbers, such as 508-555-1234, are native E.164 addresses.

Unlike AESA address formats, native E.164 addresses are not broken down into AFI, HO-DSP, ESI, and SEL portions. When a native E.164 address is translated to E.164 AESA format, the native E.164 address is stored in octets 2-9 of the 20-octet AESA address, while the HO-DSP, ESI, and SEL portions are filled with zeros. Conversely, when an E.164 AESA address is translated to the native E.164 address format, the AFI, HO-DSP, ESI, and SEL portions, as well as any leading zeros in the 8-octet AESA E.164 address, are stripped off to produce the native E.164 address.

Designing an Address Format Plan

The SVC address formats you select must support the equipment and services your network needs to provide. Keep in mind that some CPEs may not support certain address formats. To avoid address conflicts, apply for globally-recognized address space in the ATM formats you need to use.

You use address formats to develop a network numbering plan. Using an AESA address, you can design the IDP portion of an address to target a specific network; then use the HO-DSP portion of the address to identify subnetworks within that network, and use the ESI portion to identify a specific end system.

Regardless of the address format you choose, the network numbering plan should satisfy the following goals:

- Intelligently assign network addresses
- Simplify network topology using a hierarchal organization
- Minimize the size of network routing tables
- Uniquely identify each endpoint
- Provide a high level of network scalability

About Address Registration

Address information in a switch is used to determine call routing; it is also used for calling party screening. When used for route determination, the switch advertises an appropriate subset of its configured node prefixes, port prefixes, and port addresses to all other switches in the network. When used for calling party screening, the switch uses the configured node prefixes, port prefixes, and/or port addresses to determine whether or not the network should accept an SVC request.

To perform these two functions at a UNI, both the user and the network need to know the ATM addresses that are valid at the UNI. Address registration provides a mechanism for address information to be dynamically exchanged between the user and the network, enabling both to determine the valid ATM addresses that are in effect at a UNI. Address registration applies only to UNI ports on which Interim Link Management Interface (ILMI) is enabled (see Table 3-7 on page 3-29 for instructions on how to enable ILMI on a UNI logical port). Any ILMI-eligible node or port prefix will be transferred from all ILMI-enabled private UNI DCE ports and all ILMI-enabled public end-system UNI DCE ports to their peer DTE devices.

Note – Node prefixes are not exchanged from “network-to-network” UNI DCE ports. Only port prefixes are exchanged from these ports. For address registration to work, attached UNI devices must support ILMI.

ILMI-eligible prefixes include:

- All native E.164 node prefixes
- All 13-octet (104-bit) AESA node prefixes
- All native E.164 port prefixes
- All 13-octet (104-bit) AESA port prefixes

The network side of the UNI provides the network prefix, which consists of the IDP and HO-DSP portions. The user side of the UNI provides the remaining portion of the address, which consists of the IEEE MAC address (the ESI portion) and the SEL portion of an ATM address; this forms the user part of the address. Figure 14-4 shows this addressing scheme.

Note – Native E.164 prefixes sent by the network are concatenated with a NULL user part by the user, and returned to the network as native E.164 addresses. (The prefix and address are identical.)

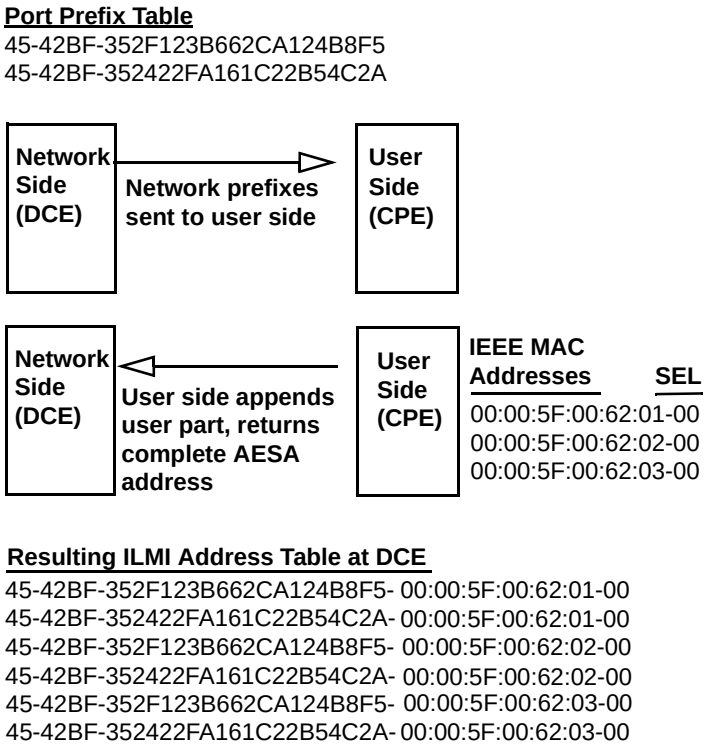


Figure 14-4. Address Registration

About Route Determination

The node prefixes, port prefixes, and port addresses configured on network nodes are used to determine the route for a given SVC. A “best match” hierarchy determines the route, starting from the left-most digit of the called party address.

Keep in mind that you use node prefixes to summarize the common address parts of the node. For example, if all addresses on the node contain the digits 15085551, you would define this as the node prefix. To allow for address routing, node prefixes should be unique to a switch; if not, the switch has to perform subsequent matching to find a route to the destination.

The following example shows three nodes configured with a combination of native E.164 node prefixes, port prefixes, and port addresses:

	Node 1	**Node 2**	**Node 3**
Node Prefixes	508 6	None	508 603
Port Prefixes	508551 508552 508553	5085 508553 6035	508554 508555
Port Addresses	5085511111 5085511112 5085511113 5085555555 5085555556	None	None

The following example shows the node to which the SVC request is routed for certain called-party addresses, and describes why the request is routed to that node:

Called Party Address	**Node**	**Reason**
5085511234	1	Port prefix 508551 on Node 1 is a longer match than port prefix 5085 on Node 2 and node prefix 508 on Node 3.
5085555555	1	This calling party address is an exact match for a port address defined on Node 1. This is a longer match than port prefix 5085 on Node 2 and port prefix 508555 on Node 3.
5085555557	3	Port prefix 508555 on Node 3 is a longer match than port prefix 5085 on Node 2 and node prefix 508 on Node 1.

Called Party Address	Node	Reason
5085561111	2	Port prefix 5085 on Node 2 is a longer match than node prefix 508 on Node 1 and node prefix 508 on Node 3.
6175551111	1	Node prefix 6 on Node 1 is the only match.
6035551111	2	Port prefix 6035 on Node 2 is a longer match than node prefix 6 on Node 1 and node prefix 603 on Node 3.
6038558888	3	Node prefix 603 on Node 3 is a longer match than node prefix 6 on Node 1. There is no matching prefix or address on Node 2.
5085531111	1 or 2	Since the longest match occurs on both Nodes 1 and 2, the Admin Cost value assigned to port prefix 508553 on each node determines where the call is routed. The call is routed to the node with the lowest Admin Cost value for port prefix 508553.
5145551234	None	The call is not routed to any of these nodes because there are no matching node prefixes, port prefixes, or port addresses. If, however, you set up a default route on a port being used for network-to-network connections, all non-matching calls are routed to that port (see “Defining Default Routes for Network-to-Network Connections” on page 15-23).

About Address Translation

This section describes how address translation occurs in various situations and at various points along a network connection. This information applies only if you enable address translation. Also, egress address translation requires matching a called party address to a configured prefix on the egress port.

Calling party and called party addresses are stored as information elements in the SETUP message, which is sent to initiate call setup. In some situations, calling party and called party sub-addresses are also stored as information elements in the SETUP message.

Calling Party Address	**Called Party Address**
Calling Party Sub-address	**Called Party Sub-address**

Egress address translation, when enabled on a network-to-network port, functions as described in Table 14-4 and Table 14-5. The following factors determine how address translation occurs:

- Whether or not local and/or remote gateway addresses are defined on the egress port
- The type of translation (tunnel or replace) selected as the egress address translation mode
- The numbering plan of the signaled calling and called addresses

Calling party and called party processing are independent. Note that in the SETUP message, the called party address is mandatory, while the calling party address is optional. In the case of a native E.164 called party or calling party address, the related sub-address field is always set to null, since the sub-address field cannot carry native E.164 addresses (note that in the tables, if the signaled calling party address is native E.164 format, the calling party sub-address field is always set to null).

Using ingress address translation, the calling party sub-address (if it is not null) overwrites the calling party address at the ingress port, and the called party sub-address (if it is not null) overwrites the called party address.

Table 14-4 shows how calling party addresses are translated at the egress port.

Table 14-4. Calling Party Address Translation at Egress Port

Signaled Address	SETUP Information Element	No Local Gateway Address	Local Gateway Address with Tunnel Option	Local Gateway Address with Replace Option
No Calling Party	Calling Party Address	Null	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Null	Null
AESA Calling Party	Calling Party Address	Signaled AESA Calling Party Address	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Signaled AESA Calling Party Address	Null
Native E.164 Calling Party	Calling Party Address	Signaled Native E.164 Calling Party Address	Local Gateway Address	Local Gateway Address
	Calling Party Sub-address	Null	Signaled Native E.164 Calling Party Address in AESA E.164 Format	Null

Table 14-5 shows how called party addresses are translated at the egress port.

Table 14-5. Called Party Address Translation at Egress Port

Signaled Address	SETUP Information Element	No Remote Gateway Address	Remote Gateway Address with Tunnel Option	Remote Gateway Address with Replace Option
AESA Called Party	Called Party Address	Signaled AESA Called Party Address	Remote Gateway Address	Remote Gateway Address
	Called Party Sub-address	Null	Signaled AESA Called Party Address	Null
Native E.164 Called Party	Called Party Address	Signaled Native E.164 Called Party Address	Remote Gateway Address	Remote Gateway Address
	Called Party Sub-address	Null	Signaled Native E.164 Called Party Address in AESA E.164 Format	Null

Examples

The following example diagrams show the state of the SETUP message calling party/called party address and sub-address elements at various points along the connection.

The example diagrams represent the calling party and called party address and sub-address elements as follows:

Calling Party Address	Called Party Address
Calling Party Sub-address	Called Party Sub-address

Example 1
- Egress tunneling enabled on Network 1's egress port
- Ingress tunneling enabled on Network 2's ingress port
- Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B
- Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B

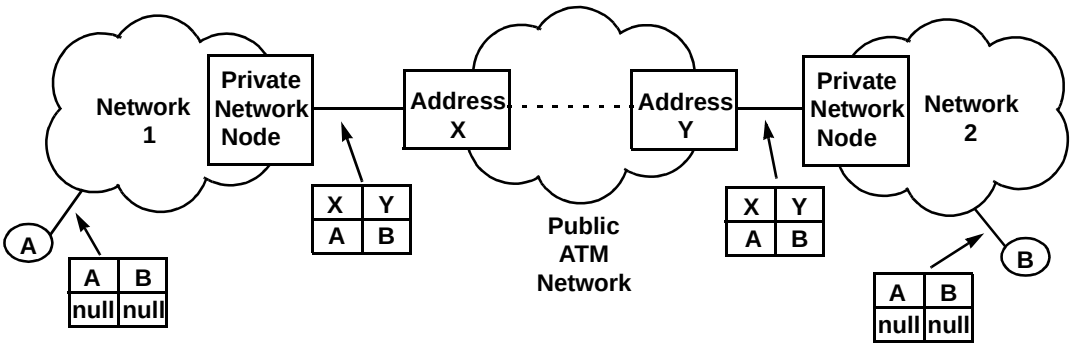


Figure 14-5. State of Connection SETUP Message Address Elements (1)

Example 2
- Egress tunneling enabled on Network 1's egress port
- Ingress tunneling enabled on Network 2's ingress port
- No Local Gateway address defined on egress port
- Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B

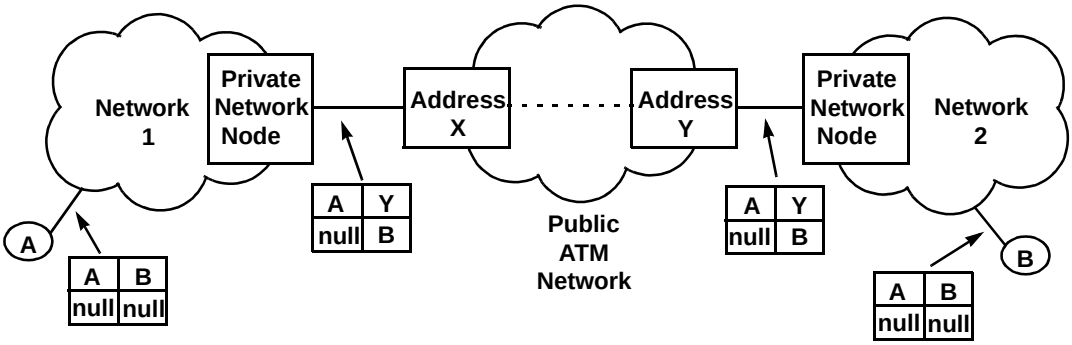


Figure 14-6. State of Connection SETUP Message Address Elements (2)

Example 3
- Replace option selected on egress port of Network 1
- Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B

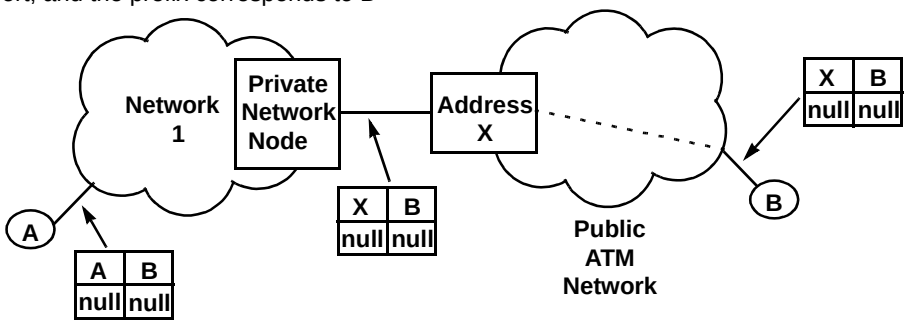


Figure 14-7. State of Connection SETUP Message Address Elements (3)

Example 4
- Replace option selected on egress port of Network 1
- Local Gateway address X configured to a prefix on Network 1's egress port, and the prefix corresponds to B
- Remote Gateway address Y configured to a prefix on Network 1's egress port, and the prefix corresponds to B

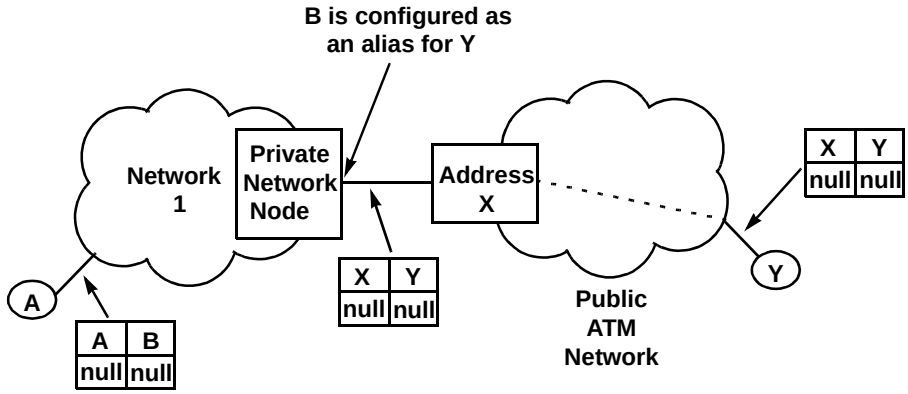


Figure 14-8. State of Connection SETUP Message Address Elements (4)

Network ID Addressing

A network ID can be used to identify an inter-exchange carrier (IXC). You can configure network ID addressing on ATM and Frame Relay UNI logical ports.

Depending on the administering authority, a network ID may be a 3-, 4-, or 8-digit carrier identification code (CIC) or a 4-digit data network identification Code (DNIC, X.121). A network ID enables you to associate a network-to-network connection with a particular IXC (using a route determination ID) and enables end-users to pre-subscribe to a particular IXC (using a source default network ID) and override this selection on a call-by-call basis (using a signaled transit network selection [TNS]). Signaled TNSs are screened by matching them against a list of pre-subscribed source validation network IDs. It is also possible to "ignore" the signaled TNS to allow routing based on the called party address instead of the TNS value; the signaled TNS is essentially stripped at the ingress port.

An SVC is routed based on one of the following addresses provided at the ingress port (selected in listed order):

- Signaled TNS
- Signaled Called Party
- Provisional Default TNS

You can configure both route determination network IDs and route determination port prefixes/addresses on a logical port at a network-to-network connection. A combination of source validation network IDs and route determination network IDs can coexist on the same port. You can provision network IDs on ATM UNI 3.x, 4.0, IISP, or FRF.4 ports.

You can configure a maximum of 1024 configurable addresses for a logical port (where configurable addresses equal the sum of all port addresses, prefixes, user parts, and network IDs). The maximum number of network IDs for a logical port equals 1024 minus the sum of port addresses, prefixes, and user parts.

15

Configuring SVC Parameters

This chapter contains procedures to perform the following tasks:

- Configure node and port prefixes to route SVC requests to a specific node or logical port. With node and port prefixes, you may take advantage of address registration.
- Configure the port user part of an address (DTE ports only). Address registration combines the port user part with a node or port prefix to route the SVC request.
- Configure SVC port addresses to route SVC requests to a specific logical port when the attached network device does not support address registration.
- Configure a network ID to uniquely identify an inter-exchange carrier (IXC).

Note – You cannot configure ATM SVCs on B-STDX switches or CBX 500 Frame-based modules.

The B-STDX switch does not support the ATM Private Network-to-Network Interface (PNNI) routing protocol.

For information about using Open Shortest Path First (OSPF) name aggregation to minimize prefix and address memory consumption in Lucent network switches, see Appendix G, “OSPF Name Aggregation.”

Configuring Node Prefixes

Node prefixes apply to all ports on the switch and are used for routing aggregation, source address validation, and address registration. You can configure multiple node prefixes on a switch; however, you do not need to configure any if you have port prefixes or port addresses defined on the node.

At the very least, a node prefix consists of the two AFI digits of the AESA address, or at least one digit of the 1-15 digit native E.164 address. You can define the node prefix to be part of or all of the AESA or E.164 address. For example, for E.164 addresses that begin with 508555, you can configure the node prefix as 5 (at a minimum), 50, 508, 5085, etc. The level of granularity you need to define depends on your network.

Node prefixes do not have to be unique to a particular node. For example, you can define node prefix 508 on multiple nodes. However, if you do so, you may need to define port prefixes or port addresses to provide more granularity for routing determination. For example, you may define port prefixes 508551, 508552, and 508553 on the first node, and port prefixes 508554, 508555, and 508556 on the second node.

Defining a Node Prefix

To define a node prefix:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All Node Prefixes. The Set All Node Prefixes dialog box appears.

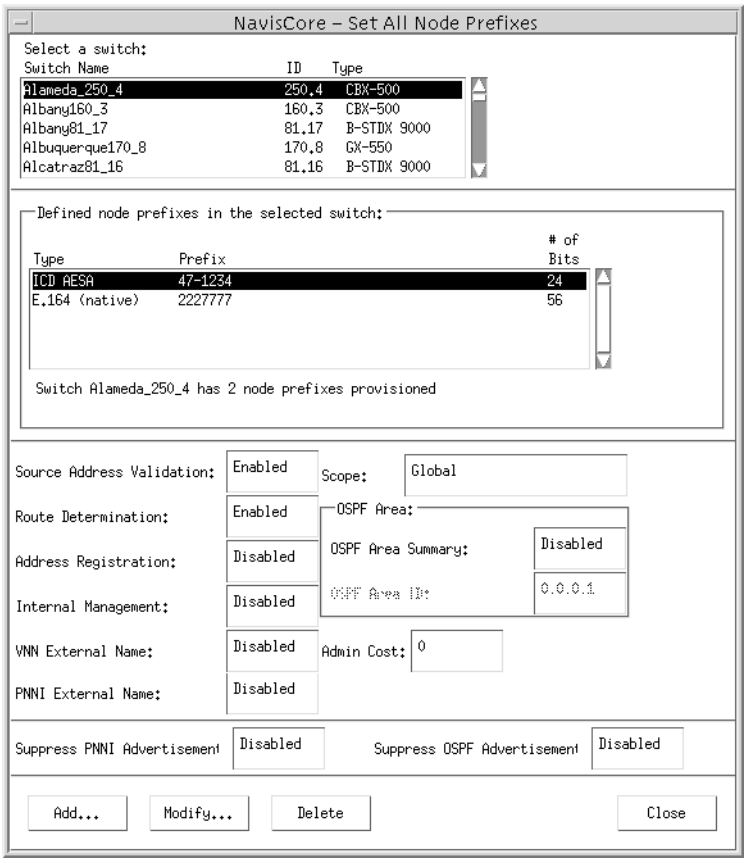


Figure 15-1. Set All Node Prefixes Dialog Box

The top list box (Select a switch:) displays all switches that are accessible from this NMS. The bottom list box (Defined Node Prefixes in the selected Switch:) displays all the node prefixes configured on the selected switch. You can display the address and routing options for each node prefix.

2. From the top list box, select the switch on which to configure node prefixes.
3. Choose Add. The Add Node Prefix dialog box appears (see Figure 15-2 on page 15-5).

4. To define a node prefix for a specific format:
   a. See Table 15-1 to select the address format.
   b. Select the scope. Organizational scope defines how far into a hierarchical PNNI domain the switch should advertise this prefix or address. For more information about PNNI, see Chapter 20, "Configuring PNNI Routing."
   c. Continue with the section that corresponds to the address format you select.

Table 15-1. Address Format Descriptions

Format	Description	See . . .
E.164 Native	Standard 1-15 digit Integrated Services Digital Network (ISDN) number, which includes telephone numbers.	"Native E.164 Node Prefix Format" on page 15-5
DCC AESA	Data country code ATM End System Address (AESA), which identifies the country in which the address is registered.	"DCC and ICD AESA Node Prefix Format" on page 15-6
DCC Anycast AESA	Provides a group address function using DCC AESA address formats. Use the DCC AESA configuration instructions.	"DCC and ICD AESA Node Prefix Format" on page 15-6
ICD AESA	International Country Designator (ICD) AESA, which identifies the international organization to which the address applies.	"DCC and ICD AESA Node Prefix Format" on page 15-6
ICD Anycast AESA	Provides a group address function using ICD AESA address formats. Use the ICD AESA configuration instructions.	"DCC and ICD AESA Node Prefix Format" on page 15-6
E.164 AESA	E.164 AESA, which encapsulates a standard 1-15 digit ISDN number, including telephone numbers.	"E.164 AESA Node Prefix Format" on page 15-7
E.164 Anycast AESA	Provides a group address function using E.164 AESA address formats. Use the E.164 AESA configuration instructions.	"E.164 AESA Node Prefix Format" on page 15-7
Custom AESA	AESA with customized octet structure and customized authority and format identifier (AFI).	"Custom AESA Node Prefix Format" on page 15-9

Native E.164 Node Prefix Format

Complete the following fields for the E.164 (Native) format:

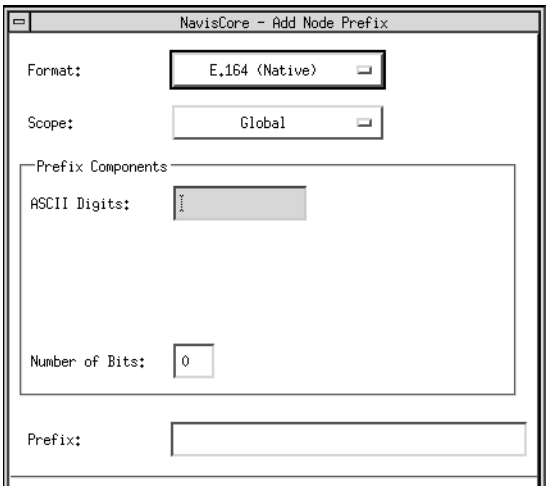


Figure 15-2. Add Node Prefix Dialog Box (E.164 Native Format)

1. In the ASCII Digits field, enter all or part of the 1-15 ASCII digits that represent the E.164 address.

   For example, enter 5085552600 (a standard 10-digit U.S. phone number), or enter a partial number (such as 508). The value you enter is converted to the ASCII hex values that represent each digit in the number. If you entered 5085552600, it converts to 35308385353532363030.

2. Configure the address routing options using the steps on page 15-10, "Defining Address and Routing Options."

3. Choose Ok to return to the Set All Node Prefixes dialog box.

Note – If PNNI is enabled on a switch, Native E.164 addresses can be advertised across the PNNI routing domain. PNNI automatically converts the Native E.164 address format to the ATM E.164 AESA format, which allows the addresses to be advertised as ATM addresses. For more information about PNNI, see Chapter 20, "Configuring PNNI Routing."

DCC and ICD AESA Node Prefix Format

Complete the following information for the DCC or ICD AESA format:

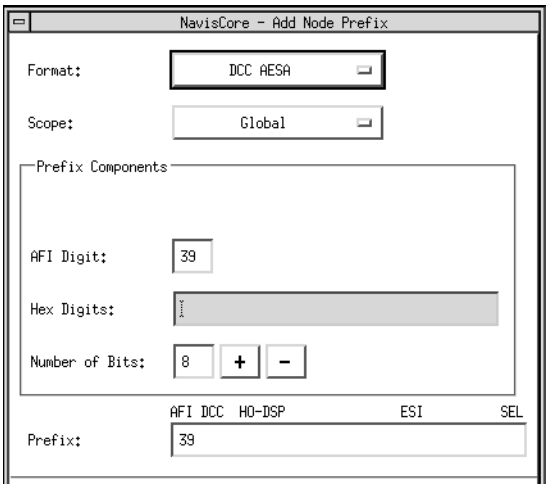


Figure 15-3. Add Node Prefix Dialog Box (DCC or ICD AESA Format)

1. In the Hex Digits field, enter the data country code (DCC) of the country in which the address is registered, or the International Code Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.
2. (*Optional*) Enter the HO-DSP, ESIA, and SEL portions of the address.

   For information on the appropriate format to use for DCC and ICD addresses, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices Interim Link Management Interface (ILMI) prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the Address Registration field set to enabled (see page 15-11).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you type.) Click on the — icon to decrease the number of address bits that are checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

For example, if you enter the partial DCC AESA address 39-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

4. Configure the address routing options using the steps on page 15-10, "Defining Address and Routing Options."

5. Choose Ok to return to the Set All Node Prefixes dialog box (Figure 15-1 on page 15-3). The new entry appears, along with the preceding AFI (39 or 47), in the bottom list box (Defined Node Prefixes in the selected Switch).

E.164 AESA Node Prefix Format

Complete the following information for the E.164 AESA format:

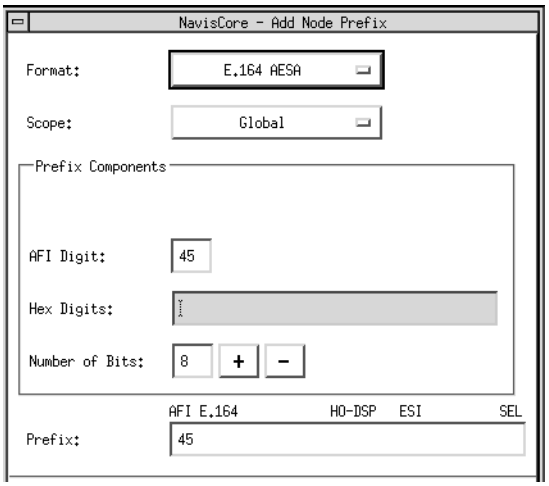


Figure 15-4. Add Node Prefix Dialog Box (E.164 AESA Format)

1. In the Hex Digits field, enter the full or partial E.164 AESA address.

2. If you enter the IDI portion of the address, you can optionally enter the HO-DSP, ESI, and SEL portions. For information about the appropriate format to use for E.164 AESA addresses, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the Address Registration field set to enabled (see page 15-11).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you enter). Click on the — icon to decrease the number of address bits that are checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial E.164 AESA address 45-00000504 (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**45-00000504**
Address in binary (40 bits):	**01000101-00000000000000000000010100000100**
Address in binary (38 bits):	**01000101-00000000000000000000000101000001**

4. Configure the address routing options using the steps on page 15-10, "Defining Address and Routing Options."
5. Choose Ok to return to the Set All Node Prefixes dialog box (Figure 15-1 on page 15-3). The new entry appears, along with the preceding AFI (45), in the bottom list box (Defined Node Prefixes in the selected Switch).

Custom AESA Node Prefix Format

Complete the following fields for the Custom AESA format:

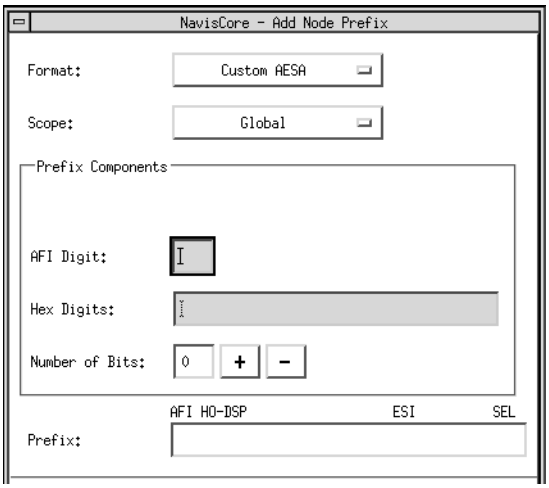


Figure 15-5. Add Node Prefix Dialog Box (Custom AESA Format)

1. In the AFI Digits field, enter the custom AFI you want to use.
2. In the Hex Digits field, enter in the customized address format, starting with the HO-DSP, followed by the ESI and SEL values (in that order).

   This address can be up to 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. You do not have to enter the entire address; the HO-DSP, ESI, and SEL entries are optional. However, you must enter the AFI digits. For information about these items, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports with prefixes that have the Address Registration field set to enabled (see page 15-11).

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits that are checked during call screening and call routing. (The value increases by eight with each pair of address digits you type.) Click the **—** icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

For example, if you enter the partial address 51-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing, click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**51-43BF12AC**
Address in binary (40 bits):	**01010001-01000011110011110001001010111100**
Address in binary (38 bits):	**01010001-0100001111001111000100101011111**

Address you entered:	**51-43BF12A8**
Address in binary (40 bits):	**01010001-01000011110011110001001010111000**
Address in binary (37 bits):	**01010001-0100001111001111000100101011**1

4. See the following section, "Defining Address and Routing Options," to configure the address and routing options.
5. Choose Ok to return to the Set All Node Prefixes dialog box (Figure 15-1 on page 15-3).

Defining Address and Routing Options

The Add Node Prefix dialog box contains fields that allow you to enable or disable the address and routing options.

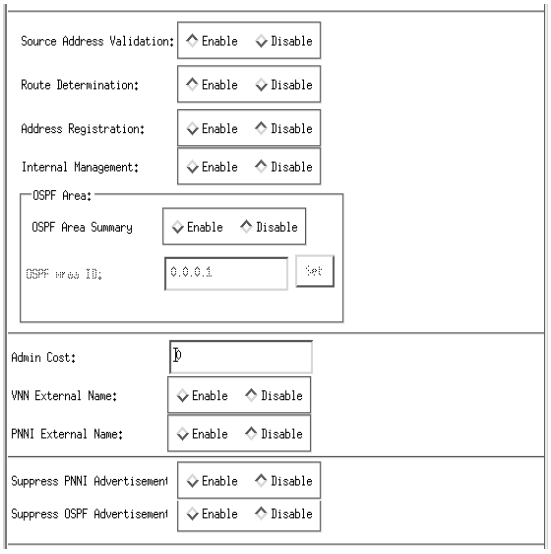


Figure 15-6. Add Node Prefix Address and Routing Fields

Use Table 15-2 to complete these fields.

Table 15-2. Add Node Prefix Address and Routing Fields

Field	Action/Description
Source Address Validation	Select enable to validate the calling party address against the node prefix associated with the UNI/NNI logical port that received the call setup message. If you disable this option, this node prefix is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this node prefix for routing aggregation. If disabled, OSPF does not use it. Enable this option to use PVC/PVP termination (see page 17-2).
Address Registration	If enabled, this node prefix is used for ILMI address registration for all UNI DCE "network-to-endsystem" logical ports that support ILMI. You cannot enable this option for AESA node prefixes that are not 13 octets long.
Internal Management	Select enable to configure the prefix that corresponds to the switch itself as an addressable entity. Select disable to disregard this feature.
OSPF Area Summary	Select enable if the node represents an area border router. Then enter an OSPF Area ID. For more information, see the *B-STDX and CBX IP Services Configuration Guide*.
OSPF Area ID	If you enable OSPF Area Summary, choose Set to select the Area ID. This assigns an OSPF area to a node prefix in cases where the node acts as an area border router. OSPF Area IDs enable the VC manager to determine which way to route the PVC.
Admin Cost	Enter the administrative cost associated with the node prefix. When an SVC is being created, if more than one node in the network is found with the same node prefix, the call is routed to the node that has the lowest administrative cost associated with the node prefix.
VNN External Name	Select enable to advertise this name within the VNN routing domain as an external name. An external name is a name that is reachable within another VNN routing domain. The default, disable, means this name is only reachable within the VNN routing domain.
PNNI External Name	Select enable to advertise this name within the PNNI routing domain as an external name. An external name is a name that is reachable within another PNNI routing domain. The default, disable, means this name is only reachable within the PNNI routing domain.

Table 15-2. Add Node Prefix Address and Routing Fields (Continued)

Field	Action/Description
Suppress PNNI Advertisement	The default, disable, allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group. Select enable to prevent advertising this address across the PNNI domain.
Suppress OSPF Advertisement	The default, disable, allows this address to be advertised across the VNN OSPF routing domain. Select enable to prevent advertising this address across the VNN OSPF routing domain.

Configuring SVC Port Prefixes

The Set All Port Prefixes function enables you to define how calls are routed to the port. Port prefixes are also used for calling party screening.

To define a port prefix:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVCParameters ⇒ Set All Port Prefixes. The Set All Port Prefixes dialog box appears (Figure 15-7).

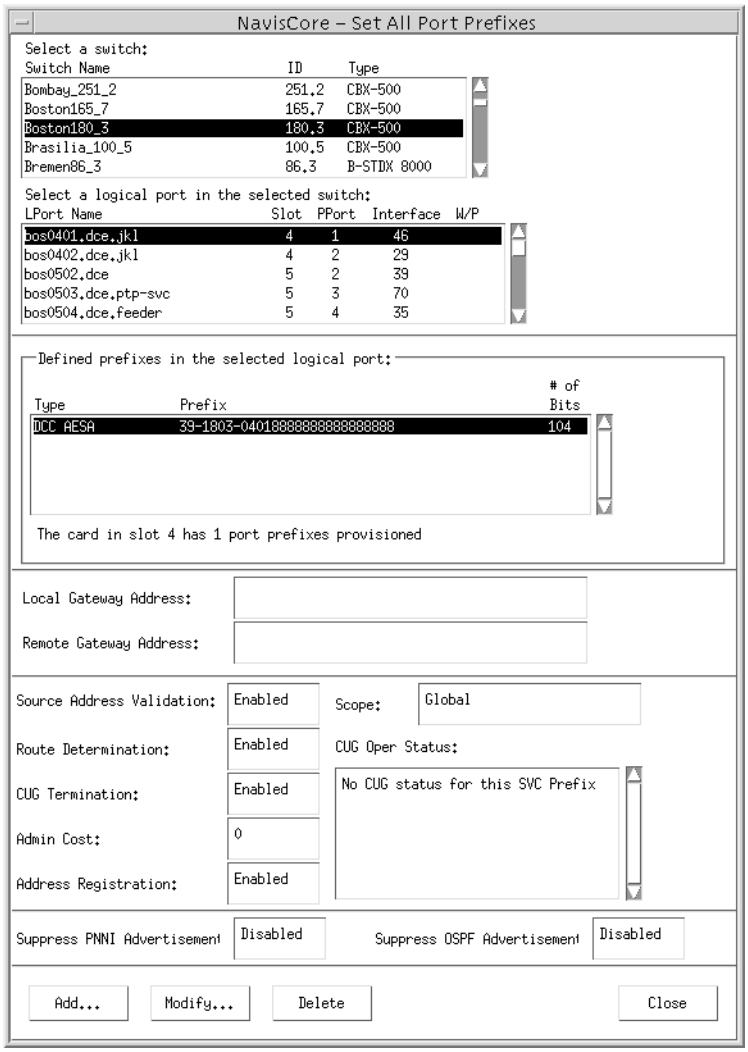


Figure 15-7. Set All Port Prefixes Dialog Box

- The Select a switch: list box displays all switches that this NMS can access.
- The Select a logical port in the selected switch: list box displays the logical ports that are configured for the selected switch, along with the slot, physical port, and MIB interface number for the logical port.
- The Defined prefixes in the selected logical port: list box displays all port prefixes that have already been defined on the selected logical port. You can display configured options for each of these prefixes.

2. Select the switch on which to configure a port prefix.
3. Select the logical port on which to configure a port prefix.
4. Choose Add. The Add Prefix dialog box appears (Figure 15-8 on page 15-15).
5. Select an address format and scope. See page 15-4 for a description of these attributes.
6. Continue with the section that corresponds to the address format you select.

Format	See
E.164 Native	page 15-15
DCC (Anycast) AESA	page 15-16
ICD (Anycast) AESA	page 15-16
E.164 (Anycast) AESA	page 15-17
Custom AESA	page 15-19
Default Route	page 15-23

E.164 Native Prefixes Port Prefix Format

Complete the following fields for the E.164 native prefix format:

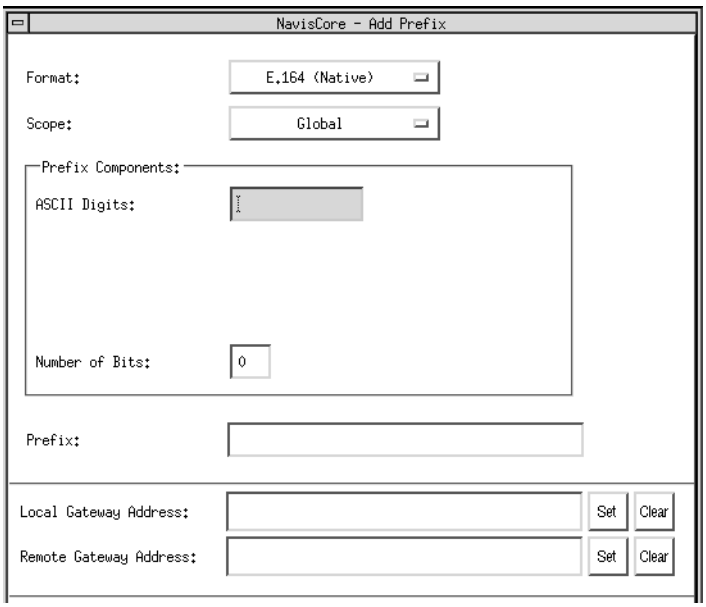


Figure 15-8. Add Prefix Dialog Box (E.164 Native Format)

1. In the ASCII Digits field, enter all or part of the 1-15 ASCII digits that represent the E.164 address.

   For example, enter 5085552600 (a standard 10-digit U.S. phone number), or enter a partial number (such as 508). The value you enter is converted to the ASCII hex values that represent each digit in the number. If you entered 508555260, it converts to 35308385353532363030.

2. If the port provides a network-to-network connection, see "Setting the Local and Remote Gateway Address for Port Prefixes" on page 15-21 for instructions. When done, proceed to step 3.

3. See Table 15-3 on page 15-24 to configure additional port prefix options.

4. Choose Ok to return to the Set All Port Prefixes dialog box (Figure 15-7 on page 15-13).

DCC and ICD AESA Port Prefix Format

Complete the following fields for the DCC or ICD AESA prefix format:

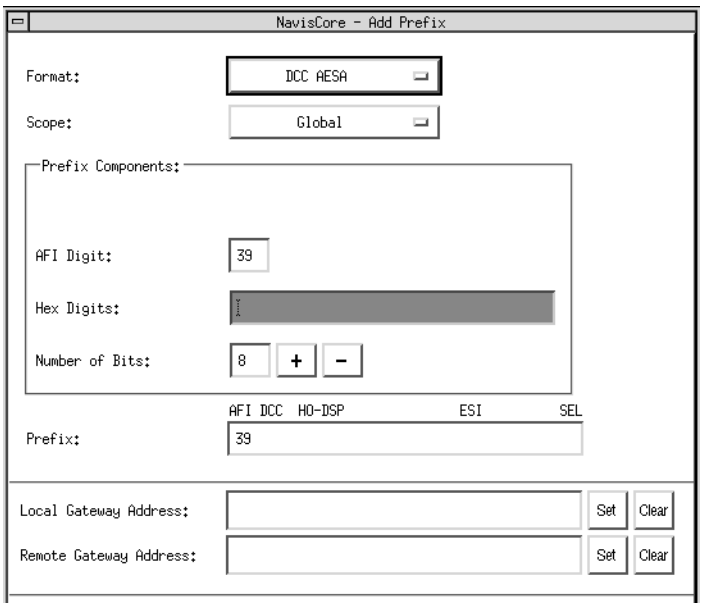


Figure 15-9. Add Prefix Dialog Box (DCC and ICD AESA Format)

1. In the Hex Digits field, enter the data country code (DCC) of the country in which the address is registered, or the International Code Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.
2. (*Optional*) Enter the HO-DSP, ESIA, and SEL portions of the address.

   For information on the appropriate format to use for DCC and ICD addresses, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening and call routing. (The value increases by eight with each address digit you type). Click the **—** icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

For example, if you enter the partial DCC AESA address 39-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two digits are binary 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**39-43BF12AC**
Address in binary (40 bits):	**00111001-0100001111001111000100101011110 0**
Address in binary (38 bits):	**00111001-010000111100111100010010101111**

Address you entered:	**39-43BF12A8**
Address in binary (40 bits):	**00111001-0100001111001111000100101011100 0**
Address in binary (37 bits):	**00111001-010000111100111100010010101 11**

4. If the port provides a network-to-network connection, see "Setting the Local and Remote Gateway Address for Port Prefixes" on page 15-21 for instructions. When done, proceed to step 5.
5. See Table 15-3 on page 15-24 to configure additional port prefix options.
6. Choose Ok to return to the Set All Port Prefixes dialog box (Figure 15-7 on page 15-13). The new entry appears, along with the preceding AFI (39 or 47), in the Defined prefixes in the selected logical port list box on the bottom half of the screen.

E.164 AESA Port Prefix Format

Complete the following fields for the E.164 AESA prefix format:

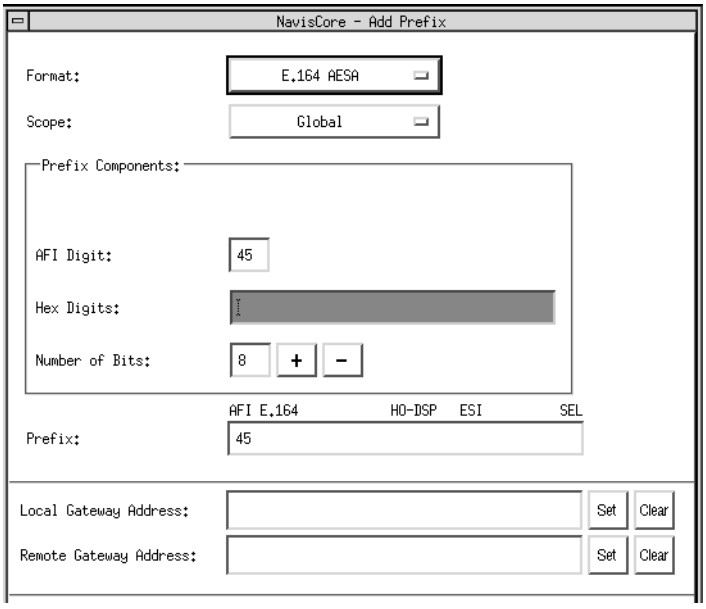


Figure 15-10. Add Prefix Dialog Box (E.164 AESA Format)

1. In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh.
2. If you enter the IDI portion of the address, you can optionally enter the HO-DSP, ESI, and SEL portions. For example, if you enter the IDI portion as 000005085551234F, you can then enter all or some of the remaining parts. For information on the appropriate format to use for E.164 addresses, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening and call routing. (The value increases by eight with each pair of address digits you type). Click the — icon to decrease the number of address bits checked, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

   For example, if you enter the partial E.164 AESA address 45-00000504 (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing (because the last two binary digits are 00), click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**45-00000504**
Address in binary (40 bits):	**01000101-0000000000000000000000010100000100**
Address in binary (38 bits):	**01000101-0000000000000000000000101000001**

4. If the port provides a network-to-network connection, see "Setting the Local and Remote Gateway Address for Port Prefixes" on page 15-21 for instructions. When done, proceed to step 5.
5. See Table 15-3 on page 15-24 to configure additional port prefix options.
6. Choose Ok to return to the Set All Port Prefixes dialog box (Figure 15-7 on page 15-13). The new entry appears, along with the preceding AFI (45), in the Defined prefixes in the selected logical port list box.

Custom AESA Port Prefix Format

Complete the following fields for the Custom AESA prefix format:

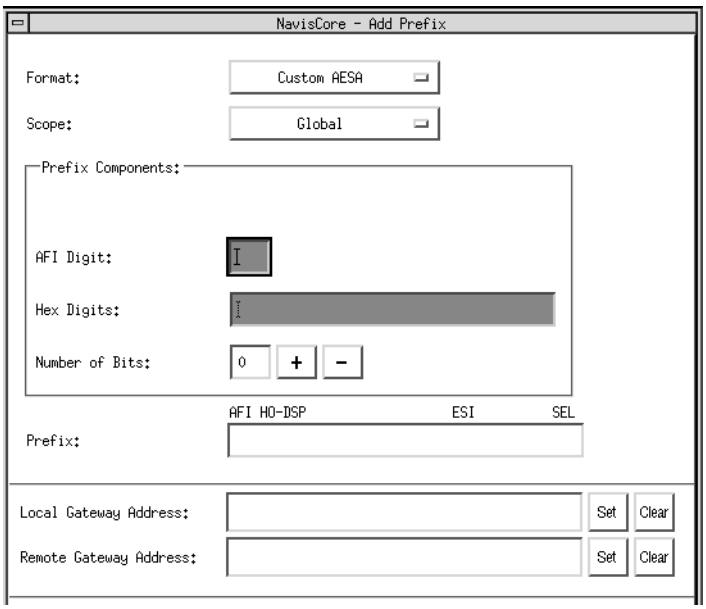


Figure 15-11. Add Prefix Dialog Box (Custom AESA Format)

1. In the AFI Digits field, enter the custom AFI you want to use.
2. In the Hex Digits field, type in the customized address format, starting with the HO-DSP, followed by the ESI and SEL values (in that order). This address can be up to 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. You do not have to enter the entire address; the HO-DSP, ESI, and SEL entries are optional. However, the AFI digits are required. For information on these items, see "ATM End System Address (AESA) Formats" on page 14-2.

Note – To register the AESA address in the attached DTE devices' ILMI prefix table, enter exactly the first 13 octets (26 digits) of the AESA address. Address registration occurs only on ILMI-enabled UNI ports.

3. As you type the address, the value in the Number of Bits field changes to indicate the number of address bits checked during call screening/call routing. (The value increases by eight with each address digit you type). Click the — icon to decrease the number of address bits, thereby enabling the node to perform call screening and call routing down to the bit level. You can decrease the value by 1-7 bits.

For example, if you enter the partial address 51-43BF12AC (which uses 40 bits) as the port prefix, but only need to check the first 38 bits of the port prefix for call screening and call routing, click the — icon until the value in the Number of Bits field is 38.

Address you entered:	**51-43BF12AC**
Address in binary (40 bits):	**01010001-0100001111001111000010010101111100**
Address in binary (38 bits):	**01010001-0100001111001111000100101011111**

Address you entered:	**51-43BF12A8**
Address in binary (40 bits):	**01010001-0100001111001111000010010101111000**
Address in binary (37 bits):	**01010001-0100001111001111000100101011**

4. If the port provides a network-to-network connection, see "Setting the Local and Remote Gateway Address for Port Prefixes" on page 15-21 for instructions. When done, proceed to step 5.
5. See Table 15-3 on page 15-24 to configure additional port prefix options.
6. Choose Ok to return to the Set All Port Prefixes dialog box (Figure 15-7 on page 15-13).

Setting the Local and Remote Gateway Address for Port Prefixes

This section describes how to set the optional local and remote gateway addresses for ports that are providing a network-to-network connection. Local and remote gateway addresses are used in conjunction with the egress address translation feature (see page 14-12).

Figure 15-12 shows which addresses to enter as the local and remote gateway addresses for each end of the network-to-network connection.

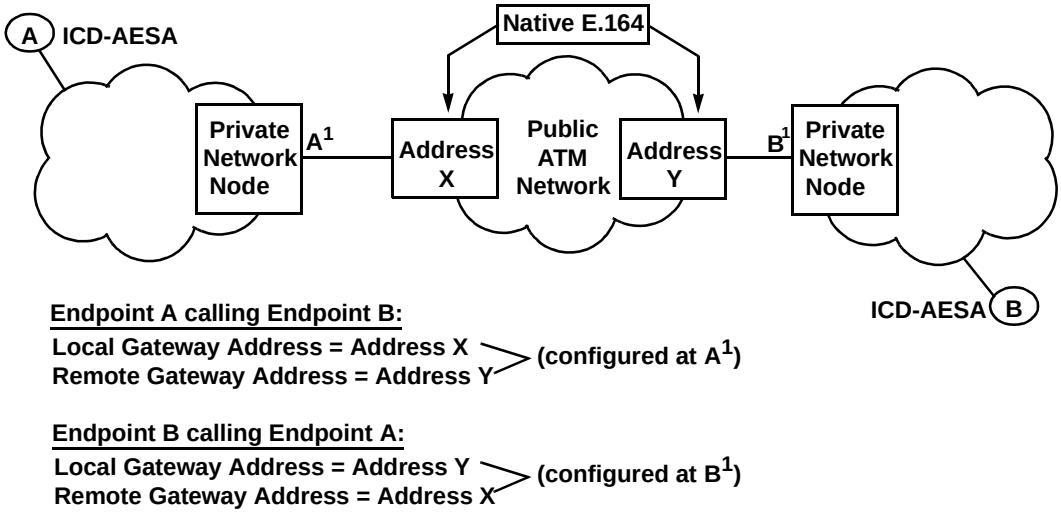


Figure 15-12. Setting Local and Remote Gateway Addresses

You can configure prefixes on a network-to-network port with the following:

- Null local and remote gateway addresses
- Only a local gateway address
- Only a remote gateway address
- Both a local and a remote gateway address

Note – You need to define gateway addresses for address translation only. For more information on egress address translation, see page 14-12.

To set the local (or remote) gateway address:

1. From the Add Prefix dialog box (Figure 15-8 on page 15-15), choose the Set button. The Set Local (or Remote) Gateway Address dialog box appears.

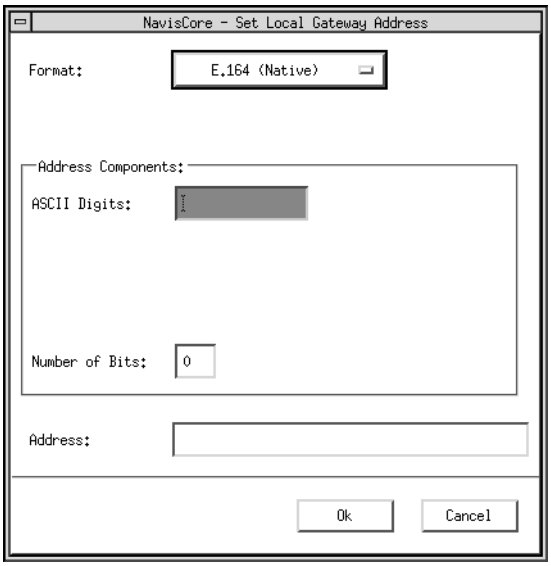


Figure 15-13. Set Local Gateway Address Dialog Box

2. Select the local (or remote) gateway address format from the Format field.
3. If you want to specify the local gateway address, enter the address of the public network gateway used to enter the public network. If you want to specify the remote gateway address, enter the address of the public network gateway used to exit from the public network back to the private network.
4. When done, choose Ok to return to the Add Prefix dialog box.
5. To configure additional port prefix options, see Table 15-3 on page 15-24.

Defining Default Routes for Network-to-Network Connections

For ports being used for network-to-network connections, you can define a default route (which is automatically assigned 0x00 as its address, with a length of 0 bits).

If the network receives a call and the calling party address does not match any port prefixes or addresses, it routes the call to the port on which the default route is defined. If more than one port has a default route defined, then the administrative cost value is used to determine the port to which the call is routed.

Note – It is important that you define a port address for calling/called party addresses. Admin cost is not always the criteria for routing a call, because the call can be placed out of the same interface on which it was received.

You can define multiple default routes within a node or network. The default route typically applies to network-to-network logical ports (Interim Inter-switch Signaling Protocol [IISP] or public UNI DTE).

Complete the following fields for a default route:

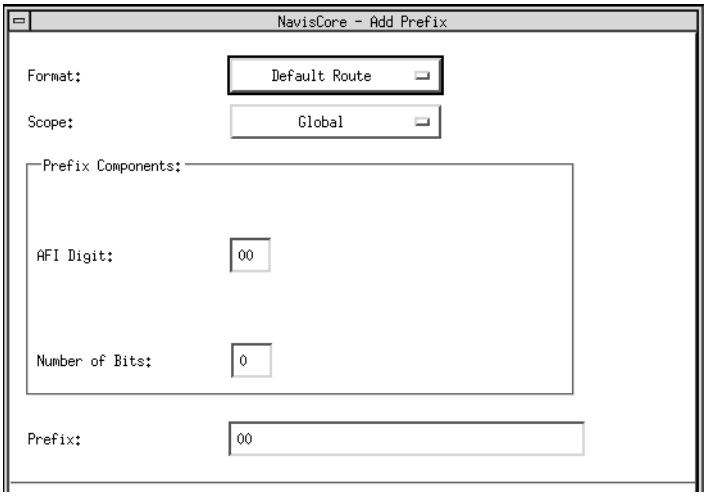


Figure 15-14. Add Prefix Dialog Box (Default Route)

1. In the Format field, select Default Route.
2. See Table 15-3 on page 15-24 to configure additional port prefix options.
3. Choose Ok to return to the Set All Port Prefixes dialog box.

Defining Port Prefix Options

When you add a port prefix, the Add Prefix dialog box contains fields which allow you to enable or disable the following options, as shown in Figure 15-15.

Figure 15-15. Add Port Prefix Option Fields

Use Table 15-3 to configure these options.

Table 15-3. Add Port Prefix Option Fields

Field	Action/Description
Source Address Validation	Select Enable to validate the calling party address against the port prefix associated with the UNI/NNI port that received the call setup message. If you disable this option, this port prefix is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this port prefix for route determination. If disabled, OSPF registration is not used. Enable this option to use PVC/PVP termination (see page 17-2).
CUG Termination	Select Enable to use this prefix as part of a closed user group (CUG). Incoming and outgoing calls with a calling or called party address that matches this prefix are subject to CUG security checks. For more information on CUGs, see Chapter 18, "Closed User Groups (CUGs)."
Admin Cost	Enter the administrative cost associated with the port prefix. When an SVC is being created, if more than one port in the network is found with the same port prefix, the call is routed to the port in the network that has the lowest administrative cost associated with the port prefix.
Address Registration	If enabled, port prefixes are used for ILMI address registration if ILMI is enabled on this logical port. This option cannot be enabled for AESA port prefixes that are not 13 octets long.

Table 15-3. Add Port Prefix Option Fields (Continued)

Field	Action/Description
Suppress PNNI Advertisement	The default, Disable, allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group. Select Enable to prevent the advertising of this address across the PNNI domain.
Suppress OSPF Advertisement	The default, Disable, allows this address to be advertised across the VNN OSPF routing domain. Select Enable to prevent advertising this address across the OSPF routing domain.

Configuring SVC Port Addresses

If the device attached to a given physical port does not support ILMI address registration, or to fully specify an address to use for calling party screening, you can define SVC addresses for all the logical ports on a given physical port. The AESA formats must have full-length address definitions and include all 20 octets (40 hex digits). That is, you must enter the AFI, IDI, HO-DSP, ESI, and SEL portions of the address. (Since ATM routing does not use the SEL portion, you can enter any value for that part of the address.) For native E.164 addresses, you enter the 1-15 digit E.164 address.

About Automatic Assignment of ESI Bytes

An SVC port address is created by appending a 13-byte node prefix with a six-byte ESI portion, followed by a selector byte. This 20-byte address can then be used as an SVC or SPVC endpoint.

The six-byte ESI portion can be automatically generated and assigned by NavisCore. These six bytes are defined based on the shelf, slot, physical port, and logical port IDs and can only be created automatically if node prefixes are already configured on the switch. The automatic assignment of ESI bytes can be done for both VNN and PNNI domains.

Note – If the node prefix is configured to be less than 13 bytes, zeros will be appended to the node prefix when the Auto ESI feature is used. Similarly, if the node prefix is greater than 13 bytes, the bytes over 13 will be truncated by the Auto ESI feature.

Table 15-4 shows how the bits and bytes of the address are assigned.

Table 15-4. ESI Byte Assignments

Number of bits/bytes	Contents/Purpose	Range/Interpretation
13 bytes	Node prefix	Remains unchanged
12 bits	Reserved for future use.	Fixed - 0x000
8 bits	Slot information If Pport is in a GX 550 ES, these bits will indicate the BIO slot in the GX 550 to which the GX 550 ES is connected.	0x00 - Slot number 0 0x01 - Slot number 1 . . . 0x10 - Slot number 16

Table 15-4. ESI Byte Assignments (Continued)

Number of bits/bytes	Contents/Purpose	Range/Interpretation
4 bits	Quadrant information	• **B-STDX or CBX switch** – 0x0 • **GX 550 ES Extender Shelf** – 0x1 - the GX 550 ES is connected to quadrant 1 in the GX 550 switch – 0x2 - the GX 550 ES is connected to quadrant 2in the GX 550 switch – 0x3 - the GX 550 ES is connected to quadrant 3 in the GX 550 switch – 0x4 - the GX 550 ES is connected to quadrant 4 in the GX 550 switch • **GX 550 Switch** – 0xa - Quadrant 1 in GX 550 – 0xb - Quadrant 2 in GX 550 – 0xc - Quadrant 3 in GX 550 – 0xd - Quadrant 4 in GX 550
8 bits	Physical port information	A range of 0x00 to 0xff represents physical ports from 0 to 255. • 1 - 64 => CBX, B-STDX, or CBX • 1 - 16 => GX 550 without a GX 550 ES • 1 - 12 => GX 550 ES connected to a GX 550
16 bits	Interface ID	Ranges from 0x0000 to 0xffff
8 bits	Selector ID	Fixed - 0x00

Note – The GX 550 and CBX 500 switches support the automatic ESI assignment feature for both VNN and PNNI. B-STDX 9000 switches will only support it for VNN.

The steps in the following sections present both the manual method of populating the ESI bytes and the automatic assignment. There may be certain situations where one method is favored over the other.

To configure SVC port addresses:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All Port Addresses. The Set All Port Addresses dialog box appears (Figure 15-16).

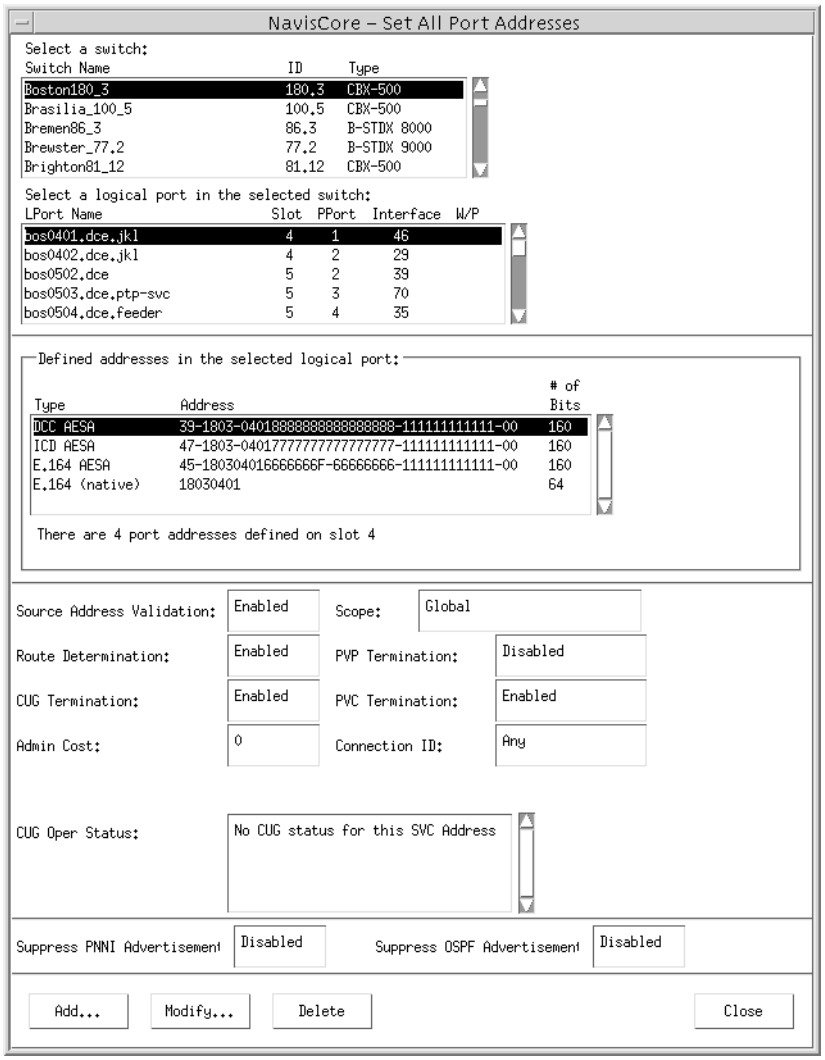


Figure 15-16. Set All Port Addresses Dialog Box

- The top list box (Select a switch) displays all switches that the NMS can access.

- The center list box (Select a logical port in the selected switch:) displays the logical ports that are configured on the selected switch.
- The bottom list box (Defined addresses in the selected logical port:) displays any SVC addresses that you already defined on the selected logical port.

2. Select the switch on which to configure SVC addresses.
3. Select the logical port on which to configure SVC addresses.
4. Choose Add. The Add Address dialog box appears (Figure 15-17).

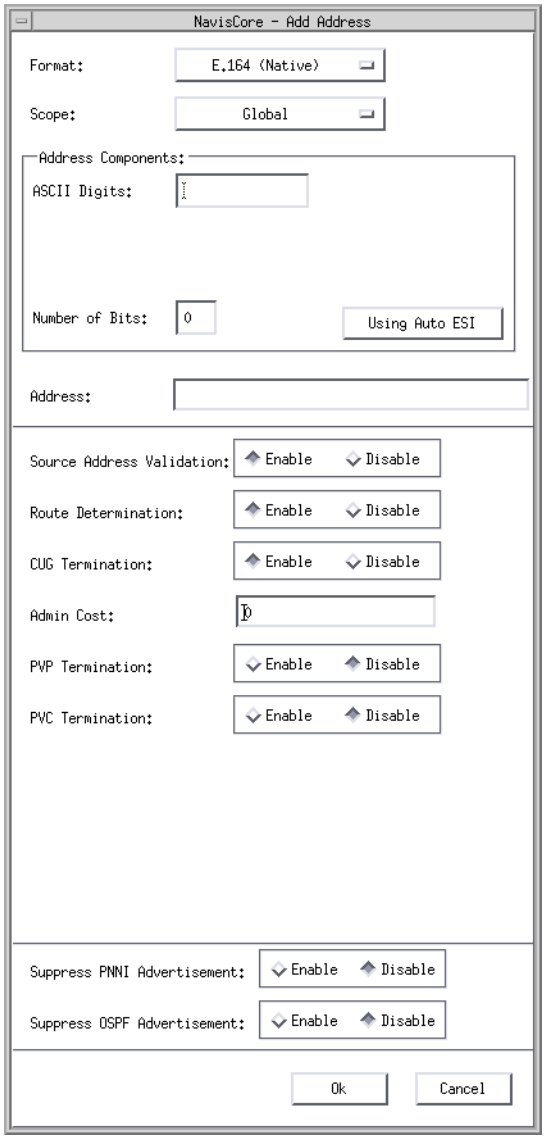


Figure 15-17. Add Address Dialog Box

5. Select an address format and scope. See page 15-4 for a description of these attributes.

6. Continue with the section that corresponds to the address format you select.

Format	See . . .
E.164 Native	page 15-31
DCC (Anycast) AESA	page 15-32
ICD (Anycast) AESA	page 15-32
E.164 (Anycast) AESA	page 15-34
Custom AESA	page 15-35

Native E.164 SVC Address Format

Complete the following fields for E.164 (Native) SVC address format:

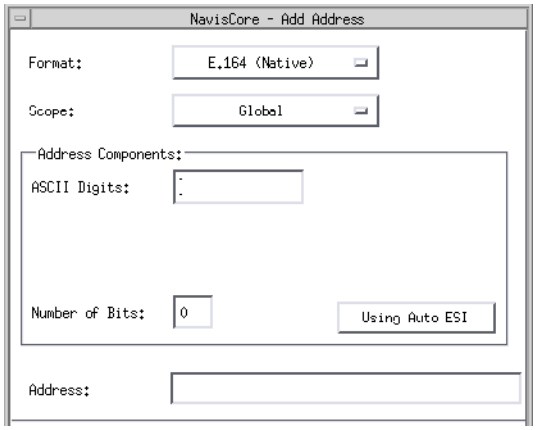


Figure 15-18. Add Address Dialog Box (Native E.164 SVC Address Format)

Note – Auto ESI Assignment cannot be used for Native E.164 or X.121 formats since only 15 bytes are required and Auto ESI Assignment will create a 20-byte address.

1. In the ASCII Digits field, enter all of the 1-15 ASCII digits that represent the E.164 address. For example, enter 5085552600 (a standard 10-digit U.S. phone number). The value you enter is converted to the ASCII hex values that represent each digit in the number. For example, 5085552600 converts to 35303835353532363030.
2. See Table 15-5 on page 15-36 to configure additional fields.
3. Choose Ok to return to the Set All Port Addresses dialog box (Figure 15-16 on page 15-28).

DCC and ICD AESA SVC Address Format

Complete the following fields for DCC or ICD AESA format:

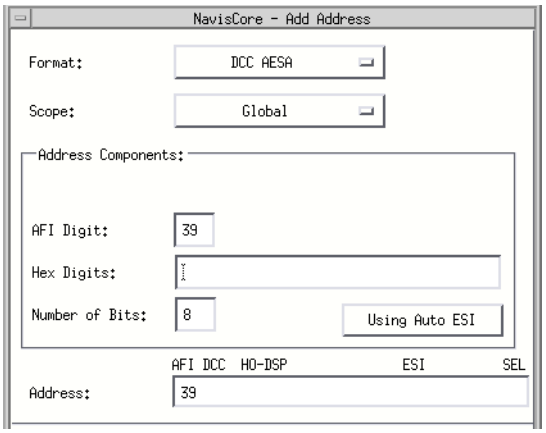


Figure 15-19. Add Address Dialog Box (DCC or ICD AESA Format)

1. If you want to create the address manually, continue with the steps a, b, and c below. If you want Auto ESI Assignment to create the address, go to step 2 below.
   a. In the Hex Digits field, enter the data country code (DCC) of the country in which the address is registered, or the International Code Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets.
   b. Enter the appropriate HO-DSP, ESIA and SEL values. For information on these items, and the appropriate format to use for DCC and ICD AESA addresses, see "ATM End System Address (AESA) Formats" on page 14-2.
   c. See Table 15-5 on page 15-36 to configure additional fields. Continue to step 6.
2. Choose Using Auto ESI.
3. The Set All Node Prefix w/Auto ESI dialog box will display (Figure 15-20 on page 15-32).

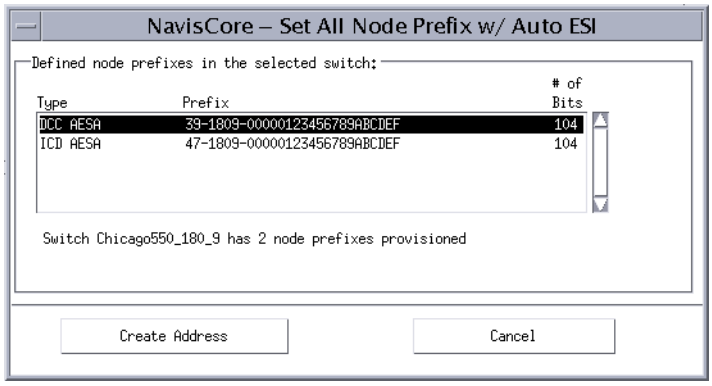


Figure 15-20. Set All Node Prefix w/Auto ESI Dialog Box

4. From the list of defined node prefixes, select a node prefix of the same type as the address you wish to configure.
5. Choose Create Address to have NavisCore automatically assign the six ESI bytes and the selector byte to the node prefix listed in the list box. The Set All Node Prefix w/Auto ESI dialog box will close and the full 20-byte address will appear in the Address field in the Add Address dialog box.
6. Choose Ok to return to the Set All Port Addresses dialog box (Figure 15-16 on page 15-28).

E.164 AESA SVC Address Format

Complete the following fields for the E.164 AESA format:

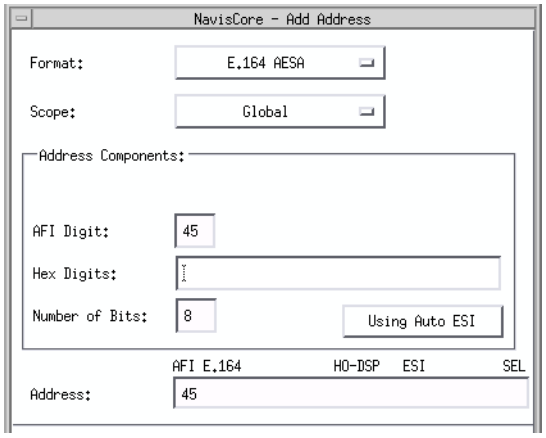


Figure 15-21. Add Address Dialog Box (E.164 AESA Format)

1. If you want to create the address manually, continue with the steps a, b, and c below. If you want Auto ESI Assignment to create the address, go to step 2 below.
   a. In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with F. For example, enter 5085551234 as 000005085551234F.
   b. After you type the IDI portion of the address, enter the appropriate HO-DSP, ESI, and SEL portions to complete the address. For information on the appropriate format to use for E.164 AESA addresses, see "ATM End System Address (AESA) Formats" on page 14-2.
   c. See Table 15-5 on page 15-36 to configure additional fields. Continue to step 6.
2. Choose Using Auto ESI.
3. The Set All Node Prefix w/Auto ESI dialog box will display (Figure 15-20 on page 15-32).
4. From the list of defined node prefixes, select a node prefix of the same type as the address you wish to configure.
5. Choose Create Address to have NavisCore automatically assign the six ESI bytes and the selector byte to the node prefix listed in the list box. The Set All Node Prefix w/Auto ESI dialog box will close and the full 20-byte address will appear in the Address field on the Add Address dialog box.
6. Choose Ok to return to the Set All Port Addresses dialog box (Figure 15-16 on page 15-28).

Custom AESA SVC Address Format

Complete the following fields for the Custom AESA format:

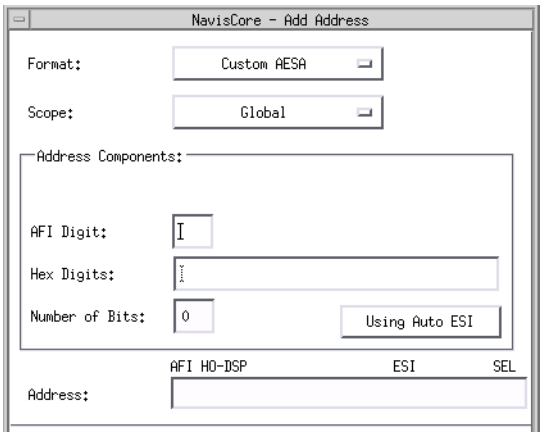


Figure 15-22. Add Address Dialog Box (Custom AESA Format)

1. In the AFI Digit field, enter the custom AFI value.
2. In the Hex Digits field, enter the customized address format, starting with the HO-DSP, followed by the ESI and SEL values (in that order).

   This address must be the full 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL. For information on these items, see "ATM End System Address (AESA) Formats" on page 14-2.
3. See Table 15-5 on page 15-36 to configure additional fields.
4. Choose Using Auto ESI.
5. The Set All Node Prefix w/Auto ESI dialog box will display (Figure 15-20 on page 15-32).
6. Choose Create Address to have NavisCore automatically assign the six ESI bytes and the selector byte to the node prefix listed in the list box. The Set All Node Prefix w/Auto ESI dialog box will close and the full 20-byte address will appear in the Address field on the Add Address dialog box.
7. Choose Ok to return to the Set All Port Addresses dialog box (Figure 15-16 on page 15-28).

Defining SVC Port Address Options

The Add Address dialog box contains fields that allow you to enable or disable the following options.

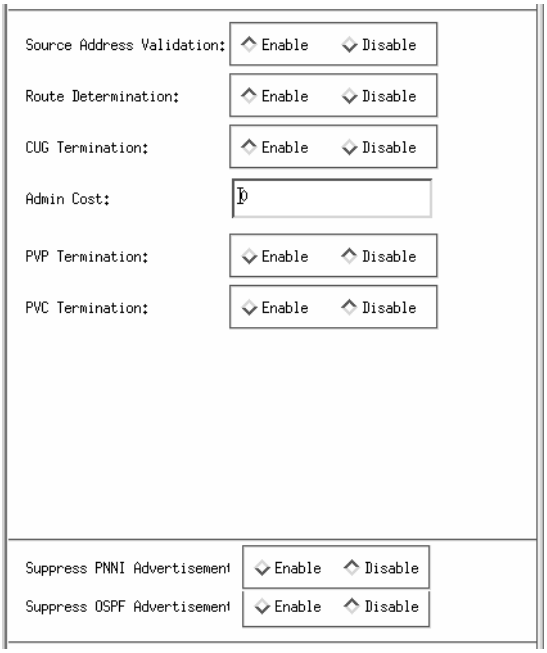


Figure 15-23. Add SVC Port Address Option Fields

Use Table 15-5 to configure the options shown in Figure 15-23. The PVP and PVC Termination options are described in the following sections, "Configuring PVP Termination" and "Configuring PVC Termination."

Table 15-5. Add SVC Port Address Option Fields

Field	Action/Description
Source Address Validation	Select Enable to validate the calling party address against the UNI/NNI port address that received the call setup message. If you disable this option, this address is not used to validate calling party addresses.
Route Determination	If enabled, the OSPF protocol uses this address for route determination. Enable this option to use PVC/PVP termination (see page 17-2).
CUG Termination	Select Enable to use this address as part of a closed user group (CUG). Incoming and outgoing calls with a calling or called party address that match this address are subject to CUG security checks. For more information about CUGs, see Chapter 18, "Closed User Groups (CUGs)."

Table 15-5. Add SVC Port Address Option Fields (Continued)

Field	Action/Description
Admin Cost	Enter the administrative cost associated with the port address. When an SVC is being created, if more than one port in the network is found with the same port address, the call is routed to the port in the network that has the lowest administrative cost associated with the port address.
Suppress PNNI Advertisement	The default, Disable, allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group. Select Enable to prevent the advertising of this address across the PNNI domain.
Suppress OSPF Advertisement	The default, Disable, allows this address to be advertised across the VNN OSPF routing domain. Select Enable to prevent advertising this address across the OSPF routing domain.

If you are using soft PVCs in your network, continue with the following section, "Configuring PVP Termination." Otherwise, choose Ok to return to the Set All Port Addresses dialog box (Figure 15-16 on page 15-28).

Configuring PVP Termination

Enable this option to terminate an SPVC to this address on the logical port. If you select Enabled, the Connection ID field appears (Figure 15-24).

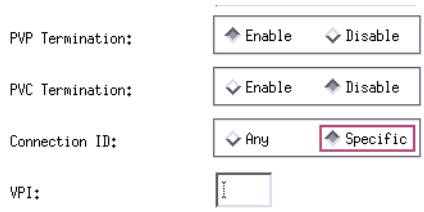


Figure 15-24. PVP Termination Fields

Complete the following fields:

Connection ID — Select Any if you want the network to allocate a VPI for the SPVPC. Select Specific to supply a VPI. Note that if you enable PVC termination, this field is set to Any and cannot be changed.

VPI — Enter the VPI of the logical port on which you want the switch to terminate this SPVPC. The logical port cell header type limits the range of values you can enter: UNI = 255, NNI = 4095.

For more information about SPVCs, see "About Point-to-Point SPVCs" on page 17-5.

Configuring PVC Termination

Enable this option to terminate an SVC (spoofing) or SPVCC to this address on this logical port. If you select Enabled, the Connection ID field (Figure 15-25) appears.

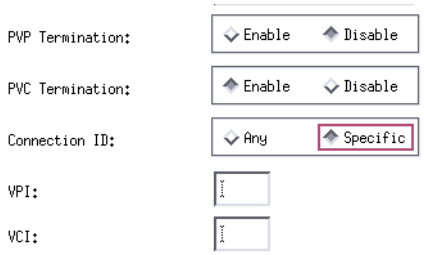


Figure 15-25. PVC Termination Fields

Complete the following fields:

Connection ID — Select Any if you want the network to allocate a VPI/VCI for the spoofed SVC or terminated SPVCC. Select Specific to supply a VPI/VCI value. Note that you cannot select Specific if you also enable PVP Termination.

VPI/VCI — Enter the VPI/VCI of the logical port on which you want the switch to terminate this SPVCC.

Configuring the Port User Part of the Address

The port user part of an AESA address consists of the ESI and SEL portions of the address. It is used for the DTE (user) ports on a Lucent switch and provides information for the address table on the DCE device attached to the UNI on the public network side (see "About Address Registration" on page 14-8). When the attached DCE device receives prefixes, the user part(s) are concatenated to form full addresses. The full addresses are then written back to the DCE device's ILMI address table.

When you configure the port user part to complete an address connection with the attached DCE device, you can supply any 7-octet value as the user part (it does not have to be a real IEEE MAC address and SEL combination). Also, you should enter any user addresses in your network that you want to make known to the attached public network. To do this, collect Media Access Control (MAC) addresses from attached devices and enter them as user parts at the public UNI port.

You may have to define user parts only on UNI DTE ports where the device attached to that port expects address registration completion. That is, the attached device is broadcasting its network prefixes to the Lucent port, and expects the Lucent switch to respond with the user part of the address.

Defining a Port User Part

To define the port user part of the address:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All Port User Parts. The Set all Port User Parts dialog box appears.

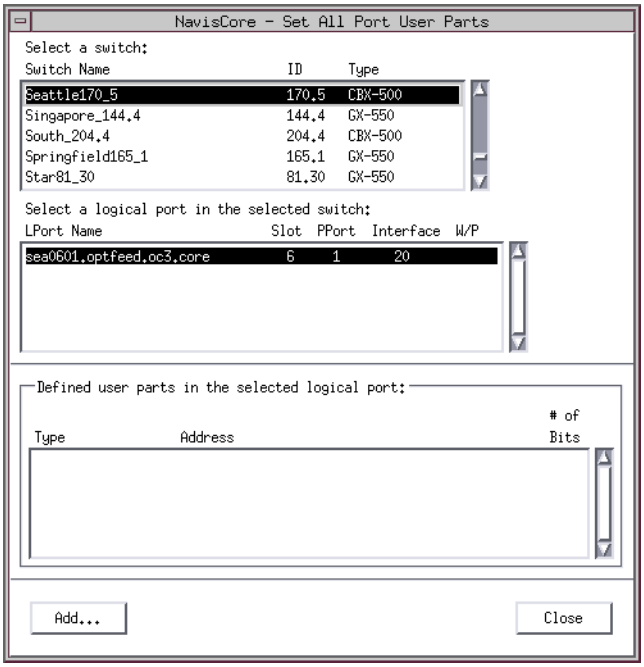


Figure 15-26. Set All Port User Parts Dialog Box

- The Select a switch list box displays all switches that this NMS can access.
- The Select a logical port in the selected switch list box displays the UNI-DTE logical ports that are configured for this switch.
- The Defined user parts in the selected logical port list box displays any user parts you already defined for this logical port.

2. In the Switch Name list box, select the switch on which you want to configure port user parts. The logical ports configured on the selected switch appear in the LPort Name list box.
3. In the LPort Name list box, select the logical port on which you want to configure user parts. If any user parts are already configured for this logical port, they appear in the list box at the bottom of the dialog box.

4. Choose Add. The Add User Part dialog box appears.

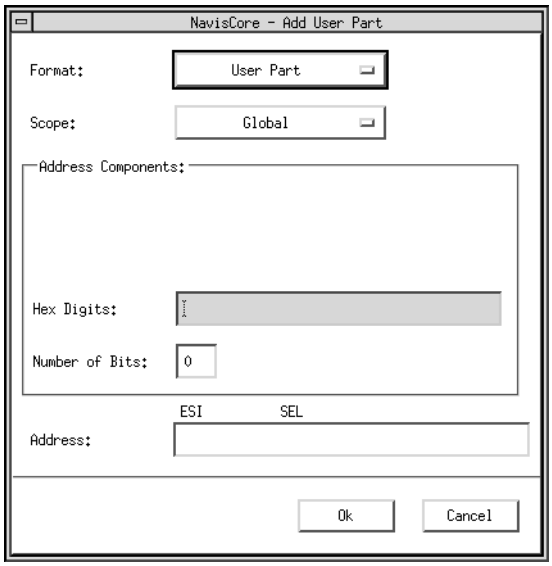


Figure 15-27. Add User Part Dialog Box

5. Enter the 7-octet (14-digit) user part in the Hex Digits field.
6. When done, choose Ok to return to the Set All Port User Parts dialog box (Figure 15-26 on page 15-40).

Defining Network ID Parameters

You can add, delete, and modify network IDs. For an overview of network ID features, see page 14-17.

Adding Network IDs

To add a network ID:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All Port Network IDs. The Set All Port Network IDs dialog box appears.

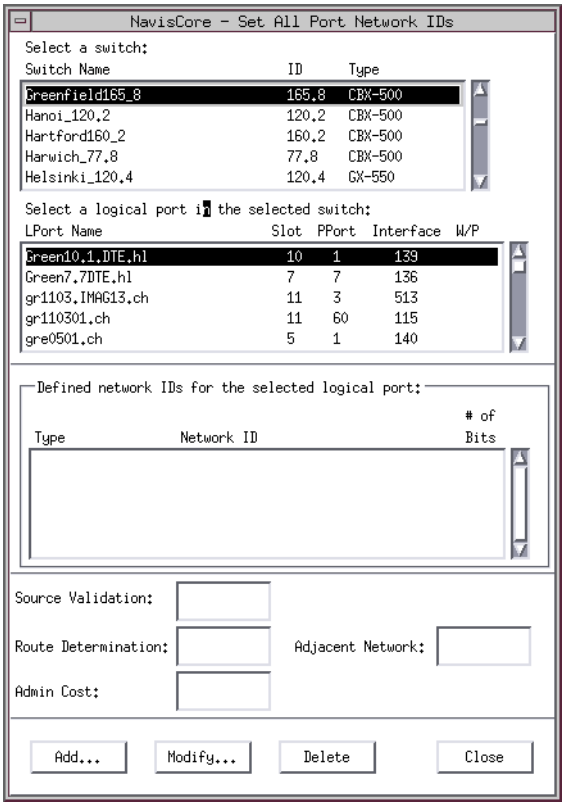


Figure 15-28. Set All Port Network IDs Dialog Box

Complete the Set All Port Network IDs fields in Table 15-6.

Table 15-6. Set All Port Network IDs Dialog Box Fields

Field	Action/Description
Select a Switch	Displays the Switch Name, ID, and Type for all existing switches in the network.
Select a logical port in the selected switch	Displays the LPort Name, Slot, PPort, and Interface for all ATM UNI and NNI, and Frame Relay UNI logical ports for the selected switch.
Defined Network IDs for the selected LPort	Displays the Type, Network ID, and # of Bits for all Network IDs created for the selected logical port.
Source Validation	Displays Enabled or Disabled for the selected Network ID.
Route Determination	Displays Enabled or Disabled for the selected Network ID.
Adjacent Network	Displays Enabled or Disabled for the selected Network ID.
Admin Cost	Displays the admin cost for the selected Network ID.

2. To add a network ID, select a switch name from the Select a switch list box and then select a logical port from the Select a logical port in the selected switch list box.

3. Choose Add. The Add Network ID dialog box appears.

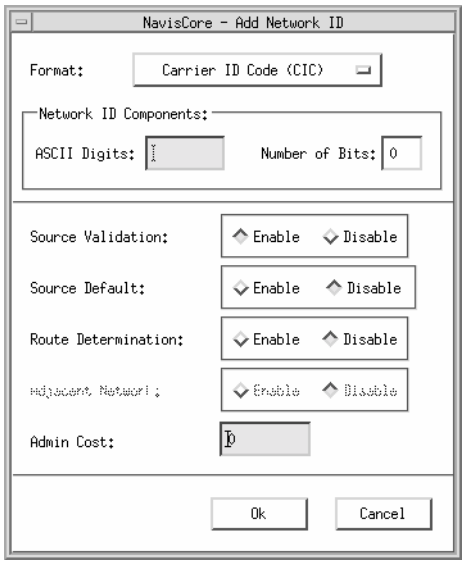


Figure 15-29. Add Network ID Dialog Box

4. Complete the Add Network ID fields described in Table 15-7.

Table 15-7. Add Network ID Dialog Box Fields

Field	Action/Description
Format	Select an ID format. Options include: *Carrier Identification Code (CIC)* *Data Network ID Code (DNIC)*
ASCII Digits	Enter a number between 0-9 for CIC or DNIC formats. CIC IDs are 3-, 4-, or 8-digit values. DNIC IDs are 4 digit values.
Number of Bits	Displays the number of bits in the network ID.
Source Validation	Enable (default) or Disable source validation for this network ID. When enabled, a signaled TNS may be screened against this network ID. If you enable this field, route determination is disabled and the source default parameter becomes active.
Source Default	Enable or Disable (default) source default for this network ID. Only one network ID on each port may have this attribute. When enabled, this network ID represents the preferred IXC for user calls originating on this logical port.
Route Determination	Enable or Disable (default) route determination for this network ID. If you enable this field, source validation is disabled and the adjacent network parameter becomes active.

Table 15-7. Add Network ID Dialog Box Fields (Continued)

Field	Action/Description
Adjacent Network	Enable or Disable (default) adjacent network for this network ID. This information is used by billing. Only one network ID on each logical port may have this attribute. When enabled, this network ID is considered to be the adjacent network (as opposed to another network reachable through the actual adjacent network). This adjacent network ID will not be signaled from this logical port.
Admin Cost	Enter an admin cost between 0 - 65535 for this network ID. The default is 0 (zero).

5. Choose Ok to add the network ID.
6. Choose Cancel to exit the dialog box.

Modifying a Network ID

To modify an existing network ID:

1. From the Set All Port Network IDs dialog box (Figure 15-28 on page 15-42), select the desired network from the Defined Network IDs for the selected logical port list box.
2. Choose Modify.
3. Modify the network ID parameters. You can not modify the Format or the ASCII Digits fields.
4. Choose OK to modify the network ID and exit the dialog box.
5. Choose Cancel to exit the dialog box.

Deleting a Network ID

To delete an existing network ID:

1. From the Set All Port Network IDs dialog box (Figure 15-28 on page 15-42), select the desired network from the Defined Network IDs for the selected logical port list box.
2. Choose Delete. The selected network is deleted from the list.
3. Choose Close to exit the dialog box.

16

Configuring SVC Proxy Signaling

Switched virtual circuit (SVC) proxy signaling is an optional CBX 500 switch and GX 550 Multiservice WAN switch feature that enables a single signaling entity to signal on behalf of multiple endpoints. You can use proxy signaling to allow endsystems that do not understand ATM signaling to set up SVCs via a proxy signaling agent (PSA). The PSA performs all signaling functions on behalf of the endsystem, known as the proxy signaling client (PSC).

Before you can configure the PSA and PSC, use the instructions in Chapter 3, "Configuring CBX 500 or GX 550 Logical Ports," to configure the ATM UNI DCE logical ports.

About Proxy Signaling

The following terms are used to define proxy signaling functions:

Proxy signaling agent (PSA) — The network port attached to the signaling entity that performs signaling for non-signaling entities. In the Lucent implementation, a PSA is an ATM UNI DCE logical port for which signaling is enabled.

Proxy signaling client (PSC) — The network port attached to the endsystem for which a PSA performs signaling duties. In the Lucent implementation, a PSC is an ATM UNI DCE logical port for which signaling is disabled.

You can use proxy signaling to enable high-end ATM equipment to support multiple physical interfaces that share the same ATM address. This application provides high-end equipment with the ability to support connections that have an aggregate bandwidth which exceeds the physical interface line rate. The individual connection(s) must be at a rate that is less than or equal to the line rate.

Proxy signaling enables a “smart device” to signal on behalf of a “dumb” device (see Figure 16-1). It allows high-end devices with multiple network interface cards (NICs) to use a single signaling channel. In this instance, you use proxy signaling to allow a single signaling entity (PSA) to signal on behalf of multiple, non-signaling endsystems (PSC). This application extends the ATM signaling protocol to endsystems that do not necessarily understand ATM signaling.

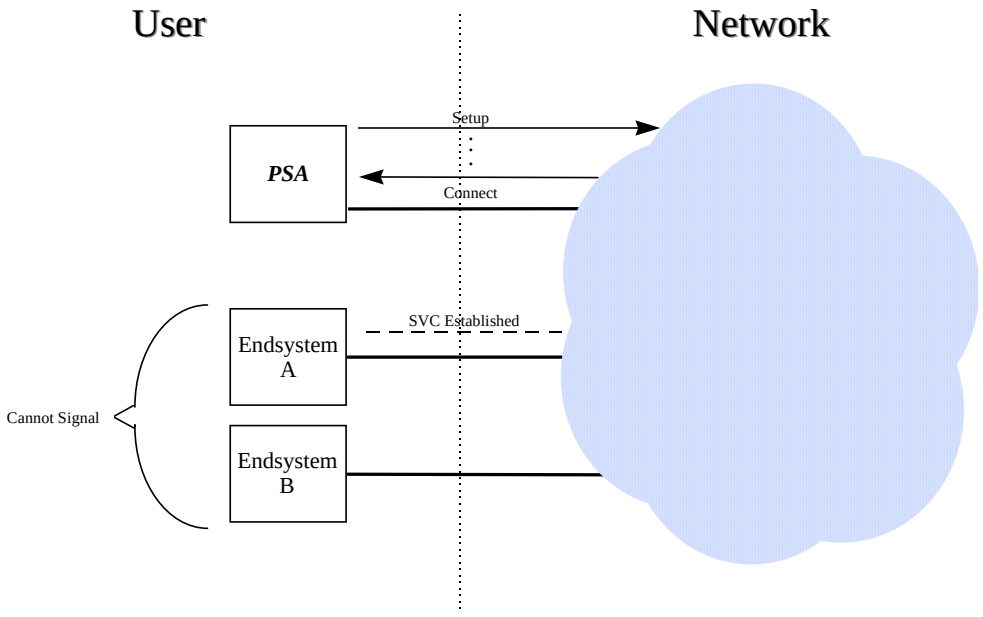


Figure 16-1. Establishing SVCs for Endsystem via Proxy Signaling Agent (PSA)

Proxy Signaling Agent

To define SVC proxy signaling functions, you must first configure the ILMI/Signaling/OAM attributes for an ATM UNI DCE logical port, and set the Proxy Admin Status to Agent. Signaling must be enabled (see "ILMI/Signaling/OAM Attributes" on page 3-28).

Acting as the PSA, the UNI DCE port uses VPI/VPCI mapping to determine if a particular SVC request is destined for a PSC. With UNI 4.0 signaling, VPCI mapping provides an alias that represents the PSC's logical port and VPI address. Each PSC needs a unique VPCI. For example, using the Add VPCI Attributes dialog box (Figure 16-4 on page 16-6), configure the following VPCI mapping on a PSA port:

- VPCI 1 means VPI 0 on port 12
- VPCI 2 means VPI 0 on port 13

If the SVC request does not include a VPCI (UNI 3.X signaling), the PSA port performs a routing lookup on the calling party address to determine the appropriate PSC. It matches the calling party address to a logical port, and then uses the VPCI that corresponds to the logical port.

Proxy Signaling Client

To define SVC proxy signaling functions, you must first modify the ILMI/Signaling/OAM attributes for a UNI DCE logical port, and set the Proxy Admin Status to Client. Signaling is disabled for this UNI DCE logical port. For each PSC, you select the switch/logical port combination that represents the controlling PSA.

Note – If you are using Lucent's VNN trunk protocol, clients and agents may reside on different switches; if you are using PNNI, clients and agents must reside on the same switch.

VPCI/SVC Address Association

There is no direct association between VPCIs and SVC addresses. The SVC address can be associated with a VPCI because the address is configured on a logical port that corresponds to the VPCI. For example, if VPCI 1 represents VPI 3 on logical port 4 and logical port 4 is configured for SVC address 5085551212, then the address 5085551212 is implicitly associated with VPCI 1.

With this configuration, an incoming SVC request at the PSA port that specifies VPCI 1 is set up on logical port 4 (proxy on VPCI); an SVC request with no VPCI selected and a calling party address of 5085551212 is also set up on logical port 4 (proxy on calling party).

Configuring the Proxy Signaling Agent

To configure the PSA:

1. Use the instructions beginning on page 3-2 to access the Set All Logical Ports in PPort dialog box.
2. Use the instructions beginning on page 3-10 to configure an ATM UNI DCE logical port. Complete the sections "Administrative Attributes" on page 3-14 and "ATM Attributes" on page 3-22.
3. Use the Set Attributes pull-down menu to access "ILMI/Signaling/OAM Attributes" on page 3-28.
4. Set the Signaling Admin Status to Enabled.
5. Select Agent in the Proxy Signaling Admin Status field. Figure 16-2 shows the Set ILMI/Signaling/OAM Attributes options.

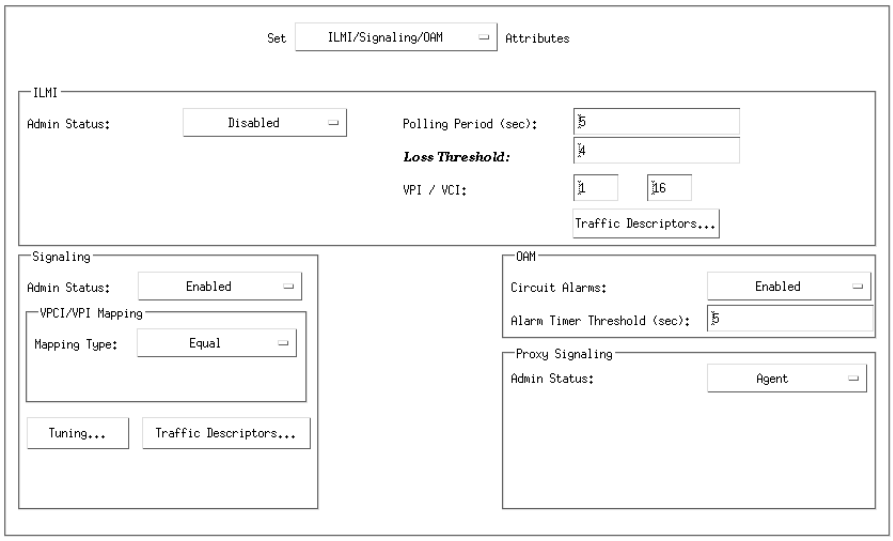


Figure 16-2. Set ILMI/Signaling/OAM Attributes (Agent) Fields

6. Continue with the instructions beginning on page 3-43 to configure the remaining logical port attributes (including SVC Attributes) and return to the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4).

   Once you have defined these basic logical port attributes, you must modify this logical port to define the VPCI table. Continue with the following section, "Configuring the VPCI Table."

Configuring the VPCI Table

To configure the VPCI table:

1. From the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4), select the PSA logical port and choose Modify.
2. Choose Ok to acknowledge the logical port type.
3. Use the Set Attributes pull-down menu to access ILMI/Signaling/OAM Attributes fields.
4. In the VPCI/VPI Mapping box, set Mapping Type to Table.
5. Choose the Set Table button to display the Set VPCI Table in Logical Port dialog box.

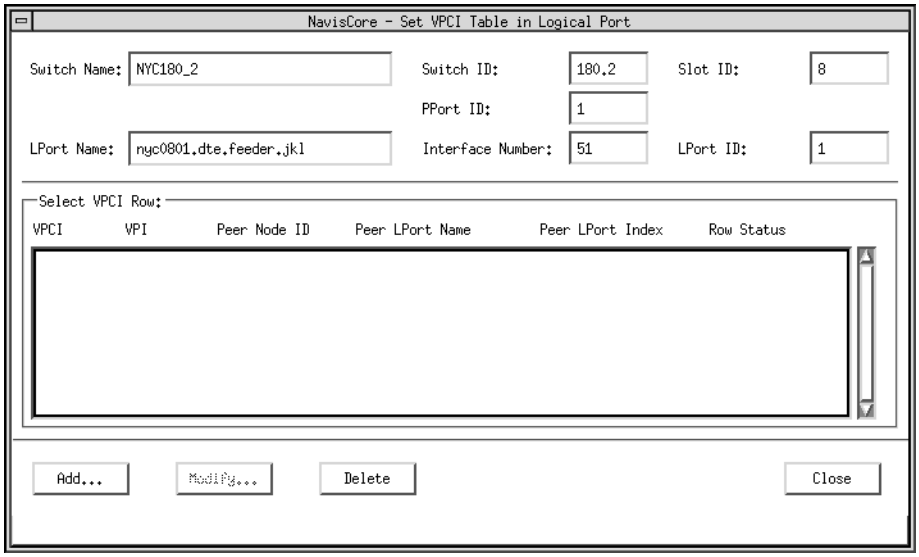


Figure 16-3. Set VPCI Table in Logical Port Dialog Box

The Set VPCI Table in Logical Port dialog box presents a series of screens that enable you to add or delete a row in the VPCI table. Each row in the VPI/VPCI table corresponds to the VPI/VPCI of the switch/logical port combination that represents the proxy signaling client (PSC).

6. Choose Add to create a VPI/VPCI combination. The Add VPCI Attributes dialog box appears.

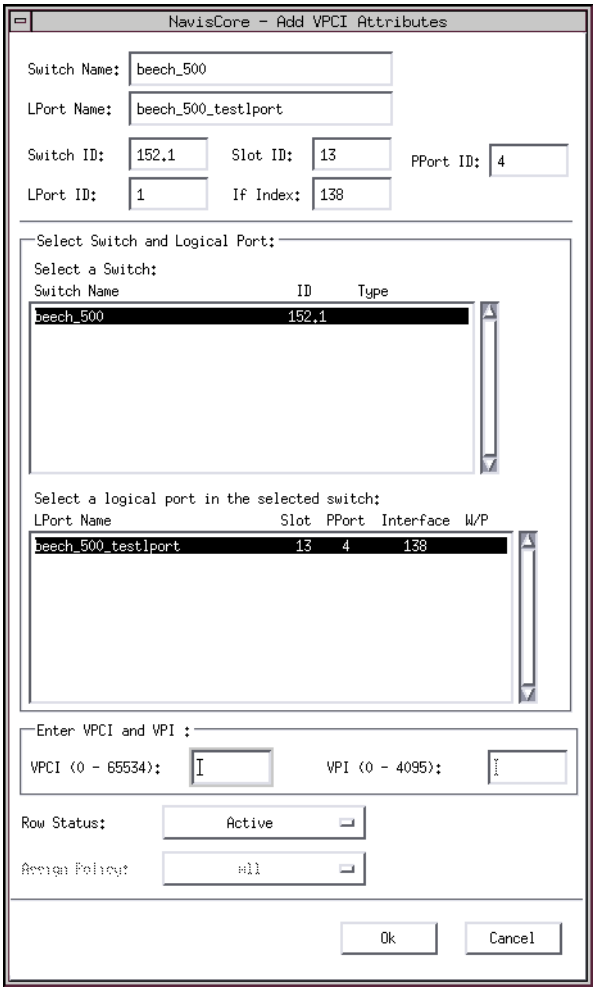


Figure 16-4. Add VPCI Attributes Dialog Box

7. Select the switch and logical port combination that identifies the PSC.
8. Enter values for the VPCI and VPI that identify the PSC.
9. Select Row Status. Active assigns this VPCI/VPI combination to the PSC; Inactive saves this VPCI/VPI combination in the database for future use.
10. Choose Ok to return to the Modify Logical Port dialog box.
11. Choose Ok to complete the PSA table configuration.

Configuring the Proxy Signaling Client

To configure the PSC:

1. Use the instructions beginning on page 3-2 to access the Set All Logical Ports in PPort dialog box.
2. Use the instructions beginning on page 3-7 to configure an ATM UNI DCE logical port. Complete the sections "Administrative Attributes" on page 3-14 and "ATM Attributes" on page 3-22.
3. Use the Set Attributes pull-down menu to access the ILMI/Signaling/OAM Attributes fields (see Figure 16-5).
4. Set the Signaling Admin Status to Disabled (default).
5. Select Client in the Proxy Signaling Admin Status field. The Proxy Signaling attributes appear as shown in Figure 16-5.

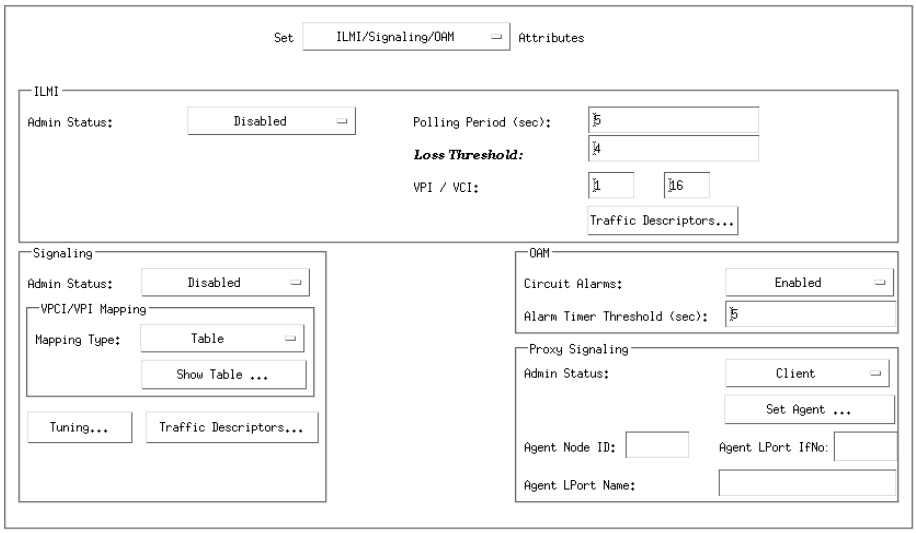


Figure 16-5. Set ILMI/Signaling/OAM Attributes (Client) Fields

6. Choose Set Agent. The Select Agent Switch and Logical Port dialog box appears.

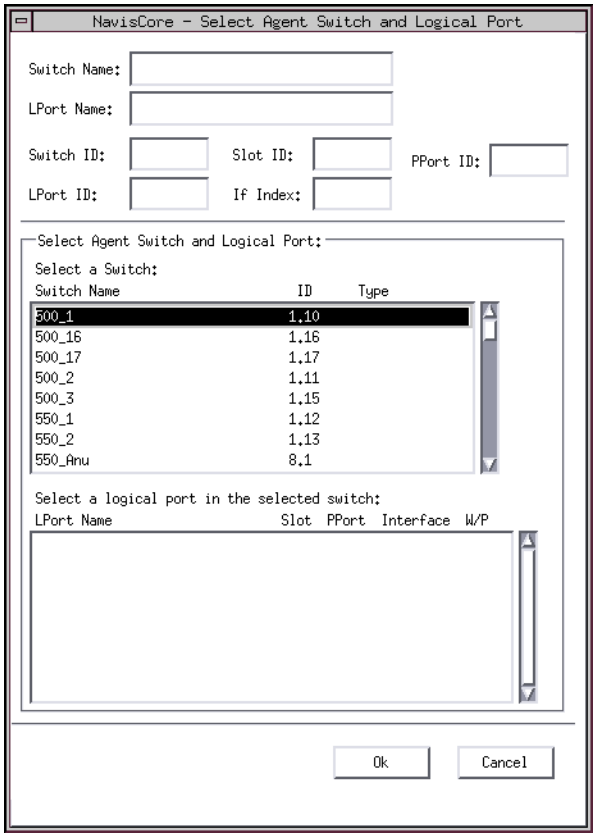


Figure 16-6. Select Agent Switch and Logical Port Dialog Box

7. Select the switch and logical port combination that identifies the PSA.
8. Choose Ok to return to the Add Logical Port dialog box.
9. Continue with the instructions beginning on page 3-43 to configure the remaining logical port attributes. You do not need to configure SVC signaling parameters for this logical port.

17

Configuring SPVCs

A permanent virtual circuit (PVC) is established administratively (that is, by network management) rather than on demand (that is, using signaling across the UNI). A soft PVC (SPVC) is established by the network using signaling. Once the SPVC configuration is in place, the switch at one end of the SPVC initiates the signaling. This release supports up to 4096K SPVCs per card.

The network management system provisions one end of the SPVC with the address identifying the egress interface from the network. The calling end has the responsibility for establishing, releasing, and re-establishing the call.

Note – The B-STDX switch does not support the SPVC feature. You also cannot configure SPVCs on CBX 500 Frame-based modules.

About SPVCs

There are two types of ATM virtual connections: virtual channel connections (VCCs) and virtual path connections (VPCs). These virtual connections are made up of a series of virtual links which form a path between two endpoints. Based on the type of virtual connection you are using (VCC or VPC), you can create either a soft permanent virtual channel connection (SPVCC) or a soft permanent virtual path connection (SPVPC).

When working with SPVCs, you can configure a connection that is point-to-point or point-to-multipoint. In a point-to-multipoint configuration, the CBX/GX endpoint defined as the root can access several terminating endpoints (configured as leaves).

When you create an SPVC, you configure one endpoint (known as the *originating endpoint*) as you would a PVC. You select the logical port on which the endpoint will reside, and assign a virtual path identifier/virtual channel identifier (VPI/VCI) value. You configure the other endpoint(s) (known as the *terminating endpoints*) with addresses, as you would an SVC. Optionally, you may also specify the remote VPI/VCI values. The originating endpoint uses signaling to access the terminating endpoints.

If you configure the terminating endpoint with a port prefix, the connected device must signal the port address. Specifying just the port prefix is not enough information. The address must be advertised by the endpoint for the SPVC to connect.

Using PVC/PVP Termination

Before you can configure SPVCs, you must first configure the SVC address or prefix you want to assign to the SPVC terminating endpoint. This endpoint may not actually terminate the SPVC. When you configure an SVC port address, you enable or disable PVC/PVP termination. If you disable termination, the egress logical port signals the SPVC on as a regular SVC.

PVC and PVP termination enable you to send calls through the network to a non-SVC endpoint, using an SVC. Table 17-1 on page 17-3 shows the results of using PVC/PVP termination.

As you configure PVC/PVP termination, consider the following:

- If you enable PVC termination, you can optionally specify a VPI/VCI or allow the SPVC originator or the network to choose a VPI/VCI. The switch terminates the SPVCC on the logical port that is associated with the VPI/VCI, and the traffic then continues on the local PVC segment.
- If you enable PVP termination, you can optionally specify a VPI or allow the SPVC originator or the network to choose a VPI, and the CBX 500 terminates the SPVPC on the associated logical port.

- If you enable both PVC and PVP termination, you must allow the SPVC originator or the network to select the VPI/VCI or VPI.

  For more information about configuring PVC/PVP Termination on the SVC, see page 15-37.

Specifying the Target Select Type

The originating endpoint may optionally specify the remote VPI or VPI/VCI for an SPVC. This feature is called the Target Select Type. A target select type of Any means that the appropriate VPI or VPI/VCI has been locally configured at the terminating endpoint or that the network is free to select a VPI or VPI/VCI.

A target select type of Specified means that the terminating endpoint is obligated to use a specific VPI or VPI/VCI, as determined by the originating endpoint. This information is propagated by signaling. However, use of the Specified target select type has the following limitations:

- You have Lucent equipment at both the originating and terminating endpoints. As long as this is the case, the connecting portion of the network can contain network equipment from any vendor, using any protocol.
- You only have Lucent equipment at one endpoint, but the SPVC traverses only Lucent Virtual Network Navigator (VNN) or PNNI links. Some LAN-based ATM networks currently support the PNNI protocol.
- If the SPVC must traverse UNI or IISP links, and one end of the SPVC is not Lucent equipment, you cannot use the Specified target select type.

Table 17-1 summarizes the results of using SPVC target select type in conjunction with PVC/PVP termination.

Table 17-1. SPVC Target Select Type

Originating Endpoint Target Select Type	Terminating Endpoint Termination Type	Behavior at Terminating Endpoint
Any	Any	Network allocates any available VPI or VPI/VCI.
Any	Specified VPI or VPI/VCI	Accept SPVC on a specified VPI or VPI/VCI. The SVC port address is dedicated to terminating this single SPVC.
Specified VPI or VPI/VCI	Any	Accept SPVC on a specified VPI or VPI/VCI; the SVC port address may terminate additional SPVCs.

Table 17-1. SPVC Target Select Type (Continued)

Originating Endpoint Target Select Type	Terminating Endpoint Termination Type	Behavior at Terminating Endpoint
Specified VPI or VPI/VCI	Specified VPI or VPI/VCI	Accept SPVC if VPI or VPI/VCI match; reject SPVC if they do not match. The SVC port address is dedicated to terminating this single SPVC.

About Point-to-Point SPVCs

To access the Set All Point-to-Point SPVCs dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Soft PVC Parameters ⇒ Point-to-Point. The Set All Point-to-Point SPVCs dialog box appears.

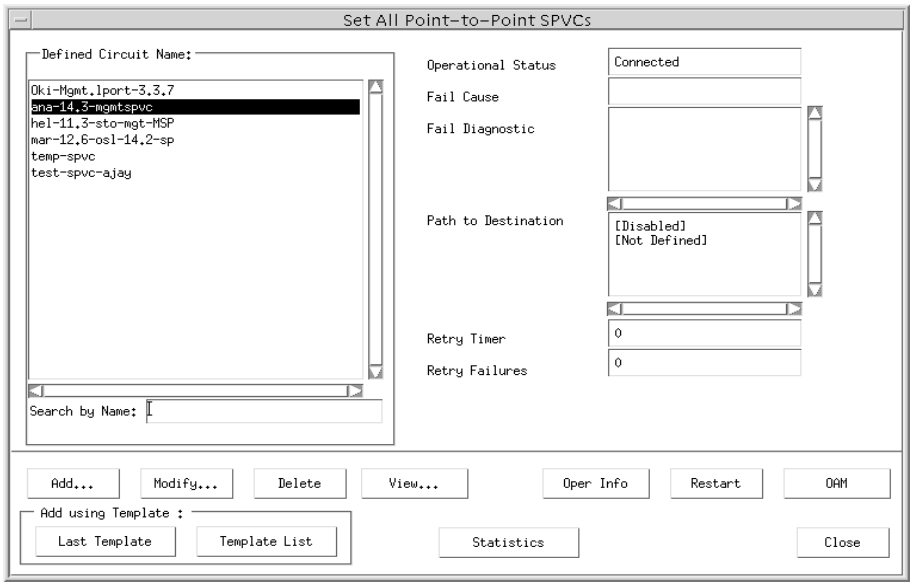


Figure 17-1. Set All Point-to-Point SPVCs Dialog Box

To view a list of configured SPVCs, position the cursor in the Search by Name field and press Return. Use any of the following wildcard searches to fine a specific SPVC name:

- Use an * to match any number of characters
- Use a ? to match a single character
- To match the ? character, type **?**
- To match the \ character, type \\

The Set All Point-to-Point SPVCs dialog box displays information about the configured options for the Defined Circuit Name you select. Table 17-2 describes the dialog box buttons, and Table 17-3 describes the dialog box fields.

Table 17-2. Set All Point-to-Point SPVCs Dialog Box Buttons

Button	Action/Description
Add	Enables you to add an SPVC.
Modify	Enables you to modify an SPVC.
Delete	Enables you to delete an SPVC.
View	Enables you to view the configured attributes for the selected SPVC.
Oper Info	Updates the information in the following operational status fields: • Fail Cause ID • Fail Diag • Actual Path • Retry Time • Retry Failure
Restart	Restarts the selected SPVC no matter what condition it is in. If the SPVC is not established, it restarts the process to establish the connection. If it is established, this button clears the existing connection and establishes it again.
OAM	Runs the Operations, Administration, and Management loopback diagnostics for the selected circuit.
Add using Template	If you have already defined an SPVC configuration and saved it as a template, use this option menu to define a new circuit using similar parameters. • Choose Last Template to use the last template you used to establish a circuit in this NMS session. • Choose Template List to display a list of templates previously defined for this map.
Statistics	Displays the summary statistics for the selected SPVC.
Close	Exits this dialog box and returns to the network map.

Table 17-3. Set All Point-to-Point SPVCs Dialog Box Fields

Field	Action/Description
Operational Status	Displays a status message: Establishing, Connected, Failed, or Other.
Fail Cause	Displays the ID of the last release failure.
Fail Diagnostic	Displays an eight-character diagnostic of the last release failure (as applicable).
Path to Destination	Displays the actual path that OSPF and/or PNNI selected for this circuit to use to get to its destination.
Retry Timer	Displays the current value of the retry timer in seconds.
Retry Failures	Displays the number of failed attempts to establish a connection.

Setting the VPI/VCI Values for SPVCs

For each SPVC you configure, you must specify a VPI value for the SPVC. For information on setting the VPI/VCI fields for SPVCs, see Table 17-4 on page 17-9.

For each SPVC you configure, specify a value from 0 – *nnnn* to represent the VPI for the SPVC. The maximum value is based on the Valid Bits in VPI that is configured for the logical port, as follows:

Maximum value = $2^{P} - 1$

where *P* is the value in the Valid Bits in VPI field. For example, if you entered 5 in the Valid Bits in VPI field, the maximum value is 31 ($2^{5} - 1 = 31$), which would give you up to 32 virtual paths (numbered 0-31).

For more information on setting the Valid Bits in VPI for the logical port, see Figure 3-5 on page 3-22.

If you are defining a soft permanent virtual channel connection (SPVCC), you must also specify a value to represent the VCI for an ATM circuit. The maximum value is based on the Valid Bits in VCI value that is configured for the logical port, as follows:

Maximum value = $2^C - 1$

where *C* is the value in the Valid Bits in VCI field. For example, if you entered 6 in the Valid Bits in VCI field, the maximum VCI value you can enter is 63, which would give you 32 virtual channels (numbered 32 to 63).

For more information on the Number of Valid Bits in VPI/VCI fields for the logical port, see Figure 3-5 on page 3-22.

Note – These VPI/VCI range restrictions only apply to SPVCCs. You can provision SPVPCs to use the following values:

- For UNI, use the VPI=0-255 range.
- For NNI cell header format, use the VPI=0-4095

Adding a Point-to-Point SPVC

To add a point-to-point SPVC:

1. From the Set All Point-to-Point SPVCs dialog box (Figure 17-1 on page 17-5), choose Add. The Select SPVC Endpoints dialog box appears.

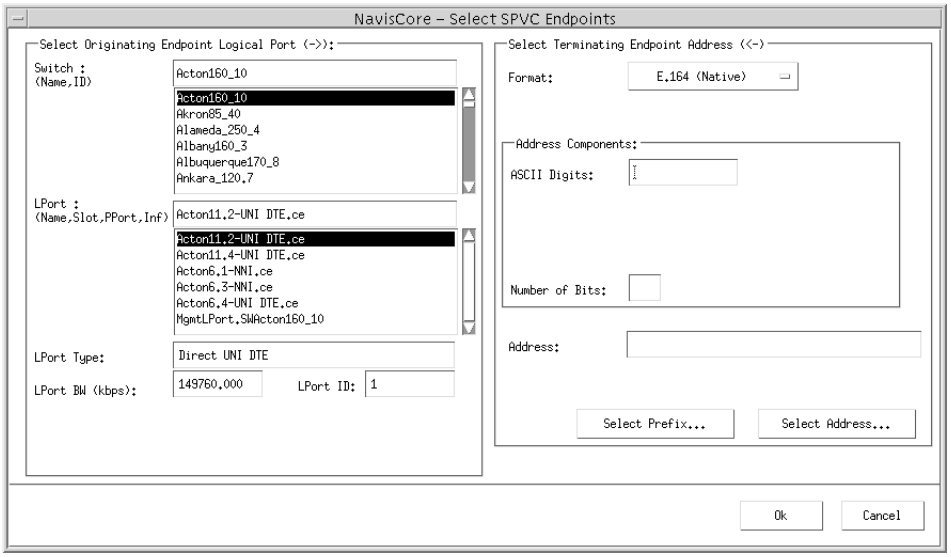


Figure 17-2. Select SPVC Endpoints Dialog Box

2. Perform the following steps to configure the originating endpoint logical port.
   a. Select the name of the switch on which the endpoint will reside.
   b. Select the name of the logical port that will be used as the endpoint. The dialog box displays the LPort Type, LPort BW (Kbps), and LPort ID for this endpoint.
3. To complete this configuration:
   - If you know the SVC terminating endpoint address, use Table 17-4 to select the address format and configure the terminating endpoint address. For more information on ATM End System Address (AESA) formats, see page 14-2.
   - If you do not know this address, or if you need to configure the terminating endpoint address, see page 17-13 for instructions on using the Select Prefix and Select Address buttons to configure this address.

Table 17-4. Configuring the SPVC Terminating Endpoint Address

Address Format	Address Components
E.164 (Native)	In the ASCII Digits field, enter all of the 1-15 ASCII digits that represent the E.164 address. The value you enter is then converted to the ASCII hex values that represent each digit in the number (this value is displayed in the Address).
DCC and ICD AESA (or Anycast)	In the Hex Digits field, enter the data country code (DCC) of the country in which the address is registered, or the International Country Designator (ICD) that identifies the international organization to which this address applies. DCCs and ICDs consist of 4 hex digits, and occupy two octets. Then enter the appropriate HO-DSP, ESI, and SEL values.
E.164 AESA (or Anycast)	In the Hex Digits field, enter the full or partial E.164 AESA address. Since the IDI portion of the address is 8 octets (16 hex digits), but the E.164 address format is a maximum of 15 digits, you must terminate the IDI portion with Fh. For example, 5085551234 should be entered as 000005085551234F. After typing in the IDI portion of the address, enter the appropriate HO-DSP, ESI, and SEL portions to complete the address.
Custom AESA	In the AFI Digits field, enter the custom AFI you want to use. In the Hex Digits field, enter the customized address format you want to use, starting with the HO-DSP, and followed by the ESI and SEL values (in that order). This address must be the full 19 octets (38 hex digits) long, with 12 octets used for the HO-DSP, 6 octets used for the ESI, and 1 octet used for the SEL.

4. Choose OK. The Add Soft PVC dialog box appears (Figure 17-3).

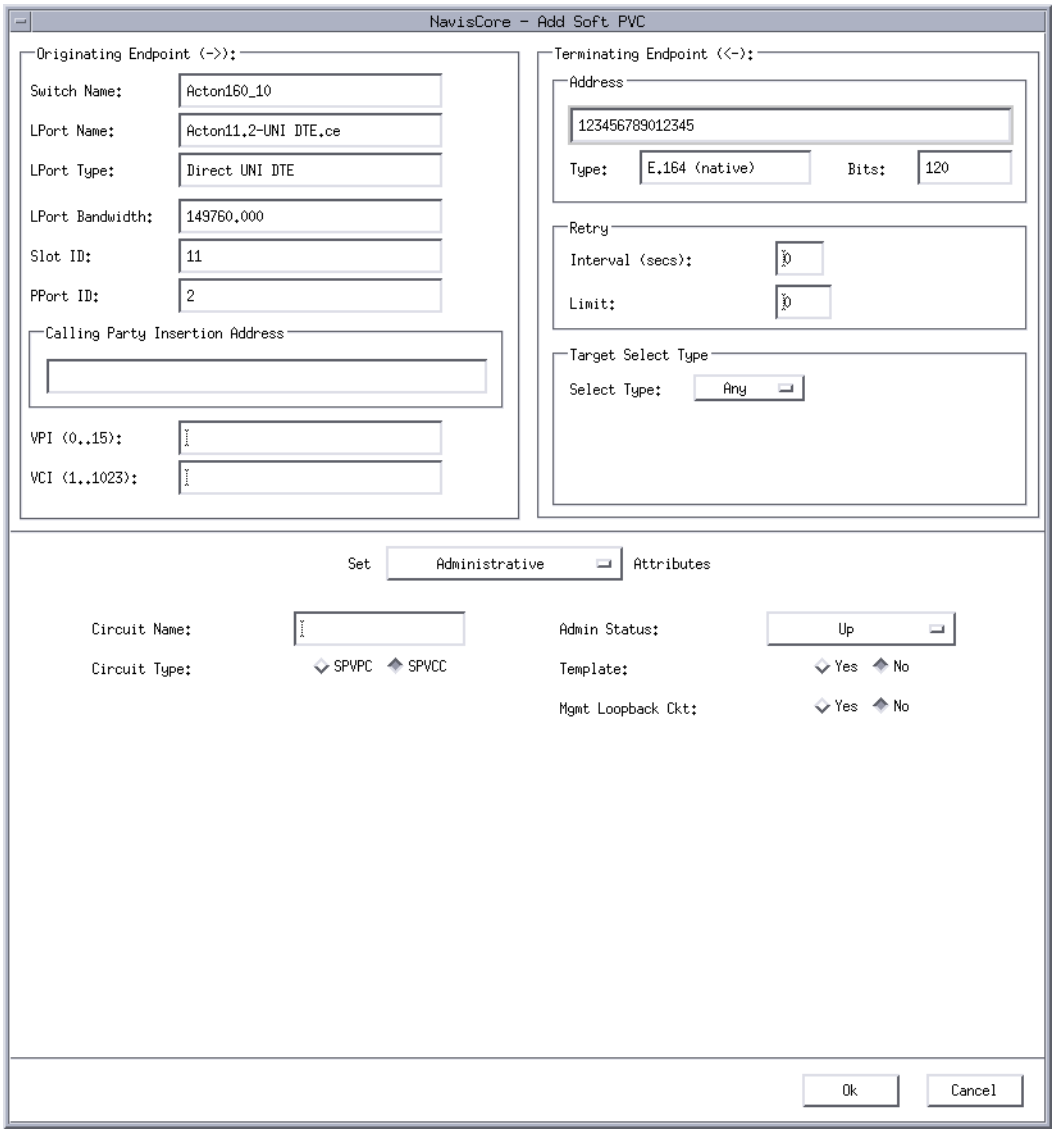


Figure 17-3. Add Soft PVC Dialog Box

5. Complete the fields in Table 17-5.

Table 17-5. Add Soft PVC Dialog Box Fields

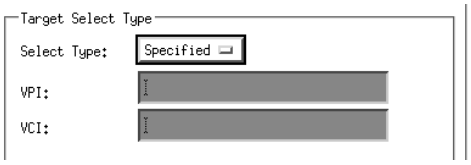
Field	Action/Description
VPI (0..15)	Enter a value from 0 – *nnnn* to represent the VPI for the SPVC; enter a value from 0 – 4095 if you use the NNI cell header format. The maximum value you can enter is based on the Valid Bits in VPI that is configured for the logical port. See page 17-7 for more information.
VCI (32..1023) (*SPVCCs only*)	If you are configuring a soft permanent virtual channel connection (SPVCC), enter a value to represent the VCI for the SPVCC. Although you can configure VCIs in the 1 – 31 range (with the exception of VCI = 4), the ATM Forum reserves VCIs in this range for various purposes. You should only use a VCI in the 1 – 31 range if you are certain that compatibility issues will not arise with any attached non-Lucent equipment.
Retry Interval (secs)	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying to reestablish a connection. Specify this interval in seconds (1 – 3600), or enter 0 (default) for no retries.
Retry Limit	This value indicates the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535), or enter 0 (default) for an unlimited number of retries.
Target Select Type	Review the information in "Specifying the Target Select Type" on page 17-3 first to determine your network needs. Then select one of the following Target Select Types: *Any* – Indicates that the terminating endpoint uses any available VPI/VCI value. If you need to specify a VPI/VCI for the terminating endpoint, you must complete the PVC/PVP Termination fields on the Add SVC Port Address dialog box. See page 15-37. *Specified* – The terminating endpoint uses the VPI/VCI address you specify. If this is an SPVPC, enter the VPI; for an SPVCC, enter the VPI and VCI. 
Circuit Name	Enter any unique, alphanumeric name to identify the SPVC. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the SPVC at switch startup, or Down if you do not want to activate the SPVC at switch startup.

Table 17-5. Add Soft PVC Dialog Box Fields (Continued)

Field	Action/Description
Circuit Type	Specify whether the circuit is a SPVPC or SPVCC (default). If you select SPVPC, the VCI field is set to 0 (zero) and cannot be changed.
Template (*Optional*)	You can save these settings as a template to configure another SPVC with similar options. To create a template, choose Yes in the Is Template field.
Mgmt Loopback Ckt	If you choose Yes, this SPVC configuration will be included in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download the configuration file to the switch, the SPVC can be used to establish NMS-to-switch connectivity. The Mgmt Loopback Ckt field is especially useful in some Management configurations. The default value is No.

6. Choose Set [Traffic Type] Attributes to select the traffic descriptors for this SPVC. Figure 17-4) shows the Set Traffic Type Attributes fields.

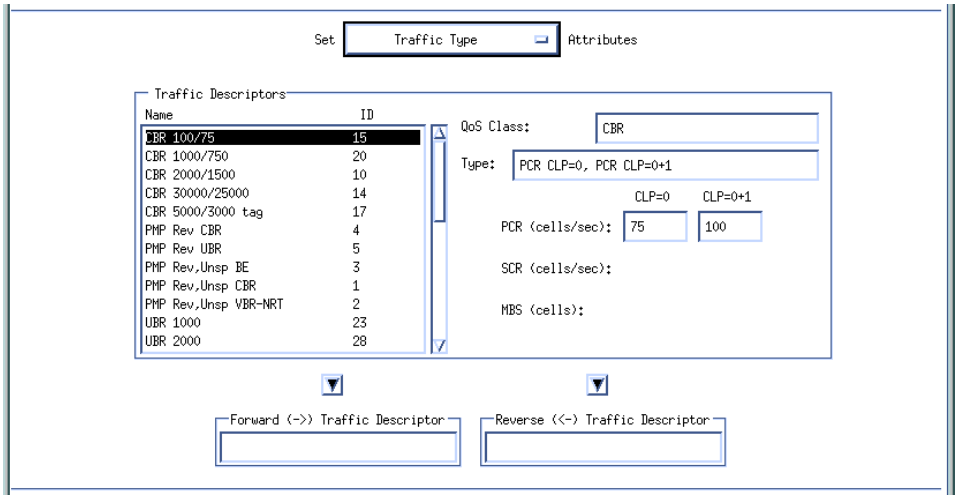


Figure 17-4. Set Traffic Type Attributes Fields

7. See "Defining Traffic Descriptor Attributes" on page 10-12 for instructions to configure these attributes.
8. Choose Ok to create the new SPVC and return to the Set All Point-to-Point SPVCs dialog box (Figure 17-1 on page 17-5).
9. Choose Close to return to the network map.

Configuring the Terminating Endpoint Address

The Select SPVC Endpoints dialog box (Figure 17-2 on page 17-8) contains the Select Prefix and Select Address buttons you can use to either select an existing or configure a new SVC terminating endpoint address.

Selecting an SVC Port Prefix

1. To select an SVC Port Prefix, choose Select Prefix. The Set All Port Prefixes dialog box appears.

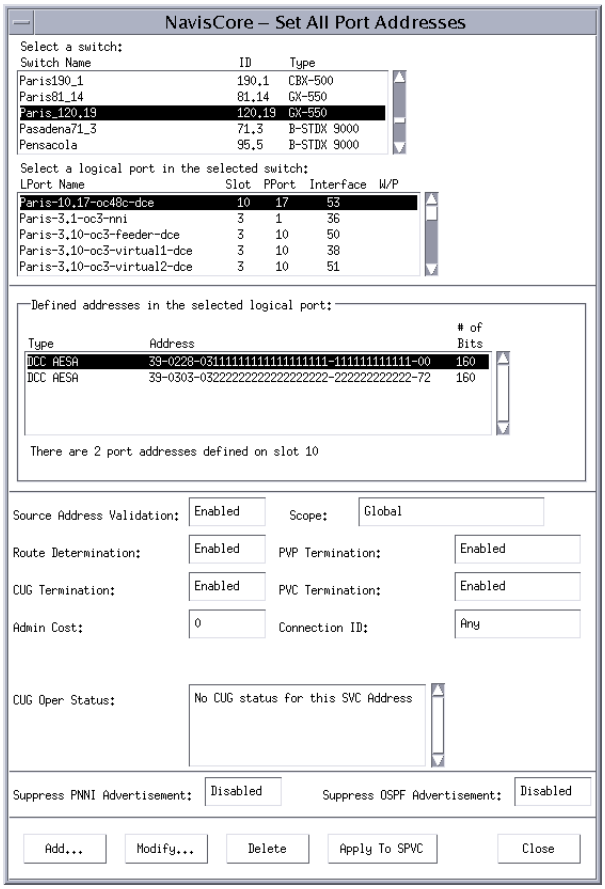


Figure 17-5. Set All Port Prefixes Dialog Box

- To add a new SVC prefix, choose Add and use the instructions beginning on page 15-13.
- To select an existing prefix, complete the following steps.

2. Select the name of the switch where the endpoint resides.
3. Select the name of the logical port that will be used as the endpoint. The dialog box displays the address information for this endpoint.

4. Choose Apply to SPVC. The Select SPVC Endpoints dialog box (Figure 17-2 on page 17-8) reappears.
5. Enter the remaining digits of the port address. If necessary, use the following procedure, "Selecting an SVC Port Address," to select a pre-configured address or to configure a new one.
6. Continue with step 4 on page 17-10.

Selecting an SVC Port Address

1. To select an SVC Port address, choose Select Address. The Set All Port Addresses dialog box (Figure 17-6) appears.

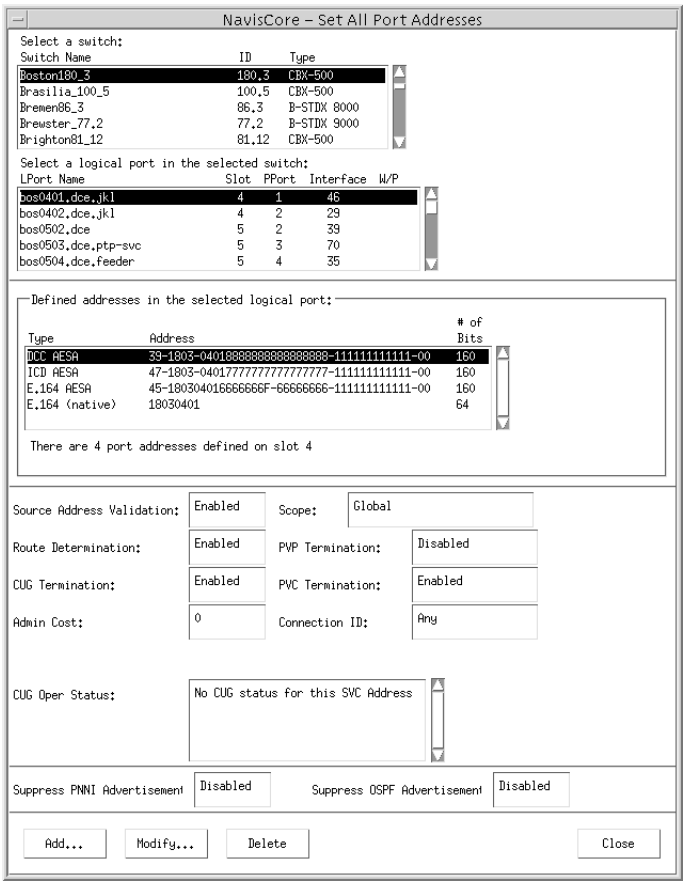


Figure 17-6. Set All Port Addresses Dialog Box

- To add a new SVC address, choose Add and use the instructions "Configuring SVC Port Addresses" on page 15-26.
- To select an existing prefix, complete the following steps.

2. Select the name of the switch where the endpoint resides.
3. Select the name of the logical port that will be used as the endpoint. The Set All Port Addresses dialog box displays the address information for this endpoint.

4. Choose Apply to SPVC. The Select SPVC Endpoints dialog box (Figure 17-2 on page 17-8) reappears.
5. Continue with step 4 on page 17-10.

Configuring Point-to-Multipoint SPVCs

To access the Set All Point-to-Multipoint SPVCs dialog box, from the Administer menu, select Lucent Parameters ⇒ Set All Soft PVCs ⇒ Point-to-Multipoint. The Set All Point-to-Multipoint SPVCs dialog box appears.

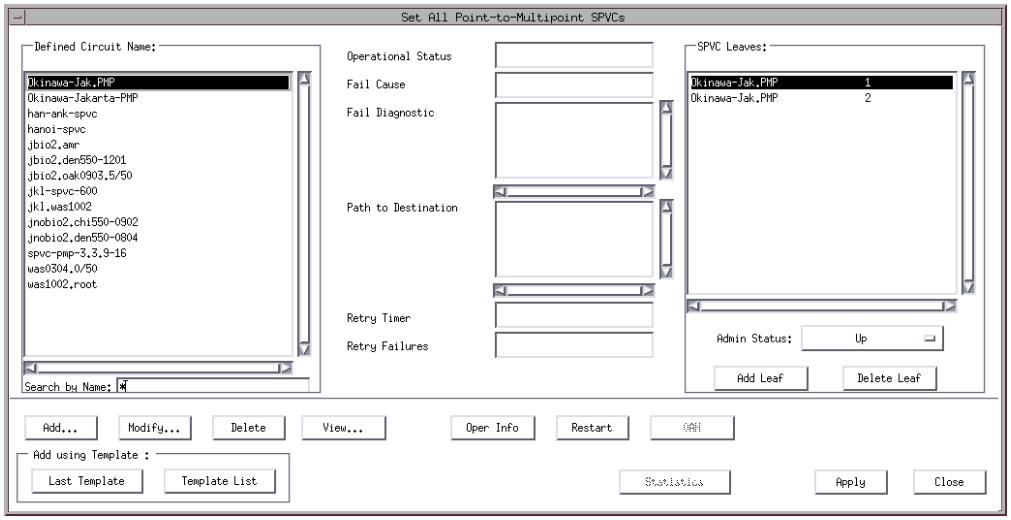


Figure 17-7. Set All Point-to-Multipoint SPVCs Dialog Box

To view a list of configured Point-to-Multipoint SPVCs, position the cursor in the Search by Name field and press Return. To use a wild card search to find a specific SPVC name, you can do any of the following:

- Use an * to match any number of characters
- Use a ? to match a single character
- To match the ? character, type **?**
- To match the \ character, type \\

The Set All Point-to-Multipoint SPVCs dialog box displays information about the selected Defined Circuit Name. Table 17-2 on page 17-6 describes the dialog box buttons, and Table 17-3 on page 17-7 describes the dialog box fields.

Adding a Point-to-Multipoint SPVC

When you configure a Point-to-Multipoint SPVC, you first define an SPVC consisting of a root (originating endpoint) and one leaf (terminating endpoint). This procedure is similar to the one for creating Point-to-Point SPVCs. Once you define the initial root/leaf combination, you can create additional leafs.

Defining the Point-to-Multipoint SPVC Root

1. From the Set All Point-to-Multipoint SPVCs dialog box, choose Add. The Select SPVC Endpoints dialog box appears (Figure 17-2 on page 17-8).
2. Configure the originating endpoint logical port (root):
   a. Select the name of the switch on which the endpoint will reside.
   b. Select the name of the logical port that will be used as the endpoint.

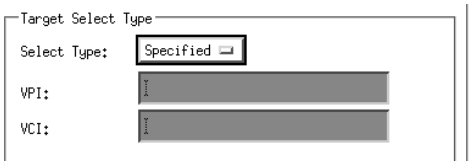
      The dialog box displays the LPortType, LPort BW (Kbps), and LPort ID for this endpoint.
3. If you know the SVC terminating endpoint address, use Table 17-4 on page 17-9 to select the address format and configure the terminating endpoint address. For more information on AESA address formats, see page 14-2.

   If you do not know this address, or if you need to configure the terminating endpoint address, see page 17-13 for instructions on using the Select Prefix and Select Address buttons to configure this address.
4. Choose Ok. The Add Soft PVC dialog box appears (Figure 17-3 on page 17-10).
5. Complete the fields described in Table 17-6.

Table 17-6. Add Point-to-Multipoint Fields

Field	Action/Description
VPI (0..15)	Enter a value from 0 – *nnnn* to represent the VPI for the SPVC. Enter a value from 0 – 4095 if you use the NNI cell header format. The maximum value you can enter is based on the Valid Bits in VPI that is configured for the logical port. (See page 17-7 for more information.)
VCI (32..1023) (*SPVCCs only*)	If you are configuring a SPVCC, enter a value to represent the VCI for the SPVCC. Although you can configure VCIs in the 1 – 31 range (with the exception of VCI = 4), the ATM Forum reserves VCIs in this range for various purposes. You should only use a VCI in the 1 – 31 range if you are certain that compatibility issues will not arise with any attached non-Lucent equipment.
Retry Interval (secs)	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying again to establish a connection. Specify this interval in seconds (1 – 3600), or enter 0 (default) for no retries.

Table 17-6. Add Point-to-Multipoint Fields (Continued)

Field	Action/Description
Retry Limit	This value indicates the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535) or enter 0 (default) for an unlimited number of retries.
Target Select Type	Review the information in "Specifying the Target Select Type" on page 17-3 first to determine your network needs. Then select one of the following Target Select Types: *Any* – Indicates that the terminating endpoint uses any available VPI/VCI value. If you need to specify a VPI/VCI for the terminating endpoint, you must complete the PVC/PVP Termination fields on the Add SVC Port Address dialog box. See page 15-37. *Specified* – The terminating endpoint uses the VPI/VCI address you specify. If this is an SPVPC, enter the VPI. For an SPVCC, enter the VPI and VCI. 
Circuit Name	Enter any unique, alphanumeric name to identify the SPVC. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (the default) to activate the SPVC at switch startup, or Down if you do not want to activate the SPVC at switch startup.
Circuit Type	Specify whether the circuit is an SPVPC or SPVCC (the default). If you select SPVPC, the VCI field is set to 0 (zero) and cannot be changed.
Template (*Optional*)	You can save these settings as a template to configure another SPVC with similar options. To create a template, choose Yes in the Is Template field.

6. See "Defining Traffic Descriptor Attributes" on page 10-12 for instructions on configuring these attributes.
7. Choose Ok to create the new SPVC and return to the Set All Point-to-Multipoint SPVCs dialog box.

Defining Additional SPVC Leafs

1. Once you configure the circuit root and initial leaf, choose Add Leaf on the Set All Point-to-Multipoint SPVC dialog box to configure additional SPVC leaves. The Add SPVC Leaf dialog box appears.

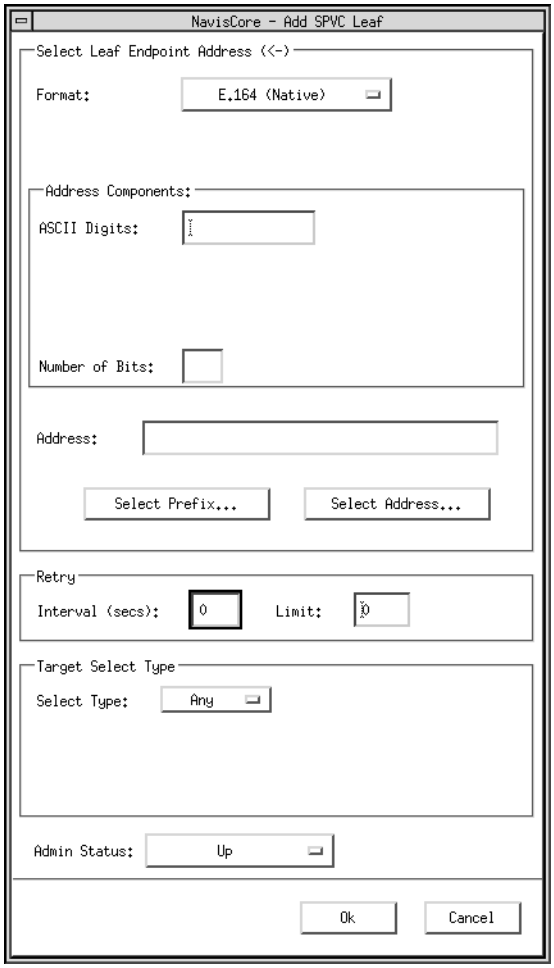


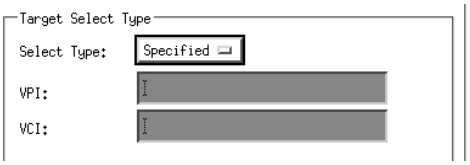
Figure 17-8. Add SPVC Leaf Dialog Box

2. If you know the SVC terminating endpoint address, use Table 17-4 on page 17-9 to select the address format and configure the address components for this leaf. For more information on AESA address formats, see "Address Formats" on page 14-2.

   If you do not know this address, or if you need to configure the terminating endpoint address, see page 17-13 for instructions on using the Select Prefix and Select Address buttons to configure this address.

3. Complete the fields described in Table 17-7.

Table 17-7. Add SPVC Leaf Fields

Field	Action/Description
Retry Interval (secs)	The originating endpoint makes several attempts to connect to the terminating endpoint. This value indicates the number of seconds the originating endpoint waits before trying again to establish a connection. Specify this interval in seconds (1 – 3600) or enter 0 (default) for no retries.
Retry Limit	This value indicates that the number of times the originating endpoint tries to connect to the terminating endpoint. Specify the number of retries (1 – 65535) or enter 0 (default) for an unlimited number of retries.
Target Select Type	Review the information in "Specifying the Target Select Type" on page 17-3 first to determine your network needs. Then select one of the following Target Select Types: *Any* – Indicates the terminating endpoint uses any available VPI/VCI value. If you need to specify a VPI/VCI for the terminating endpoint, you must complete the PVC/PVP Termination fields described in Chapter 15, sections "Configuring PVP Termination" and "Configuring PVC Termination.". *Specified* – The terminating endpoint uses the VPI/VCI address you specify. If this is an SPVPC, enter the VPI. For an SPVCC, enter the VPI and VCI. 

4. Choose Ok to return to the Set All Point-to-Multipoint SPVC dialog box (Figure 17-7 on page 17-15).

18

Closed User Groups (CUGs)

A closed user group (CUG) is a division of all SVC network users into logically linked groups of users. Members of the same CUG have particular calling privileges that members of different CUGs may not have. CUGs form one level of security between users of a network, allowing only those users who are members of the CUG to set up calls to each other.

A CUG is comprised of a set of members and rules. These rules represent SVC port addresses and prefixes for which you have enabled the CUG termination field (see Table 15-3 on page 15-24). You configure CUG member rules in either AESA or E.164 address format. When you configure a member rule, you can replace some digits with the * or ? UNIX wildcard characters. If a member rule does not contain a wildcard character, it maps to a specific network user. If the member rule includes a wildcard, then this rule can potentially map to multiple network users.

Note – Throughout this document, most address descriptions use the term *SVC address*. Unless otherwise noted, the term *SVC address* is used interchangeably with the term *SVC prefix*.

About CUG Member Rules

CUG member rules correspond to SVC addresses. You can enter a rule as a UNIX-style expression. You can use the * as a wildcard to replace zero (0), one, or more digits, or the (?) as a wildcard to replace a single digit. You can only use the * once in a string. Keep in mind that an AESA digit is 4 bits and an E.164 digit is 8 bits.

The following table shows how you can use wildcards to represent multiple E.164 addresses:

Example	Description
1508952*	This CUG includes all numbers using area code 508 and exchange number 952.
1508952148?	This CUG includes all numbers using area code 508, exchange number 952, and an extension starting with 148 (that is, 1480 – 1489).

When you define a CUG member, these addresses define the *member value* for the CUG member rule. Each CUG member rule is defined by an ASCII name, an address type (either E.164 or AESA), and the CUG member value (rule).

Defining Incoming and Outgoing Access

In addition to defining CUG member address values, you can also define the incoming and outgoing access attributes that complete the CUG member rule.

The incoming access (IA) attribute enables you to define how a CUG member handles calls coming from other CUGs or non-CUG users. If a CUG member has incoming access enabled, a mapped user can receive calls coming from non-CUG users as well as calls coming from other CUGs. If you disable incoming access, the CUG member can only receive calls from other members of the same CUG.

The outgoing access (OA) attribute enables you to define how a CUG member handles calls to other CUGs and non-CUG users. If a CUG member has outgoing access enabled, a mapped user can makes calls to other CUGs and non-CUG users. If you disable outgoing access, the CUG member can only make calls to other members of the same CUG.

Member Rule Example

You define the following CUG member rule:

Member Rule Name	**Rule1**
Member Value/Type	1508* (E.164)
Incoming Access	Y
Outgoing Access	N

This member rule applies to E.164 addresses beginning with digits 1508. Users who map to this rule can receive calls from members of their own CUG, members of other CUGs, and non-CUG users (incoming access is enabled), but they cannot make calls outside their own CUG.

Developing Closed User Groups (CUGs)

For each CUG you create, you can assign up to 128 different member rules. You can also use an individual member rule in up to 16 different CUGs. In this way, a CUG is made up of all users who map to the addresses that these rules define. You can configure up to 1024 CUGs per switch.

When you create a CUG (for example, “CUG A”), the attributes you configure for each CUG member rule (“Rule1”) that you associate with the CUG define how the CUG handles calls between members. For example, if you enable the incoming calls barred (ICB) attribute for Rule1, users who map to Rule1 cannot receive calls from other CUG A members. Conversely, disable ICB to allow users who map to Rule1 to receive calls from other CUG A members.

If you enable the outgoing calls barred (OCB) attribute for Rule1, users who map to Rule1 cannot make calls to other CUG A members. Conversely, disable OCB to allow users who map to Rule1 to make calls to other CUG A members.

Using CUGs in the Network

Figure 18-1 illustrates how you can implement CUGs in your network.

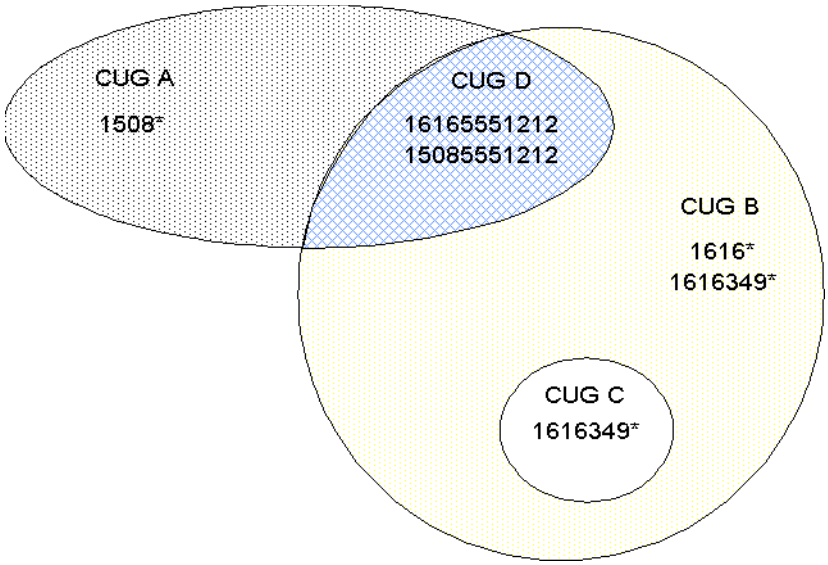


Figure 18-1. Implementing CUGs

The CUGs used in this example represent the following:

- CUG A: Business Unit A
- CUG B: Business Unit B
- CUG C: Independent entity within Unit B
- CUG D: Joint venture between Units A and B

For each of these CUGs, Table 18-1 defines the ICB and OCB attributes and member rules. Each member rule is made up of an expression that represents an E.164 address and an incoming access (IA) and outgoing access (OA) attribute.

Table 18-1. Incoming and Outgoing Calls Barred Example

	ICB	OCB	Member Rules	IA	OA
CUG A	No	No	1508*	No	No
CUG B	No Yes	No Yes	1616* 1616349*	No No	Yes No
CUG C	No	No	1616349*	No	No
CUG D	No No	No No	16165551212 15088881212	No Yes	Yes No

Call Setup Examples

- A call is made from 15085551212 to 16165551212:
  - 15085551212 (IA enabled): Address belongs to CUG A and CUG D
  - 16165551212 (OA enabled): Address belongs to CUG B and CUG D

  Result: Call succeeds because both addresses belong to CUG D.
- A call is made from 16163498888 to 16165551212:
  - 1616349: Address belongs to CUG B (ICB, OCB enabled) and CUG C
  - 16165551212 (OA enabled): Address belongs to CUG B and CUG D

  Result: Although both addresses belong to CUG B, the call fails because the outgoing calls barred (OCB) attribute is enabled on CUG B for member 1616349*. Users mapping to matching rule 1616349* cannot make calls to other CUG B members.
- A call is made from 12035551212 to 15085551212:
  - The address 12035551212 does not belong to any CUG.
  - 15085551212 (IA enabled): Address belongs to CUG A and CUG D

  Result: Call succeeds because the incoming access (IA) attribute is enabled for 15085551212. This member rule allows users mapped to 15085551212 to receive calls from non-CUG users.

Configured Addresses and CUG Membership

Using the CUG design depicted in Figure 18-1 on page 18-4, Table 18-2 illustrates how a single configured address can match multiple member rules, and can belong to more than one CUG.

Table 18-2. Configured Address and Corresponding CUG Membership

Address	OA	IA	CUG	ICB	OCB
15085551212	N	Y	A	N	N
			D	N	N
16165551212	Y	N	B	N	N
			D	N	N
15082178989	N	N	A	N	N
16161234567	Y	N	B	N	N
16163498888	Y	N	B	Y	Y
			C	N	N

Member rules that specify an address prefix can simplify call routing, since the logical port only needs to check the address prefix digits to route the call. However, if the port to which the call is routed contains other CUGs with member rules that begin with the same prefix (for example, 1616), CUG membership must be recalculated at call time.

For example, if a CUG contains a member rule that uses a prefix format (for example, 1616*) as well as other member rules that are more specific (1616349*), you are likely to encounter performance issues due to address ambiguity.

The more specific you make the CUG member rules, the more quickly CUG membership can be determined.

Configuring Closed User Groups (CUGs)

Use the following sequence to configure CUGs. Remember that each member rule should correspond to at least one SVC address.

Step 1. Create SVC addresses and enable CUG termination (see page 15-24).

Step 2. Define the CUG member rules that represent the member addresses and call access (see page 18-7).

Step 3. Define the CUG (by assigning names) (see page 18-10).

Step 4. Assign CUG members rules to CUGs. You can also modify call access attributes for a specific CUG (see page 18-11).

Defining CUG Members

A CUG member is defined by a rule that matches one or more port addresses/prefixes and attributes which specify incoming and outgoing call access. Once you define these members, you can associate them with specific CUGs.

To define a CUG member:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUG Members. The Set All SVC CUG Members dialog box appears (see Figure 18-2).

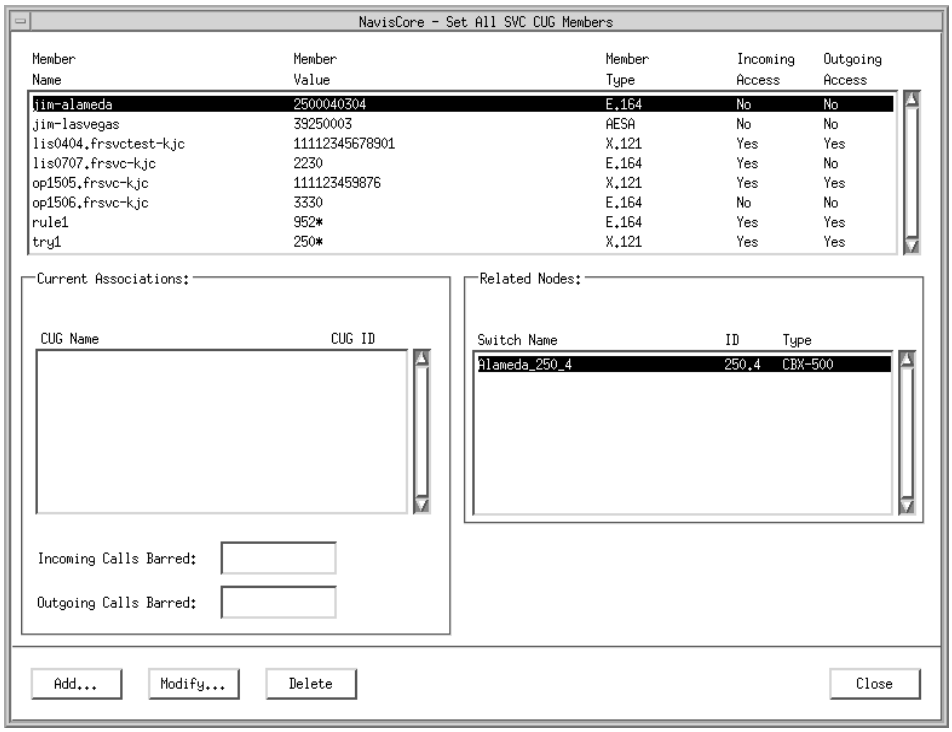


Figure 18-2. Set All SVC CUG Members Dialog Box

This dialog box provides a list of previously defined CUG members and their rules. For each member name you select, it provides the name of the CUG(s) with which the member is associated.

- To modify an existing CUG member name, select a name from this list and choose Modify.
- To delete an existing CUG member name, select a name from this list and choose Delete.

2. Choose Add to define a CUG member. The Add SVC CUG Member dialog box appears.

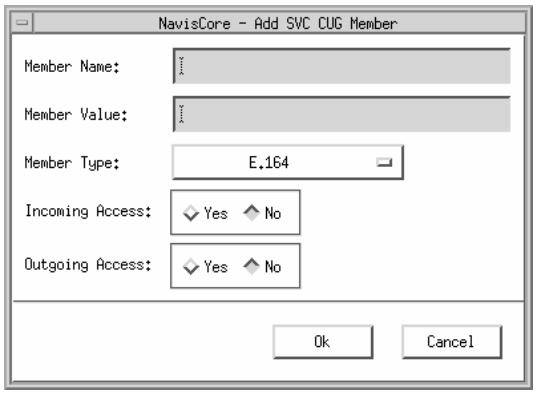


Figure 18-3. Add SVC CUG Member Dialog Box

3. Complete the fields in Table 18-3.

Table 18-3. Add SVC CUG Member Dialog Box Fields

Field	Action/Description
Member Name	Enter a name (up to 32 characters).
Member Value	Enter the CUG member rule using the guidelines on page 18-2. Do not enter more than 15 characters for an E.164 address or more than 40 characters for an AESA address.
Member Type	Select either AESA or E.164.
Incoming Access	This attribute specifies how incoming calls from non-CUG users or users of a different CUG are handled. • Select Yes to accept calls from users who do not belong to the same CUG. • Select No (default) to reject calls from users who do not belong to the same CUG.
Outgoing Access	This attribute specifies how outgoing calls to non-CUG users or users of a different CUG are handled. • Select Yes to allow calls to users who do not belong to the same CUG. • Select No (default) to block calls to users who do not belong to the same CUG.

4. When you finish, choose Ok.
5. You can use these fields to define additional members, or choose Cancel to exit this dialog box.

Defining a Closed User Group

Before you assign member rules, you need to set up the CUGs for your network. This is a simple process of supplying a name for each CUG. NavisCore supports up to 1024 CUGs per switch.

To create a CUG:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The Set All SVC CUGs dialog box appears.

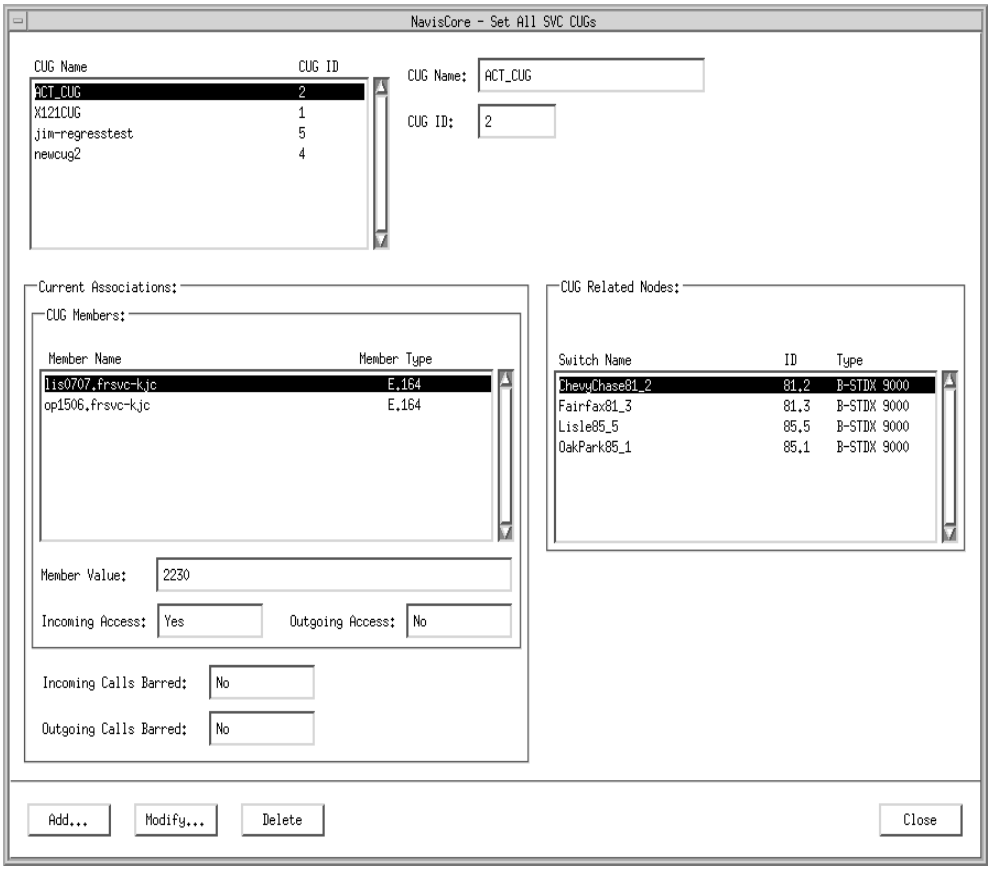


Figure 18-4. Set All SVC CUGs Dialog Box

This dialog box lists previously configured CUG names as well as members for each CUG you select.

- To modify an existing CUG, select a name from the CUG Members List box and choose Modify.
- To delete an existing CUG, select a name from the CUG Members List box and choose Delete.

2. Choose Add to create a new CUG. The Add SVC CUG dialog box appears.

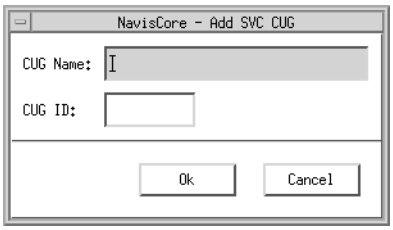


Figure 18-5. Add SVC CUG Dialog Box

3. Enter a CUG name (up to 32 characters). The NMS assigns a CUG ID.
4. Choose Ok.

Assigning Member Rules to CUGs

To complete the CUG definition process, you need to assign member rules to each CUG. You can assign up to 128 members per CUG. You can assign each member to as many as 16 CUGs.

To assign members to a CUG:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The Set All SVC CUGs dialog box appears (Figure 18-4 on page 18-10).
2. From the CUG Name list box, select the CUG to which you want to add members.

3. Choose Modify. The Modify CUG dialog box appears (Figure 18-6).

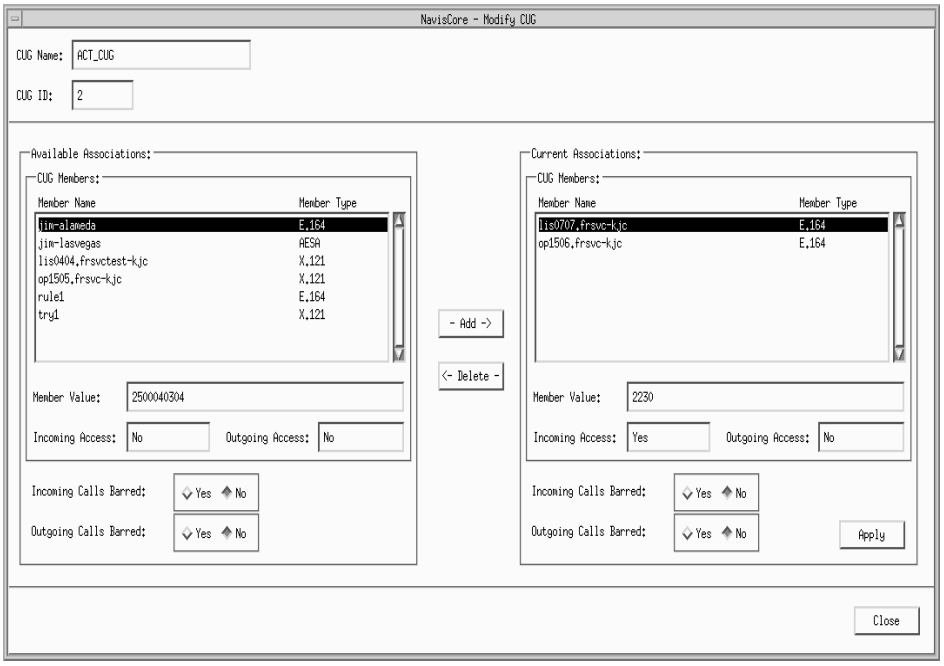


Figure 18-6. Modify CUG (Assign Member Rules) Dialog Box

This dialog box displays the current list of CUG member rules with Current Associations. It also provides a list of available member names you can associate with this CUG.

4. From the Available Associations list box, select the member you want to associate with this CUG and specify the ICB and OCB options:

   Incoming Calls Barred — Specifies how incoming calls from the same CUG are handled. Select Yes to reject calls from users of the same CUG. Select No (default) to allow calls from users of the same CUG.

   Outgoing Calls Barred — Specifies how outgoing calls to the same CUG are handled. Select Yes to block calls to users of the same CUG. Select No (default) to allow calls to users of the same CUG.

5. Choose -Add->. The member name appears in the Current Associations list box. All SVC addresses and prefixes that match the member rule inherit the attributes specified for this CUG.

6. To associate additional member names, repeat step 4 and step 5. When you finish, choose Close to exit this dialog box.

Modifying Call Access for CUG Members

Use the following steps to modify the incoming and outgoing call access for an existing CUG member.

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All SVC CUGs. The Set All SVC CUGs dialog box appears (Figure 18-4 on page 18-10).
2. From the CUG Name list box, select the CUG that contains this member.
3. Choose Modify. The Modify CUG dialog box appears (Figure 18-6 on page 18-12).
4. Select the CUG member name from the Current Associations list box.

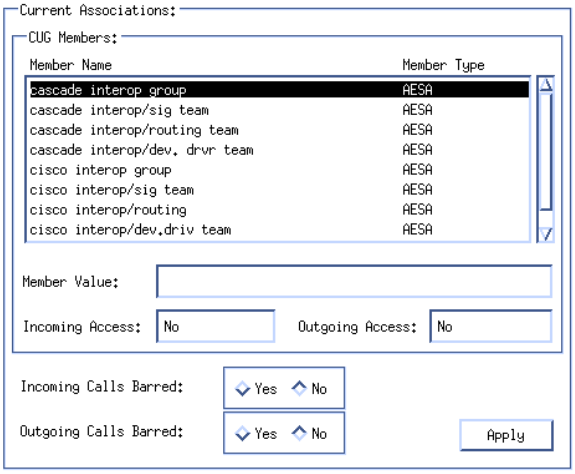


Figure 18-7. Modify CUG (Call Access) Dialog Box

5. Complete the fields in Table 18-3 on page 18-9 to modify incoming and outgoing call access.
6. Choose Apply.
7. Choose Close to exit this dialog box.

19

Port Security Screening

The Port Security Screening feature ensures that your network cannot be compromised by unauthorized SVC access. You do this by creating screens that can allow/disallow incoming and outgoing SVCs. You configure each screen with the following information:

SVC direction — Screen either ingress (incoming) or egress (outgoing) SVCs.

Screen type — Pass or block SVCs according to the configured screen.

Address type — Any address type used in a public or private UNI. This includes E.164, E.164-AESA, DCC-AESA, ICD-AESA, and custom AESA.

Matching information — Address criteria that either allows or disallows the SVC.

Once you develop a set of screens, you can apply them to any ATM UNI or NNI logical port in your network. You can use a maximum of 16 different screens per port. Using these screens, the port checks every SVC it receives and/or sends for the matching criteria specified in the screen(s). If the SVC matches criteria specified in at least one of these screens, the port either passes or blocks that SVC according to the security screen design.

Implementing Port Security Screening

Although you can apply multiple security screens to a single logical port, whether an SVC is passed or blocked is based on the combined effects of the following:

- The default ingress/egress screen mode for the logical port.
- The security screens you assign to this logical port.
- The incoming/outgoing SVC address criteria defined in the security screen.

Default Screens

For each logical port, you configure default screen criteria that specifies the behavior of any SVC on this port. You can configure security screens on both ingress user ports (which represent SVC originating endpoints) or egress user ports (which represent SVC terminating endpoints). The default screens enable you to quickly override the security screens you assign to the logical port. Use the default screens to either pass or block all incoming or outgoing SVCs.

Table 19-1 describes the default ingress and egress security screen options. These defaults represent the port screen activation parameters.

Table 19-1. Default Screens

Default	Value	Description
Ingress Screen Mode	All Screens	All ingress screens you apply to this port determine whether an incoming SVC is passed or blocked.
	Default Screen (default)	Disables the ingress security screens applied to this port. Incoming SVCs are screened according to how you set the Default Ingress Screen.
Default Ingress Screen	Pass (default)	If you set the Ingress Screen Mode to Default Screen, all incoming SVCs to this port are passed. If it is set to All Screens, all incoming SVCs are passed, unless one of the ingress security screens assigned to this port blocks the SVC.
	Block	If you set the Ingress Screen Mode to Default Screen, all incoming SVCs to this port are blocked. If it is set to All Screens, all incoming SVCs are blocked unless one of the ingress security screens assigned to this port passes the SVC.
Egress Screen Mode	All Screens	All egress screens you apply to this port determine whether an outgoing SVC is passed or blocked.
	Default Screen (default)	Disables the egress security screens applied to this port. Outgoing SVCs are screened according to the Default Egress Screen.

Table 19-1. Default Screens (Continued)

Default	Value	Description
Default Egress Screen	Pass (default)	If you set the Egress Screen Mode to Default Screen, all outgoing SVCs from this port are passed. If it is set to All Screens, all outgoing SVCs are passed, unless one of the egress security screens assigned to this port blocks the SVC.
	Block	If you set the Egress Screen Mode to Default Screen, all outgoing SVCs from this port are blocked. If it is set to All Screens, all outgoing SVCs are blocked, unless one of the egress security screens assigned to this port passes the SVC.

Security Screens

The security screens you assign to a logical port represent exceptions to the default screens. You can assign up to 16 security screens per logical port. Once you assign security screens to a port and set the ingress/egress screen mode to All Screens, the logical port uses these security screens to screen SVCs that match the criteria they specify.

You define a security screen based on two attributes: SVC direction and screen type. SVC direction defines the SVCs to which this screen applies, either ingress (incoming) or egress (outgoing). The screen type attribute determines whether the port passes or blocks these SVCs.

About Security Screen Addresses

To provide a more detailed level of SVC screening, you can specify either an E.164 or AESA-style address. You can enter the entire address as a number, or enter a UNIX-style expression using wildcards. When you use a UNIX expression, a single screen can match multiple endpoint addresses. Use the ? wildcard to replace a single digit or the * wildcard to replace one or more digits. You can only use the * once in a string. See “Address Formats” on page 14-2 for more information on addressing.

The following examples show how you can use a UNIX expression to represent an E.164 North American address.

Example	Description
1508952*	This screen applies to all numbers using area code 508 and exchange number 952.
1508952148?	This screen applies to all numbers using area code 508, exchange number 952, and an extension starting with 148 (that is, 1480 – 1489).
150895?*5?	This screen applies to all numbers using area code 508, with an exchange number value of 950 – 959. The number 5 must appear as one digit from the end of the address.

Table 19-2 describes some examples using the port security screens.

Table 19-2. Port Security Screen Examples

SVC Direction	Screen Type	Calling Address	Calling Subaddress	Called Address	Called Subaddress	Description
Ingress	Pass	Ignore	Ignore	1800* Type: E.164	Ignore	Pass all incoming calls to 1800 numbers.
Ingress	Block	Ignore	Ignore	1800* Type: E.164	Ignore	Block all incoming calls to 1800 numbers.
Egress	Block	Ignore	Ignore	* Type: E.164	Ignore	Block all outgoing calls with E.164 called addresses.
Egress	Block	15089700705 Type: E.164	Ignore	1908870* Type: E.164	Ignore	Block all calls to called address 1908870* from calling address 15089700705.

Port Security Screening Sample Configuration

Once you assign security screens to a logical port, if you set the ingress and egress screen modes to All Screens (see Figure 19-3 on page 19-12), the port checks incoming/outgoing SVCs for the matching criteria specified in each assigned screen. If an SVC meets the criteria specified in at least one screen, then the SVC is screened according to the action this screen recommends. The SVC is further checked to see if it matches this screen's default behavior. If it matches the criteria specified in at least one of these screens, then the SVC exhibits the default behavior (either pass or block).

Although you can apply multiple screens to a single port, whether the port should block or pass an SVC is based on:

- The combined effect of the default screens specified for the logical port
- The security screens you assign to that port
- The matching address criteria defined in each screen (if applicable)

If you set the ingress/egress screen mode to Default Screens, the port does not check SVCs for the matching criteria specified in an assigned security screen. It takes the action (either pass or block) specified in the Default Screen.

The following example provides a logical port configuration that blocks all incoming SVCs, except incoming 1800 SVCs, with one exception: you want to block all incoming SVCs that contain the 234 exchange number.

Logical Port Configuration Examples

1. For the logical port, configure the following default screen:

Ingress Screen Mode:	All Screens
Default Ingress Screen:	Block

Setting the default ingress screen to Block enables you to block all incoming SVCs on this port by default; setting the ingress screen mode to All Screens enables the port to screen SVCs based on the ingress security screens.

2. Create and assign two security screens.

- The following screen passes all incoming 1800 SVCs:

Screen Name:	pass_in_800
SVC Direction:	Ingress
Screen Type:	Pass
Calling Address:	Ignore
Calling Subaddress:	Ignore
Called Address:	Type: E.164 1800*
Called Subaddress:	Ignore

- The following screen blocks all SVCs from the 234 exchange:

Screen Name:	blk_234_exchg
SVC Direction:	Ingress
Screen Type:	Block
Calling Address:	Ignore
Calling Subaddress:	Ignore
Called Address:	Type: E.164 1???234*
Called Subaddress:	Ignore

Port Security Screening Configuration Summary

As you design port security screening features for your network, consider the following:

1. Configure the default screen for a logical port. This default mode determines whether to pass or block SVCs from certain addresses. The previous example blocks all incoming SVCs for the logical port. You can quickly revert back to the default mode if necessary.
2. Configure and assign the security screen exceptions. The previous example passes all incoming 1800 SVCs.
3. Configure and assign any exceptions to the screen. The previous example specifically blocks incoming SVCs from the 234 exchange; including incoming SVCs from 1800234*.

Configuring Port Security Screening

Perform the following steps to configure port security screening:

Step 1. Configure logical ports (see Chapter 3).

Step 2. Configure SVCs parameters (see Chapter 15).

Step 3. Create a set of port security screens (see "Creating Port Security Screen Definitions").

Step 4. Define the logical port security screening defaults. If necessary, assign the security screens that provide exceptions to these defaults (see page 19-11).

Creating Port Security Screen Definitions

To create a security screen:

1. From the Administer menu, select Lucent Parameters ⇒ Set All SVC Parameters ⇒ Set All Port Security Screens. The Set All Port Security Screens dialog box appears.

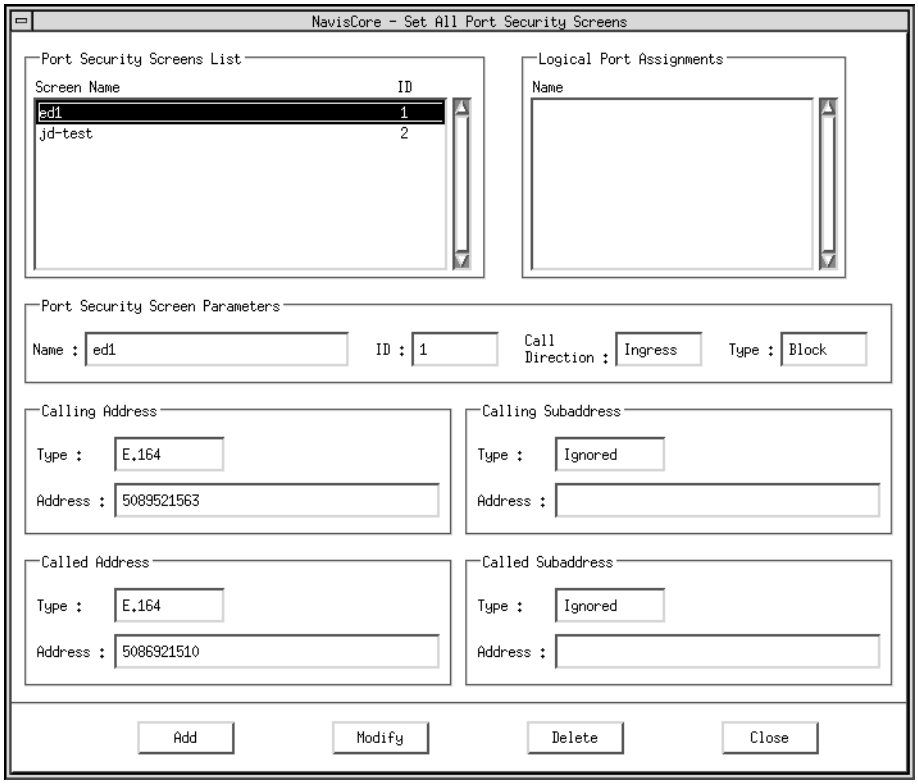


Figure 19-1. Set All Port Security Screens Dialog Box

This dialog box displays a list of previously configured security screens. It displays the configured parameters for each screen you select from the Port Security Screens List box.

- To modify an existing screen, select a Screen Name and choose Modify.
- To delete an existing screen, select a Screen Name and choose Delete.

2. Choose Add to create a new screen. The Adding Port Security Screens dialog box appears.

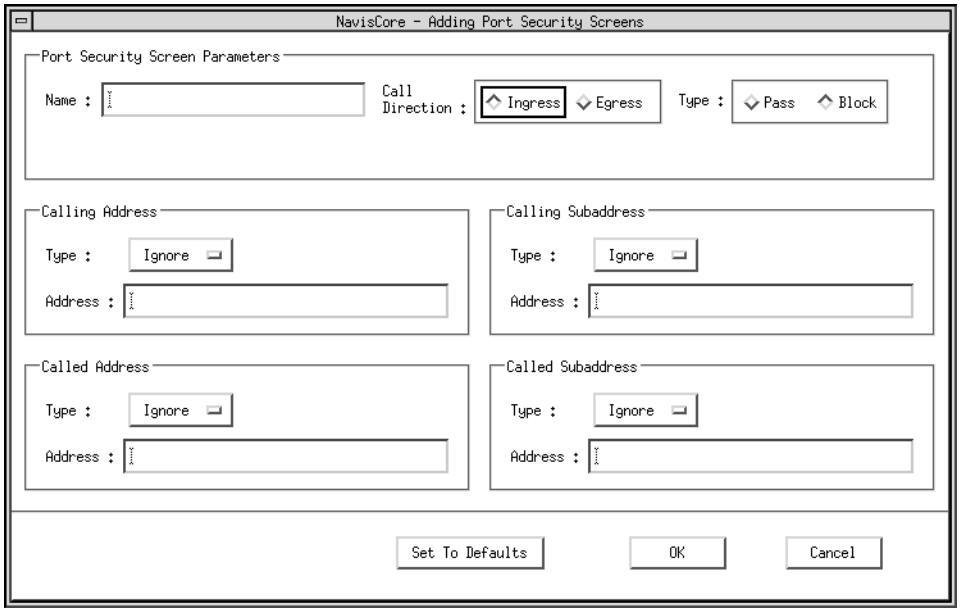


Figure 19-2. Adding Port Security Screens Dialog Box

3. Complete the fields described in Table 19-3.

Table 19-3. Adding Port Security Screens Dialog Box Fields

Field	Action/Description
Name	Enter a name (up to 32 characters) for this security screen.
Call Direction	The screen you configure is applied as follows: *Ingress* – (default) Screen incoming SVCs. *Egress* – Screen outgoing SVCs.
Type	Select the Type of screen (your selection determines the action this screen performs): *Block* – (default) Blocks all SVCs that match the criteria. *Pass* – Passes all SVCs that match the criteria.
Calling Address	Configure the Calling Address if this screen is for incoming SVCs: *Type* – Select the address type, either AESA or E.164. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen using the guidelines on page 19-3. Enter up to 15 characters for an E.164 address; enter up to 40 characters for an AESA address.

Table 19-3. Adding Port Security Screens Dialog Box Fields (Continued)

Field	Action/Description
Calling Subaddress	Configure the Calling Subaddress for incoming AESA SVCs only (this parameter provides an optional level of screening): *Type* – Select AESA. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen (up to 40 characters) using the guidelines on page 19-3.
Called Address	Configure the Called Address if this screen is for outgoing SVCs: *Type* – Select the address type, either AESA or E.164. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen using the guidelines on page 19-3. Enter up to 15 characters for an E.164 address; enter up to 40 characters for an AESA address.
Called Subaddress	Configure the Called Subaddress for outgoing AESA SVCs only (this parameter provides an optional level of screening): *Type* – Select AESA. Select Ignore (default) if the screen does not use this parameter. *Address* – Enter the address screen (up to 40 characters) using the guidelines on page 19-3.

4. Choose Ok to create the new screen.
5. The Adding Port Security Screens dialog box (Figure 19-2 on page 19-9) is designed to allow you to create several screens in a single session. To create additional screens, repeat step 3 on page 19-9 and step 4 on page 19-10. Choose Set To Defaults to retrieve the default values if necessary.
6. When you finish creating your screens, choose Cancel to exit this dialog box.

Assigning Security Screens to Logical Ports

Once you create the security screens, you assign these screens to the individual logical ports. The default security screens you configure for each logical port enable you to quickly pass or block incoming or outgoing SVCs, without having to remove or modify the screen you have applied. For information about reverting back to the default security screen, see "Activating Default Screens" on page 19-13.

You also have the option of assigning several different security screens to this port, but configuring them as "inactive." You can then activate them as necessary, at a later time. For more information, see "Activating and Deactivating Security Screens" on page 19-14.

To assign security screens to a port:

1. Use the instructions on page 3-2 to access the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4).
2. Select the logical port to which you will assign a screen and choose Modify.
3. Review the logical port type and ID and choose Ok. The Modify Logical Port dialog box reappears.
4. From the Select:Options: menu, select Screen Assignments and choose Set. The Assigning and Activating Port Security Screens dialog box appears.

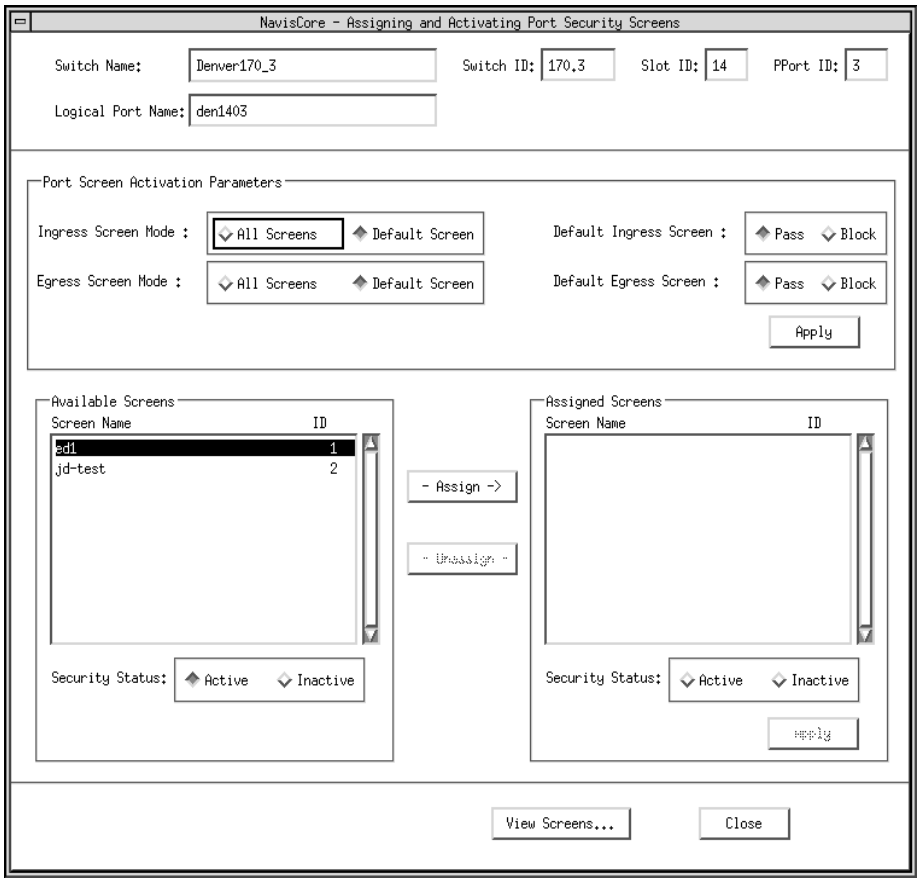


Figure 19-3. Assigning and Activating Port Security Screens Dialog Box

5. See Table 19-1 on page 19-2 to configure the Port Screen Activation Parameters to meet your network needs.
6. Choose Apply to set the Port Screen Activation Parameters.
7. Select the name of the screen you want to assign from the Available Screens list box. The Security Status of the screen you select defaults to Active. Using the Active Security Status, after you choose Apply, the logical port begins screening SVCs according to the rules of this screen.
8. Skip this step to make a screen active immediately. To assign a screen to this logical port without making it active immediately, select Inactive and choose Apply.

Note – You can choose View Screens to view the parameters configured for the screen you want to use.

9. Choose -Assign-> to assign a screen to this logical port. The screen name appears in the Assigned Screens list box.

10. To create additional screens, repeat step 7 through step 9. (You can assign up to 16 screens per logical port.) The Assigning and Activating Port Security Screens dialog box (Figure 19-3 on page 19-12) is designed to allow you to assign several screens in a single session.
11. When you finish creating your screens, choose Close to exit this dialog box.

Deleting Security Screen Assignments

Use the following steps to remove a security screen assignment for a logical port:

1. Use step 1 through step 4 starting on page 19-11 to access the Assigning and Activating Port Security Screens dialog box (Figure 19-3 on page 19-12).
2. Review the list of Assigned Screens and select the screen.
3. Choose Unassign. This screen should now appear in the Available Screens list box.

Activating Default Screens

Use the following steps to activate the default screening parameter(s) to temporarily override assigned security screens.

1. Use the instructions on page 3-2 to access the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4).
2. Select the logical port for which you will activate the default screen(s) and choose Modify.
3. Review the logical port type and ID and choose Ok. The Modify Logical Port dialog box reappears.
4. From the Select:Options: menu, select Screen Assignments and choose Set. The Assigning and Activating Port Security Screens dialog box appears (Figure 19-3 on page 19-12).

5. Review the information configured in the Port Screen Activation Parameters fields. See Table 19-1 on page 19-2 if you need information to modify these parameters.

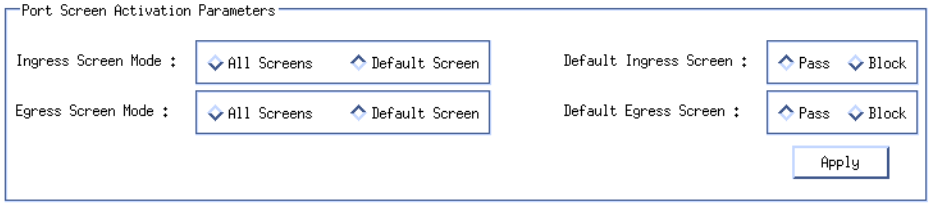


Figure 19-4. Port Screen Activation Parameter Fields

6. Choose Apply to activate the default screen.
7. Choose Close to exit this dialog box.

Activating and Deactivating Security Screens

Use the following steps to activate or deactivate a security screen according to your network needs:

1. Use the instructions on page 3-2 to access the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4).
2. Select the logical port for which you will change the security status and choose Modify.
3. Review the logical port type and ID and choose Ok. The Modify Logical Port dialog box reappears.
4. From the Select:Options: menu, select Screen Assignments and choose Set. The Assigning and Activating Port Security Screens dialog box appears (Figure 19-3 on page 19-12).
5. In the Assigned Screens list box, select the screen and modify the Security Status as necessary (Active or Inactive).

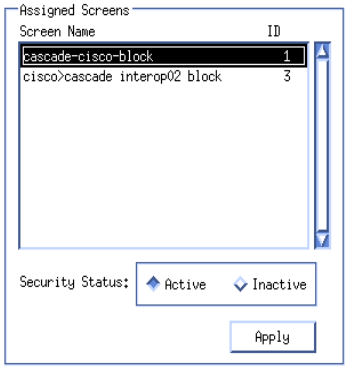


Figure 19-5. Assigned Screens List Box

Note – You can choose the View Screens button to view the parameters configured for the screen you want to modify.

6. Choose Apply. The change takes effect immediately.
7. Repeat step 5 and step 6 to activate/deactivate additional screens.
8. When you finish, choose Close to exit this dialog box.

Viewing Screen Assignments

Use the following steps to view screen assignments for a specific logical port:

1. Use the instructions on page 3-2 to access the Set All Logical Ports in PPort dialog box (Figure 3-1 on page 3-4).
2. Select the logical port for which you want to view screen assignments.
3. Use the Select:Options menu to select Screen Assignments.
4. Choose View. The Assignments of Port Security Screens dialog box appears.

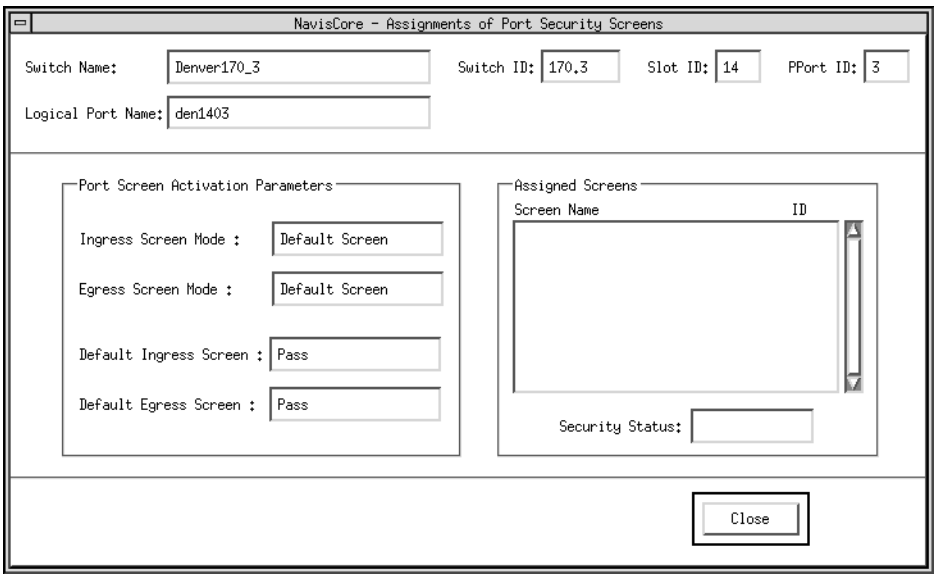


Figure 19-6. Assignments of Port Security Screens Dialog Box

The Port Screen Activation Parameters fields provide the default security screen settings for this logical port. See Table 19-1 on page 19-2 for field descriptions.

The Assigned Screens list box provides each screen name assigned to this logical port.

5. Choose Close to exit this dialog box.

20

Configuring PNNI Routing

This chapter describes how to configure the ATM Private Network-to-Network Interface (PNNI) routing protocol and routing hierarchies in your Lucent network. The PNNI is a standard designed by the ATM Forum. This standard defines both an ATM routing protocol and an ATM signaling protocol. Lucent supports PNNI on both the CBX 500 switch and GX 550 Multiservice WAN switch platforms.

For a detailed explanation of PNNI routing and signaling, see the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0* (af-pnni-0055.000), available from the ATM Forum's Web site: **`http://www.atmforum.com`**.

This chapter describes the following topics and tasks:

- Supported PNNI Features
- PNNI Routing Protocol Overview
- PNNI Signaling Overview
- Integrating VNN OSPF and PNNI Networks
- Frame Relay-to-PNNI Interworking
- PNNI Reroute Load Balancing
- Resilient UNI and APS Resilient UNI Over PNNI
- Configuring PNNI Routing
- Configuring Offnet PVCs Over PNNI
- PNNI Trap Support

Supported PNNI Features

The following table displays the supported PNNI features for this and previous releases of Lucent NavisCore and switch code. These features are PNNI 1.0 compliant.

Table 20-1. Supported PNNI Features

Feature	NavisCore 5.1.0.0 GX 2.2.2.0 CBX 4.2.2.0	NavisCore 5.3.1.0 GX 2.3.1.0 CBX 4.3.1.0	NavisCore 8.0.0.0 GX 8.0.0.0 CBX 8.0.0.0	NavisCore 8.1.0.0 GX 8.1.0.0 CBX 8.1.0.0	NavisCore 9.0.0.0 GX 9.0.0.0 CBX 9.0.0.0
CBX/GX PVC					
VNN	Y	Y	Y	Y	Y
PNNI	Y	Y	Y	Y	Y
Mixed*	Y	Y	Y	Y	Y
SPVC					
VNN	Y	Y	Y	Y	Y
PNNI	Y	Y	Y	Y	Y
Mixed*	Y	Y	Y	Y	Y
Hierarchical PNNI					
3 Levels	N	Y	Y	Y	Y
4 Levels	N	N	N	N	Y
PNNI-VNN Integration	Y	Y	Y	Y	Y
PSAX Integration					
Flat PNNI	Y	Y	Y	Y	Y
Hierarchical PNNI	N	N	N	N	N
UBR Load Balancing					
VNN	Y	Y	Y	Y	Y
PNNI	Y	Y	Y	Y	Y
Mixed*	Y	Y	Y	Y	Y
Route Advertisement Suppression	N	Y	Y	Y	Y

Table 20-1. Supported PNNI Features (Continued)

Feature	NavisCore 5.1.0.0 GX 2.2.2.0 CBX 4.2.2.0	NavisCore 5.3.1.0 GX 2.3.1.0 CBX 4.3.1.0	NavisCore 8.0.0.0 GX 8.0.0.0 CBX 8.0.0.0	NavisCore 8.1.0.0 GX 8.1.0.0 CBX 8.1.0.0	NavisCore 9.0.0.0 GX 9.0.0.0 CBX 9.0.0.0
Reroute Load Balancing					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	Y	Y
Mixed*	N	N	N	N	N
Frame/ATM Interworking					
PVC - VNN					
Frame/Frame	Y	Y	Y	Y	Y
ATM/Frame	Y	Y	Y	Y	Y
Frame/ATM	Y	Y	Y	Y	Y
PVC - PNNI					
Frame/Frame	Y	Y	Y	Y	Y
ATM/Frame	Y	Y	Y	Y	Y
Frame/ATM	Y	Y	Y	Y	Y
PVC - Mixed*					
Frame/Frame	Y	Y	Y	Y	Y
ATM/Frame	Y	Y	Y	Y	Y
Frame/ATM	Y	Y	Y	Y	Y
SPVC - VNN					
Frame/Frame	N	N	N	N	N
ATM/Frame	N	N	N	N	N
Frame/ATM	N	N	N	N	N
ATM/ATM	Y	Y	Y	Y	Y
SPVC - PNNI					
Frame/Frame	N	N	N	N	N
ATM/Frame	N	N	N	N	N

Table 20-1. Supported PNNI Features (Continued)

Feature	NavisCore 5.1.0.0 GX 2.2.2.0 CBX 4.2.2.0	NavisCore 5.3.1.0 GX 2.3.1.0 CBX 4.3.1.0	NavisCore 8.0.0.0 GX 8.0.0.0 CBX 8.0.0.0	NavisCore 8.1.0.0 GX 8.1.0.0 CBX 8.1.0.0	NavisCore 9.0.0.0 GX 9.0.0.0 CBX 9.0.0.0
Frame/ATM	N	N	N	N	N
ATM/ATM	Y	Y	Y	Y	Y
SPVC - Mixed*					
Frame/Frame	N	N	N	N	N
ATM/Frame	N	N	N	N	N
Frame/ATM	N	N	N	N	N
SVC - VNN					
Frame/Frame	Y	Y	Y	Y	Y
ATM/Frame	N	N	N	N	N
Frame/ATM	Y	Y	Y	Y	Y
SVC - PNNI					
Frame/Frame	N	N	N	N	N
ATM/Frame	N	N	N	N	N
Frame/ATM	N	N	N	N	N
SVC - Mixed*					
Frame/Frame	N	N	N	N	N
ATM/Frame	N	N	N	N	N
Frame/ATM	N	N	N	N	N
Resilient UNI					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	Y	Y
VNN-PNNI	N	N	N	Y	Y
PNNI-VNN	N	N	N	Y	Y
VNN-PNNI-VNN	N	N	N	N	N
PNNI-VNN-PNNI	N	N	N	Y	Y

Table 20-1. Supported PNNI Features (Continued)

Feature	NavisCore 5.1.0.0 GX 2.2.2.0 CBX 4.2.2.0	NavisCore 5.3.1.0 GX 2.3.1.0 CBX 4.3.1.0	NavisCore 8.0.0.0 GX 8.0.0.0 CBX 8.0.0.0	NavisCore 8.1.0.0 GX 8.1.0.0 CBX 8.1.0.0	NavisCore 9.0.0.0 GX 9.0.0.0 CBX 9.0.0.0
Automatic Protection Switching	N	N	N	Y	Y
Connection Trace					
VNN	N	N	N	N	N
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
Layer 2 VPN					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
Circuit Definted Path (Beta in 9.0.0.0)					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
FRF.5					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
Point-MultiPoint PVC					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
Circuit List					
VNN Trunk	Y	Y	Y	Y	Y
PNNI Trunk	N	N	N	N	Y

Table 20-1. Supported PNNI Features (Continued)

Feature	NavisCore 5.1.0.0 GX 2.2.2.0 CBX 4.2.2.0	NavisCore 5.3.1.0 GX 2.3.1.0 CBX 4.3.1.0	NavisCore 8.0.0.0 GX 8.0.0.0 CBX 8.0.0.0	NavisCore 8.1.0.0 GX 8.1.0.0 CBX 8.1.0.0	NavisCore 9.0.0.0 GX 9.0.0.0 CBX 9.0.0.0
Redundancy of Management Traffic					
MPVC					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y
MSPVC					
VNN	Y	Y	Y	Y	Y
PNNI	N	N	N	N	Y
Mixed*	N	N	N	N	Y

* Mixed signifies network configurations with VNN/PNNI combined setups, including VNN-PNNI, PNNI-VNN, VNN-PNNI-VNN, and PNNI-VNN-PNNI.

PNNI Routing Protocol Overview

The PNNI routing protocol provides for dynamic routing configuration and a highly scalable routing scheme. In an ATM network, nodes (switches) that support PNNI routing are organized into peer groups. Each peer group is identified by a *peer group identifier*. All nodes within the same peer group have identical peer group identifiers. A peer group identifier consists of two parameters:

1st byte — peer group *level* (0 – 104)

Bytes 2-14 — peer group *identifier*

Each switch within a peer group is identified by a PNNI *node identifier*. The switch derives the node identifier by concatenating its peer group level, the hexadecimal value 0xA0, and its 20-octet private ATM address. (If the ATM address is not configured, its value defaults to the concatenation of the peer group identifier and the Media Access Control [MAC] address of the switch.) For more information about these PNNI node parameters, see "Configuring PNNI Node Parameters" on page 20-29.

Hierarchical Organization

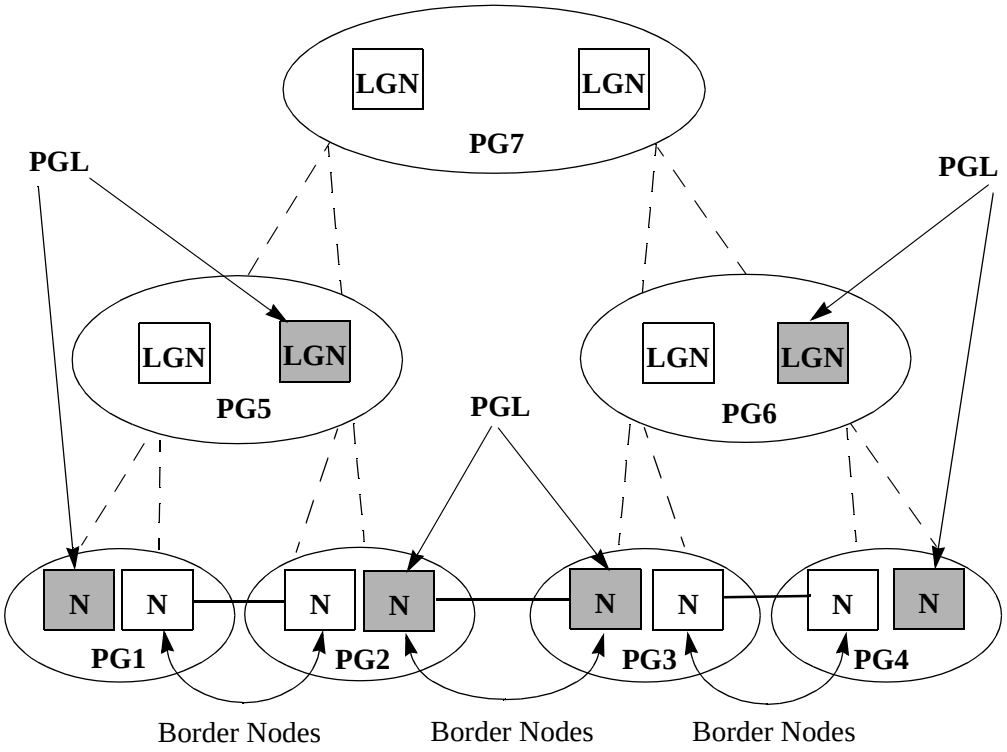
Peer groups can be organized hierarchically. To accomplish a hierarchical organization of peer groups, each peer group is represented to the next level of hierarchy by an abstract entity called a logical group node (LGN). A node in the child peer group, called the peer group leader (PGL), performs the logical group node functions. Members of the peer group communicate to elect the PGL based on leadership priority. If a node is configured with a higher leadership priority value than zero, it is eligible to become the PGL of a peer group. The member that has the highest leadership priority is chosen to be the PGL. The PGL summarizes information and supplies that information to the LGN in the next level.

Note – To ensure redundancy if a PGL is disabled, Lucent recommends that you configure at least two PGL-capable switches for each lower-level peer group in the hierarchy.

Configuring a PGL is not necessary, nor is it recommended, at the highest peer group level in the hierarchy.

For more information about configuring PGL leadership priority, see Table 20-6 on page 20-37.

Figure 20-1 shows an example of a three-tiered PNNI routing hierarchy, with eight lower-level nodes divided into four peer groups (PG1 - PG4). Nodes with links to other peer groups act as border nodes. A node acting as the LGN is also a PGL of the child peer group at the next lower level.



Legend
N = Lowest-level Node
LGN = Logical Group Node
PG = Peer Group
PGL = Peer Group Leader

Figure 20-1. Three-Tiered PNNI Routing Hierarchy Example

Note – Lucent switches support a maximum of 400 nodes and 1000 links per peer group. However, Lucent recommends a maximum peer group size of 100 nodes and 500 links to take advantage of the significant scalability provided by PNNI routing hierarchy.

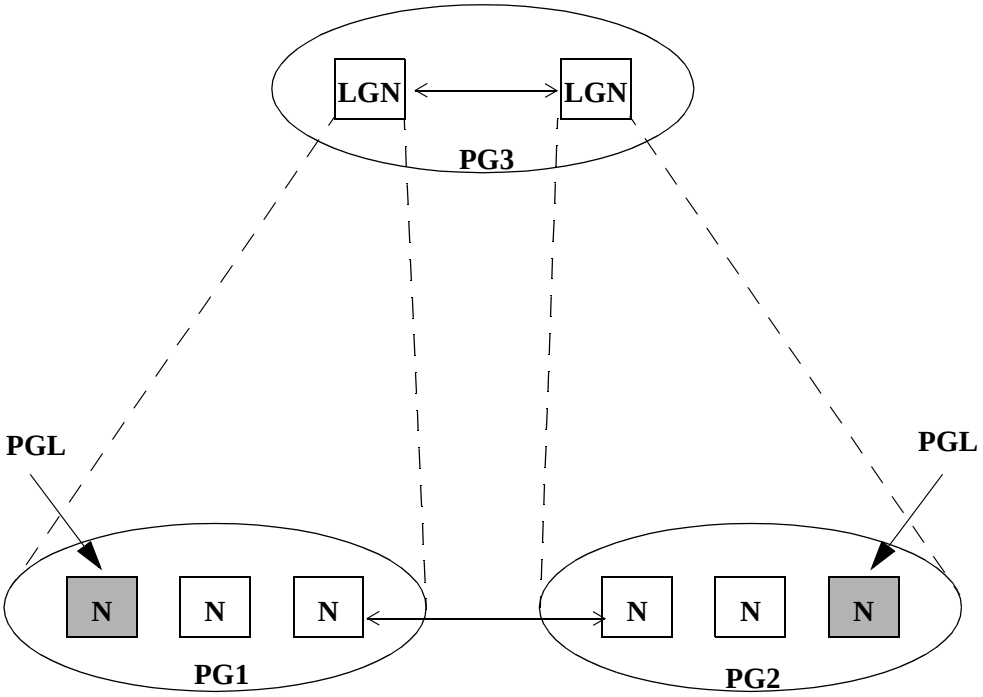
As the parent of its child peer group, the LGN joins the next highest peer group in the hierarchy, which can be made up of other parents (that is, LGNs) representing other child peer groups. In turn, the members of the next highest peer group in the hierarchy choose a PGL, which summarizes information to the LGN in the hierarchical chain, forming multiple peer group levels.

PNNI Routing Example

Figure 20-2 shows a simple two-tiered PNNI routing hierarchy, with six lowest-level nodes divided into two child peer groups (PG1 and PG2). The LGNs that are the parents of each of the child peer groups form a top-tier peer group (PG3).

Peer groups may contain both LGNs and lowest-level nodes. For example, in Figure 20-2, a lowest-level node could also be a member of PG3. A node's membership within the hierarchy is determined by the network configuration. In other words, the network administrator configures the hierarchical structure.

Neighboring nodes (LGN or lowest-level node) within a peer group exchange information to synchronize their topology databases. The topology database contains information about the peer group in which a node resides and information that allows the node to reach destinations in other peer groups. A node receives information about the network beyond the peer group from its PGL.



Legend
N = Lowest-level Node
LGN = Logical Group Node
PG = Peer Group
PGL = Peer Group Leader

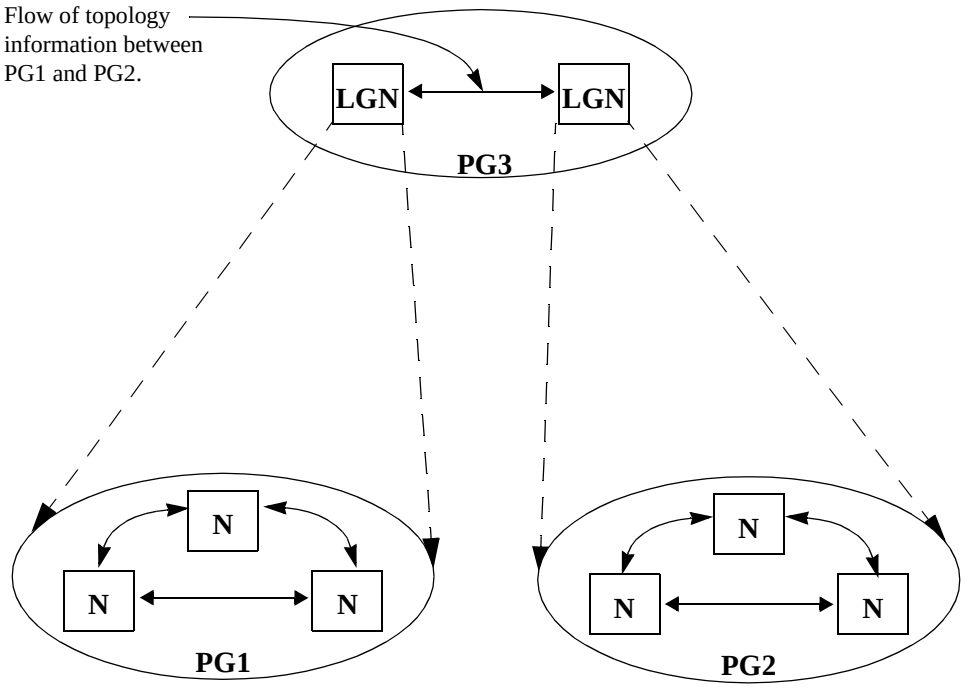
Figure 20-2. Two-Tiered PNNI Routing Hierarchy Example

The PGL node aggregates all of the topology information from its peer group and propagates (distributes) a summarized version of that information to the LGN higher-level peer group. In turn, the PGL receives summarized routing information from its LGN and distributes that information to the other nodes in its peer group.

Note – Each PGL exchanges aggregated topology information with its own LGN vertically within the hierarchy. Peer group leaders do not exchange topology information with other peer group leaders.

This automated collection and propagation process eliminates the need for manual configuration and maintenance of routing information about network nodes. In effect, PNNI allows network nodes to automatically learn the topology of the network, and use the topological knowledge they acquire to route data to its correct destination.

Figure 20-3 illustrates the flow of PNNI topology information within peer groups and between peer groups. The neighboring nodes in each peer group exchange topology information to synchronize each other's topology databases. The LGNs also propagate information about how to reach their child groups to other LGNs.



Legend
N = Lowest-level Node
LGN = Logical Group Node
PG = Peer Group

Figure 20-3. Flow of PNNI Topology Information

PNNI Packets

The following packets carry PNNI control information during exchanges between neighbors:

Hello Packets — Contain information that neighboring nodes exchange to discover and verify each other's identity and to determine the status of the links that connect them.

Database Summary Packets — Contain the identifying information of all **PNNI Topology State Elements (PTSEs)** in a node's topology database. A PTSE is a collection of PNNI topology information that is sent to all nodes in a peer group. PTSEs contain network resource information used to determine the least-cost path between two endpoints. PTSEs can represent information that pertains to PNNI nodes, links, or ATM addresses.

When a node first learns that a neighboring peer node residing in the same peer group exists, it initiates a database exchange process in order to synchronize its topology database with its neighbor. When one neighbor sends a database summary packet to another neighbor, the other neighbor responds with its own database summary packet.

PTSE Request Packets — Contain one or more entries that request PTSEs. When a node examines received database summary packets from neighbors and detects one or more missing PTSEs in its topology database, it builds a PTSE request packet. This packet contains a list of IDs that identify the missing PTSEs. The node sends the PTSE request packet to neighbors, which respond with a PTSP.

PNNI Topology State Packets (PTSPs) — Contain one or more PTSEs. A node sends PTSPs when it:

- Detects that its local topology information has changed, in which case it immediately sends PTSP(s) containing information about the change to its neighbors.
- Receives a PTSP containing new topology information from a neighbor; the node then propagates this information to other neighbors in PTSP packets.
- Responds to PTSE requests during topology database synchronization.

The first two items above describe the most common reasons for sending PTSPs. The last item describes the initial database exchange between neighboring PNNI nodes.

PTSE Acknowledgment Packets — Contain acknowledgments of PTSEs received from a neighbor. A node acknowledges receipt of PTSEs from its neighbors by sending one PTSE acknowledgement packet for each valid PTSE received.

Fast Inter-card APS 1+1 PNNI Interworking with the PSAX 4500

The Fast Inter-card Automatic Protection Switching (APS) 1+1 option is available on the GX 550 switch for PNNI link connections to PSAX 4500 devices. Fast Inter-card APS 1+1 (Fast APS 1+1) PNNI interworking with the PSAX 4500 is supported only on GX 550 OC-3c/STM-1 and OC-12c/STM-4 modules. If an equipment failure occurs, SVCs and SPVCs traversing the PNNI link connection are preserved.

Note – Bellcore GR-253-CORE, ITU G.841, Annex B (formerly ITU G.783, Annex B), and ITU G.841 section 7.1 (formerly ITU G.783, Annex A) standards form the basis of the Lucent APS implementation. Review these specifications and standards for further information on how you can use APS in a network environment.

For information on configuring Fast APS 1+1 on GX 550 4-port OC-3c/STM-1 and 1-port OC-12c/STM-4 modules, see the *B-STDX, CBX, and GX Switch Module Configuration Guide*.

See the following sections in this guide for more information on configuring Fast APS 1+1 on GX 550 PNNI links:

- "About Automatic Protection Switching" on page 7-5
- "Configuring Fast APS 1+1 for PNNI Links (GX 550 to PSAX 4500 Only)" on page 7-39

Note – Fast APS 1+1 is not supported in hierarchical PNNI network configurations.

The current release supports GX 550 Fast APS 1+1 PNNI interworking with the PSAX 4500 for SVCs and SPVCs *only*. PVCs routed over PNNI links by means of a Lucent ATM SPVC node prefix will not be preserved during a protection switch. PVCs established between NNI logical ports are also not protected during an APS switchover.

Logical Port and Protocol Types

In Lucent's PNNI implementation, you can configure both virtual and direct PNNI logical ports. When you use NavisCore to configure PNNI logical ports, the logical port type is ATM NNI (Network-to-Network Interface), and the protocol type is PNNI 1.0.

PNNI Administrative Weight

When you configure a logical port, you can assign an administrative weight to each Quality of Service (QoS) category. This weight allows you to configure the network to favor one path over another path for a given QoS category, when the path constraint for an ATM virtual circuit is administrative weight. The weights of all the network interfaces along a path are added up. Switches choose the path with the lowest cumulative weight when making routing decisions, assuming that all links can provide the resources requested by the call.

Note – Administrative weight (Admin Cost) is the default routing metric. Administrative weight is not used if you select a different routing metric (end-to-end delay or cell delay variation [CDV]). For more information about routing metrics, see "Setting Quality of Service Parameters" on page 3-44.

The following examples describe how PNNI administrative weight configurations can function in a PNNI network:

- Suppose that variable bit rate-real time (VBR-RT) traffic has two available paths for reaching a given destination. One path has a weight of 1000 while another path has a weight of 4000. The switch will choose the path with the weight of 1000, if the call requests VBR-RT QoS and administrative weight as a metric *and* if the path has sufficient bandwidth and other metric resources.
- In a network that supports both constant bit rate (CBR) and unspecified bit rate (UBR) calls, PNNI administrative weight values can be configured so that the switch will choose one path for the CBR calls and a different path for the UBR calls.

For information about configuring PNNI administrative weight parameters, see Table 20-10 on page 20-46.

UBR Load Balancing Over Parallel PNNI Links

When the unspecified bit rate (UBR) service class is supported in a network, load balancing distributes UBR calls equally over parallel PNNI links between the same two switches. You can disable this feature by assigning different administrative weights to the parallel links.

For information about the UBR service class, see Chapter 10, "Configuring ATM Traffic Descriptors."

PNNI Signaling Overview

This section provides a brief overview of PNNI signaling. For a detailed explanation of PNNI signaling, see the *ATM Forum Technical Committee Private Network-Network Interface Specification Version 1.0* (af-pnni-0055.000), available from the ATM Forum's Web site: **`http://www.atmforum.com`**.

PNNI signaling allows ATM SVC and soft permanent virtual circuit (SPVC) calls to be set up across a private network that supports the PNNI protocol.

Note – In the current release, PNNI signaling is supported for ATM Point-to-Point and Point-to-Multipoint SVCs and ATM Point-to-Point SPVCs only. PNNI signaling is not currently supported for use with ATM Point-to-Multipoint SPVCs.

Lucent ATM PVCs can be established over a PNNI routing domain as well as over a routing domain that supports both VNN ATM and PNNI.

PNNI signaling is based on a subset of User-to-Network Interface (UNI) 4.0 signaling.

UNI 4.0 Signaling Features

PNNI signaling adds support for the following UNI 4.0 signaling features:

- PNNI routing for dynamic call setup.
- PNNI crankback for reattempting a connection setup in progress that has encountered a partial failure. Crankback allows the dynamic rerouting of call setups around failed nodes or links (or links with insufficient resources).

PNNI signaling does not support some UNI 4.0 signaling features, such as leaf-initiated join capability or user-to-user supplementary service.

PNNI signaling makes use of PNNI routing information. PNNI uses the route calculations derived from the reachability, connectivity, and resource information dynamically maintained by PNNI routing. These routes are calculated as needed from the node's view of the current topology.

PNNI and CBX/GX PVCs

NavisCore allows for the configuration of CBX/GX PVCs through the selection of PVC endpoints (node/lport), only. The optimal circuit *path* that the PVC traverses is not defined; instead, the path is chosen dynamically by Lucent internal routing protocols. This feature provides a significant degree of fault tolerance for the circuit. In case of circuit failure, an alternate path is chosen automatically and the PVC is rerouted over the new path, without requiring that you reconfigure the permanent virtual circuit.

This dynamic routing support for PVCs can now extend to PNNI networks or PNNI/VNN hybrid networks through the use of an automatically advertised address, called the *Lucent ATM SPVC node prefix*. This feature allows PVCs with any combination of Frame Relay UNI, ATM UNI, or PPP logical ports to be routed over a PNNI path or PNNI/VNN path combination.

Lucent ATM SPVC Node Prefix

Each CBX 500 and GX 550 switch can automatically advertise a unique 13-byte ATM node prefix, in which is embedded the switch's 4-byte internal IP address. You can identify the SPVC node prefix address in the following way: the address is formed by concatenating the Local AFI value (0x49), the Lucent OUI (0x00C07B), and x02. The switch's internal IP address is then inserted in the last 4 bytes (hexadecimal format).

For example, a switch that has an internal IP address of 153.167.1.5 advertises the following SPVC node prefix:

```
0x4900C07B020000000099A70105
```

Both the VNN OSPF and PNNI routing protocols on the switch advertise the SPVC node prefix. Therefore, if the path for an ATM PVC cannot be determined using the traditional VNN routing mechanism, the calling node instead will automatically attempt to establish a path to the destination node's SPVC prefix. This function allows the use of both PNNI paths and hybrid PNNI/VNN paths to establish the ATM PVC.

When an ATM PVC is routed using the destination node's SPVC node prefix as the destination address, a 20-byte ATM address is constructed, using the SPVC node prefix as the first 13 bytes; the destination LPort is inserted in the last two bytes. If the call traverses the PNNI domain, the destination VPI/VCI is inserted in both the Broadband Higher Level Information (BHLI) information element (IE) and the Called Party SPVC IE.

Because this routing mechanism is performed automatically, it allows the establishment of ATM PVCs over PNNI domains or over a combination of PNNI/VNN domains, without requiring any reconfiguration of ATM permanent virtual circuits.

Integrating VNN OSPF and PNNI Networks

The following sections describe how Virtual Network Navigator (VNN) networks, which use the Lucent Open Shortest Path First (OSPF) implementation, can integrate with PNNI networks through Lucent PNNI/VNN gateway support.

PNNI/VNN Gateway Support

A PNNI/VNN gateway is a switch that is configured with both PNNI ATM NNI logical ports and OSPF ATM Direct or OPTimum trunks. The PNNI/VNN gateway switch connects to and is a member of both routing domains. PNNI/VNN gateway support allows a VNN backbone network to interconnect PNNI regional networks, or a PNNI backbone network to interconnect VNN OSPF regional networks. The backbone network handles the internetworking traffic between all the regional networks.

Importing Exterior Addresses

To activate dynamic routing over a backbone network of ATM circuits that terminate in different regional networks, you must enable the Import Exterior Addresses function on all PNNI/VNN gateway switches. Enabling this function allows addresses from one regional network to be automatically routed across the backbone network to other regional networks. (See "Configuring Global Variables" on page 20-41 for information about enabling the Import Exterior Addresses function.)

Once the addresses are imported, PNNI and VNN OSPF call interworking automatically routes the ATM calls to the appropriate destinations, as described in the following section.

PNNI and VNN OSPF Call Interworking

CBX 500 and GX 550 switches support ATM call interworking between PNNI and VNN OSPF routing domains. When addresses are shared between PNNI and VNN OSPF routing domains, ATM call interworking dynamically routes ATM PVCs, ATM SVCs, ATM Point-to-Point SPVCs, and ATM Point-to-Multipoint PVCs across both domains. PNNI and VNN OSPF call interworking is automatic, provided the switch is configured as a PNNI node.

Interworking VNN ATM PVCs with PNNI

VNN ATM PVCs can be reestablished over complete or partial PNNI paths without reconfiguring the PVCs.

Native E.164 Address Advertisement

PNNI automatically advertises local Native E.164 addresses as well as Native E.164 addresses reachable from VNN OSPF over the PNNI routing domain. To advertise these addresses, PNNI converts the Native E.164 address format to the ATM E.164 End System Address (AESA) format. This function allows Frame Relay addresses to be advertised as ATM addresses across the ATM PNNI routing domain.

For information about address formats and routing options, see Chapter 15, "Configuring SVC Parameters."

Filtering PNNI and VNN OSPF Address Advertisements

You can partially or totally filter address advertisements between VNN OSPF and PNNI routing domains, as described in the following sections.

Disabling PNNI/VNN Gateway Support

You can turn off PNNI/VNN gateway support on any gateway switch to prevent addresses from being advertised between VNN OSPF and PNNI routing domains. To turn off PNNI/VNN gateway support on a gateway switch, you can disable the node global address sharing variables, VNN to PNNI and/or PNNI to VNN. (See "Configuring Global Variables" on page 20-41 for more information.)

Route Advertisement Suppression

You can filter, or suppress, *specific* ATM address or prefix advertisements between adjacent VNN OSPF and PNNI routing domains by enabling the Suppress PNNI and/or OSPF Advertisement parameter(s) when you configure ATM addresses or prefixes. You must enable route advertisement suppression for the protocol of the domain(s) where you want to suppress address advertisement.

For example, if the ATM prefix, 0x4711111111, is configured on a PNNI/VNN gateway with Suppress PNNI Advertisement enabled, the switch will not advertise any addresses that have this prefix in the PNNI domain. See Chapter 15, "Configuring SVC Parameters," for more information.

Connection Trace

You can use the Connection Trace feature to determine the logical nodes and logical links traversed by an existing ATM circuit (PVC, SVC, or SPVC). Connection Trace enables you to view the circuit path from the trace source node to the trace destination node. Connection tracing is supported both in PNNI routing domains and in combined PNNI/VNN networks.

You can view Connection Trace information for any of the following ATM circuit types:

- ATM point-to-point PVCs
- ATM point-to-multipoint PVCs
- ATM SVCs
- ATM point-to-point SPVCs
- ATM point-to-multipoint SVCs
- Offnet PVCs

When you display information for one of these ATM circuit types in the appropriate Set All [*Circuit-Type*] or Show [*Circuit-Type*] dialog box in NavisCore, Connection Trace information appears in the Circuit Path, Actual Path, or Path to Destination field. For example, Connection Trace information for an ATM point-to-point PVC is displayed in the Circuit Path field on the Set All PVCs on Map dialog box, as shown in the example in Figure 20-4.

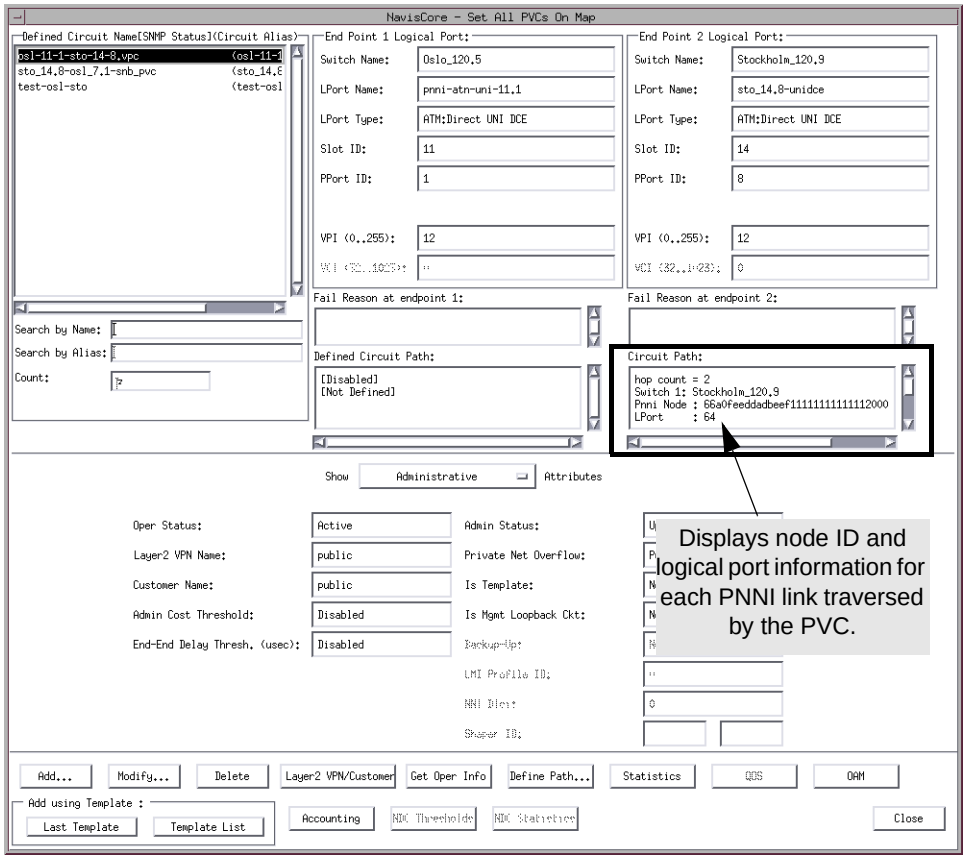


Figure 20-4. Set All PVCs on Map Dialog Box (Connection Trace Information)

Table 20-2 lists the dialog box and field name in NavisCore that displays Connection Trace information for each supported ATM circuit type, and where to look in this guide and other Lucent documentation for more information.

Table 20-2. Displaying Connection Trace Information for ATM Circuits

Circuit Type	NavisCore Dialog Box	Dialog Box Field	See
ATM Point-to-Point PVCs	Set All PVCs On Map	Circuit Path	Table 8-3 on page 8-12
ATM Point-to-Multipoint PVCs	Set All Point-to-Multiple Point Circuit Roots	Actual Path	Table 8-22 on page 8-77
ATM SVCs	Show Active SVC Attributes	Path to Destination	Chapter 12, "Monitoring ATM Circuits," in *B-STDX, CBX, and GX Switch Diagnostics User's Guide*
ATM Point-to-Point SPVCs	Set All Point-to-Point SPVCs	Path to Destination	Table 17-3 on page 17-7
ATM Point-to-Multipoint SVCs	Set All Point-to-Multipoint SVCs	Path to Destination	Chapter 12, "Monitoring ATM Circuits," in *B-STDX, CBX, and GX Switch Diagnostics User's Guide*
Offnet PVCs	Set All Offnet PVCs on Map	Path to Destination	Figure 20-13 on page 20-53

Frame Relay-to-PNNI Interworking

CBX 500 and GX 550 switches support Frame Relay-to-PNNI interworking of CBX/GX PVCs (that is, proprietary SPVCs) across either PNNI or ATM OSPF/PNNI networks.

Note – The current release does not support Frame Relay-to-PNNI interworking of SVCs or SPVCs.

Circuit endpoints can be any combination of Frame Relay UNI, Frame Relay NNI, ATM UNI, or Point-to-Point Protocol (PPP) logical ports. All intermediate trunk endpoints must be configured as PNNI ATM NNI logical ports, or OSPF direct or OPTimum trunk logical ports.

Note – OSPF can interwork Frame UNI or Frame trunk logical ports onto an ATM trunk; PNNI can interwork Frame UNI or PPP logical ports onto a PNNI trunk. Interworking an OSPF Frame trunk with a PNNI trunk is *not* currently supported.

Frame Relay-to-PNNI interworking is supported on both cell-based and frame-based I/O modules for the CBX 500 and GX 550 switch platforms, as follows:

- Frame Relay support is provided by CBX 500 IOM2 modules.
- ATM support is provided by CBX 500 IOM1 and IOM4 modules, and GX 550 BIO1, BIO2, and BIO-C modules.

PNNI Reroute Load Balancing

This section describes the PNNI Reroute Load Balancing feature. This feature automatically reroutes active PVCs and SPVCs within the PNNI routing domain to lower cost paths as they become available. In addition, this feature also provides graceful recovery when PNNI link connections or modules go out of service (due to upgrades, reboots, or network failures).

When a PNNI link returns to service following a network disruption, Reroute Load Balancing gradually reroutes circuits over their original path without requiring manual intervention. This function also operates when new paths are established in the network, distributing circuits on a controlled basis to newly available links. By pacing circuit reroutes, Reroute Load Balancing prevents congestion on PNNI links and promotes efficient reuse of network resources.

PNNI Reroute Load Balancing Criteria

PNNI Reroute Load Balancing periodically examines active circuits in round-robin order to determine whether a better path through the PNNI routing domain is available. If a better path is detected, the circuit is first cleared over the original path and then re-established over the new path.

When a PNNI route returns to service, Reroute Load Balancing reroutes circuits back to their original path using the following criteria:

- When both the original and alternate PNNI routes are similar in cost, no reroute load balancing occurs and neither circuit is rerouted.
- When the original PNNI route offers a cost advantage, all circuits are rerouted back to this path.
- Reroute Load Balancing is performed according to the configured values for the Reroute Count and Reroute Delay parameters. See "Defining Reroute Tuning" on page 20-23 for more information.

Defining Reroute Tuning

PNNI Reroute Load Balancing uses the Reroute Tuning settings that you define on the switch to look for alternate routing paths. The Tuning feature 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.

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

Load Balancing Example

If a switch has four modules, each with 50 PVCs, and you set the reroute count to five 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.

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

Configuring Circuit Reroute-Tuning Parameters

To set the tuning parameters:

1. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears for the selected switch. (For more information about the Switch Back Panel dialog box, see the *B-STDX, CBX, and GX Getting Started User's Guide*.)
2. To configure switch parameters, choose Attrs. The Set Switch Attributes dialog box appears. (For more information about the Set Switch Attributes dialog box, see the *B-STDX, CBX, and GX Getting Started User's Guide*.)
3. On the Set Switch Attributes dialog box, choose Tuning from the Select:Options option menu, and then choose Set. The Set Switch Tuning Attributes dialog box appears, displaying the name and number of the selected switch (Figure 20-5).

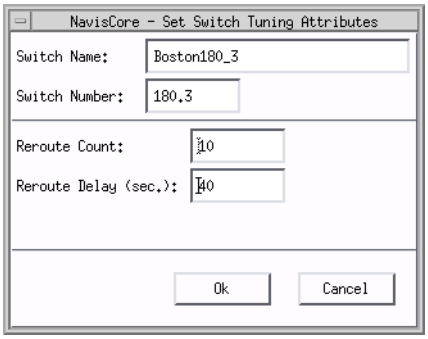


Figure 20-5. Set Switch Tuning Attributes Dialog Box

4. Complete the fields described in Table 20-3.

Table 20-3. Set Switch Tuning Attributes Fields

Field	Action/Description
Reroute Count	Enter a value between 0 (zero) 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 (sec.)	Enter a value between 1 and 32767 (in seconds). Choose an even value to enable load balancing, or choose an odd value to disable it. 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 180 seconds is a very conservative setting for normal operation.

5. Choose OK to return to the Set Switch Attributes dialog box.
6. Choose Apply to set the parameters and Close to exit the dialog box.

Resilient UNI and APS Resilient UNI Over PNNI

This section describes PNNI Resilient UNI and Automatic Protection Switching (APS) Resilient UNI support for ATM PVC circuits. This feature enables you to use the Resilient UNI or APS Resilient UNI features to configure fault-tolerant ATM PVCs across a PNNI or combined VNN/PNNI routing domain.

About Resilient UNI and APS Resilient UNI Over PNNI

A fault-tolerant ATM PVC configuration enables ATM UNI DCE and ATM DTE logical ports to serve as a backup for any number of active UNI ports. You manually activate the backup port if a primary port fails or if you need to take a primary port offline. This function is sometimes referred to as *resilient UNI*.

To automate resilient UNI/fault-tolerant ATM PVC functions, you can configure the CBX 500 or GX 550 physical port on which the ATM UNI logical port resides for Automatic Protection Switching (APS). APS Resilient UNI allows you to protect optical interfaces by provisioning a backup (protection) port that automatically takes over for the primary (working) port when a physical layer fault or module failure occurs.

You configure both Resilient UNI and APS Resilient UNI by associating a Service Name Binding with the working and protection logical port pair. The Service Name Binding is advertised to all switches in the network and contains address information indicating whether the primary (working) or backup (protection) port is currently active. If the primary (working) port fails and a manual or automatic switchover occurs, the Service Name Binding is re-advertised throughout the network to indicate that the backup (protection) port has been activated. When a switch receives this information, it reroutes circuits from the primary (working) port to the specified backup (protection) port.

The PNNI routing protocol advertises and recognizes Service Name Bindings using a specially-formatted ATM address. This extends Resilient UNI and APS Resilient UNI support to PVCs using paths that are entirely or partially within the PNNI routing domain.

Configuring Resilient UNI and APS Resilient UNI

You configure Resilient UNI and APS Resilient UNI over PNNI links just as you would for ATM VNN OSPF networks. For general information and configuration procedures, see the following sections in this guide and other Lucent documentation:

To Learn About	See
Resilient UNI (Fault Tolerant PVC)	
Configuring Fault Tolerant ATM PVCs (Resilient UNI)	• Chapter 12, "Configuring Fault-Tolerant PVCs"
APS Resilient UNI	
Enabling APS on CBX 500/GX 550 physical ports.	• Chapter 11, "Configuring Automatic Protection Switching (CBX and GX)," in *B-STDX, CBX, and GX Switch Module Configuration Guide*
Configuring APS Resilient UNI for ATM PVCs	• "About Automatic Protection Switching" on page 7-5 • Chapter 12, "Configuring Fault-Tolerant PVCs"

Using the show pnni names Command

You can use the **`show pnni names`** console command to display a list of all PNNI-reachable names, including Type 1 addresses (Resilient UNI names) that are used by PNNI to advertise Service Name Bindings in the network.

For detailed information about using the **`show pnni names`** command, see the *B-STDX, CBX, and GX Console Command User's Reference*.

Configuring PNNI Routing

Figure 20-6 displays the step sequence to configure PNNI routing for your network:

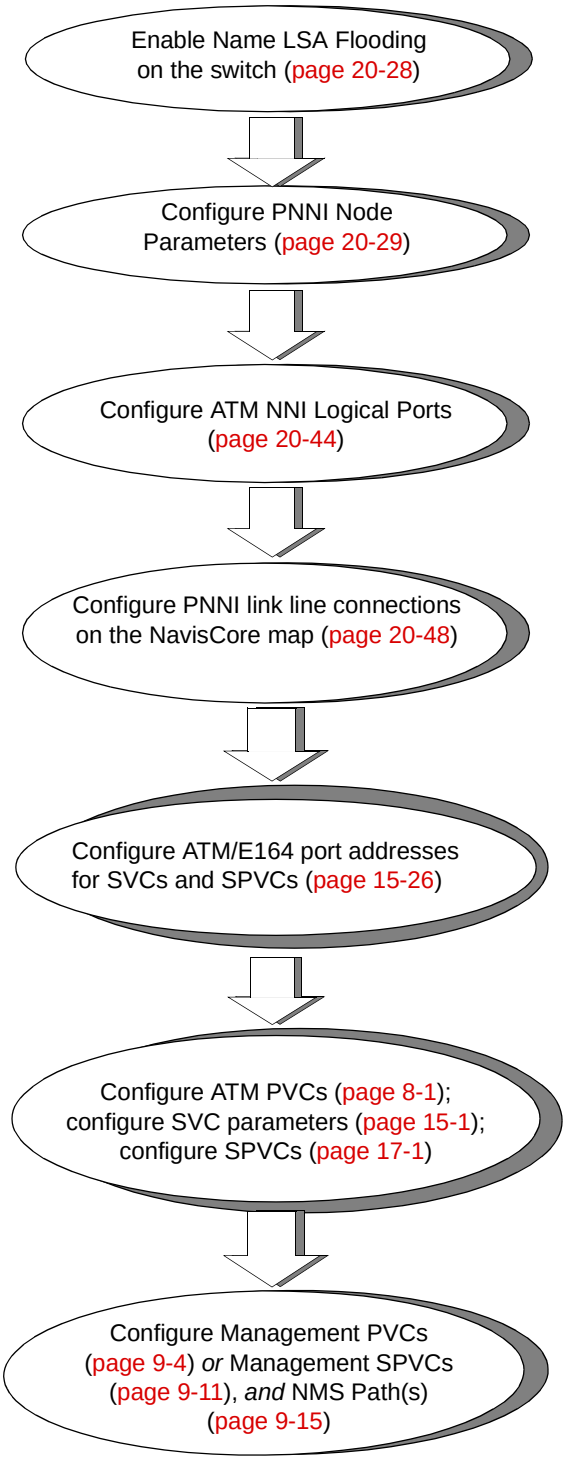


Figure 20-6. Configuring PNNI Routing

Enabling Name LSA Flooding on the Switch

To enable Lucent switches to use PNNI routing or to interoperate with PNNI switches in your network, you *must enable* the flooding of Name link state advertisements (LSAs) on the switch. Lucent switches flood NAME(3) and SUMM_NM(3) type LSAs over the VNN trunk interfaces. These LSAs bind the VNN switch IP address to an ATM address so the PNNI and VNN switches can communicate.

To enable Name LSA flooding on a CBX 500 or GX 550 switch:

1. From the network map, select the appropriate switch object. (If you are not already logged on, select NavisCore ⇒ Logon from the Misc menu, and enter your operator password.)
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel for the selected switch appears. (See the *B-STDX, CBX, and GX Getting Started User's Guide* for information about the functions you can access from the Switch Back Panel dialog box.)
3. Choose Attrs. The Set Switch Attributes dialog box appears. (See the *B-STDX, CBX, and GX Getting Started User's Guide* for more information about the Set Switch Attributes dialog box.)
4. In the PNNI Name Translation field on the Set Switch Attributes dialog box, select *Enable* to allow flooding of NAME(3) and SUMM_NM(3) LSAs for this switch.

Note – You *must enable* the PNNI Name Translation field if the switch uses PNNI routing or interoperates with other PNNI switches in your network.

5. Choose Apply to save your changes and close the dialog box.

For more information about configuring Name LSA flooding for VNN OSPF, see the *B-STDX and CBX IP Services Configuration Guide*.

Configuring PNNI Node Parameters

To begin using the PNNI routing protocol in your Lucent network, you need to configure the PNNI node parameters for each switch that supports PNNI in the network.

Accessing PNNI Node Parameter Functions

To access PNNI functions from the NavisCore Administer menu, select Lucent Parameters ⇒ Set All PNNI Node Parameters. The Set all PNNI Node Parameters dialog box (Figure 20-7) appears. All switches that support PNNI in the network are listed in the Node Name list box. Select the Node Name of the switch for which you want to display node parameter information.

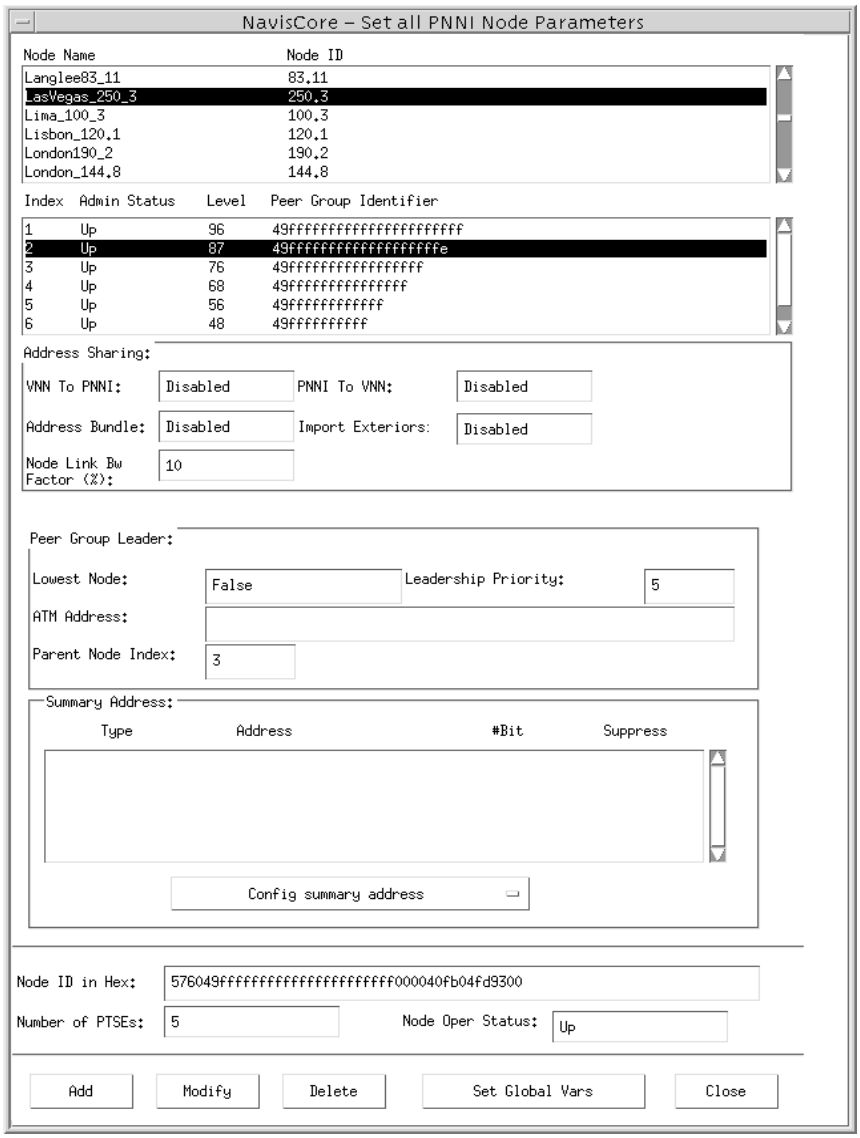


Figure 20-7. Set All PNNI Node Parameters Dialog Box

The Set All PNNI Node Parameters dialog box displays node information and allows you to perform the following actions:

- Once you add a PNNI node, the Set All PNNI Node Parameters dialog box displays the configured information for that node. To learn more about the Set All PNNI Node Parameters dialog box fields, continue with the following section.
- To add PNNI node information for the switch you select, see "Adding PNNI Node Parameters" on page 20-36.
- To add summary addresses, see "Adding PNNI Summary Addresses" on page 20-39.
- To configure global variables for address sharing, see "Configuring Global Variables" on page 20-41.

About the Set All PNNI Node Parameters Dialog Box

The Set All PNNI Node Parameters dialog box displays information about existing node parameters for the switch you select, and enables you to add, modify, or delete PNNI node information for this switch. It also provides several buttons that you can use to access additional node parameter functions.

Table 20-4 describes the buttons on the Set All PNNI Node Parameters dialog box.

Table 20-4. Set All PNNI Node Parameters Dialog Box Buttons

Field	Description
Add	Adds PNNI node information for the switch you select.
Modify	Modifies an existing PNNI node that you select.
Delete	Deletes an existing PNNI node that you select.
Set Global Vars	Enables you to configure variables for address sharing within the PNNI routing domain. Select this button to display the Set PNNI Node Global Variables dialog box. See Table 20-8 on page 20-42 for information about configuring these variables.

Table 20-5 describes the fields on the Set All PNNI Node Parameters dialog box.

Table 20-5. Set All PNNI Node Parameters Dialog Box Fields

Field	Description
Node Name	Displays the name of the switch.
Node ID	Displays the switch number used as the host assignment in the switch's internal IP address. ***Note:*** *This number is different from the PNNI Node ID, which is formatted as a 22-byte address.*
Index	Displays the row entry index value for the specific node instance that this entry represents. The index value can be from one to eight. A maximum of eight separate node instances can be configured per switch. Each additional node entry indicates that this switch is capable of being a peer group LGN at that level of the PNNI hierarchy. For example, a value of eight would indicate that this switch is capable of being an LGN at seven levels of the hierarchy.
Admin Status	Displays the PNNI administrative status (Up or Down). If PNNI Admin Status is Down, then PNNI Node Oper Status is also Down.
Level	Displays the PNNI level in the hierarchy of the selected node's peer group. It also represents the number of significant bits available for forming the PNNI peer group identifier. The value can be from 0 (zero) to 104. By determining the number of bits allocated for the peer group identifier, the PNNI level determines the level at which that node participates in the hierarchy. The numeric value of peer group level decreases as you move higher up in the hierarchy. For example, a node that is the ancestor of a peer group two levels lower will have fewer bits reserved for its peer group identifier than its grandchildren. As a result, the grandparent will have a smaller peer group identifier than the peer group identifier of its grandchildren.
Peer Group Identifier	Displays the identifier of the peer group to which the switch belongs. The number of significant bytes in the identifier is determined by the PNNI level value.
Global Variables for Address Sharing	
VNN To PNNI	Indicates whether or not internal addresses known to Virtual Network Navigator (VNN) should be advertised within the PNNI routing domain. Disabling this variable on a gateway switch prevents addresses from being advertised from VNN to PNNI routing domains. This parameter applies only to switches that have both VNN OSPF and PNNI trunks.

Table 20-5. Set All PNNI Node Parameters Dialog Box Fields (Continued)

Field	Description
PNNI To VNN	Indicates whether or not internal addresses known to PNNI should be advertised within the VNN domain. Disabling this variable on a gateway switch prevents addresses from being advertised from PNNI to VNN routing domains. This parameter applies only to switches that have both VNN OSPF and PNNI trunks.
Import Exteriors	Indicates whether or not addresses that are external to the PNNI (or VNN OSPF) routing domain can be imported to the PNNI (or VNN OSPF) routing domain. When this variable is enabled on PNNI/VNN gateway switches, addresses from different regional networks are automatically routed across a VNN OSPF or PNNI network backbone to other regional networks. This parameter applies only to switches that have both VNN OSPF and PNNI trunks. ***Note:*** *To prevent advertisement or call setup looping, the following safeguards are built into address exportation:* • *Addresses can be dynamically advertised across a* maximum *of three separate routing domains.* • *An address is not exported to a neighboring routing domain if that address is already defined as an interior reachable address within that domain.* *These safeguards cannot be disabled.*
Address Bundle	Indicates whether or not to support bundling addresses of equal cost into a single PTSE. Address bundling provides more efficient memory usage. ***Note:*** *This parameter applies to all PNNI switches, whether or not the switches support both VNN OSPF and PNNI trunks.*
Node Link BW Factor (%)	Represents the degree of significance in the change of Bandwidth on a PNNI link for a particular QoS service class, before that link is re-advertised in the network. The default is 10%. The range of possible values is 10% to 99%. For example, if BW Factor is 10%, a new horizontal link PTSE is advertised by the switch every time the available bandwidth of one of its links changes by 10% (or greater) of the maximum available bandwidth.

Table 20-5. Set All PNNI Node Parameters Dialog Box Fields (Continued)

Field	Description
Peer Group Leader	
Lowest Node	Indicates whether or not this node is configured as a lowest-level node in the switching system. This field displays one of the following values: *True* – (default) This node instance represents a lowest-level node in the switching system. *False* – This node instance represents a logical group node (LGN) that becomes active when its child node instance becomes a peer group leader (PGL). ***Note:*** *If multiple node instances are configured, only one node can have Lowest Node set to True.*
ATM Address	Represents this node's 20-octet private ATM address. If this node is an LGN, neighboring LGNs use this ATM address to establish the LGN switched virtual channel connection (SVCC) routing control channel (RCC) circuit to it, allowing for the exchange of PNNI protocol packets between the LGNs. In addition, the Node ID of the PNNI node instance is derived from the ATM address as follows: <PNNI level><0xA0><ATM address> ***Note:*** *If the ATM address is not configured, the value for this address defaults to the concatenation of the peer group ID and the MAC address.*
Parent Node Index	Identifies the node that will represent this peer group at the next higher level of the PNNI hierarchy, if the node becomes peer group leader. The range of values for this field is zero to eight. A value of zero (default) indicates this entry does not have a parent node. Any value greater than eight is invalid. ***Note:*** *When the LGN is configured, the parent node index of the child entry must be set to the index of the LGN entry, and the leadership priority value of the child must be higher than zero, which allows the LGN node to become active.*

Table 20-5. Set All PNNI Node Parameters Dialog Box Fields (Continued)

Field	Description
Leadership Priority	Indicates this node's priority status for becoming the PGL of its peer group. The node with the highest leadership priority within its peer group becomes the PGL and participates at the next level of the hierarchy. The range for this field is zero (default) to 205. A value of zero indicates this node is not PGL/LGN-capable. ***Notes:*** *When the PNNI hierarchical topology is rebuilt, for example, during a switch software upgrade, redundancy can be provided by configuring at least two PGL-capable nodes for each peer group. For more information about configuring leadership priority, see* *Table 20-6 on page 20-37**.* *If this node becomes the PGL of its peer group, it automatically increases its leadership priority by 50 to reduce the number of PGLs taking over in the hierarchy.*
Summary Address	
Type	Indicates the type of summary address selected. This field displays one of the following values: *Internal* – (default) Indicates the summary address is inside the PNNI routing domain. *Exterior* – Indicates the summary address is outside the PNNI routing domain.
Address	Displays the summary address. The summary address is an address prefix that indicates how the node summarizes reachability information.
# Bit	Displays the length of the summary address. The maximum length is 152 bits. The value can be zero if the Address field contains only zeros.
Suppress	Indicates whether or not the addresses summarized by this summary instance will be advertised. This field displays one of the following values: *False* – (default) Indicates that the summary should propagate to the peer group. *True* – Prevents the summary and the reachable addresses it summarizes from being advertised to the peer group.

Table 20-5. Set All PNNI Node Parameters Dialog Box Fields (Continued)

Field	Description
Config summary address	Enables you to add a new summary address prefix to be advertised by higher-level PNNI logical group nodes (LGNs) for possible aggregation within a given peer group. Aggregation results in fewer address advertisements outside of the peer group, which provides greater scalability. Select this option to add or delete PNNI summary instance address options. See Table 20-7 on page 20-40 for more information about configuring summary address parameters. ***Note:*** *Up to 128 ATM summary addresses can be configured per switch.*
Node ID and Status	
Node ID in Hex	Displays the PNNI node ID of the switch. This ID is not directly configurable; it is, however, indirectly configurable because it is derived from the node's ATM address, which can be configured. The switch derives the node ID by concatenating the PNNI Level, the hexadecimal value 0xA0, and the ATM address.
Number of PTSEs	Displays the number of PTSEs in the topology database of the switch. A PTSE is a collection of PNNI topology information that is sent to all nodes in a peer group.
Node Oper Status	Displays the PNNI operating status for the switch (Up or Down). If PNNI Admin Status is Down, then PNNI Node Oper Status is also Down.

Adding PNNI Node Parameters

To configure PNNI node information for up to eight node instances for the switch you select:

1. Complete the steps in "Accessing PNNI Node Parameter Functions" on page 20-29.
2. From the Node Name list box at the top of the Set All PNNI Node Parameters dialog box, select the switch for which you want to configure PNNI node parameters.
3. Choose Add. The Add PNNI Node Instance dialog box appears.

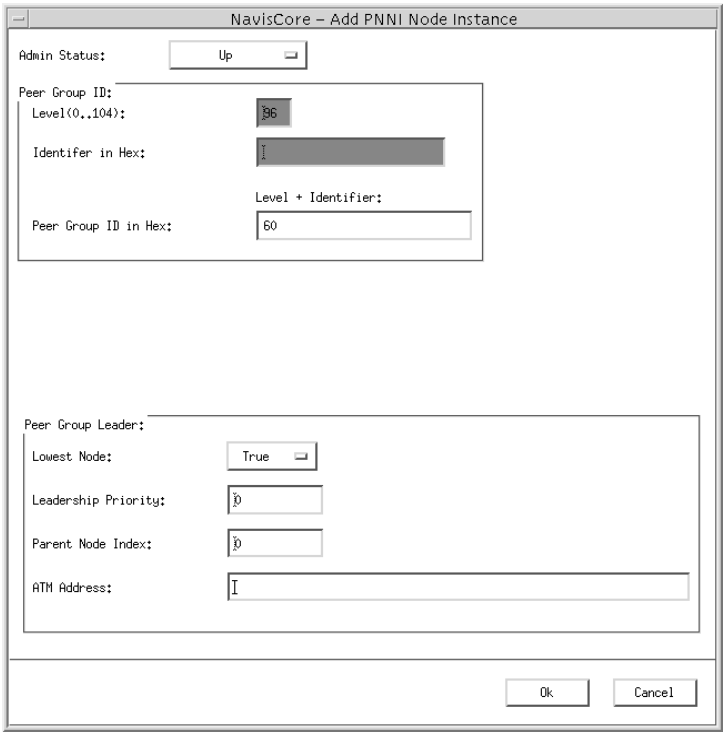


Figure 20-8. Add PNNI Node Instance Dialog Box

4. Complete the fields described in Table 20-6.

Table 20-6. Add PNNI Node Instance Dialog Box Fields

Field	Action/Description
Admin Status	Set the Admin Status Up (default) or Down. If PNNI Admin Status is Down, then PNNI Node Oper Status is also Down. (See Table 20-5 on page 20-31 for more information about the Node Oper Status field.)
Peer Group ID	
Level (0..104)	Sets the number of significant bits available for forming the PNNI peer group identifier. The value can be from 0 (zero) to 104. By determining the number of bits allocated for the peer group identifier, the PNNI Level also determines the level of the switch in the PNNI routing hierarchy. As you ascend the hierarchy, the number of bits allocated for peer group identifiers decreases, resulting in smaller peer group identifiers. For example, a node that is the grandparent of a peer group two levels lower will have fewer bits reserved for its peer group identifier than its grandchildren. As a result, the grandparent will have a smaller peer group identifier than the peer group identifier of its grandchildren.
Identifier in Hex	Enter a PNNI peer group identifier. This identifier functions as a routing prefix.
Peer Group ID in Hex	Displays the entered peer group level and identifier in hexadecimal format.
Peer Group Leader	
Lowest Node	Select *True* (default) to configure this node as a lowest-level node in the switching system. Select *False* if this node represents a higher-level logical group node (LGN) that becomes active when one of the other nodes in this switching system becomes a peer group leader (PGL).

Table 20-6. Add PNNI Node Instance Dialog Box Fields (Continued)

Field	Action/Description
Leadership Priority	Indicates this node's priority status for becoming the PGL of its peer group. The node with the highest leadership priority within its peer group becomes the PGL and participates at the next level of the hierarchy. Enter a number from zero (default) to 205. You must configure the value 0 (zero) if this node is *not* PGL/LGN-capable. Values greater than 205 are invalid. ***Note:*** *To ensure redundancy when the PNNI hierarchical topology is rebuilt (for example, during a switch software upgrade), you should configure at least two PGL-capable nodes in each peer group. If you want to guarantee that the same node will always be the primary PGL of its peer group (provided it remains active in the peer group), you must set the leadership priority of this node to a value that is 51 or higher than the leadership priority of any other PGL-capable nodes in the peer group.*
Parent Node Index	Enter a value from zero (default) to eight that identifies the node that will represent this peer group at the next higher level of the PNNI hierarchy (if the node becomes peer group leader). A value greater than 0 (zero) indicates this entry has a parent node. (Values greater than eight are invalid.) ***Note:*** *When you configure the LGN, the parent node index of the child entry must be set to the index of the LGN entry, and the leadership priority value of the child must be higher than zero, which allows the LGN node to become active.*
ATM Address	Enter a value up to 20 bytes long that represents this node's private ATM address. If it is an LGN, remote LGNs exchange PNNI protocol packets with this node by directing packets or calls to this address. If you enter fewer than 20 bytes, this field is right-padded with 0s (zeros). If you do not configure a value for the ATM address, NavisCore fills the field with all 0s (zeros), and passes this value to the switch. The switch then derives the node's private ATM address using the peer group ID and the MAC address.

5. Choose Ok to set the PNNI node instance parameters and return to the Set All PNNI Node Parameters dialog box.

Adding PNNI Summary Addresses

You can add a new address prefix to be advertised by higher-level PNNI logical group nodes (LGNs) for possible aggregation within a given peer group.

Note – You can also configure summary addresses for lowest-level node instances.

To add a new address prefix to be advertised by higher-level PNNI logical group nodes (LGNs):

1. Complete the steps in "Accessing PNNI Node Parameter Functions" on page 20-29.
2. Choose Config summary address.
3. Choose Add. The Add PNNI Summary Instance dialog box appears.

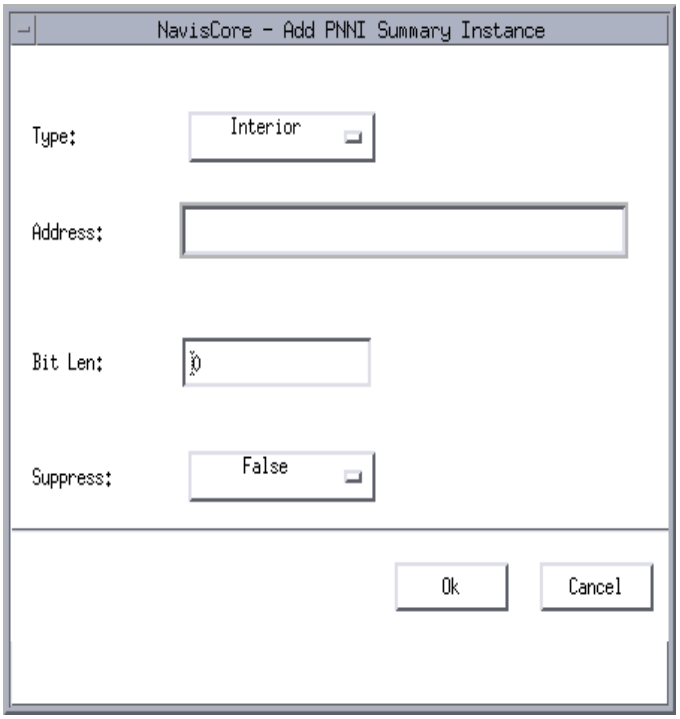


Figure 20-9. Add PNNI Summary Instance Dialog Box

4. Complete the fields described in Figure 20-7.

Table 20-7. Add PNNI Summary Instance Dialog Box Fields

Field	Action/Description
Type	Sets the summary address type for this summary instance. Select one of the following options: *Interior* – (default) Indicates the summary address is inside the PNNI routing domain. *Exterior* – Indicates the summary address is outside the PNNI routing domain.
Address	Enter the summary address (up to 19 octets). The summary address is an address prefix that indicates how the node summarizes reachability information. This field is padded to the right with 0s (zeros) if you enter fewer than 19 bytes.
Bit Len	Enter the length in bits of the summary address. The maximum value is 152 bits. You can enter a value of 0 (zero) if the address field contains only zeros.
Suppress	Determines whether or not to advertise the addresses summarized by this summary instance. Select one of the following values: *False* – (default) Indicates that the summary should be advertised to the peer group. *True* – Prevents the summary and the reachable addresses it summarizes from being advertised to the peer group.

5. Choose Ok to set the PNNI summary instance parameters and return to the Set All PNNI Node Parameters dialog box.

Configuring Global Variables

To configure global variables for address sharing within the PNNI routing domain:

1. Complete the steps in "Accessing PNNI Node Parameter Functions" on page 20-29.
2. Choose Set Global Vars. The Set PNNI Node Global Variables dialog box appears.

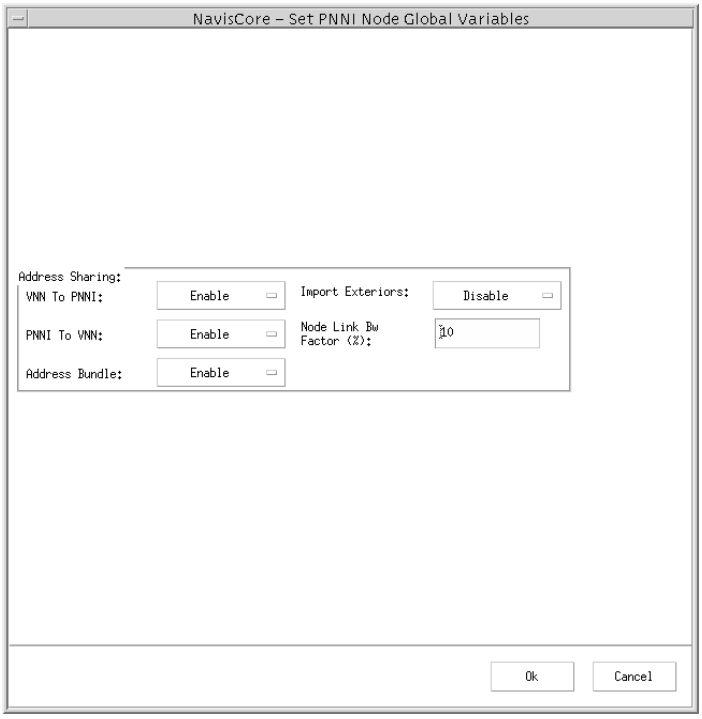


Figure 20-10. Set PNNI Node Global Variables Dialog Box

3. Complete the fields described in Figure 20-8.

Table 20-8. Set PNNI Node Global Variables Dialog Box Fields

Field	Description
VNN To PNNI	Indicates whether or not internal addresses known to VNN should be advertised within the PNNI routing domain. Select one of the following values: *Enable* – (default) Indicates that internal VNN addresses can be advertised within the PNNI routing domain. *Disable* – Prevents internal addresses known to VNN from being advertised within the PNNI routing domain. Disabling this variable on a gateway switch prevents addresses from being advertised from VNN to PNNI routing domains. This parameter applies only to switches that have both VNN OSPF and PNNI trunks.
PNNI To VNN	Indicates whether or not internal addresses known to PNNI should be advertised within the VNN domain. Select one of the following values: *Enable* – (default) Indicates that the internal address can be advertised within the VNN domain. *Disable* – Prevents internal addresses known to PNNI from being advertised within the VNN routing domain. Disabling this variable on a gateway switch prevents addresses from being advertised from PNNI to VNN routing domains. This parameter applies only to switches that have both PNNI and VNN OSPF trunks.
Import Exteriors	Indicates whether or not addresses that are external to the PNNI (or VNN OSPF) routing domain can be imported to the PNNI (or VNN OSPF) routing domain. Select one of the following values: *Enable* – Indicates that exterior addresses can be imported to the PNNI (or VNN OSPF) routing domain. When this variable is enabled on PNNI/VNN gateway switches, addresses from different regional networks are automatically routed across a VNN OSPF or PNNI network backbone to other regional networks. *Disable* – (default) Prevents exterior addresses from being imported to the PNNI (or VNN OSPF) routing domain. This parameter applies only to switches that have both VNN OSPF and PNNI trunks.

Table 20-8. Set PNNI Node Global Variables Dialog Box Fields (Continued)

Field	Description
Address Bundle	Supports address bundling within the PNNI routing domain on a per-node basis. Select one of the following values: *Enable* – (default) Indicates that address bundling is supported within the PNNI routing domain. ATM addresses or prefixes associated with the same level and having the same cost will be bundled in the same PTSE, up to 94 addresses per PTSE. Bundling saves 164 bytes for each name that can be bundled, which saves both memory and bandwidth consumption of control traffic. *Disable* – Prevents address bundling within the PNNI routing domain. ***Note:*** *This parameter applies to all PNNI switches.*
Node Link BW Factor (%)	Represents the degree of significance in the change of Bandwidth on a PNNI link for a particular QoS service class, before that link is re-advertised in the network. The default is 10%. The range of possible values is 1 to 99%. For example, if BW Factor is 10%, a new horizontal link PTSE is advertised by the switch every time the available bandwidth of one of its links changes by 10% (or greater) of the maximum available bandwidth.

4. Choose Ok to set the PNNI node global variables parameters and return to the Set All PNNI Node Parameters dialog box.

Completing the PNNI Node Parameter Configuration

To complete the PNNI node parameter configuration from the Set All PNNI Node Parameters dialog box, choose Close to return to the network map.

Configuring an ATM NNI Logical Port

You configure PNNI links as ATM NNI logical ports. To configure an ATM NNI logical port for PNNI:

1. Select the switch to which you want to add a logical port. From the Administer menu, select Lucent Parameters ⇒ Set Parameters. The Switch Back Panel dialog box appears.
2. Select the physical port you want to configure and press the third (right) mouse button to display a pop-up menu. Select Logical Port. The Set All Logical Ports in PPort dialog box appears (Figure 3-1 on page 3-4).
3. Choose Add. The Add Logical Port Type dialog box appears (Figure 3-2 on page 3-10).
4. Select ATM NNI as the LPort Type.
5. Choose Ok. The Add Logical Port dialog box appears (Figure 3-3 on page 3-11).
6. Use the instructions in Table 20-9 to set the logical port attributes.

Table 20-9. Configuring an ATM NNI Logical Port

Use the instructions on	To set the
page 3-14	Administrative Attributes to enter a logical port name
page 3-22	ATM Attributes to select the ATM Protocol, PNNI 1.0
page 3-28	ILMI/Signaling/OAM Attributes to enable signaling. For PNNI logical ports, signaling is enabled by default and ILMI is disabled.
page 3-36	ATM FCP Attributes (*optional*)
page 3-50	SVC attributes: • SVC Connection ID Parameters • SVC Parameters • SVC Priorities • SVC TD Limits • ATM SVC Parameters

7. Select Set PNNI Parameters Attributes to display the following fields:

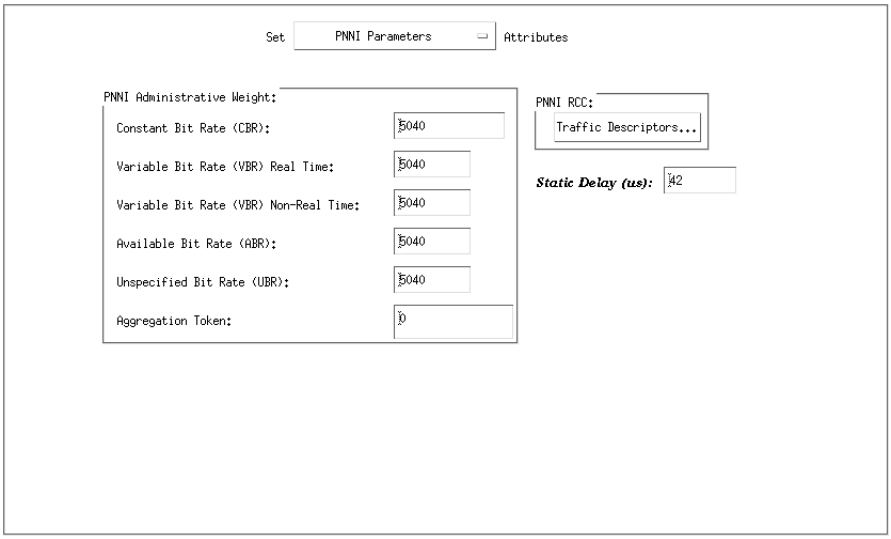


Figure 20-11. Set PNNI Parameters Attributes Fields

The Set PNNI Parameter Attributes menu enables you to configure the PNNI administrative weight status by assigning an administrative weight to each QoS category field. This weight allows you to configure the network to favor one path over another path for a given category. The weights of all the network interfaces along a path are added up, and switches choose the path with the lowest cumulative weight when making routing decisions.

For example, suppose that VBR-RT traffic has two available paths for reaching a given destination: one path has a weight of 1000 and the other path has a weight of 4000. If the call requests VBR-RT QoS and administrative weight as a metric and if the path has sufficient bandwidth and other metric resources, the switch will choose the path with the weight of 1000.

In a network that supports, for example, both CBR and UBR calls, you can configure PNNI Administrative Weight values so that the switch will choose one path for the CBR calls and a different path for the UBR calls.

8. Complete the fields described in Table 20-10.

Table 20-10. PNNI Parameters Attributes Fields

Field	Action/Description
Constant Bit Rate (CBR)	Indicates the administrative weight to assign to the CBR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Variable Bit Rate (VBR) Real Time	Indicates the administrative weight to assign to the VBR-RT QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Variable Bit Rate (VBR) Non-Real Time	Indicates the administrative weight to assign to the VBR-NRT QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Available Bit Rate (ABR)	Indicates the administrative weight to assign to the ABR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Unspecified Bit Rate (UBR)	Indicates the administrative weight to assign to the UBR QoS category for the network interface associated with the logical port. Enter a value between one and 16,777,215, or accept the default value (5040).
Aggregation Token	Enter a value in this 4-byte field to identify a PNNI outside link that interconnects two separate peer groups. The default value is 0 (zero). The aggregation token determines how this link is aggregated at the next higher level in the hierarchy. Outside links connecting the same two peer groups are aggregated if they have the same aggregation token or if one link has an aggregation token value of 0 (zero). If the aggregation tokens of different outside links are not equal and nonzero, each will be advertised in a separate horizontal link PTSE by the associated parent LGN nodes. ***Note:*** *The aggregation token value is important only for outside links where the neighboring nodes belong in different peer groups.*

Table 20-10. PNNI Parameters Attributes Fields (Continued)

Field	Action/Description
PNNI RCC	Allows you to configure the traffic descriptor values for PNNI routing control channels (RCCs). The RCC is a virtual channel connection (VCC) used between neighboring LGNs for the exchange of PNNI routing protocol messages. It's used only in a hierarchical PNNI network. Choose the Traffic Descriptors button to display the Set Logical Port PNNI RCC Traffic Descriptors dialog box (see Figure 10-3 on page 10-12 to view the dialog box fields). Use step 2 through step 4 beginning on page 10-12 to configure PNNI RCC traffic descriptor values.
Static Delay (µs)	Static delay for PNNI links in a path is summed to determine the end-to-end delay of the path. Higher values represent slower links. The valid range for this field is 0 (zero) to 167777214 µsec. Default values (in microseconds) are: DS1 – 522 DS3 – 42 OC-3c/STM-1 – 22 E1 – 370 E3 – 41 OC-12c/STM-4 – 10 ***Note:*** *Changing the value for this attribute does not admin down the logical port.*

9. Use the instructions on page 3-43 to complete the logical port configuration.
10. Repeat step 2 through step 9 beginning on page 20-44 for each ATM NNI logical port you need to configure.

Note – For information about configuring Virtual NNI logical ports, see "Virtual UNI/NNI" on page 2-10. Virtual logical ports allow you to configure more than one logical port on the same physical port. Each logical port that you configure uses a portion of the total physical port bandwidth.

Creating a PNNI Link Line Connection

To monitor the status of PNNI links using NavisCore, you can create a PNNI link line connection on the network map. This process is similar to creating a trunk line connection (see Chapter 7, “Configuring Trunks”). You use the Add Connection dialog box to draw a line to connect the two switches on the network map.

To add a PNNI link line connection:

1. From the Edit menu, select Add Connection. The Add Connection dialog box appears (see Figure 7-6 on page 7-27).
2. Select a connection class from the Connection Classes list box. The Add Connection dialog box displays the subclasses for the connection class you select (see Figure 7-7 on page 7-28).
3. Select a connection subclass from the Connection Subclasses list box.
4. To create a PNNI link line connection between two switches on the network map, click on the first switch object (source symbol) and then on the second switch object (destination symbol). The Add Object dialog box appears (see Figure 7-8 on page 7-29).

   Complete the Add Object dialog box fields described in Table 7-6 on page 7-29.

5. Select Cascade View from the Object Attributes list box and then choose Set Object Attributes. The Add Object - Set Attributes dialog box appears (Figure 20-12).

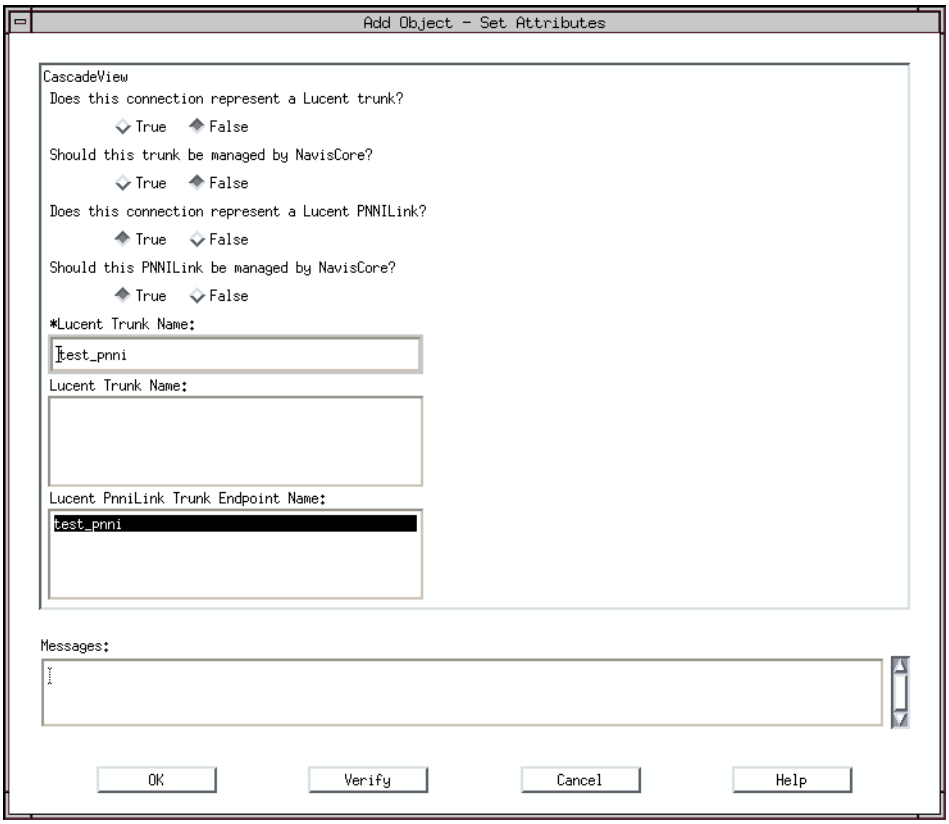


Figure 20-12. Add Object – Set Attributes Dialog Box

6. To create a PNNI link line connection, complete the Add Object – Set Attributes dialog box fields as follows:

Table 20-11. Add Object – Set Attributes Dialog Box

Field	Action/Description
Does this connection represent a Lucent trunk?	Select False. Note: If you select True, a Lucent trunk line connection will be added to the map by default.
Should this trunk be managed by NavisCore?	Select False. Note: If you select True, a Lucent trunk line connection will be added to the map by default.
Does the connection represent a Lucent PNNI Link?	Select True.

Table 20-11. Add Object – Set Attributes Dialog Box (Continued)

Field	Action/Description
Should this PNNI Link be managed by NavisCore?	Select True.
*Lucent Trunk Name	Select the name assigned to this PNNI link from the Lucent PnniLink Trunk Endpoint Name list box. The list box displays all PNNI logical ports configured on the switch selected as the source switch for the PNNI link connection. Select the logical port that corresponds to the PNNI link you want to manage. The name you select appears in the *Lucent Trunk Name field.

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

Understanding PNNI Link Line Coloring

Like Lucent trunks, PNNI link lines are periodically polled for status. The PNNI link lines on the network map change color. These colors indicate link status according to the polled status and the traps received by the Lucent Alarms Browser. Table 20-12 describes the color scheme that identifies the status of a PNNI link connection on the network map.

Table 20-12.PNNI Link Line Color Status Indicators

Color	Status
Black	Either the line connection has not been defined as a PNNI link, or the environment variable $XUSERFILESEARCHPATH does not point to: **/opt/CascadeView/app-defaults**. [1]
Green	PNNI link line connection is Up.
Red	PNNI link line connection is down.

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

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

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

Configuring PVCs

Lucent ATM PVCs can be established over a PNNI routing domain as well as over a routing domain that supports both VNN ATM and PNNI.

PNNI signaling establishes Lucent ATM PVCs over a PNNI routing domain, but you do not need to configure the PVC addresses manually. PNNI signaling uses a unique SPVC node prefix, which is automatically generated by each switch, as the destination address. All SPVC node prefixes begin with the same four bytes (4900C07B).

PNNI routing does not require changes to the way you usually configure PVCs. For information about configuring Lucent ATM PVCs, see Chapter 8, “Configuring ATM PVCs.”

PVCs can be established with endpoints that are any combination of ATM UNI, Frame Relay UNI, or PPP logical ports.

Configuring SVC and SPVC Parameters

PNNI routing can connect your network of switches using SVCs instead of PVCs. Once you have configured the ATM NNI logical ports, you configure SVC prefixes or addresses using an AESA or E.164 format. Addresses can also be “learned” dynamically through address registration if Interim Link Management Interface (ILMI) is enabled on UNI ports. If necessary, review Chapter 14, “About SVCs,” for an overview of SVC addressing and address registration. To configure SVC prefixes and addresses, see Chapter 15, “Configuring SVC Parameters.”

In addition to SVCs, PNNI routing can access switches using SPVCs. For information about configuring SPVCs, see Chapter 17, “Configuring SPVCs.”

Configuring Offnet PVCs Over PNNI

Frame Relay-to-ATM Network Interworking (FRF.5) allows you to connect a Frame Relay endpoint to either a Frame Relay or ATM endpoint over an ATM backbone via a PNNI link. Using FRF.5, offnet PVCs over PNNI can be configured to route traffic from a Lucent Frame Relay network to an offnet ATM network, and back to a Frame Relay or ATM network.

This service uses Frame Relay-based UNI Lports established over a PNNI network. Endpoint 1 is chosen from a switch on the NavisCore map and Endpoint 2 is defined as either an ATM or Frame Relay address. Endpoint 1 is the originator of the circuit and Endpoint 2 is determined by the PNNI routing protocol by choosing the switch which is advertising the destination address with the lowest cost.

Note – ATM to ATM offnet PVCs are not supported in this release.

Use the following steps to configure an offnet PVC over an existing PNNI link.

1. From the Administer menu, select Lucent Parameters ⇒ Set All Circuits ⇒ Offnet. The Set All Offnet PVCs On Map dialog box appears (Figure 20-13).

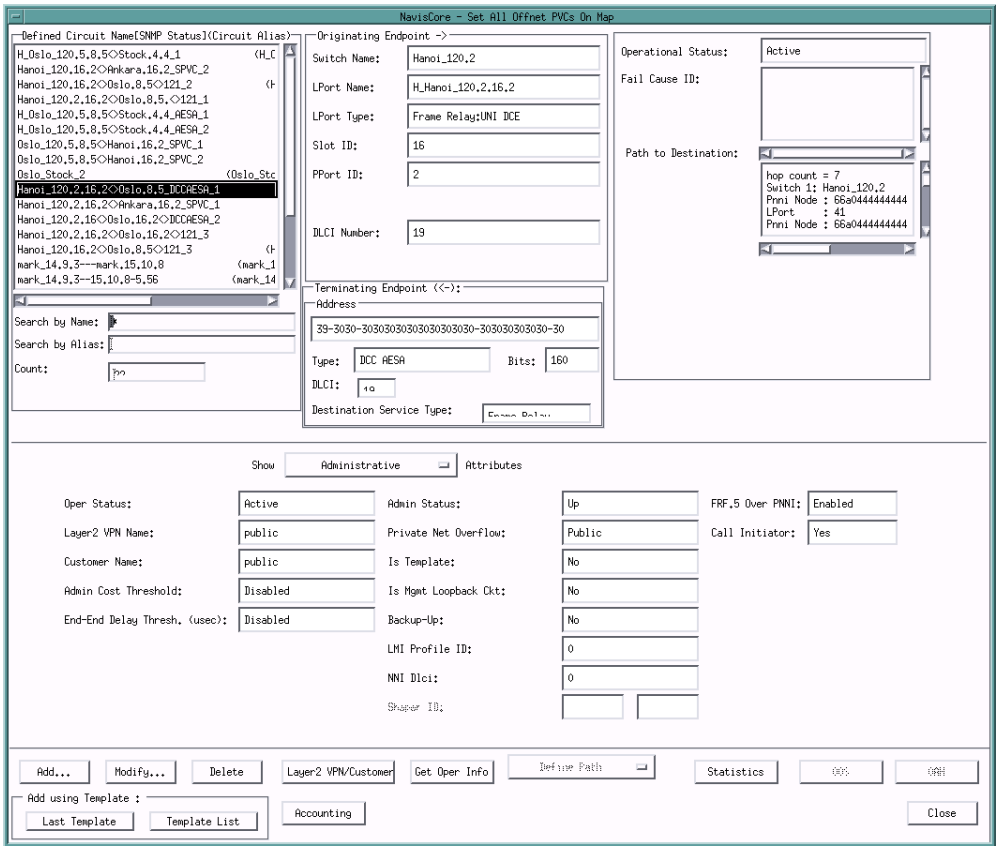


Figure 20-13. Set All Offnet PVCs On Map Dialog Box

To view a list of configured offnet PVCs, position the cursor in the Search by Name field and press Return. Use any of the following wildcard searches to fine a specific offnet PVC name:

- Use an * to match any number of characters
- Use a ? to match a single character
- To match the ? character, type **\?**
- To match the \ character, type \\

The Set All Offnet PVCs On Map dialog box displays information about the configured options for the Defined Circuit Name you select. Table 20-13 describes the dialog box buttons, and Table 20-14 describes the dialog box fields.

Table 20-13. Set All Offnet PVCs On Map Dialog Box Buttons

Button	Action/Description
Add	Enables you to add an offnet PVC.
Modify	Enables you to modify an offnet PVC.
Delete	Enables you to delete an offnet PVC.
Layer2 VPN/Customer	Assigns the selected circuit to a specific Layer2 VPN and customer name.
Get Oper Info	Displays the selected circuit's current operational status in the Oper Status field. See Oper Status on page 8-14 for an explanation of these status messages.
Define Path	Not applicable for offnet PVCs.
Statistics	Displays the summary statistics for the selected offnet PVC.
QOS	Not applicable for offnet PVCs.
OAM	Not applicable for offnet PVCs.
Add using Template	If you have already defined an offnet PVC configuration and saved it as a template, use this option menu to define a new circuit using similar parameters. • Choose Last Template to use the last template you used to establish a circuit in this NMS session. • Choose Template List to display a list of templates previously defined for this map.
Accounting	Accesses the NavisXtend Accounting Server functions for a circuit.
Close	Exits this dialog box and returns to the network map.

Table 20-14. Set All Offnet PVCs On Map Dialog Box Fields

Field	Action/Description
Defined Circuit Name (Circuit Alias Name)	Displays a list of the offnet PVCs configured in the network. Use a wildcard search to find a specific offnet PVC name. If applicable, this field also lists the configured offnet PVC alias.
Count	Displays the number of offnet PVCs found depending on the criteria used in the Search by Name field.
Originating Endpoint	*Switch Name* – The name of the switch at the originating end point. *LPort Name* – The name of the logical port for the switch at the originating end point. *LPort Type* – The configured type of the selected logical port. *Slot ID* – The physical slot number where the I/O module containing the selected port is installed. *PPort ID* – The number of the physical port for which the selected logical port is configured. *DLCI Number* – The DLCI number chosen for this circuit.
Terminating Endpoint	Displays the terminating endpoint for the selected circuit.
Operational Status	Displays a status message: Active or Inactive.
Fail Cause ID	Displays the reason for the operational failure.
Path to Destination	Displays the actual path that OSPF and/or PNNI selected for this circuit to use to get to its destination.
Show [Administrative] Attributes	Displays the appropriate attributes configured for the selected option. See the following sections for more information: “Administrative Attributes” on page 20-60 “Traffic Type Attributes” on page 20-62 “User Preference Attributes” on page 20-63 “Selectable Statistics Attribute” on page 20-64

Table 20-14. Set All Offnet PVCs On Map Dialog Box Fields (Continued)

Field	Action/Description
Oper Status	Displays the current operational status of the selected circuit. Messages include: *Active* – The circuit is operational through the network end-to-end. *Inactive* – The circuit is not operational. Check the Fail Cause ID field for possible reasons. *Unknown* – The NMS cannot reach the higher-numbered node for status. *Invalid* – The circuit definition is not found in the higher-numbered node. You may need to save the circuit definition; it may also be necessary to PRAM synch the host card.
Admin Status	Displays whether the selected circuit is online (*Up*) or offline (*Down*).
FRF.5 Over PNNI	Displays whether the FRF.5 over PNNI capability is enabled or disabled (default).
Layer2 VPN Name	Assigns the selected circuit to a specific VPN and customer name.
Private Net Overflow	Displays how offnet PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Displays one of the following values: *Public* – (default) Offnet PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – Offnet PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Call Initiator	Displays Yes if this endpoint is the call initiator, otherwise displays No.
Customer Name	Displays the customer name for the selected offnet PVC (if applicable).
Is Template	Displays Yes if you can use this circuit as a template to create other circuits using similar parameters.
Admin Cost Threshold	Not applicable for offnet PVCs.

Table 20-14. Set All Offnet PVCs On Map Dialog Box Fields (Continued)

Field	Action/Description
Is Mgmt Loopback Ckt	Displays the current state of this PVC configuration in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity. This option is especially useful in some management configurations.
End-End Delay Thres. (usec)	Not applicable for offnet PVCs.
Backup-Up	Indicates whether the selected circuit has a backup circuit. Options include: *No* – (default) This circuit does not have a backup circuit. *Yes* – This circuit has a backup circuit.
LMI Profile ID	Displays the LMI Profile ID. The default is zero. If 1 is displayed, this is signified as an FRF.5 circuit.
NNI DLCI	Displays the NNI DLCI for the offnet PVC. The NNI DLCI can differ from the DLCI configured at the UNI port. The LMI that the NNI runs will use the NNI DLCI to identify the network interworking PVC.
Shaper ID	Not applicable for Offnet PVCs.

Adding an Offnet Circuit

To add an offnet PVC:

1. From the Set All Offnet PVCs On Map dialog box (Figure 20-13 on page 20-53), choose Add. The Select Offnet PVC Endpoints dialog box appears.

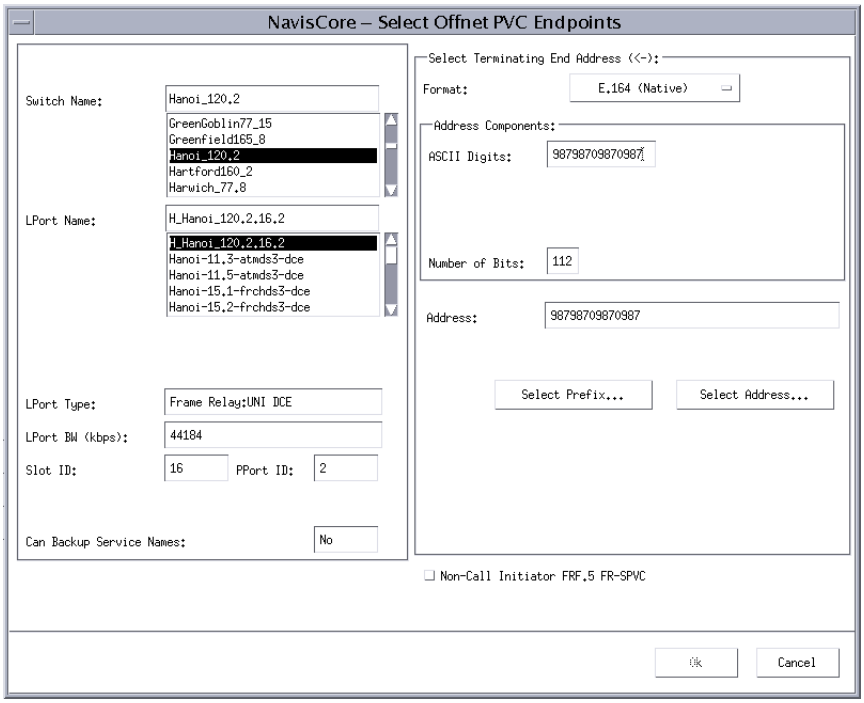


Figure 20-14. Select Offnet PVC Endpoints Dialog Box

2. Perform the following steps to configure the originating endpoint logical port.
   a. Select the name of the switch on which the endpoint will reside.
   b. Select the name of the logical port that will be used as the endpoint. The dialog box displays the LPort Type, LPort BW (Kbps), and LPort ID for this endpoint.
   c. Select the Non-call initiator FRF.5 FR-SPVC button if this endpoint is not the Call Initiator in the circuit. The Select Terminating End Address section of the dialog box will become grayed out since this information will not be needed.

      If this endpoint is the Call Initiator, do not select this button.

3. To complete this configuration:
   - If you know the offnet PVC terminating endpoint address, use Table 17-4 on page 17-9 to select the address format and configure the terminating endpoint address. For more information on ATM End System Address (AESA) formats, see page 14-2.
   - If you do not know this address, or if you need to configure the terminating endpoint address, see page 17-13 for instructions on using the Select Prefix and Select Address buttons to configure this address.

4. Choose OK. The Add Offnet Circuit dialog box appears (Figure 20-15).

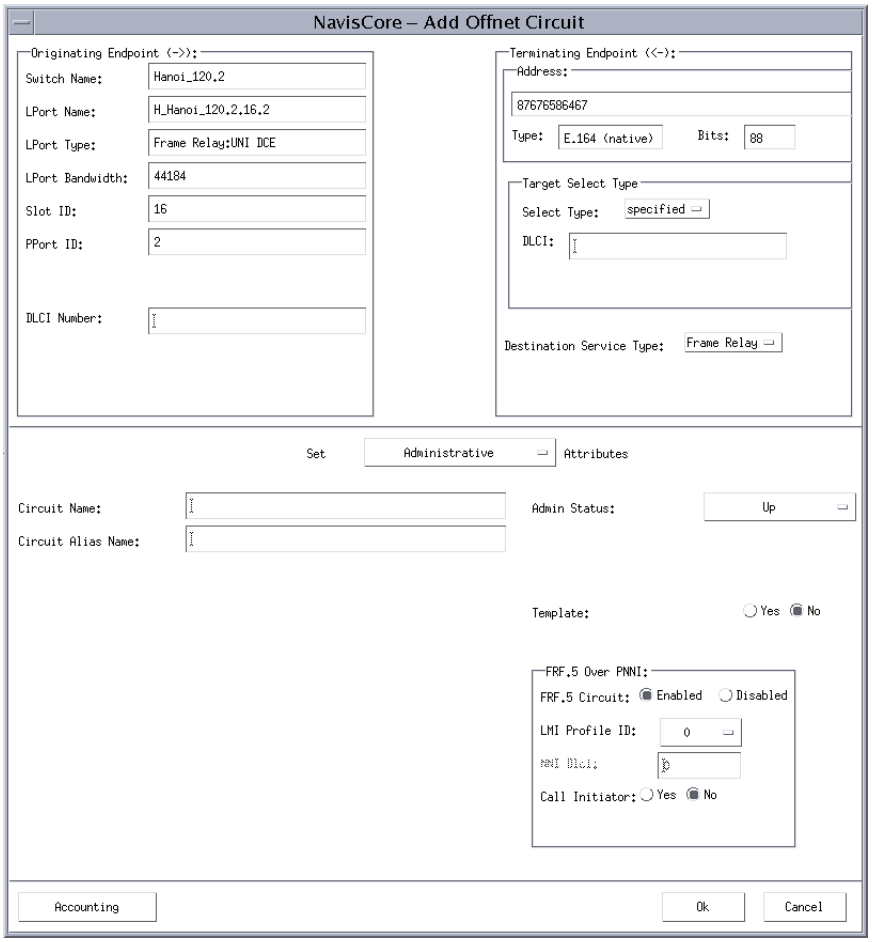


Figure 20-15. Add Offnet Circuit Dialog Box

5. Complete the fields in Table 20-15.

Table 20-15. Add Offnet Circuit Dialog Box Fields

Field	Action/Description
Originating Endpoint DLCI Number	Enter a unique DLCI number (16 through 991) for the endpoint logical ports.
Target Select Type	Select *specified* as the Target Select Type. If the endpoint is Frame Relay, the terminating endpoint uses the DLCI address you specify. If the endpoint is ATM, you will be prompted to enter the VPI/VCI numbers for this circuit. ***Note** – If the target service is Frame Relay, the DLCI entered here must match the DLCI in the originating endpoint for the FRF.5 PVC configuration of the receiving endpoint where the call initiator field is set to No.*

6. Using the Set Attributes menu, complete the following sections:
   - "Administrative Attributes" on page 20-60
   - "Traffic Type Attributes" on page 20-62
   - "User Preference Attributes" on page 20-63
   - "Selectable Statistics Attribute" on page 20-64

Administrative Attributes

From the Add Offnet Circuit dialog box (Figure 20-15 on page 20-59), select Set [Administrative] Attributes and complete the fields described in Table 20-16.

Table 20-16. Set Administrative Attributes Fields

Field	Action/Description
Circuit Name	Enter any unique, alphanumeric name to identify the offnet PVC. Do not use parentheses and asterisks. This name must be unique to the entire map.
Admin Status	Select Up (default) to activate the offnet PVC at switch startup, or Down if you do not want to activate the offnet PVC at switch startup.
Circuit Alias Name	*(Optional)* The circuit alias is used by service providers to identify the circuit in a way that is meaningful to their customers. Enter any unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Private Net Overflow	Determines how offnet PVC traffic is managed during trunk overflow or failure conditions. This feature is used with virtual private networks (VPNs). For more information about VPNs, see Chapter 11. Select one of the following options: *Public* – (default) Offnet PVCs are routed over dedicated VPN trunks. However, in the event of failure, the customer's traffic is allowed to run over common trunks (shared by a variety of different customers). *Restricted* – Offnet PVCs can only use dedicated VPN trunks. A customer using this mode must purchase redundancy trunks to be used in the event of outages or other trunk failures.
Template	*(Optional)* You can save these settings as a template to configure another offnet PVC with similar options. To create a template, choose Yes in the Template field.
Admin Cost Threshold	Not applicable for offnet PVCs.

Table 20-16. Set Administrative Attributes Fields (Continued)

Field	Action/Description
Mgmt Loopback Ckt	If you choose Yes, this offnet PVC configuration will be included in the NMS initialization script file. This file contains all the SNMP set requests necessary to replicate the entire switch configuration. Once you download the configuration file to the switch, the offnet PVC can be used to establish NMS-to-switch connectivity. The Mgmt Loopback Ckt field is especially useful in some Management configurations. The default value is No.
End-End Delay Threshold	Not applicable for offnet PVCs.
FRF.5 Circuit	Select Enabled to enable FRF.5 over PNNI for this circuit.
LMI Profile ID	Select 1 or 0 for the LMI Profile ID. The default is zero. Selecting 1 will signify this is an FRF.5 circuit. ***Note** – This LMI Profile ID must match the Terminating Endpoint LMI Profile ID.*
NNI DLCI	If you enable an LMI profile ID, you *must* specify the NNI DLCI for the offnet PVC. The NNI DLCI can differ from the DLCI configured at the UNI port. The LMI that the NNI runs will use the NNI DLCI to identify the network interworking PVC. Enter the NNI DLCI. The valid range of values for this field is 16 - 991, and 1022. This NNI DLCI number must match the Terminating Endpoint NNI DLCI number. ***Note:** Review the Restrictions and Special Considerations section of the* Software Release Notice for CBX Switch Software *that comes with your release for information about setting the NNI DLCI value.*
Call Initiator	Select Enabled to enable this endpoint as the call initiator or Disabled to configure this endpoint as the call recipient. If Call Initiator is set to Enabled, Target Select Type must be Specified.

Traffic Type Attributes

Select Set [Traffic Type] Attributes from the Add Offnet Circuit dialog box (Figure 20-15 on page 20-59) to specify Traffic Descriptor settings for forward and reverse traffic. Figure 20-16 shows the Set Traffic Type Attributes fields.

Note – If the Call Initiator field is set to No, the Traffic Type Attributes are unavailable and do not need to be set.

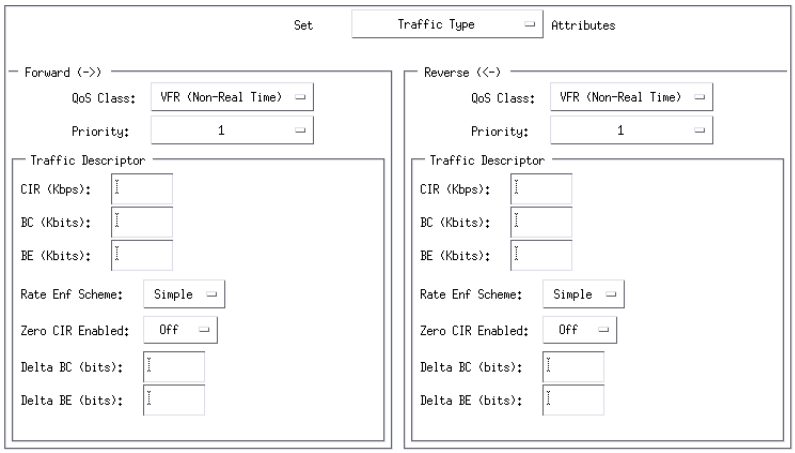


Figure 20-16. Set Traffic Type Attributes

The Reverse QoS class is not configurable by the user, but will be set by the NMS based on the service type of the destination endpoint and the QoS class of the originating endpoint. However the traffic descriptors for the destination endpoint can be configured by the user. If both endpoints are Frame Relay service, then the QoS class of the originating endpoint will be used for the terminating endpoint.

Table 20-17 lists the allowed supported QoS classes for the offnet PVC endpoints.

Table 20-17. Allowable QoS Classes

QoS Class	ATM Endpoint	Frame Relay Endpoint
Real Time VBR	X	
Non-Real Time VBR	X	
UBR	X	
Real Time VFR		X
Non-Real Time VFR		X
UFR		X

For more information about configuring these attributes, see "Traffic Type Attributes" on page 8-30.

User Preference Attributes

Select Set [User Preference] Attributes to select the traffic descriptors for this offnet PVC. Figure 20-17 shows the Set User Preference Attributes fields.

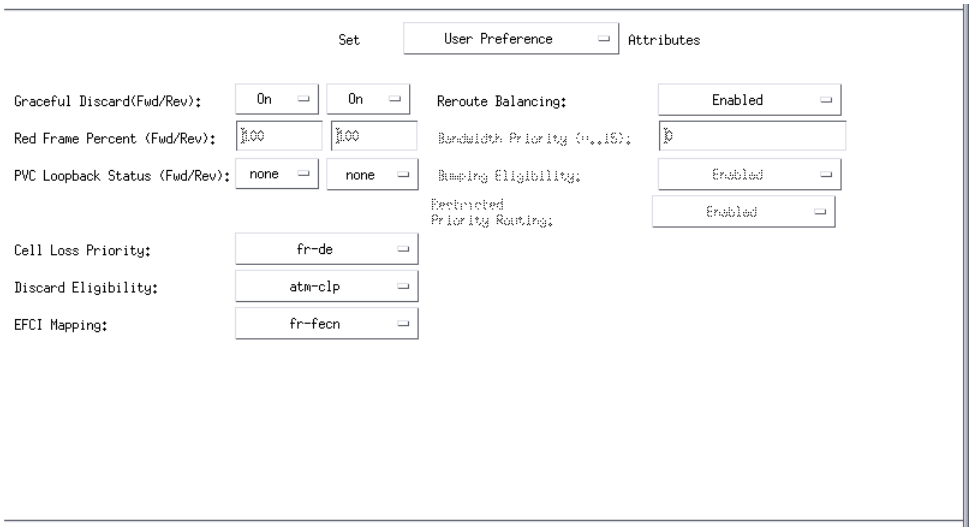


Figure 20-17. User Preference Attributes

For more information about configuring these attributes, see "User Preference Attributes" on page 8-57.

Selectable Statistics Attribute

This option is available with the NavisXtend Statistics Server. This feature allows you to enable and disable offnet PVC bulk statistics collection.

Select Set [Statistics] Attributes to enable or disable (default) the Bulk Statistics option for this offnet PVC. Figure 20-18 shows the Set Statistics Attributes fields.

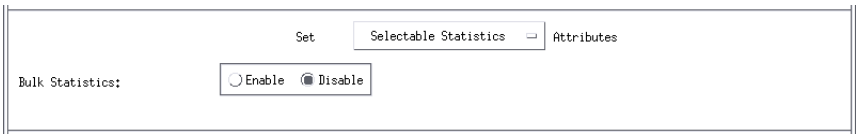


Figure 20-18. Set Selectable Statistics Attributes

Bulk statistics for the logical port must be enabled before enabling bulk statistics for offnet PVCs. For more information, see "Selectable Statistics Attributes" on page 3-42.

For information about using the feature, see the *NavisXtend Statistics Server User's* Guide.

Configuring Management PVCs

A Management PVC (MPVC) can be used for all applications involving a switch and an attached NMS or IP host. An MPVC is a PVC between the UNI or NNI logical port, to which the NMS or IP host connects, and the processor module on the remote switch. The switch that connects the NMS or IP host is not burdened by the traffic traversing the MPVC.

To configure MPVCs, see Chapter 9, "Configuring Management Paths."

Configuring Management SPVCs

A Management SPVC (MSPVC) connects the switch management port to an SVC terminating address located on an adjacent switch. Use this management connection as the NMS path to enable the NMS to manage the switch.

MSPVCs originate at an internal logical port located on the switch's processor module, either the CBX 500 switch processor (SP) or GX 550 node processor (NP). They terminate at the switch's I/O interface: IOM for a CBX 500, and BIO for a GX 550. MSPVCs provide a data path that accesses internal network management functions. The MSPVC internal logical port is designated as MgmtLPort.SW<*switch name*>. It uses an interface number (ifnum) of 4093. To form the MSPVC, connect the MgmtLPort. SW <*switch name*> endpoint to any target AESA address configured on an ATM UNI logical port.

To configure MSPVCs, see Chapter 9, "Configuring Management Paths."

Viewing PNNI Links

A list of all PNNI links on a selected switch can be viewed in NavisCore. See Chapter 7 in the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information.

PNNI Trap Support

Lucent switches can receive PNNI traps that report status changes in PNNI protocol states. These traps are configured by selecting Event Configuration from the NavisCore Options menu. See Chapter 14, “Managing Traps,” in the *B-STDX, CBX, and GX Switch Diagnostics User’s Guide* for more information on managing traps.

NavisCore supports the PNNI traps described in Table 20-18

Table 20-18. PNNI Traps

Trap Name	Description
pnniLinkHelloMismatch	This trap is generated whenever a Hello mismatch has occurred on a PNNI link. The PNNI link line color on the network map will change to signify that the link is down (red).
pnniNbrStateChange	This trap is generated when a neighboring peer state changes to Full or Down with respect to the neighbor finite state machine (FSM).
pnniPglStateChange	This trap is generated when the local switch has either activated as LGN or deactivated from LGN within a PNNI peer group.
pnniBorderLinkStateChange	This trap is generated when there is a change in the Border node link state with respect to hello FSM states. The PNNI link line color on the network map will change to signify that the link is down (red) if the link to a neighboring peer is not in a 2-way inside or common hierarchy state.

If a Lucent switch receives a PNNI trap indicating a change in PNNI link status, the information is transmitted over one or more Lucent switches to the NMS and can be viewed in the Lucent Alarms Browser.

For more information about the Alarms Browser, see the *HP OpenView Network Node Manager User’s Guide* or choose Help from HP OpenView.

A

Adjusting the CAC

This appendix describes how to tune the Lucent Call Master Connection Admission Control (CAC) to achieve a desired cell loss ratio objective across all physical ports in your network. The Lucent CAC is responsible for the bandwidth allocation on all ATM cards on the CBX 500, GX 550, and B-STDX 8000/9000. It is also responsible for bandwidth allocation on all frame cards with the priority frame capability.

When you create a circuit, the CAC function computes a bandwidth allocation for that circuit and updates the bandwidth allocation for the circuit's QoS class. This bandwidth allocation depends on the specified CAC implementation, the circuit's QoS class, and the circuit's specified traffic descriptor. If you try to create a circuit that causes the allocated bandwidth for a given QoS class to exceed the bandwidth available for that class, the circuit will not be created.

The CAC configuration option enables you to choose one of the following three CAC implementations:

Lucent CAC — Allows you to control the Quality of Service (QoS) and bandwidth allocation by specifying cell loss ratio and cell delay variation objectives.

Customize VBR-NRT and ABR — Allows you to control the amount of bandwidth that is reserved for VBR-NRT and available bit rate (ABR) circuits.

Customize VBR-RT, VBR-NRT, and ABR— Allows you to control the amount of bandwidth that is reserved for VBR-RT, VBR-NRT, and ABR circuits.

In either of the customizable implementations, you can control the amount of bandwidth reserved based on either the physical port type or the configurable range of SCR values, or both. With the two customized implementations you can also control circuit establishment based on the configurable range of maximum MBS values.

Note – Quality of Service for the VBR-RT and VBR-NRT QoS classes is not guaranteed when you use the “customize VBR-RT, VBR-NRT, and ABR” CAC implementation. Also, the Quality of Service for the VBR-NRT QoS class is not guaranteed when you use the “customize VBR-NRT and ABR” CAC implementation.

When you adjust the CAC function, choose only one of these options. Whether you are tuning the Lucent CAC or configuring a customized CAC, the adjustments you make apply only to the VBR-RT, VBR-NRT, and ABR traffic types.

Note – Before tuning the Lucent CAC or configuring a customized CAC, you should closely monitor your network to achieve a good understanding of the network’s traffic profile. Be conservative when you adjust the CAC to ensure QoS. After you make adjustments, monitor the network closely to determine the effect of these adjustments, making sure you have not adversely impacted the QoS on the network.

About the Customizable CAC Options

Both of the customizable CAC implementations enable you to directly control the amount of bandwidth reserved for VBR-NRT and ABR circuits. In addition, you can control the amount of bandwidth reserved for VBR-RT circuits if you choose the "customize VBR-RT, VBR-NRT, and ABR" CAC implementation. You control the amount of bandwidth reserved based on either the physical port type, the SCR requirements of the circuit, or both. When you use the customized CAC options, the following formula determines the amount of bandwidth required for a given circuit:

```
Bwidthreq = SCR*F1*F2
```

where F1 is the physical port factor (entered as a percentage) and F2 is the SCR scale factor (entered as a percentage). You can configure only an F1 factor, only an F2 factor, or both factors. If you do not configure one of these factors, then the value of that factor is, by default, 100%.

Note – On frame cards with priority frame capability, the Bwidthreq=SCR.

Customizable CAC Example

A circuit request is made, and the circuit needs to reserve bandwidth based on an SCR of 10,000 cells/sec. You configure the F1 factor for DS3 ports at 150%, the F1 factor for OC3c ports at 80%, and the F2 factor for circuits with an SCR from 8,001-15,000 cells/sec at 80%.

- If the circuit request is made on a DS3 port, then the circuit bandwidth requirements are based on an SCR of 12,000 cells/sec, instead of 10,000 cells/sec (10,000 x 150% x 80% = 12,000).
- If the circuit request is made on an OC3c port, then the circuit bandwidth requirements are based on an SCR of 6,400 cells/sec (10,000 x 80% x 80%= 6,400).

Configuring the CAC

To configure a customized CAC:

1. On the network map, select the switch for which you need to adjust the CAC.
2. From the Administer menu, select Lucent Parameters ⇒ Set All CAC Parameters. The Set All CAC Parameters dialog box appears. Figure A-1 shows this dialog box configured for the Customize VBR-NRT and ABR CAC implementation.

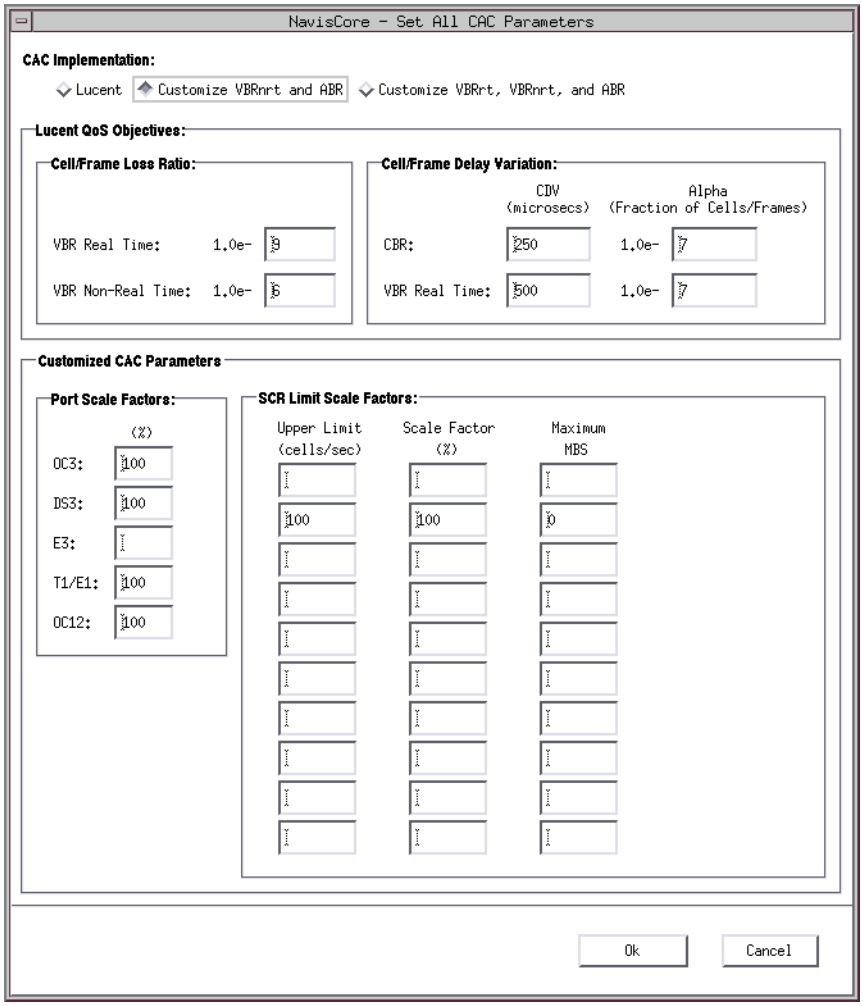


Figure A-1. Set All CAC Parameters Dialog Box

3. Select one of the following CAC Implementations:

   Lucent — Enables you to tune the cell loss ratio (CLR) and cell delay variation (CDV) only. See "Tuning the CAC" on page A-5 for more information.

   Customize VBRnrt and ABR — Enables you to tune the CLR, CDV, and customized CAC parameters.

   Customized VBRrt, VBRnrt, and ABR — Enables you to tune Customized CAC parameters only.

Tuning the CAC

To tune the CAC, specify the cell loss ratio objectives you want to meet across your network. You can specify a cell loss ratio objective in the range of 10^{-1} to 10^{-12}. For example, an entry of 10^{-5} specifies that circuits will not be created on any physical port on which:

- The cell drop ratio is currently 1 in 100,000 (because 10^{-5} is equal to 1/100,000)

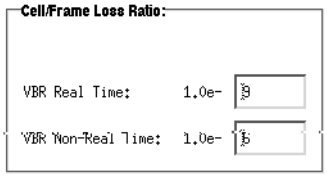
  OR

- The creation of the circuit would potentially cause the cell drop ratio to exceed 1 in 100,000

Note – Lucent recommends that you adjust the CAC when you first configure a switch. Adjusting the CAC after several circuits have been created will not automatically change the bandwidth allocation for these circuits and may not guarantee the defined Quality of Service.

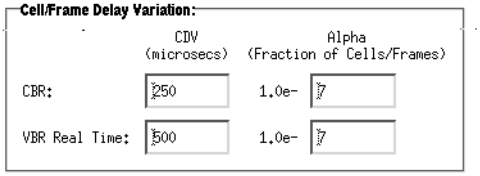
To tune the CAC:

1. On the Set All CAC Parameters dialog box (Figure A-1 on page A-4), select Lucent in the CAC Implementation field.
2. In the Cell/Frame Loss Ratio field, VBR Real Time and VBR Non-Real Time, specify the cell loss ratio objective you want to meet for each of these traffic types. This value is a negative power of ten (1.0e–). For example, if you enter 5, your cell loss ratio objective is a maximum of one dropped cell for every 100,000 cells. If the CAC determines that the creation of a circuit on a physical port will cause more than one in 100,000 cells to be dropped, then the circuit will not be created on that physical port.



By default, VBR Real Time is set to 9 (1 in 1,000,000,000) and VBR Non-Real Time is set to 6 (1 in 1,000,000).

3. In the Cell/Frame Delay Variation field, CBR and VBR Real Time, specify the CDV (in microseconds). This value represents the CDV objective for the CBR and VBR-RT QoS class. Although this value represents an upper bound on the delay variation for most physical interfaces, the CAC algorithm allows the actual CDV values on slow interfaces (such as T1 cards) to exceed this configured value.



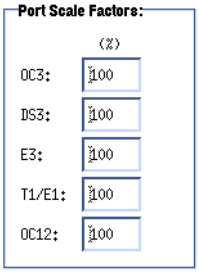
Note – Keep in mind that since both the CDV and CLR calculations are non-linear in nature, the resulting equivalent bandwidth for VBR-RT and VBR-NRT circuits may not be the same as it was in previous releases. Since the circuits might end up with a larger equivalent bandwidth as a result of the CDV objectives, one or more existing circuits many no longer be admitted because of insufficient bandwidth on a port where they were previously admitted.

4. In the Alpha column, specify the fraction of the CBR (or VBR-RT) cells that can exceed this CDV objective. This value is a negative power of ten (1.0e–). By default, the Alpha field for each of the CBR and VBR Real Time classes is set to 7 (1 in 10,000,000).
5. When you finish, choose Ok to send the values you entered to the selected switch.
6. To send these values to another switch on the network map, select the switch and use Step 2 on page A-4 to access the Set All CAC Parameters dialog box. Choose Ok.

Customizing the CAC for the VBR-RT, VBR-NRT, and ABR Classes

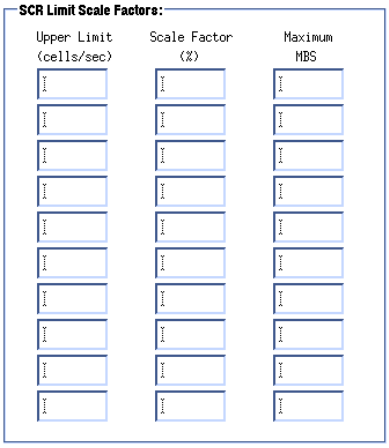
To customize the CAC for VBR-RT, VBR-NRT, and ABR:

1. On the Set All CAC Parameters dialog box (Figure A-1 on page A-4), select Customize VBRrt, VBRnrt, and ABR in the CAC Implementation field.
2. In the Port Scale Factors list box, enter a scale factor percentage to use for computing bandwidth requirements on the physical port.



For example, if you enter a value of 125% in the DS3 field, a circuit that would normally reserve bandwidth based on an SCR of 10,000 cells/sec would be allocated bandwidth of 12,500 cells/sec.

3. To customize the CAC based on the SCR and MBS values:



a. In the Upper Limit column of the SCR Limit Scale Factors field, enter the Upper Limit (cells/sec) of the SCR range for which you want to customize the amount of bandwidth reserved. You can specify up to ten upper limits. The following list shows several examples.

Example 1	Example 2	Example 3
10,000	10,000	8,000
20,000	16,000	12,000
35,000	20,000	15,000
—	24,000	20,000
—	28,000	25,000
—	35,000	30,000
—	—	35,000

This would give you the following ranges of SCR values:

Range	Example 1	Example 2	Example 3
1	0-10,000	0-10,000	0-8,000
2	10,001-20,000	10,001-16,000	8,001-12,000
3	20,001-35,000	16,001-20,000	12,001-15,000
4	—	20,001-24,000	15,001-20,000
5	—	24,001-28,000	20,001-25,000
6	—	28,001-35,000	25,001-30,000
7	—	—	30,001-35,000

b. To determine the ranges you should configure, monitor the VBR traffic on your network, then group your VBR circuits into appropriate SCR ranges.

c. In the Scale Factor (%) column, enter a scale factor percentage to use when computing bandwidth requirements for circuits in each of the SCR ranges you defined.

For example, if you enter a value of 125%, a circuit with an SCR of 12,000 cells/sec would be allocated a bandwidth of 15,000 cells/sec (assuming you did not define physical port scale factors).

d. In the Maximum MBS column, enter an MBS value that defines the maximum MBS value allowed for each range of SCR values.

For example, if you enter a maximum MBS value of 256 for the range of SCR values (0-10000), a circuit with an SCR of 7,000 cells/sec and MBS of 300 cells is rejected by the CAC function because its MBS exceeds the specified maximum MBS.

4. When you finish, choose Ok to send the values you entered to the selected switch.

5. To send these values to another switch on the network map, select that switch and use Step 2 on page A-4 to access the Set All CAC Parameters dialog box. Choose Ok.

Customizing the CAC for the VBR-NRT and ABR Classes

To customize the CAC for VBR-NRT and ABR:

1. On the Set All CAC Parameters dialog box (Figure A-1 on page A-4), select Customize VBRnrt and ABR in the CAC Implementation field.
2. See "Tuning the CAC" on page A-5 to enter the desired values for the cell loss ratio and cell delay variation objectives.
3. See "Customizing the CAC for the VBR-RT, VBR-NRT, and ABR Classes" on page A-7 to enter the desired values in the Port Scale Factors and SCR Limit Scale Factors fields.
4. When you finish, choose Ok to send these values to the selected switch.

B

ATM Traffic Descriptors

This appendix describes how each traffic descriptor combination affects the cell streams under different traffic conditions. When you create either a PVC or a point-to-multipoint circuit, you select one of several traffic descriptor combinations. The traffic descriptor combination specifies which traffic parameters are used for traffic control. It also determines the number and type of cells that are admitted into a congested queue, and whether or not high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds.

Peak Cell Rate (PCR) CLP=0 and PCR CLP=0+1

You can select this option for constant bit rate (CBR) traffic. Traffic conformance is based on the peak cell rate (PCR) of both the cell loss priority (CLP)=0 and CLP=0+1 cell streams with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0 stream; if the cell rate exceeds the PCR of CLP=0, the switch drops the CLP=0 cells arriving above that rate.
- The switch checks the cell rate of the CLP=0+1 stream; if the cell rate exceeds the PCR of CLP=0+1, the switch drops cells arriving above that rate. Cells are dropped according to a ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

Table B-1 illustrates what would happen to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the PCR for CLP=0 to 50,000 cells/sec and the PCR for CLP=0+1 to 70,000 cells/sec.

All values in the table represent the measured traffic rate at a given point in time.

Table B-1. PCR CLP=0 and PCR CLP=0+1

CLP=0 (cells/sec)	CLP=1 (cells/sec)	Result
45,000	22,000	The switch does not drop any cells because the CLP=0 and CLP=0+1 streams did not exceed the PCR.
50,000	22,000	The switch drops 2,000 cells/sec because the cell transmission rate exceeded the PCR of the CLP=0+1 cell stream. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	17,000	Since CLP=0 exceeds the PCR, the switch drops 5,000 CLP=0 cells/sec. This leaves 67,000 cells/sec in the CLP=0+1 stream, which is below the PCR of CLP=0+1. Therefore, no additional cells are dropped.
55,000	22,000	Since CLP=0 exceeds the PCR, the switch drops 5,000 CLP=0 cells/sec. This leaves 72,000 cells/sec in the CLP=0+1 stream, which also exceeds the traffic contract. Therefore, 2,000 additional cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells will be dropped for every 22 CLP=1 cells that are dropped.

PCR CLP=0 and PCR CLP=0+1 With Tagging

You can select this option for CBR traffic. Traffic conformance is based on the PCR of both the CLP=0 and CLP=0+1 cell streams with Tagging enabled. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0 stream; CLP=0 cells arriving above the PCR of CLP=0 are tagged as CLP=1 cells.
- The switch checks the cell rate of the CLP=0+1 stream; if the cell rate exceeds the PCR of CLP=0+1, the switch drops additional cells, based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

Table B-2 illustrates what would happen to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the PCR for CLP=0 to 50,000 cells/sec and the PCR for CLP=0+1 to 70,000 cells/sec.

All values in the table represent the measured traffic rate at a given point in time.

Table B-2. PCR CLP=0 and PCR CLP=0+1 With Tagging

CLP=0 (cells/sec)	CLP=1 (cells/sec)	Result
45,000	22,000	The switch does not tag or drop any cells because the CLP=0 and CLP=0+1 streams did not exceed the PCR.
50,000	22,000	The switch drops 2,000 cells/sec because the cell transmission rate exceeded the PCR of the CLP=0+1 cell stream. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	17,000	Since CLP=0 exceeds the PCR, 5,000 CLP=0 cells/sec are tagged as CLP=1. This still leaves 72,000 cells/sec in the CLP=0+1 stream, which exceeds the PCR of CLP=0+1. Therefore, 2,000 cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 22, approximately 50 CLP=0 cells are dropped for every 22 CLP=1 cells that are dropped.
55,000	22,000	Since CLP=0 exceeds the PCR, 5,000 CLP=0 cells/sec are tagged as CLP=1 cells. This still leaves 77,000 cells/sec in the CLP=0+1 stream, which exceeds the PCR of CLP=0+1. Therefore, 7,000 cells/sec are dropped. Since the ratio of CLP=0 to CLP=1 cells is 50 to 27, approximately 50 CLP=0 cells are dropped for every 27 CLP=1 cells that are dropped.

PCR CLP=0+1

You can select this option for CBR and unspecified bit rate (UBR) traffic. Traffic conformance is based only on the PCR of the CLP=0+1 aggregate cell stream with no best effort. If you select this option, when the cell rate of the aggregate cell stream exceeds the specified PCR of CLP=0+1, the switch drops all non-conforming cells, whether they are CLP=0 or CLP=1 cells.

PCR CLP=0+1 With Best Effort

You can select this option only for UBR traffic. A “best effort” attempt is made to deliver all traffic, but there is no guarantee the switch will not drop cells due to congestion.

PCR CLP=0+1, SCR CLP=0, MBS CLP=0

You can select this option only for variable bit rate (VBR) traffic. Traffic conformance is based on the PCR of the CLP=0+1 aggregate cell stream, as well as the sustainable cell rate (SCR) and maximum burst size (MBS) of the CLP=0 cell stream with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR. The number of CLP=0 and CLP=1 cells dropped is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0 stream. If the cell rate exceeds the SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and cell delay variation tolerance (CDVT). The switch drops cells that arrive above the SCR once the stream exceeds this tolerance level.

Note – For more information about these traffic conformance parameters, see the *ATM UNI Specification, Version 3.1* or *Bellcore’s GR-1110-CORE Specification*.

Table B-3 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0 is 40,000
- MBS of CLP=0 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table B-3. PCR CLP=0+1, SCR CLP=0, MBS CLP=0

CLP=0+1 (cells/sec)	SCR of CLP=0 Stream	MBS of CLP=0 Stream	Result
68,000	40,000	30	The switch does not drop any cells because the stream does not exceed traffic parameters.
70,000	40,000	60	The switch drops CLP=0 cells from the aggregate cell stream if the burst tolerance is exceeded. The number of cells that are dropped depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are dropped.
70,000	50,000	30	The switch drops 10,000 CLP=0 cells/sec because CLP=0 exceeds the SCR. It may drop additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The switch drops 7,000 cells/sec from the CLP=0+1 stream because the stream exceeds the PCR. The number of CLP=0 and CLP=1 cells dropped depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. In addition, the switch will drop some CLP=0 cells if they exceed the burst tolerance.

PCR CLP=0+1, SCR CLP=0, MBS CLP=0 With Tagging

You can select this option only for VBR traffic. Traffic conformance is based on the PCR of the CLP=0+1 aggregate cell stream, as well as the SCR and MBS of the CLP=0 cell stream with Tagging enabled. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR of CLP=0+1. The number of CLP=0 and CLP=1 cells dropped is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0 stream. If the stream exceeds SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and CDVT. The switch tags cells that arrive above the SCR once the stream exceeds this tolerance level.

Note – For more information about these traffic conformance parameters, see the *ATM UNI Specification, Version 3.1 or Bellcore's GR-1110-CORE Specification*.

Table B-4 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0 is 40,000
- MBS of CLP=0 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table B-4. PCR CLP=0+1, SCR CLP=0, MBS CLP=0, With Tagging

CLP=0+1 Cells/sec	SCR of CLP=0 Stream	MBS of CLP=0 Stream	Result
68,000	40,000	30	The switch does not drop or tag any cells because the stream does not exceed traffic parameters.
70,000	40,000	60	CLP=0 cells from the aggregate cell stream are tagged if the burst tolerance is exceeded. The number of cells that are tagged depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are tagged.
70,000	50,000	30	The switch tags as many as 10,000 CLP=0 cells/sec because CLP=0 exceeds the SCR. It may tag additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The switch drops 7,000 cells/sec from the CLP=0+1 stream because CLP=0+1 exceeds the PCR. The number of CLP=0 and CLP=1 cells that are dropped depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. In addition, the switch will tag some CLP=0 cells if they exceed the burst tolerance.

PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1

You can select this option only for VBR traffic. Traffic conformance is based on the PCR, SCR, and MBS of the CLP=0+1 cell stream with no Tagging. The cell streams are checked for traffic conformance as follows:

- The switch checks the cell rate of the CLP=0+1 stream; the switch drops cells arriving above the PCR of CLP=0+1. The number of CLP=0 and CLP=1 cells that it drops is based approximately on the ratio of CLP=0 to CLP=1 cells.

  For example, if the ratio of CLP=0 to CLP=1 cells is 8 to 5, approximately 8 CLP=0 cells are dropped for every 5 CLP=1 cells that are dropped.

- The switch checks the SCR and the MBS of the CLP=0+1 stream. If the stream exceeds SCR, cells arriving above the SCR are admitted until the stream exceeds tolerance for such cells. Tolerance is based on the MBS, PCR, and CDVT. The switch drops cells that arrive above the SCR once the stream exceeds this tolerance level.

Note – For more information about these traffic conformance parameters, see the *ATM UNI Specification, Version 3.1* or *Bellcore's GR-1110-CORE Specification*.

Table B-5 illustrates what happens to CLP=0 and CLP=1 cells in different situations if you select this option. This example assumes you set the traffic parameters as follows:

- PCR of CLP=0+1 is 70,000 cells/sec
- SCR of CLP=0+1 is 40,000
- MBS of CLP=0+1 is 32

All values in the table represent the measured traffic rate at a given point in time.

Table B-5. PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1

CLP=0+1 (cells/sec)	SCR of CLP=0+1 Stream	MBS of CLP=0+1 Stream	Result
68,000	40,000	30	The switch does not drop any cells because the streams do not exceed traffic parameters.
70,000	40,000	60	CLP=0+1 cells are dropped from the aggregate cell stream if the burst tolerance is exceeded. The number of cells that are dropped depends on the traffic pattern combination of sustained and burst cells. The larger the burst, the more cells are dropped.
70,000	50,000	30	The switch drops 10,000 CLP=0+1 cells/sec because CLP=0+1 exceeds the SCR. It may drop additional cells because the cell burst of 30 cells at PCR, combined with the sustained traffic, may exceed the burst tolerance.
77,000	40,000	60	The CLP=0+1 stream drops 7,000 cells/sec because CLP=0+1 exceeds the PCR. The number of CLP=0 and CLP=1 cells that the switch drops depends on the ratio of CLP=0 to CLP=1 cells in the aggregate stream. In addition, the switch may drop some CLP=0+1 cells if they exceed the burst tolerance.

C

Allocating Logical Port Bandwidth on CBX 500 Shared SP Threads

CBX 500 chassis slots 3-4, 5-6, 7-8, 9-1, 10-2, 11-12, 13-14, and 15-16 are associated with the switch processor (SP) threads. This means that if you have an IOM installed in slots 3 and 4, you are "sharing" an SP thread. If you have an IOM in slot 9 or 10, you are sharing a thread with the SP itself. In this case, there are no thread limitations; the IOM has the full 599.040 Mbps of bandwidth available.

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

The 599.040 Mbps number is derived from the maximum user cell bandwidth supported by the OC-12/STM-4 interface. The OC-12/STM-4 physical layer bandwidth is 622.080 Mbps, but the maximum user traffic bandwidth that any OC-12/STM-4 port can support is 599.040 Mbps. This 599.040 thread limitation is also derived from the maximum user cell bandwidth that the four OC-3/STM-1 interfaces can support. OC-3/STM-1 physical layer bandwidth is 155.020 Mbps, but the maximum user traffic bandwidth that any OC-3/STM-1 port can support is 149.76 Mbps. Refer to "About Logical Port Bandwidth" on page 2-16 for a detailed description of mapping physical port bandwidth to logical port bandwidth.

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

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

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

Shared SP Thread Example

When a switch has two IOMs installed on an SP thread, you will notice the NMS enforcement of the SP thread bandwidth whenever you attempt to provision two OC-3/STM1 cards on the same SP fabric thread. As you provision logical ports, the NMS subtracts the assigned bandwidth from the 599.040 Mbps total. After you provision four OC-3/STM1 logical ports on the first OC-3/STM1 card using the maximum 149.76 Mbps of bandwidth, there will not be any bandwidth left for the other OC-3/STM1 card and its logical ports.

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

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

D

ATM Flow Control Processor Rate Profile Tables

This appendix describes ATM Flow Control Processor (FCP) rate profile tables, including organization and default values. For more information about the FCP rate profile tables, see “Rate Profile Tables” on page 5-15.

About FCP Rate Profile Tables

You can provision FCP rate profile tables in four separate files. You then use NavisCore to download these files to the ATM Flow Control Processor. See “Downloading Buffer Threshold and Rate Profile Tables” on page 6-5 for more information.

The FCP rate profile tables include:

- Rate Increase Exponent (RIE)
- Rate Decrease Exponent (RDE)
- Local Discard Threshold
- Local Congestion Threshold

Note – Contact a qualified Lucent organization for network design validation before enabling the FCP.

Determining FCP Rate Profile Values

Perform the following tasks to determine the minimum cell rate (MCR) class, local discard threshold, local congestion threshold, RIE, and RDE for each virtual circuit (VC) you configure.

1. Find the MCR class based on the module configuration as explained in "MCR Class Mappings" on page D-4.
2. Use the MCR class found in step 1 to find the FCP rate profile table values. Table D-1 shows the default FCP profile values.

Table D-1. FCP Rate Profile Values (by MCR class)

MCR Class	Local Discard Threshold (in cells)	Local Congestion Threshold (in cells)	RIE	RDE
0	32	16	6	3
1-27	32	16	11	3
28-55	32	16	10	4
56-83	32	16	9	5
84-110	32	16	8	5
111-138	32	16	7	6
139-166	32	16	6	6
167-194	32	16	5	7
195-221	32	16	4	8
222-255	32	16	3	8

3. If necessary, edit the rate profile tables as follows:

a. Make a backup copy of the default FCP rate profile table files using the UNIX copy command. For example:

```
cp /opt/CascadeView/etc/cvDiscard.dat
/opt/CascadeView/etc/cvDiscard.old
```

Note – It is important to create backup copies of these files in case you want to restore the default FCP rate profile tables in the future.

You might also want use unique filenames for your custom rate profile table files. If you choose to replace the default filenames in the Load Rate Profile Tables dialog box (Figure 6-2 on page 6-6) with your unique filenames, you can edit the `cascadeview.cfg` file. If you are unfamiliar with the procedures for updating the `cascadeview.cfg` file, please contact the Lucent Technical Assistance Center for more information.

The file names for the default FCP rate profile tables are as follows:

`/opt/CascadeView/etc/cvDiscard.dat`

`/opt/CascadeView/etc/cvCongestion.dat`

`/opt/CascadeView/etc/cvRif.dat`

`/opt/CascadeView/etc/cvRdf.dat`

b. Edit the default rate profile tables to include your customized values and save your edits.

c. Using the Load Rate Profile Tables dialog box (Figure 6-2 on page 6-6), download the edited rate profile table files to the FCP. See “Downloading Buffer Threshold and Rate Profile Tables” on page 6-5 for instructions.

MCR Class Mappings

The ATM Flow Control Processor performs per-VC flow control using values from the rate profile tables to assign buffers and adjust rates. These buffer and rate values are organized into 256 groups referred to as MCR classes.

This section provides MCR class mappings for the following modules:

- "DS3/E3 IOM MCR Class Mapping" on page D-4
- "T1/E1 IOM MCR Class Mapping" on page D-8
- "OC-3/STM-1 IOM MCR Class Mapping" on page D-10
- "OC-12/STM-4 IOM MCR Class Mapping" on page D-14

DS3/E3 IOM MCR Class Mapping

Table D-2 shows the MCR ranges and corresponding MCR classes for DS3/E3 IOMs.

Table D-2. DS3/E3 IOM MCR Class Mapping

MCR Range	MCR Class
100 - 127	3
128 - 159	4
160 - 191	5
192 - 223	6
224 - 255	7
256 - 287	8
288 - 319	9
320 - 351	10
352 - 383	11
384 - 415	12
416 - 447	13
448 - 479	14
480 - 511	15
512 - 543	16
1440 - 1471	45

MCR Range	MCR Class
544 - 575	17
576 - 607	18
608 - 639	19
640 - 671	20
672 - 703	21
704 - 735	22
736 - 767	23
768 - 799	24
800 - 831	25
832 - 863	26
864 - 895	27
896 - 927	28
928 - 959	29
960 - 991	30
2496 - 2559	71

MCR Range	MCR Class
992 - 1023	31
1024 - 1055	32
1056 - 1087	33
1088 - 1119	34
1120 - 1151	35
1152 - 1183	36
1184 - 1215	37
1216 - 1247	38
1248 - 1279	39
1280 - 1311	40
1312 - 1343	41
1344 - 1375	42
1376 - 1407	43
1408 - 1439	44
4224 - 4351	97

Table D-2. DS3/E3 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
1472 - 1503	46
1504 - 1535	47
1536 - 1567	48
1568 - 1599	49
1600 - 1631	50
1632 - 1663	51
1664 - 1695	52
1696 - 1727	53
1728 - 1759	54
1760 - 1791	55
1792 - 1823	56
1824 - 1855	57
1856 - 1887	58
1888 - 1919	59
1920 - 1951	60
1952 - 1983	61
1984 - 2015	62
2016 - 2047	63
2048 - 2111	64
2112 - 2175	65
2176 - 2239	66
2240 - 2303	67
2304 - 2367	68
2368 - 2431	69
2432 - 2495	70
7552 - 7679	123

MCR Range	MCR Class
2560 - 2623	72
2624 - 2687	73
2688 - 2751	74
2752 - 2815	75
2816 - 2879	76
2880 - 2943	77
2944 - 3007	78
3008 - 3071	79
3072 - 3135	80
3136 - 3199	81
3200 - 3263	82
3264 - 3327	83
3328 - 3391	84
3392 - 3455	85
3456 - 3519	86
3520 - 3583	87
3584 - 3647	88
3648 - 3711	89
3712 - 3775	90
3776 - 3839	91
3840 - 3903	92
3904 - 3967	93
3968 - 4031	94
4032 - 4095	95
4096 - 4223	96
13568 - 13823	149

MCR Range	MCR Class
4352 - 4479	98
4480 - 4607	99
4608 - 4735	100
4736 - 4863	101
4864 - 4991	102
4992 - 5119	103
5120 - 5247	104
5248 - 5375	105
5376 - 5503	106
5504 - 5631	107
5632 - 5759	108
5760 - 5887	109
5888 - 6015	110
6016 - 6143	111
6144 - 6271	112
6272 - 6399	113
6400 - 6527	114
6528 - 6655	115
6656 - 6783	116
6784 - 6911	117
6912 - 7039	118
7040 - 7167	119
7168 - 7295	120
7296 - 7423	121
7424 - 7551	122
24064 - 24575	175

Table D-2. DS3/E3 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
7680 - 7807	124
7808 - 7935	125
7936 - 8063	126
8064 - 8191	127
8192 - 8447	128
8448 - 8703	129
8704 - 8959	130
8960 - 9215	131
9216 - 9471	132
9472 - 9727	133
9728 - 9983	134
9984 - 10239	135
10240 - 10495	136
10496 - 10751	137
10752 - 11007	138
11008 - 11263	139
11264 - 11519	140
11520 - 11775	141
11776 - 12031	142
12032 - 12287	143
12288 - 12543	144
12544 - 12799	145
12800 - 13055	146
13056 - 13311	147
13312 - 13567	148
41984 - 43007	201

MCR Range	MCR Class
13824 - 14079	150
14080 - 14335	151
14336 - 14591	152
14592 - 14847	153
14848 - 15103	154
15104 - 15359	155
15360 - 15615	156
15616 - 15871	157
15872 - 16127	158
16128 - 16383	159
16384 - 16895	160
16896 - 17407	161
17408 - 17919	162
17920 - 18431	163
18432 - 18943	164
18944 - 19455	165
19456 - 19967	166
19968 - 20479	167
20480 - 20991	168
20992 - 21503	169
21504 - 22015	170
22016 - 22527	171
22528 - 23039	172
23040 - 23551	173
23552 - 24063	174
55296 - 56319	214

MCR Range	MCR Class
24576 - 25087	176
25088 - 25599	177
25600 - 26111	178
26112 - 26623	179
26624 - 27135	180
27136 - 27647	181
27648 - 28159	182
28160 - 28671	183
28672 - 29183	184
29184 - 29695	185
29696 - 30207	186
30208 - 30719	187
30720 - 31231	188
31232 - 31743	189
31744 - 32255	190
32256 - 32767	191
32768 - 33791	192
33792 - 34815	193
34816 - 35839	194
35840 - 36863	195
36864 - 37887	196
37888 - 38911	197
38912 - 39935	198
39936 - 40959	199
40960 - 41983	200
71680 - 73727	227

Table D-2. DS3/E3 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
43008 - 44031	202
44032 - 45055	203
45056 - 46079	204
46080 - 47103	205
47104 - 48127	206
48128 - 49151	207
49152 - 50175	208
50176 - 51199	209
51200 - 52223	210
52224 - 53247	211
53248 - 54271	212
54272 - 55295	213

MCR Range	MCR Class
56320 - 57343	215
57344 - 58367	216
58368 - 59391	217
59392 - 60415	218
60416 - 61439	219
61440 - 62463	220
62464 - 63487	221
63488 - 64511	222
64512 - 65535	223
65536 - 67583	224
67584 - 69631	225
69632 - 71679	226

MCR Range	MCR Class
73728 - 75775	228
75776 - 77823	229
77824 - 79871	230
79872 - 81919	231
81920 - 83967	232
83968 - 86015	233
86016 - 88063	234
88064 - 90111	235
90112 - 92159	236
92160 - 94207	237
94208 - 96000	238

T1/E1 IOM MCR Class Mapping

Table D-3 shows the MCR ranges and corresponding MCR classes for T1/E1 IOMs.

Note – If you have a T1 channel configuration for the 3-Port Channelized DS3/1 IMA IOM, use Table D-3 to determine the MCR class.

To determine the MCR class for IMA group configurations on the 3-Port Channelized DS3/1 IMA IOM, see "IMA Group Configuration" on page D-18.

Table D-3. T1/E1 IOM MCR Class Mapping

MCR Range	MCR Class
100 - 111	6
112 - 127	7
128 - 143	8
144 - 159	9
160 - 175	10
176 - 191	11
192 - 207	12
208 - 223	13
224 - 239	14
240 - 255	15
256 - 271	16
272 - 287	17
288 - 303	18
304 - 319	19
320 - 335	20
336 - 351	21
352 - 367	22
368 - 383	23
384 - 399	24

MCR Range	MCR Class
480 - 495	30
496 - 511	31
512 - 527	32
528 - 543	33
544 - 559	34
560 - 575	35
576 - 591	36
592 - 607	37
608 - 623	38
624 - 639	39
640 - 655	40
656 - 671	41
672 - 687	42
688 - 703	43
704 - 719	44
720 - 735	45
736 - 751	46
752 - 767	47
768 - 783	48

MCR Range	MCR Class
864 - 879	54
880 - 895	55
896 - 911	56
912 - 927	57
928 - 943	58
944 - 959	59
960 - 975	60
976 - 991	61
992 - 1007	62
1008 - 1023	63
1024 - 1055	64
1056 - 1087	65
1088 - 1119	66
1120 - 1151	67
1152 - 1183	68
1184 - 1215	69
1216 - 1247	70
1248 - 1279	71
1280 - 1311	72

Table D-3. T1/E1 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
400 - 415	25
416 - 431	26
432 - 447	27
448 - 463	28
464 - 479	29
1472 - 1503	78
1504 - 1535	79
1536 - 1567	80
1568 - 1599	81
1600 - 1631	82
1632 - 1663	83
1664 - 1695	84
1696 - 1727	85
1728 - 1759	86
1760 - 1791	87
1792 - 1823	88
1824 - 1855	89
1856 - 1887	90
1888 - 1919	91
1920 - 1951	92
1952 - 1983	93
1984 - 2015	94
2016 - 2047	95
2048 - 2111	96

MCR Range	MCR Class
784 - 799	49
800 - 815	50
816 - 831	51
832 - 847	52
848 - 863	53
2048 - 2111	96
2112 - 2175	97
2176 - 2239	98
2240 - 2303	99
2304 - 2367	100
2368 - 2431	101
2432 - 2495	102
2496 - 2559	103
2560 - 2623	104
2624 - 2687	105
2688 - 2751	106
2752 - 2815	107
2816 - 2879	108
2880 - 2943	109
2944 - 3007	110
3008 - 3071	111
3072 - 3135	112
3136 - 3199	113
3200 - 3263	114

MCR Range	MCR Class
1312 - 1343	73
1344 - 1375	74
1376 - 1407	75
1408 - 1439	76
1440 - 1471	77
3264 - 3327	115
3328 - 3391	116
3392 - 3455	117
3456 - 3519	118
3520 - 3583	119
3584 - 3647	120
3648 - 3711	121
3712 - 3775	122
3776 - 3839	123
3840 - 3903	124
3904 - 3967	125
3968 - 4031	126
4032 - 4095	127
4096 - 4223	128
4224 - 4351	129
4352 - 4479	130
4480 - 4534	131

OC-3/STM-1 IOM MCR Class Mapping

Table D-4 shows the MCR ranges and MCR classes for OC-3/STM-1 IOMs.

Table D-4. OC-3/STM-1 IOM MCR Class Mapping

MCR Range	MCR Class	MCR Range	MCR Class	MCR Range	MCR Class
100 - 255	1	3200 - 3327	25	6272 - 6399	49
256 - 383	2	3328 - 3455	26	6400 - 6527	50
384 - 511	3	3456 - 3583	27	6528 - 6655	51
512 - 639	4	3584 - 3711	28	6656 - 6783	52
640 - 767	5	3712 - 3839	29	6784 - 6911	53
768 - 895	6	3840 - 3967	30	6912 - 7039	54
896 - 1023	7	3968 - 4095	31	7040 - 7167	55
1024 - 1151	8	4096 - 4223	32	7168 - 7295	56
1152 - 1279	9	4224 - 4351	33	7296 - 7423	57
1280 - 1407	10	4352 - 4479	34	7424 - 7551	58
1408 - 1535	11	4480 - 4607	35	7552 - 7679	59
1536 - 1663	12	4608 - 4735	36	7680 - 7807	60
1664 - 1791	13	4736 - 4863	37	7808 - 7935	61
1792 - 1919	14	4864 - 4991	38	7936 - 8063	62
1920 - 2047	15	4992 - 5119	39	8064 - 8191	63
2048 - 2175	16	5120 - 5247	40	8192 - 8447	64
2176 - 2303	17	5248 - 5375	41	8448 - 8703	65
2304 - 2431	18	5376 - 5503	42	8704 - 8959	66
2432 - 2559	19	5504 - 5631	43	8960 - 9215	67
2560 - 2687	20	5632 - 5759	44	9216 - 9471	68
2688 - 2815	21	5760 - 5887	45	9472 - 9727	69
2816 - 2943	22	5888 - 6015	46	9728 - 9983	70
2944 - 3071	23	6016 - 6143	47	9984 - 10239	71
3072 - 3199	24	6144 - 6271	48	10240 - 10495	72

Table D-4. OC-3/STM-1 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
10496 - 10751	73
10752 - 11007	74
11008 - 11263	75
11264 - 11519	76
11520 - 11775	77
11776 - 12031	78
12032 - 12287	79
12288 - 12543	80
12544 - 12799	81
12800 - 13055	82
13056 - 13311	83
13312 - 13567	84
13568 - 13823	85
13824 - 14079	86
14080 - 14335	87
14336 - 14591	88
14592 - 14847	89
14848 - 15103	90
15104 - 15359	91
15360 - 15615	92
15616 - 15871	93
15872 - 16127	94
16128 - 16383	95
16384 - 16895	96
16896 - 17407	97
17408 - 17919	98

MCR Range	MCR Class
17920 - 18431	99
18432 - 18943	100
18944 - 19455	101
19456 - 19967	102
19968 - 20479	103
20480 - 20991	104
20992 - 21503	105
21504 - 22015	106
22016 - 22527	107
22528 - 23039	108
23040 - 23551	109
23552 - 24063	110
24064 - 24575	111
24576 - 25087	112
25088 - 25599	113
25600 - 26111	114
26112 - 26623	115
26624 - 27135	116
27136 - 27647	117
27648 - 28159	118
28160 - 28671	119
28672 - 29183	120
29184 - 29695	121
29696 - 30207	122
30208 - 30719	123
30720 - 31231	124

MCR Range	MCR Class
31232 - 31743	125
31744 - 32255	126
32256 - 32767	127
32768 - 33791	128
33792 - 34815	129
34816 - 35839	130
35840 - 36863	131
36864 - 37887	132
37888 - 38911	133
38912 - 39935	134
39936 - 40959	135
40960 - 41983	136
41984 - 43007	137
43008 - 44031	138
44032 - 45055	139
45056 - 46079	140
46080 - 47103	141
47104 - 48127	142
48128 - 49151	143
49152 - 50175	144
50176 - 51199	145
51200 - 52223	146
52224 - 53247	147
53248 - 54271	148
54272 - 55295	149
55296 - 56319	150

Table D-4. OC-3/STM-1 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
56320 - 57343	151
57344 - 58367	152
58368 - 59391	153
59392 - 60415	154
60416 - 61439	155
61440 - 62463	156
62464 - 63487	157
63488 - 64511	158
64512 - 65535	159
65536 - 67583	160
67584 - 69631	161
69632 - 71679	162
71680 - 73727	163
73728 - 75775	164
75776 - 77823	165
77824 - 79871	166
79872 - 81919	167
81920 - 83967	168
83968 - 86015	169
86016 - 88063	170
88064 - 90111	171
90112 - 92159	172
92160 - 94207	173
94208 - 96255	174

MCR Range	MCR Class
96256 - 98303	175
98304 - 100351	176
100352 - 102399	177
102400 - 104447	178
104448 - 106495	179
106496 - 108543	180
108544 - 110591	181
110592 - 112639	182
112640 - 114687	183
114688 - 116735	184
116736 - 118783	185
118784 - 120831	186
120832 - 122879	187
122880 - 124927	188
124928 - 126975	189
126976 - 129023	190
129024 - 131071	191
131072 - 135167	192
135168 - 139263	193
139264 - 143359	194
143360 - 147455	195
147456 - 151551	196
151552 - 155647	197
155648 - 159743	198

MCR Range	MCR Class
159744 - 163839	199
163840 - 167935	200
167936 - 172031	201
172032 - 176127	202
176128 - 180223	203
180224 - 184319	204
184320 - 188415	205
188416 - 192511	206
192512 - 196607	207
196608 - 200703	208
200704 - 204799	209
204800 - 208895	210
208896 - 212991	211
212992 - 217087	212
217088 - 221183	213
221184 - 225279	214
225280 - 229375	215
229376 - 233471	216
233472 - 237567	217
237568 - 241663	218
241664 - 245759	219
245760 - 249855	220
249856 - 253951	221
253952 - 258047	222

Table D-4. OC-3/STM-1 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
258048 - 262143	223
262144 - 270335	224
270336 - 278527	225
278528 - 286719	226
286720 - 294911	227

MCR Range	MCR Class
294912 - 303103	228
303104 - 311295	229
311296 - 319487	230
319488 - 327679	231
327680 - 335871	232

MCR Range	MCR Class
335872 - 344063	233
344064 - 352255	234
352256 - 353208	235

OC-12/STM-4 IOM MCR Class Mapping

Table D-5 shows the MCR ranges and corresponding MCR classes for OC-12/STM-4 IOMs.

Table D-5. OC-12/STM-4 IOM MCR Class Mapping

MCR Range	MCR Class	MCR Range	MCR Class	MCR Range	MCR Class
100 - 1023	1	12800 - 13311	25	25088 - 25599	49
1024 - 1535	2	13312 - 13823	26	25600 - 26111	50
1536 - 2047	3	13824 - 14335	27	26112 - 26623	51
2048 - 2559	4	14336 - 14847	28	26624 - 27135	52
2560 - 3071	5	14848 - 15359	29	27136 - 27647	53
3072 - 3583	6	15360 - 15871	30	27648 - 28159	54
3584 - 4095	7	15872 - 16383	31	28160 - 28671	55
4096 - 4607	8	16384 - 16895	32	28672 - 29183	56
4608 - 5119	9	16896 - 17407	33	29184 - 29695	57
5120 - 5631	10	17408 - 17919	34	29696 - 30207	58
5632 - 6143	11	17920 - 18431	35	30208 - 30719	59
6144 - 6655	12	18432 - 18943	36	30720 - 31231	60
6656 - 7167	13	18944 - 19455	37	31232 - 31743	61
7168 - 7679	14	19456 - 19967	38	31744 - 32255	62
7680 - 8191	15	19968 - 20479	39	32256 - 32767	63
8192 - 8703	16	20480 - 20991	40	32768 - 33791	64
8704 - 9215	17	20992 - 21503	41	33792 - 34815	65
9216 - 9727	18	21504 - 22015	42	34816 - 35839	66
9728 - 10239	19	22016 - 22527	43	35840 - 36863	67
10240 - 10751	20	22528 - 23039	44	36864 - 37887	68
10752 - 11263	21	23040 - 23551	45	37888 - 38911	69
11264 - 11775	22	23552 - 24063	46	38912 - 39935	70
11776 - 12287	23	24064 - 24575	47	39936 - 40959	71

Table D-5. OC-12/STM-4 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class	MCR Range	MCR Class	MCR Range	MCR Class
12288 - 12799	24	24576 - 25087	48	40960 - 41983	72
41984 - 43007	73	71680 - 73727	99	124928 - 126975	125
43008 - 44031	74	73728 - 75775	100	126976 - 129023	126
44032 - 45055	75	75776 - 77823	101	129024 - 131071	127
45056 - 46079	76	77824 - 79871	102	131072 - 135167	128
46080 - 47103	77	79872 - 81919	103	135168 - 139263	129
47104 - 48127	78	81920 - 83967	104	139264 - 143359	130
48128 - 49151	79	83968 - 86015	105	143360 - 147455	131
49152 - 50175	80	86016 - 88063	106	147456 - 151551	132
50176 - 51199	81	88064 - 90111	107	151552 - 155647	133
51200 - 52223	82	90112 - 92159	108	155648 - 159743	134
52224 - 53247	83	92160 - 94207	109	159744 - 163839	135
53248 - 54271	84	94208 - 96255	110	163840 - 167935	136
54272 - 55295	85	96256 - 98303	111	167936 - 172031	137
55296 - 56319	86	98304 - 100351	112	172032 - 176127	138
56320 - 57343	87	100352 - 102399	113	176128 - 180223	139
57344 - 58367	88	102400 - 104447	114	180224 - 184319	140
58368 - 59391	89	104448 - 106495	115	184320 - 188415	141
59392 - 60415	90	106496 - 108543	116	188416 - 192511	142
60416 - 61439	91	108544 - 110591	117	192512 - 196607	143
61440 - 62463	92	110592 - 112639	118	196608 - 200703	144
62464 - 63487	93	112640 - 114687	119	200704 - 204799	145
63488 - 64511	94	114688 - 116735	120	204800 - 208895	146
64512 - 65535	95	116736 - 118783	121	208896 - 212991	147
65536 - 67583	96	118784 - 120831	122	212992 - 217087	148
67584 - 69631	97	120832 - 122879	123	217088 - 221183	149

Table D-5. OC-12/STM-4 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
69632 - 71679	98
225280 - 229375	151
229376 - 233471	152
233472 - 237567	153
237568 - 241663	154
241664 - 245759	155
245760 - 249855	156
249856 - 253951	157
253952 - 258047	158
258048 - 262143	159
262144 - 270335	160
270336 - 278527	161
278528 - 286719	162
286720 - 294911	163
294912 - 303103	164
303104 - 311295	165
311296 - 319487	166
319488 - 327679	167
327680 - 335871	168
335872 - 344063	169
344064 - 352255	170
352256 - 360447	171
360448 - 368639	172
368640 - 376831	173

MCR Range	MCR Class
122880 - 124927	124
376832 - 385023	174
385024 - 393215	175
393216 - 401407	176
401408 - 409599	177
409600 - 417791	178
417792 - 425983	179
425984 - 434175	180
434176 - 442367	181
442368 - 450559	182
450560 - 458751	183
458752 - 466943	184
466944 - 475135	185
475136 - 483327	186
483328 - 491519	187
491520 - 499711	188
499712 - 507903	189
507904 - 516095	190
516096 - 524287	191
524288 - 540671	192
540672 - 557055	193
557056 - 573439	194
573440 - 589823	195
589824 - 606207	196

MCR Range	MCR Class
221184 - 225279	150
606208 - 622591	197
622592 - 638975	198
638976 - 655359	199
655360 - 671743	200
671744 - 688127	201
688128 - 704511	202
704512 - 720895	203
720896 - 737279	204
737280 - 753663	205
753664 - 770047	206
770048 - 786431	207
786432 - 802815	208
802816 - 819199	209
819200 - 835583	210
835584 - 851967	211
851968 - 868351	212
868352 - 884735	213
884736 - 901119	214
901120 - 917503	215
917504 - 933887	216
933888 - 950271	217
950272 - 966655	218
966656 - 983039	219

Table D-5. OC-12/STM-4 IOM MCR Class Mapping (Continued)

MCR Range	MCR Class
983040 - 999423	220
999424 - 1015807	221
1015808 - 1032191	222
1032192 - 1048575	223
1048576 - 1081343	224
1081344 - 1114111	225

MCR Range	MCR Class
1114112 - 1146879	226
1146880 - 1179647	227
1179648 - 1212415	228
1212416 - 1245183	229
1245184 - 1277951	230
1277952 - 1310719	231

MCR Range	MCR Class
1310720 - 1343487	232
1343488 - 1376255	233
1376256 - 1409023	234
1409024 - 1440000	235

IMA Group Configuration

If you have an IMA group configuration for the 3-Port Channelized DS3/1 IMA IOM, use these instructions to determine the MCR class.

1. Calculate the MCR class using the following formula:

$$3 + \left[\frac{\log_2(MCR)}{\log_2(LPortBW)} \right] \times \left[\frac{1.544(Channels)}{375} \right]$$

Table D-6 describes the arguments in the formula.
.

Table D-6. IMA Configuration MCR Formula Arguments

Argument	Description
MCR	Enter the MCR value for the virtual circuit (VC).
LPortBW	Enter the value of bandwidth configured for the logical port.
Channels	Enter the number of T1 channels configured for the IMA group.

2. When you have calculated the MCR class, round the figure up to the nearest integer value.

E

Priority Routing

Priority routing enables you to prioritize virtual circuits (PVCs and SVCs) in your network. Priority routing can provide the following advantages:

- Higher up time for high-priority circuits
- Optimal paths for high-priority circuits, which results in lower delay
- Higher capacity to burst past the guaranteed QoS rates for high-priority circuits

The switch treats priority routing, QoS class, and circuit priority as independent elements. Priority routing rules are used for connection setup. QoS class is applied after the connection is set up. Circuit priority rules are applied once QoS class is established. Keep in mind that you must assign a higher priority to real-time QoS classes.

About Priority Routing

When you use priority routing to prioritize virtual circuits, the circuits configured with higher priorities attempt to select more optimal network paths during initial circuit setup, load balance rerouting, and trunk-failure recovery.

Network Convergence Time

Priority routing introduces *network convergence time* in the network. When you configure a logical port's PVC or SVC routing priority, you specify the *bandwidth priority* (or level of importance) and *bumping eligibility* (enabled or disabled) of each PVC or SVC in the network. The lower the number for bandwidth priority, the higher is the priority. During circuit provisioning or trunk-failure recovery, higher priority circuits can bump existing lower priority circuits. The network attempts to reestablish the lower priority circuits, which may cause further bumping of still lower priority circuits. The period of network convergence required for the network to stabilize is directly proportional to the number of priorities defined in the network.

You can maintain network stability by using *restricted priority routing* to override configured bandwidth priority and bumping eligibility settings when you provision new circuits (PVCs and SVCs). Restricted priority routing uses the lowest bandwidth priority during initial circuit setup and load balance rerouting, regardless of configured higher bandwidth priority and bumping eligibility settings.

Specifying Routing Priorities

When you configure a logical port's PVC or SVC routing priority, you specify the bandwidth priority (or level of importance) and bumping eligibility of each PVC or SVC in the network. To *override* configured bandwidth priority and bumping eligibility settings for new circuits, you must enable (default) the restricted priority routing option.

If you do not override the default values for bandwidth priority (highest priority for PVCs; eight [8] for SVCs) and bumping eligibility, all PVCs in the network have the *same* routing priority, and all SVCs in the network have the *same* routing priority. If your network uses only PVCs, or only SVCs, priority routing is in effect turned off, since the priority of all circuits is the same.

However, if you prioritize circuits and disable restricted priority routing in your network, the switch assigns circuits with the highest priority to the lowest-cost paths through the network. These high-priority circuits are guaranteed full bandwidth wherever possible. Circuit prioritizing occurs at the cost of the lower-priority circuits.

Note – If your network uses *both* PVCs and SVCs, priority routing is turned on in the network because the default priority settings are different for each type of circuit. If you do not want priority routing to function in your network, Lucent recommends that you set the bandwidth priority for all SVCs to match the PVC bandwidth priority (highest).

To use priority routing, you provision the following options for new PVCs and SVCs:

Bandwidth priority — A value from 0 – 15, where 0 (zero) indicates the highest priority. For PVCs, the default value is 0 (zero); for SVCs, the default value is 8. The bandwidth priority setting is used in route calculations.

Bumping eligibility — Enables (PVC default) or disables (SVC default) bumping eligibility for the circuit. This option is valid only for non-real time circuits, based on Quality of Service (QoS) classes. Real-time circuits ignore this setting.

Restricted priority routing — Enabled (default) provisions new circuits at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings. You must disable this option if you want to use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits. When enabled, restricted priority routing functions only during initial setup and load balance rerouting; higher priority circuits can bump other circuits only during trunk-failure recovery.

The default settings for bandwidth priority, bumping eligibility, and restricted priority routing are the *recommended* settings for provisioning new circuits. See "Defining SVC Priorities Attributes" on page 3-61 and "User Preference Attributes" on page 8-32 for more information about configuring these options:

Using Restricted Priority Routing

Restricted priority routing works in the following ways:

- If restricted priority routing is disabled, a non-real time circuit that has been bumped and has bumping eligibility enabled will become active whether or not sufficient bandwidth exists. If bumping eligibility is disabled, the circuit remains in retry mode until sufficient bandwidth is available.
- If restricted priority routing is enabled, a non-real time circuit that has been bumped remains in retry mode until sufficient bandwidth is available, regardless of the bumping eligibility setting (disabled or enabled).
- Restricted priority routing allows circuits to become active only if sufficient bandwidth is available in the network. Load balancing reroutes circuits to optimal paths that do not require bumping existing circuits.
- Trunk-failure recovery uses configured bandwidth priority and bumping eligibility settings, *not* restricted priority routing. When restricted priority routing is enabled, higher priority circuits can bump other circuits only during trunk-failure recovery.
- If circuits fail to reroute because of negative bandwidth, you can disable restricted priority routing for individual circuits. These circuits will then use their configured bandwidth priority and bumping eligibility settings to find optional paths, without causing large-scale network rerouting.

Routing Priority Rules

The switch uses the following rules to implement priority routing at the time of circuit provisioning, trunk-failure recovery, and balance rerouting.

Note – These rules work as described when restricted priority routing is disabled.

Circuit Provisioning

At the time of provisioning and load balance rerouting, a circuit selects a path ignoring all circuits with lower bandwidth priority. In doing so, a circuit will force lower bandwidth priority circuits from their selected path until available link bandwidth is positive and can accommodate circuit bandwidth needs. The following sequence is used to force circuits from their path:

1. Bandwidth priority order, where lowest bandwidth priority circuits are chosen first. Keep in mind that bandwidth priority values range from 0 (zero) to 15, with 15 being the lowest priority.
2. Bumping eligibility, where circuits with bumping eligibility disabled are chosen first. Bumping eligibility values are enabled (highest priority) or disabled (lowest priority).
3. Equivalent bandwidth (EBW) order, where higher EBW circuits are chosen first.
4. Virtual channel identifier (VCI) order.

Trunk-Failure Recovery

Virtual circuits always attempt to reroute themselves when a trunk goes down. The switch software allows a trunk to reach negative bandwidth for circuits recovering from trunk failure if there is no other available path with positive bandwidth.

Priority routing modifies these rules as follows:

- A virtual circuit of higher bandwidth priority selects an optimal path in response to trunk failure without taking into account the bandwidth consumed by circuits of lower bandwidth priority. The circuits of lower priority may be forced to use paths that are not optimal (as defined in the provisioning rules).
- Virtual circuits of lower bandwidth priority are not allowed to cross trunks where there is at least one circuit of higher priority and the bandwidth is negative, with the exception of circuits configured with bumping eligibility enabled. Circuits with bumping eligibility enabled are allowed to push a trunk to negative bandwidth and rely on reroute balancing to correct the negative bandwidth at a future time.

- Virtual circuits of higher priority may push a trunk to negative bandwidth if there are no more circuits of lower priority to force off the trunk. In this case, all of the lower priority circuits (excluding circuits with bumping eligibility enabled) are forced off the trunk. Circuits configured with bumping priority enabled are given special permission to share the negative bandwidth trunk with higher priority circuits until the reroute balancing corrects this at a future time.

Balance Rerouting

Balance rerouting is a switch function that periodically tests the efficiency of each virtual circuit route. A circuit that was rerouted due to trunk failure may not be on the most optimal path at any given time or may be traversing a negative bandwidth trunk. Balance rerouting corrects these conditions by rerouting the circuit to a new path.

Priority routing modifies the switch balance-rerouting functions so that a circuit with a higher bandwidth priority is given an optimal path, and the bandwidth used by the lower-priority circuits is not considered by the switch. For this reason, circuits of lower priority may be forced onto a path that is not optimal. See "Circuit Provisioning" on page E-4 for details about path selection.

Priority Routing and Path Cost

By assigning specific bandwidth priority and bumping eligibility to ATM UNI logical ports and virtual circuits, you can guarantee that the needs of high priority circuits are met first. In addition, you can also accommodate circuits where the path cost is not important. By assigning a routing priority, you can guarantee that when a link fails or network congestion exists, the higher priority circuits are given preference in the network over circuits with a lower priority.

Priority Routing and Path Cost Example

There are two paths (Path 1 and Path 2) between a pair of nodes (A and B). The cost of Path 1 is 100, while the cost of Path 2 is 200. Multiple PVCs within the network are defined with the following priority routing settings: bandwidth priority 2, bumping eligibility enabled, and restricted priority routing disabled. These virtual circuits use all of the bandwidth on the Path 1 link. Without priority routing, additional virtual circuits are forced to use Path 2, which could involve higher delays and more hops.

With priority routing, you can define additional circuits between A and B with a Bandwidth priority of 0 (zero) and bumping enabled. The switch running the priority-routing software can detect that Path 1 is entirely populated by the circuits with the bandwidth priority 2 and bumping enabled priority. The switch then forces enough of these circuits (priority 2; bumping eligibility enabled) from Path 1 to ensure that every trunk in Path 1 has enough bandwidth to satisfy the Quality of Service (QoS) of the highest-priority (bandwidth priority 0 [zero]; bumping eligibility enabled) circuits. As a result, some priority 2 circuits are forced to Path 2.

Restricted Priority Routing and Path Cost Example

There are two paths (Path 1 and Path 2) between a pair of nodes (A and B). The cost of Path 1 is 100, while the cost of Path 2 is 200. Multiple PVCs within the network are defined with the following priority routing settings: bandwidth priority 10, bumping eligibility enabled, and restricted priority routing enabled. These virtual circuits use all of the bandwidth on the Path 1 link.

With restricted priority routing enabled, you can define additional circuits between A and B, with bandwidth priority of 0 (zero) and bumping eligibility enabled. These circuits will establish over the higher cost trunk (Path 2). With restricted priority routing enabled, new circuits are not allowed to bump existing active circuits.

If you disable Path 2, the circuits with bandwidth priority of 0 (zero) will re-establish over Path 1, bumping the lower priority circuits. With restricted priority routing enabled, circuits are allowed to bump other lower priority circuits only during trunk-failure recovery.

F

Reliable Scalable Circuit

The tables in this appendix list the NMS SNMP set errors that can occur during Circuit Add, Modify, and Delete operations for standard and redirect permanent virtual circuits (PVCs). When you perform these operations, the errors and, when possible, the circuit end point that caused the error are reported to you. When an error occurs, the Abort, Retry, and Ignore options available to you are sensitive to the end point that caused the failure.

Error information is based on both the end point that experiences the SNMP set failure and the type of SNMP set failure. Types of failures include time-outs (usually caused by switch reachability problems) and circuit-not-present conditions (usually caused by disabled or missing end-point cards). For each error combination (circuit operation, type of error, and end-point failure), the error information indicates the:

- Effect on the NMS database
- State of both switches
- Out of sync status
- Effect of performing a PRAM sync
- Other special considerations

The tables in this appendix designate end-point switches and cards for both standard and redirect PVC configurations:

Standard PVC Configuration — Designates end-point switches and cards as 1st and 2nd, indicating the send order for the SNMP set commands. An SNMP set is sent to the 1st end point, and (if successful) it is then sent to the 2nd end point. Note that for Circuit Add and Modify operations, the 1st end point is the lower-numbered node. For Circuit Delete, the 1st end point is the higher-numbered node.

Redirect PVC Configuration — Designates end-point switches and cards as Pivot, Primary, and Secondary. Note that for Circuit Add and Modify operations, the send order for the SNMP set commands is Primary, followed by (if successful) Secondary, and Pivot. For Circuit Delete, the send order for the SNMP commands is Pivot, followed by (if successful) Primary, and Secondary. The Pivot end point is the higher-numbered node for all operations.

Note – Several of the table descriptions in this appendix list “Nothing marked out of sync” after choosing Abort. This is only true if the configuration variable CV_PRAM_UPLOAD_ ABORT_ENABLED is set to 1 (the default). Any other variable setting results in both end-point cards being placed out of sync when the indicated failure occurs

Circuit Add Errors

The following table describes error messages and lists choice buttons for typical SNMP set failures encountered during attempts to add a circuit.

Note – For a *standard* Circuit Add, the SNMP set command is first sent to the lower-numbered node (switch circuit end point), *not* the higher-numbered node, as is done with a Circuit Delete operation.

For a *redirect* Circuit Add, the SNMP set commands are sent in the order of Primary, Secondary, and Pivot end points, *not* in the order of Pivot, Primary, and Secondary, as is done with a Circuit Delete operation.

Table F-1. Errors Encountered During Circuit Add Procedure

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – 1st switch unreachable (lower-numbered node). **Redirect PVC** – Primary or Secondary switch unreachable.	The SNMP request timed out (1st [or Primary or Secondary] end point identified).	**Abort** – Discontinue attempt to add circuit. (NMS database, switches, and out-of-sync status unmodified.). **Retry** – Attempt to add circuit again.
Standard PVC – 2nd switch unreachable (higher-numbered node). **Redirect PVC** – Pivot switch unreachable.	The SNMP request timed out (2nd [or Pivot] end point identified).	**Abort** – Discontinue attempt to add circuit (NMS database unmodified, circuit dangling on 1st [or Primary or Secondary] switch; nothing marked out-of-sync.) PRAM sync of end-point cards will remove traces of circuit from switches. **Ignore** – Discontinue attempt to add circuit, but add the circuit to the NMS database (circuit dangling on 1st [or Primary or Secondary] switch, 2nd [or Pivot] end-point card marked out-of-sync.) PRAM sync of end-point cards will put circuit into switches. **Retry** – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the retry.

Table F-1. Errors Encountered During Circuit Add Procedure (Continued)

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – Circuit not present on 1st switch (lower-numbered node). **Redirect PVC** – Circuit not present on the Primary or Secondary switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to add circuit (NMS database unmodified, nothing marked out-of-sync.) PRAM sync of end-point cards will remove traces of circuit from switches. **Retry** – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the Retry.
Standard PVC – Circuit not present on 2nd switch (higher-numbered node). **Redirect PVC** – Circuit not present on the Pivot switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to add circuit (NMS database unmodified, circuit dangling on 1st [or Primary or Secondary] switch; nothing marked out-of-sync.) PRAM sync of end-point cards will remove traces of circuit. **Retry** – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the Retry.

Circuit Modify Errors

The following table describes error messages and lists choice buttons for typical SNMP set failures encountered during attempts to modify an existing circuit.

Note – For a *standard* Circuit Modify, the SNMP set command is first sent to the lower-numbered node (switch circuit end point), *not* the higher-numbered node, as is done with a Circuit Delete operation.

For a *redirect* Circuit Modify, the SNMP set commands are sent in the order of Primary, Secondary, and Pivot end points, *not* in the order of Pivot, Primary, and Secondary, as is done with a Circuit Delete operation.

Table F-2. Errors Encountered During Circuit Modify Procedure

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – 1st switch unreachable (lower-numbered node). **Redirect PVC** – Primary or Secondary switch unreachable.	The SNMP request timed out (1st [or Primary or Secondary] end point identified).	**Abort** – Discontinue attempt to modify circuit. (NMS database, switches, and out-of-sync status unmodified.) **Retry** – Attempt to modify circuit again.
Standard PVC – 2nd switch unreachable (higher-numbered node). **Redirect PVC** – Pivot switch unreachable.	The SNMP request timed out (2nd [or Pivot] end point identified).	**Abort** – Discontinue attempt to modify circuit (NMS database unmodified, circuit dangling on 1st [or Primary or Secondary] switch; nothing marked out-of-sync.) PRAM sync of end-point cards will remove circuit modification. **Ignore** – Discontinue attempt to modify circuit, but modify the circuit in the NMS database (circuit modify on 1st [or Primary or Secondary] switch, 2nd [or Pivot] end-point card marked out-of-sync.) PRAM sync of end-point cards will modify circuit on both switches. **Retry** – Attempt to modify the circuit again. Dangling circuit modification on 1st (or Primary or Secondary) switch will not interfere with the retry.

Table F-2. Errors Encountered During Circuit Modify Procedure (Continued)

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – Circuit not present on 1st switch (lower-numbered node). **Redirect PVC** – Circuit not present on the Primary or Secondary switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to modify circuit (NMS database unmodified). **Retry** – Attempt to modify the circuit again.
Standard PVC – Circuit not present on 2nd switch (higher-numbered node). **Redirect PVC** – Circuit not present on the Pivot switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to modify circuit (NMS database unmodified, circuit dangling on 1st [or Primary or Secondary] switch; nothing marked out-of-sync.) PRAM sync of end-point cards will remove circuit modification. **Retry** – Attempt to modify the circuit again. Begin with 1st (or Primary or Secondary) switch, where dangling circuit modification will not interfere with the Retry.

Circuit Delete Errors

Table F-3 describes error messages and lists choice buttons for typical SNMP set failures encountered during attempts to delete an existing circuit.

Note – For a *standard* Circuit Delete, the SNMP set command is first sent to the higher-numbered node (switch circuit end point), *not* the lower numbered node, as is done with a Circuit Add or Modify operation.

For a *redirect* Circuit Delete, the SNMP set commands are sent in the order of Pivot, Primary, and Secondary end points, *not* in the order of Primary, Secondary, and Pivot, as is done with a Circuit Add or Modify operation.

Table F-3. Errors Encountered During Circuit Delete Procedure

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – 1st switch unreachable (higher-numbered node). **Redirect PVC** – Pivot switch unreachable.	The SNMP request timed out (1st [or Pivot] end point identified).	**Abort** – Discontinue attempt to delete circuit. (NMS database, switches, and out-of-sync status unmodified.) **Ignore** – Discontinue attempt to delete circuit, but delete the circuit from the NMS database (circuit not deleted on either switch, both end-point cards marked out-of-sync.) PRAM sync of end-point cards will delete circuit on switches. **Retry** – Attempt to delete the circuit again.

Table F-3. Errors Encountered During Circuit Delete Procedure (Continued)

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – 2nd switch unreachable (lower-numbered node). **Redirect PVC** – Primary or Secondary switch unreachable.	The SNMP request timed out (2nd [or Primary or Secondary] end point identified).	**Abort** – Discontinue attempt to delete circuit. (NMS database unmodified, circuit deleted on 1st [or Pivot] switch but left dangling on 2nd [or Primary or Secondary] switch, nothing marked out-of-sync.) PRAM sync of cards will restore the circuit on switches. **Ignore** – Discontinue attempt to delete circuit, but delete the circuit from the NMS database. (Circuit deleted on 1st [or Pivot] switch but left dangling on 2nd [or Primary or Secondary] switch, both end-point cards marked out-of-sync.) PRAM sync of end-point cards will delete circuit on switches. **Retry** – Attempt to delete the circuit again, which now will not be able to succeed completely. ***Note:*** *Retry process starts with 1st (or Pivot) switch, which has a deleted circuit that results in an error message.*
Standard PVC – Circuit not present on 1st switch (higher-numbered node). **Redirect PVC** – Circuit not present on Pivot switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to delete circuit. (NMS database, switches, and out-of-sync status unmodified.) **Ignore** – Discontinue attempt to delete circuit, but delete the circuit from the NMS database. (Circuit not deleted on 1st [or Pivot] switch - but it may not be there in the first place, which caused the error - or 2nd [or Primary or Secondary] end point.) Both circuit end-point cards marked out-of-sync. PRAM sync cards delete circuits on switches. **Retry** – Attempt to delete the circuit again.

Table F-3. Errors Encountered During Circuit Delete Procedure (Continued)

Type of Failure	SNMP Set Failure Reason	Available Choices
Standard PVC – Circuit not present on 2nd switch (higher-numbered node). **Redirect PVC** – Circuit not present on Primary or Secondary switch.	There is no such variable name in this MIB - possibly the card is down or not present (specific end point not identified).	**Abort** – Discontinue attempt to delete circuit. (NMS database unmodified, circuit deleted from 1st [or Pivot] switch, but left dangling on 2nd [or Primary or Secondary] switch, nothing marked out-of-sync.) PRAM sync of cards will restore the circuit on switches. **Ignore** – Discontinue attempt to delete circuit, but delete the circuit from the NMS database. (Circuit deleted on 1st [or Pivot] switch, but is left dangling on the 2nd [or Primary or Secondary] switch. Error condition would also occur if circuit was never present. 2nd [or Primary or Secondary] end-point card marked out-of-sync.) PRAM sync of end-point cards will delete circuits on switches. **Retry** – Attempt to delete the circuit again, which will not be able to succeed completely.

G

OSPF Name Aggregation

This appendix provides guidelines for using Open Shortest Path First (OSPF) name aggregation. Using OSPF name aggregation minimizes memory consumption when you provision prefixes and addresses for ATM SVC/SPVC or Frame Relay SVC connections across Lucent network switches.

About OSPF Name Aggregation

Using OSPF name aggregation enables you to use node and port prefixes to represent many port addresses at remote switches. For example, if a particular switch has 100 port addresses that start with the same number, you can provision that number as a node or port prefix. This prefix, instead of 100 addresses, is then advertised to the remote switch.

OSPF Names

An OSPF name represents any type of node prefix, port prefix, port address, port user part, or network ID. The OSPF function names each prefix or address that you provision and shares the entry throughout the network to ensure that wherever the SVC call enters the network, the intended route to the called party will be found.

The OSPF treats all prefixes and addresses the same regardless of address format (for example, E.164, X.121, DCC, and ICD). The OSPF also treats Interim Local Management Interface (ILMI) registered addresses and provisioned addresses the same.

Name Limitations

Each OSPF name in the network database consumes a small amount of IOP/IOM, BIO, and CP/SP/NP memory. Because the network has a fixed amount of memory for all Lucent switch cards, it is not possible to provision unlimited OSPF names in the network. However, you can use OSPF name aggregation to maintain a balance between the maximum number of OSPF names the network can support and the total amount of memory available for other required switch functions.

Note – See the current switch Software Release Notice (SRN) for recommended OSPF name limitations for each card and switch, and for the entire network. These limitations can change with each switch software release.

Using OSPF Name Aggregation

This section provides a sample network configuration, summarizes the drawbacks of the typical approach to address provisioning, and describes two ways of using OSPF name aggregation to provision the sample network prefixes and addresses more efficiently.

Sample Network Scenario

The network scenario in Figure G-1 displays sample configuration and addressing information for Switches 1, 2, and 3. These switches can represent any combination of B-STDX, CBX, or GX switches.

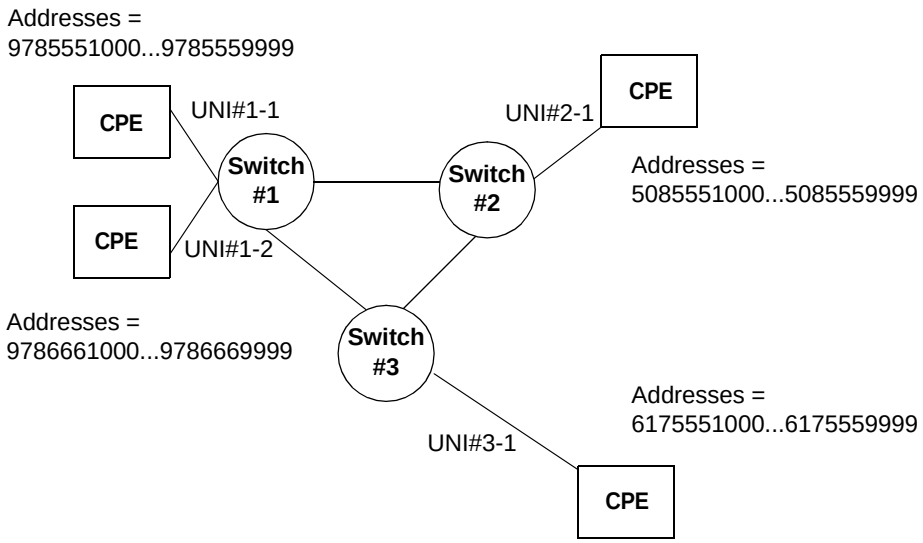


Figure G-1. Sample Network Addressing Scenario

As the network operator, you provision prefixes and addresses on Lucent equipment UNI ports to support customer premise equipment (CPE) routing requirements. The CPE can be any equipment (for example, switches or routers) that supports SVCs (or SPVCs). Table G-1 shows the addresses that require routing in the sample network shown in Figure G-1 on page G-2.

Table G-1. Address Routing Requirements for Sample Network

Switch	Port	Addresses That Require Routing
1	UNI#1-1	9785551000 through 9785559999
1	UNI#1-2	9786661000 through 9786669999
2	UNI#2-1	5085551000 through 5085559999
3	UNI#3-1	6175551000 through 6175559999

You must decide how best to use prefixes and addresses to accommodate the routing needs of the CPE users that are associated with these addresses. This example uses E.164 addresses, but the procedures described in this appendix also apply to other addressing formats (for example, X.121, DCC, and ICD).

In the sample network, assume that 1000 port addresses are possible on the CPE UNI#1-1, and all of these addresses start with 978555. Provisioning all 1000 addresses as separate port addresses on UNI#1-1 would accommodate the routing requirements for these addresses. However, this approach has the following disadvantages:

- You must manually enter 1000 address values.
- The OSPF creates a separate name for each address. Propagating all names in the OSPF database throughout the network would consume a significant amount of memory at the host switch and at the remote switches in the network.

The following sections describe two OSPF name aggregation approaches that can reduce memory consumption when provisioning addresses in the sample network.

Port-Level Name Aggregation

Instead of provisioning many individual port addresses in the sample network, you could provision a single port *prefix*, 978555, which is the value that all the CPE UNI#1-1 port addresses have in common in the sample network. The OSPF name for this port prefix would then route all SVCs (or SPVCs) from the CPE UNI#1-1 port to their destination ports. This method saves provisioning time and requires only one port-prefix OSPF name, rather than many port-address OSPF names.

Switch-Level Name Aggregation

OSPF name aggregation can also work at the switch level through the use of *node prefixes*. Node prefixes let you aggregate multiple port prefixes into one OSPF node-prefix name for remote switches.

In the sample network (Figure G-1 on page G-2), Switch #1 has two UNI ports. All of the addresses at each UNI port start with 978. As described in the preceding section, you could use name aggregation at the port level to provision two port prefixes (978555 and 978666). This solution would accommodate the routing requirements of both ports. However, the OSPF names associated with both local ports would be shared with, and consume memory on, all the other switches in the network.

Using *switch-level* name aggregation is a better solution when, for example, a network has hundreds of port prefixes on a switch and many switches throughout the network. OSPF name aggregation at the switch level minimizes the size of the name database by aggregating groups of multiple port prefixes into individual OSPF node-prefix names for remote switches, thereby reducing memory consumption in switch cards for all switches in the network.

In the sample network (Figure G-1 on page G-2), you could use switch-level name aggregation to provision a node prefix of 978 at Switch #1. This provision would aggregate all node prefixes starting with 978 into one OSPF name at remote switches. At the local host switch, OSPF names would still exist for the individual prefixes and the names would consume the required memory on the local switch cards. However, this solution would save significant memory at remote switches, which would have a single (instead of multiple) OSPF name.

Network Hierarchical Addressing Plans

Using OSPF name aggregation in conjunction with a network *hierarchical addressing plan* can reduce memory consumption by minimizing the number of OSPF names required for provisioning addresses. This section summarizes some important hierarchical addressing concepts used in both voice and data networks and relates the concepts to OSPF name aggregation.

Standards for planning voice switch networks are in place to ensure that each town in the United States has at least one unique area code and local exchange code combination. For example, Westford MA uses the 978-692 combination. If a different town in the country used the same area code and local exchange code, the voice switch network could route calls to the wrong place.

The need for similar standards exists when planning data networks that use SVCs. For example, referring to the sample network scenario shown in Figure G-1 on page G-2, suppose that addresses for both CPE at UNI#1-1 and CPE at UNI#3-1 started with 978555. You *could* provision each unique address in the network, which would route the calls correctly. However, this solution would result in a separate OSPF name entry for each address, which would cause significant memory consumption throughout the network.

Figure G-2 enhances the network scenario in Figure G-1 on page G-2 to show a hierarchical addressing plan that uses the E.164 public network addressing standard. (Any addressing standard would work the same way.)

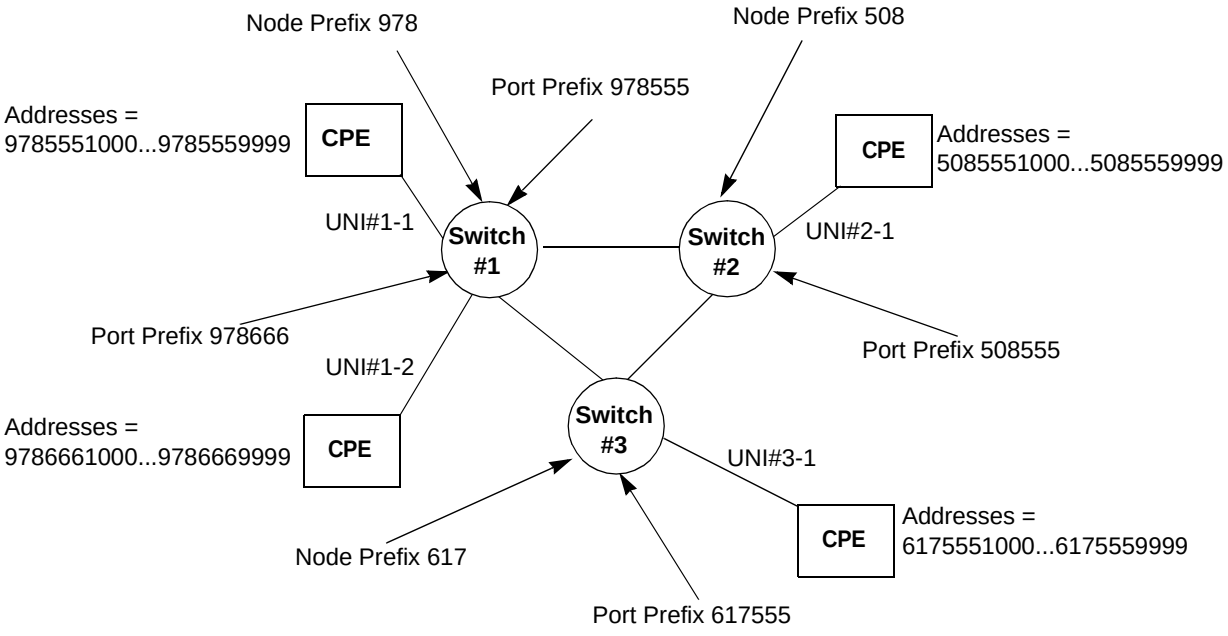


Figure G-2. Sample Network Showing Port and Network Prefixes

Assume that 1,000 addresses are possible at each of the switches in Figure G-2 on page G-5. If you do not use OSPF name aggregation, the OSPF name database for this small network may contain more than 3,000 names. This number may surpass the OSPF names limitations stated in the SRN.

As another option, you can use node prefix name aggregation to create a much smaller OSPF name database, thereby saving memory on all of the network switches. Using node prefixes for the sample network in Figure G-2 on page G-5 reduces the size of the OSPF name database to the product of the number switches in the network multiplied by the number of node prefixes per switch (plus any non-aggregated names).

You can also have multiple node prefixes on a switch (not shown in Figure G-2 on page G-5). With this solution, node prefixes may cover all possibilities. However, you must maintain the hierarchical addressing plan and ensure that the same node prefix does not exist on more than one switch.

Monitoring Network OSPF Name Activity

You can use switch console commands to view and count the number of prefixes and addresses on individual ports, cards, and switches. (You can also use NavisCore to view this information, but the process is more difficult.) See the *B-STDX, CBX, and GX Console Command User's Reference* for more information.

Viewing OSPF Names at the Network Level

Use the `show ospf statistics` command to view the total number of OSPF names in the network. The following text is a sample excerpt from the output for this console command.

```
show ospf statistics

Switch IP address:     150.201.250.1
Secondary address:     0. 0.0. 0


# switches             8               # reachable switches:   8
# Dijkstra runs:       24603           # Trunks:               46 (0)
Max LSA size:          156             Stub links:           8 (9)
# LSAs:                1019            Database checksum:    0x20ee60b
#router-LSAs:          8               # network-LSAs:         0
# AS-external-LSAs:    21              # name-LSAs:            948
# opaque-LSAs:         0
# name-summary LSAs:   0

# local names:         929             # network names:        948
```

The highlighted fields represent:

name-LSAs — The total number of names in the OSPF database from the local OSPF area.

name-summary LSAs — The total number of name summaries received from other OSPF areas. The sum of these two numbers must be lower than the limits recommended in the switch SRN. If the number exceeds the limits, you should examine all of the switches in the network to try to use additional OSPF name aggregation to reduce the size of the OSPF name database.

You can use the following techniques to examine the OSPF name database at the switch level:

- Look at the *local names* field. This field is new with switch releases B-STDX 06.02.00.00, CBX 03.02.00.00, GX 01.02.00.00, and greater. This field shows the total number of OSPF names being advertised by the local switch.

- Look at the other new field, *network names*. This field displays the same information as the sum of the existing *name-LSAs* and *name-summary LSAs* fields.

Viewing OSPF Names at the Switch Level

If you do not have the new fields in the switch software release you are running in your network, you can still monitor OSPF name activity at the switch level. Use the `show ospf names` command to view the entire OSPF name database in the network. Running this command on the switch you are examining lets you view and count the names that are associated with each switch. The following text is a sample excerpt from the output for this console command.

```
Switch#1> show ospf names

Type  Flags          Cost  State   Name/Len Primary (Secondaries)
2     0x00000000     0     N/A     508/24 250.3/0
2     0x00000000     0     N/A     617/24 250.2/0
2     0x00000000     0     N/A     978/24 250.1/0
2     0x00000000     0     N/A     978555/56 250.1/10
2     0x00000000     0     N/A     978666/56 250.1/11
2     0x00000000     0     N/A     202666/56 250.1/12
```

You can use this command to determine the names that are associated with specific switches. The highlighted field displays the entry 978/24 250.1/0, which means that the OSPF name 978 (which has 24 bits) is being advertised by switch 250.1. A zero appearing after the switch number means that a node prefix is used. A number other than zero appearing after the switch number refers to the logical port interface index (that is, it is a port prefix or port address).

The output from the `show ospf names` command will be slightly different on each switch in the network. The following text shows the output for each switch in the sample network shown in Figure G-2 on page G-5, including the results of OSPF name aggregation used in provisioning addresses for the network.

```
Switch#1> show ospf names

Type  Flags          Cost  State   Name/Len Primary (Secondaries)
2     0x00000000     0     N/A     508/24 250.3/0
2     0x00000000     0     N/A     617/24 250.2/0
2     0x00000000     0     N/A     978/24 250.1/0
2     0x00000000     0     N/A     978555/56 250.1/10
2     0x00000000     0     N/A     978666/56 250.1/11
2     0x00000000     0     N/A     202666/56 250.1/12


Switch#2> show ospf names

Type  Flags          Cost  State   Name/Len Primary (Secondaries)
2     0x00000000     0     N/A     508/24 250.3/0
2     0x00000000     0     N/A     617/24 250.2/0
2     0x00000000     0     N/A     978/24 250.1/0
2     0x00000000     0     N/A     202666/56 250.1/12
2     0x00000000     0     N/A     617555/56 250.2/10


Switch#3> show ospf names

Type  Flags          Cost  State   Name/Len Primary (Secondaries)
2     0x00000000     0     N/A     508/24 250.3/0
2     0x00000000     0     N/A     617/24 250.2/0
2     0x00000000     0     N/A     978/24 250.1/0
2     0x00000000     0     N/A     202666/56 250.1/12
2     0x00000000     0     N/A     508555/56 250.3/10
```

The sample output shows that the port prefixes are aggregated by the node prefixes so that only the node prefix is shared with other network switches. (The OSPF names associated with the port prefixes only consume memory at the local switch.) The one exception in the sample output is the port prefix 202666 on Switch #1. This prefix does not follow the hierarchical numbering plan used in the network and, as a result, the OSPF name associated with it must be advertised to all switches in the network.

Viewing OSPF Names at the Card Level

You can also use the `show pram` command to monitor the total number of OSPF names provisioned on an individual card by looking at the size of the PRAM table. The following text is a sample excerpt from the output for the PRAM table for card in slot 3 of CBX-500#1.

```
Switch#1> show pram 3

                                Configuration Database

version=6.48,     tables=16,     checksum=00007979   signature=36AC7423
size=13100720

Table    Offset   Length  RSize   Max        Count
card     800      404     156     1          1
nrtscd   1204     2316    2304    1          1
pport    3520     7520    300     24         4
lport    11040    53500   439     120        8
path     64540    4328    43      100        3
addrs    68868    98384   96      1024       113
```

The highlighted text indicates that 113 addresses and prefixes are provisioned on this particular card. However, this number does not translate directly to the number of OSPF names. You could have all or many of the provisioned entries aggregated by one (or more) port or node prefixes. For this reason, switch- and network-level monitoring techniques are recommended.

H

Customer Names

Customer Names is an *optional* software feature that enables network providers to assign ATM logical ports to a specific customer so that they can then use the customer name as a filter when viewing logical ports.

You can configure the Customer Names feature with or without the use of a virtual private network (VPN). For more information on using Customer Names with VPNs, see Chapter 11, “Configuring Layer2 VPNs.”

Configuring Customer Names

Use the following sequence to set up a Customer Name and apply it to a logical port:

Step 1. Add the Customer Name.

Step 2. Associate logical ports with this Customer Name. For specific information about configuring logical ports, see Chapter 3, “Configuring CBX 500 or GX 550 Logical Ports.”

Adding Customer Names

To add customer names:

1. From the Administer menu, select Lucent Parameters ⇒ Set All VNN Customers. The Set All Customers dialog box (Figure H-1) appears.

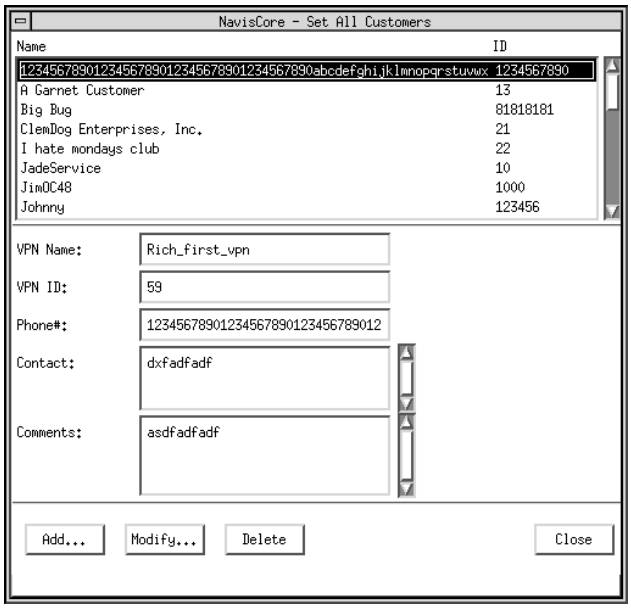


Figure H-1. Set All Customers Dialog Box

2. Choose Add. The Add Customer dialog box (Figure H-2) appears.

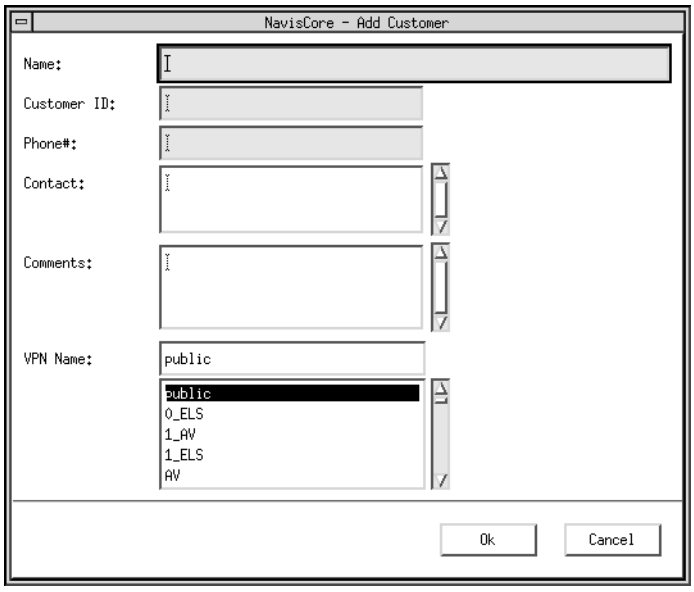


Figure H-2. Add Customer Dialog Box

3. Enter a customer name in the Name field.
4. Assign a value from 1 to 65535 in the Customer ID field.
5. (*Optional*) Enter a Phone #, Contact, and any Comments in the appropriate fields.
6. Make sure the VPN Name field defaults to public.
7. Choose Ok.
8. Choose Close to return to the network map.

Associating a Logical Port with a Customer Name

Once you configure a logical port, use the following steps to associate it with a customer name:

1. Select the switch on which the logical port resides.
2. From the Administer menu, select Lucent Parameters ⇒ Set Parameters.
3. Select the physical port on which the logical port resides.
4. Press the third (right) mouse button to display a pop-up menu. Select Logical Ports ⇒ All on Physical Port. The Set All Logical Port in PPort dialog box (Figure H-3) appears.

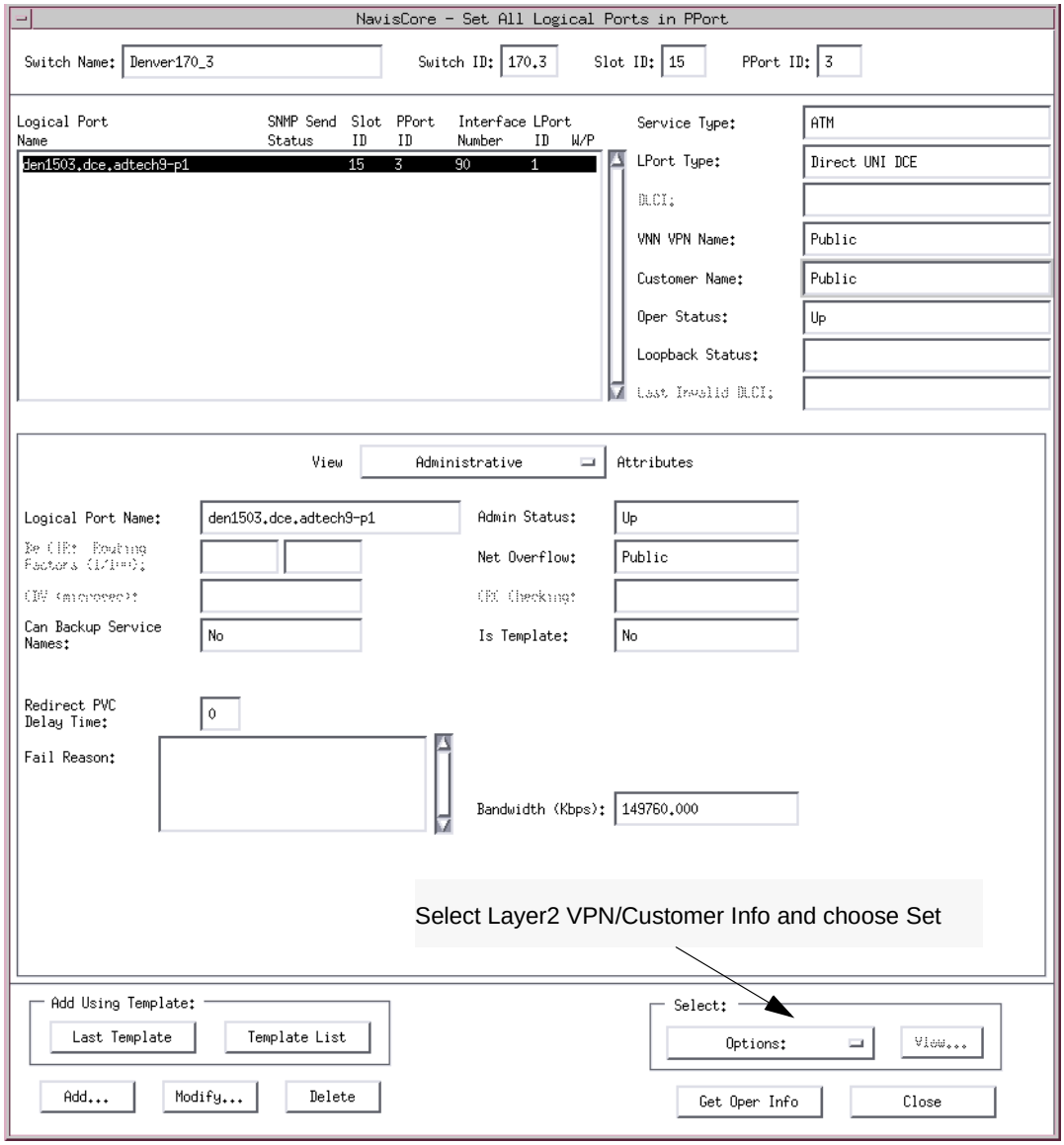


Figure H-3. Set All Logical Ports in PPort Dialog Box

5. From the Logical Port Name list box, select the name you want to associate with a customer name.

6. Using the Select: Options button, select Layer2 VPN/Customer Info and choose Set. The Select Customer and Layer2 VPN dialog box (Figure H-4) appears.

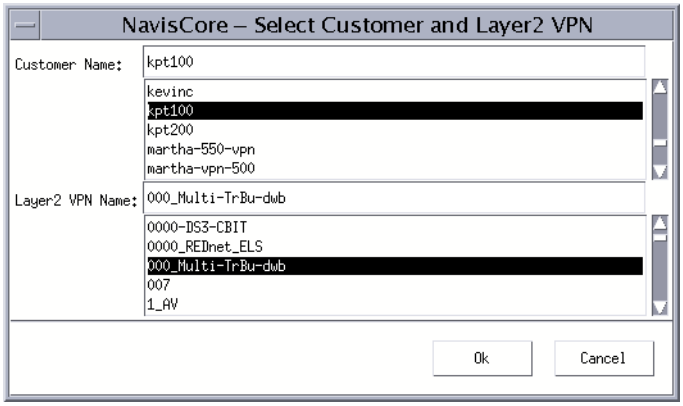


Figure H-4. Select Customer and Layer2 VPN Dialog Box

7. Select the customer name.
8. Make sure the Layer2 VPN Name defaults to Public.
9. Choose Ok.
10. Choose Close to exit.

Using the Layer2 VPN/Customer View Feature

The Layer2 VPN/Customer View feature enables a network map view for a specific customer, making it easy to identify those logical ports that belong to the customer. When you create PVCs with the Layer2 VPN/Customer View feature enabled, the Select End Logical Ports dialog box only displays the logical ports that belong to the customer you selected.

To use Layer2 VPN/Customer View:

1. From the Administer menu, select Lucent Layer2/IP VPN ⇒ Select Layer2 VPN/VNN Customer. The Select Layer2 Customer/Layer2 VPN View dialog box (Figure H-5) appears.

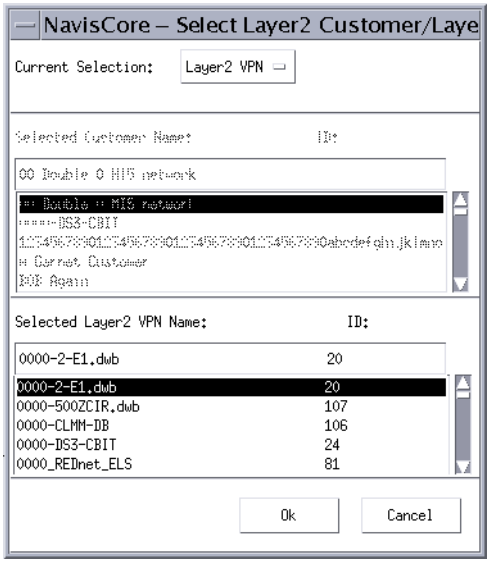


Figure H-5. Select Layer2 Customer/Layer2 VPN View Dialog Box

2. Use the Current Selection button to select Customer.
3. Select the customer name.
4. Choose Ok.

Abbreviations and Acronyms

This section lists abbreviations for units of measure (in specifications) and terms and acronyms used in Lucent documentation.

Abbreviations

The following table lists some of the abbreviations used in Lucent documentation and product specifications.

Abbreviation	Meaning
bit	binary digit
bpi	bits per inch
bps	bits per second
GB	gigabyte(s)
Gbps	gigabits per second
hex	hexadecimal
Hz	hertz (cycles per second)
ID	identification
i.e.	id est (that is)
in.	inch (es)
k	kilo (1,000)
Kb	kilobit
KB	kilobyte(s)
Kbps	kilobits per second
kg	kilogram

Abbreviation	Meaning
kHz	kilohertz
Mb	megabit
MB	megabyte(s)
Mbps	megabits per second
MHz	megahertz
min	minute(s)
modem	modulator/demodulator
msec	millisecond
usec	microsecond (abbreviate with lowercase “u” for micro)
sec	second
vs.	versus
#	number; pound
x	by (multi)

Acronyms

This guide uses the following acronyms:

Acronym	Description
AAL	Asynchronous Transfer Mode (ATM) Adaptation Layer
ABR	available bit rate
ACR	allowed cell rate
AESA	ATM End System Address
AFI	authority and format identifier
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
ASE	Autonomous System External
ASR	Application Specific Route
ATM	Asynchronous Transfer Mode
BCM	backward congestion message
BER	bit error rate
BI	backward indicator
BICI	Broadband Inter-Carrier Interface
BIO	Base Input/Output
CAC	Connection Admission Control
CBR	constant bit rate
CCRM	Cascade Communications Resource Management
CDE	Common Desktop Environment
CDV	cell delay variation
CDVT	cell delay variation tolerance
CE	circuit emulation
CFR	constant frame rate
CI	congestion indication
CIC	carrier identification code

Acronym	Description
CIR	committed information rate
CLP	cell loss priority
CLR	cell loss ratio
CP	control processor
CPE	customer premise equipment
CRC	cyclic redundancy check
CSR	Customer Specific Route
CSU	channel service unit
CTD	cell transfer delay
CUG	closed user group
DCC	data country code
DCE	data communications equipment
DE	discard eligible
DLCI	Data Link Connection Identifier
DNIC	data network identification code
DSL	digital subscriber line
DSU	data service unit
DSX	digital signal cross-connect
DTE	data terminal equipment
DXI	Data Exchange Interface
EBR	excess burst rate
EBW	equivalent bandwidth
EFCI	explicit forward congestion indication
EPD	early packet discard
ESI	end system identifier
FCP	Flow Control Processor
FEAC	Far-End Alarm and Control

Acronym	Description
FECN	forward explicit congestion notification
FR	Frame Relay
FTP	File Transfer Protocol
FUNI	Frame-User-to-Network Interface
GUI	graphical user interface
HCS	header check sequence
HDLC	High-level Data Link Control
HO-DSP	high-order domain-specific part
H-PNNI	Hierarchical PNNI
HSSI	High-Speed Serial Interface
IA	incoming access
IARP	Inverse Address Resolution Protocol
ICB	incoming calls barred
ICD	International Code Designator
ICMP	Internet Control Message Protocol
ICR	initial cell rate
ID	identifier
IDI	initial domain identifier
IDP	initial domain part
IE	information element
IFNUM	interface number
IGMP	Internet Group Multicast Protocol
IISP	Interim Inter-switch Signaling Protocol
ILMI	Interim Local Management Interface
I/O	input/output
IOA	input/output adapter
IOM	input/output module

Acronym	Description
IOP	input/output processor
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
IWU	Interworking Unit
IXC	inter-exchange carrier
KA	keep alive
LAN	local area network
LAP	Link Access Protocol
LATA	Local Access and Transport Area
LGN	logical group node
LMI	Link Management Interface
LSA	link state advertisement
LSP	label switch path
LTP	Link Trunk Protocol
MAC	Media Access Control
MBS	maximum burst size
MCR	minimum cell rate
MIB	Management Information Base
MPT	Multipoint-to-Point Tunnel
MPVC	management permanent virtual circuit
MSPVC	management soft permanent virtual circuit
NDC	Network Data Collection
NHRP	Next Hop Resolution Protocol
NI	no increase
NIC	Network Interface Card
NMS	Network Management Station

Acronym	Description
NNI	Network-to-Network Interface
NP	node processor
NPA	node processor adapter
NPC	network parameter control
NTM	network traffic management
OA	outgoing access
OAM	Operations, Administration, and Maintenance
OCB	outgoing calls barred
OPTimum	Open Packet Trunking
OSPF	Open Shortest Path First
PAD	packet assembler/disassembler
PCR	peak cell rate
PDN	public data network
PDU	protocol data unit
PG	peer group
PGL	peer group leader
PLCP	Physical Layer Convergence Protocol
PMP	point-to-multipoint
PNNI	Private Network-to-Network Interface
PPD	partial packet discard
PPP	Point-to-Point Protocol
PRAM	parameter random access memory
PRI	Primary Rate Interface
PSA	proxy siganling agent
PSC	proxy signaling client
PTSP	PNNI Topology State Packet
PTSE	PNNI Topology State Element

Acronym	Description
PVC	permanent virtual circuit
PVP	permanent virtual path
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RBOC	Regional Bell Operating Company
RCC	routing control channel
RDE	Rate Decrease Exponent
RDF	Rate Decrease Factor
RFC	Request For Comments
RIE	Rate Increase Exponent
RIF	Rate Increase Factor
RIP	Routing Information Protocol
RLMI	Resilient Link Management Interface
RM	resource management
SCR	sustainable cell rate
SD	Signal Degrade
SF	Signal Fail
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP	switch processor
SPVC	soft permanent virtual circuit
SPVCC	soft permanent virtual channel connection
SPVPC	soft permanent virtual path connection
SVC	switched virtual circuit
SVCC	switched virtual channel connection
SVPC	switched virtual path connection

Acronym	Description
TAC	Technical Assistance Center
TCP	Transmission Control Protocol
TD	traffic descriptor
TDM	timed division multiplexing
TM	timing module
TNS	transit network selection
UBR	unspecified bit rate
UDP	User Datagram Protocol
UFR	unspecified frame rate
UIO	Universal Input/Output
UNI	User-to-Network Interface
UPC	usage parameter control
VBR	variable bit rate
VBR-RT/NRT	variable bit rate-real time/non-real time
VC	virtual circuit; vortia; cjamme;
VCC	virtual channel connection; virtual circuit connection
VCI	virtual channel identifier; virtual circuit identifier
VCL	virtual circuit link; virtual channel link
VFR	variable frame rate
VFR-RT/NRT	variable frame rate-real time/non-real time
VNN	Virtual Network Navigator™
VP	virtual path
VPC	virtual path connection
VPCI	virtual path connection identifier
VPI	virtual path identifier
VPN	Virtual Private Network
WAN	wide area network

Index

A

Address
  registration for SVCs, 14-8
  translation
    disabling on egress, 3-68
    disabling on ingress, 3-69
    examples, 14-12
    on ingress, 3-69
Admin status
  for ATM logical ports, 4-38
  for B-STDX ATM logical ports, 4-15, 4-29
  for CBX/GX ATM logical ports, 3-14
  for PVCs, 8-65
  setting for circuits, 8-50
Administrative
  cost
    circuits, 8-28, 8-51
    threshold, 8-14, 8-20, 8-29, 8-66, 20-56
    trunks, 7-2, 7-23, 8-14, 8-20, 8-66
  tasks
    deleting management VPI/VCI, 2-25
AESA, *see* ATM End System Address
AFI, *see* Authority and Format Identifier
Allow VFR-rt Negative, 4-23
Allowed cell rate (ACR), 5-12
Anycast formats
  for SVCs, 14-2
APS, *see* Automatic protection switching
ASE, *see* Autonomous system external
Assigning
  IMA group logical ports, 3-7
  VNN VPN circuits, 8-20
Asynchronous Transfer Mode (ATM)
  B-STDX logical ports
    accessing functions, 4-10
    ATM direct trunk, direct cell trunk, 4-27
    Data Exchange Interface (DXI), 4-8
    I/O modules used with, 4-7
    OPTimum Frame trunk, 4-37
    selecting a logical port type, 4-10 to 4-13
    UNI DCE, 4-14 to 4-50
    UNI DTE, 4-14 to 4-50
  CBX/GX logical ports
    CE, 2-9
    NNI, 2-9
    specifying QoS parameters, 3-44 to 3-46
    specifying signaling tuning parameters, 3-33 to 3-36
    UNI DCE, 2-2
    UNI DTE, 2-2
    virtual UNI, 2-10
  overview of B-STDX service, 4-4
  overview of CBX/GX service, 2-1
  traffic descriptors, 10-5 to 10-8, B-1 to B-4
ATM End System Address (AESA)
  Authority and Format Identifier (AFI), 14-4
  Domain-Specific Part, 14-5
  End System Identifier (ESI), 14-5
  formats, 14-2 to 14-6
  High-Order Domain-Specific Part (HO-DSP), 14-5
  Initial Domain Identifier (IDI), 14-4

Initial Domain Part (IDP), 14-4
octet formats, 14-6
Selector (SEL), 14-5
ATM Flow Control Processor (FCP), 5-1 to 6-14
architecture, 5-4
buttons, 6-3
cell buffers, 5-4, 5-17
cell rate adjustment, 5-13
configuring, 6-1
configuring logical port attributes
description, 5-1
disabling, 6-11
discard, 8-34, 8-60
discard mechanisms, 5-18
enabling, 6-2
fair bandwidth determination, 6-14
fields, 6-3
frequently asked questions, 6-11
Load Rate Profile Table Dialog Box, 6-6
logical port attributes, 6-12
default configuration, 6-12
user-defined configuration, 6-12
managed VC limit, 6-8
managing traffic
UBR, 6-4
VBR-NRT, 6-4
multicast cells, 5-20
multicast rate, 6-4
performance limitations, 6-12
queues, 5-16, 5-18
rate profile tables
description of, 5-15
determining MCR value, D-2 to D-18
downloading, 6-5 to 6-6
traffic shaping, 5-15
with VP shaping, 3-16
ATM Forum UNI 4.0
supported features, 2-3
ATM Service Classes
ABR, 5-3
UBR+, 5-3
VBR-NRT, 5-3
ATM SVC parameters, 3-67
ATM UNI OC-3c/STM-1 modules (CBX)
minimum cell rate (MCR) class, D-10 to D-13
ATM, *see* Asynchronous Transfer Mode
Authority and Format Identifier (AFI), 14-4
Automatic protection switching (APS)
described, 7-5
fast Inter-card APS 1+1, 7-8
intra-card APS, 7-6
resilient UNI, 12-8
trunk backup, 7-5
Unidirectional, over PNNI, 7-9
Autonomous system external (ASE), 9-2, 9-16
ASE Advertise, 9-17
configuring, 9-16
Available bit rate (ABR)
back-pressure threshold, 6-10
closed-loop flow control, 5-13
QoS class, 10-4
RM cells, 5-5, 5-13
traffic descriptor, 10-7

B

Back-pressure threshold
FCP UBR/ABR traffic, 6-10
FCP VBR-NRT traffic, 6-9
Backup ports
activating fault tolerant PVCs, 12-4, 12-6
reverting to a primary port, 12-4
Backward Congestion Message (BCM)
cells
defining, 3-36
description of, 5-5, 5-9, 5-10
generation, 5-11, 6-8
termination, 5-12, 6-8
CI bit, 6-13
Protocol ID, 6-3
Backward Indicator (BI) bit, 5-9
Bad PVC factor, 4-19
Bandwidth
allocating for each service class, 3-45
policing for UNI logical ports, 3-24, 4-25
specifying on UNI ports, 3-16
Bandwidth (BW)
description of, 5-9, 5-12
displaying for circuit logical ports, 8-23

Bandwidth priority, 3-63, 8-33, E-3
BCM, *see* Backward Congestion Message (BCM)
Best effort traffic delivery, 10-6
Bit stuffing
  for ATM logical ports, 4-16
Buffers
  ATM FCP, 5-4, 5-17
  downloading threshold tables, 6-5
  Global Discard threshold, 6-9
  ports, 6-8
Bumping eligibility, 3-63, 8-33, E-3
BW, *See* Bandwidth (BW)

C

CAC, *see* Connection Admission Control
Call screening
  on node prefix, 3-55
  on port addresses, 3-55
  specifying on SVCs, 3-55
Calling and called endpoints
  rules for determining, 8-4
Calling Party
  address tunneling, 3-68
  disabling Insertion Mode, 3-53
  inserting address, 3-53
  Presentation Mode, 3-55
  replacing the address, 3-53, 3-68
  Screen Mode, 3-55
  specifying insertion addresses, 3-54
  SVC Insertion Mode, 3-53
Cascade Communications Resource Management (CCRM)
  cells
    defining, 3-36
    generation, 5-9, 6-8
    termination, 5-9, 6-8
  description of, 5-5
  Protocol ID, 6-3
CBR, *see* Constant bit rate
CBX modules
  ATM Flow Control Processor (FCP), 5-1 to 6-14
CCRM, *see* Cascade Communications Resource Management (CCRM)
CDV, *see* cell delay variation
CE, *see* Circuit Emulation
Cell buffers, 5-17
Cell delay variation (CDV)
  configuring tolerance, 8-35, 8-78
  enabling, 8-29
  for PVCs, 8-38
  maximum on OPTimum trunks, 3-17, 4-30
  tolerance, 3-70
Cell loss priority (CLP), 10-5
Cell rate adjustment, 5-13
Cell tagging, 10-6
Cell transfer delay (CTD)
  for PVCs, 8-38
Channels, E1
  ID number, 3-7
Check interval
  setting for ATM logical ports, 4-19
CI, *see* congestion indication
CIR, *see* committed information rate
Circuit Emulation (CE) logical ports
  configuring, 3-9
  described, 2-9
Circuit path
  manually defining, 8-69 to 8-72
Circuits, *see* permanent virtual circuit (PVC)
Clear delay
  setting for ATM logical ports, 4-19
Closed user group (CUG)
  assigning member rules, 18-11 to 18-13
  defined, 1-5, 18-1
  defining for a switch, 18-10 to 18-11
  defining members, 18-7 to 18-9
  member address, 18-2
Closed-loop flow control
  ABR RM cells, 5-5
  BCM cells, 5-5
  CCRM cells, 5-5
  configuring, 5-5, 5-7
Colors
  PNNI link line connection status, 20-50
  trunk status, 7-33
Committed burst size (BC), 8-53
Committed information rate (CIR), 8-53
Configurable control channel, 10-9

for ILMI, 3-29
for signaling, 3-31
Configuring
ATM Flow Control Processor (FCP), 6-1
private net overflow, 8-66
trunks, 7-20 to 7-33
Congestion
BCM, 6-3, 6-8
CCRM, 6-8
control
ATM FCP, 5-1
closed-loop algorithm, 5-1
setting threshold parameters, 4-18
EFCI, 6-9
local threshold, 6-5
network, 5-1
Congestion indication (CI) bit, 5-7, 5-9
Connection Admission Control (CAC)
adjusting, A-1 to A-9
customizing, A-3 to A-9
for ATM UNI DCE/DTE ports, 3-24, 4-25
Connection class, 3-22
Console Commands
modifications for PNNI Resilient UNI/APS Resilient UNI, 20-27
Constant bit rate (CBR), 10-4
Control loss threshold (CLT)
enabling, 8-29
CRC, *see* cyclic redundancy check
CTD, *see* Cell transfer delay
CUG, *see* closed user group
Custom AESA addresses
format of, 14-6
Custom AESA port prefixes, 15-19
Customer Names
configuring, H-1
customer view feature, H-6
using a virtual private network (VPN), 11-2
Cyclic redundancy check (CRC)
for ATM logical ports, 4-15

D

Data country code (DCC) addresses, 15-32
address format, 14-6
port prefixes, 15-16
Data link connection identifier (DLCI)
defined, 8-41
for frame relay circuits, 8-49
Data terminal equipment (DTE) prefix screen mode, 3-30
DCC, *see* data country code
DE/CLP mapping, 4-33, 4-48
Default route
for port prefixes, 15-23
Defining
ATM interworking PVCs, 8-41
ATM logical ports (B-STDX), 4-14
ATM logical ports (CBX/GX), 3-9
ATM PVCs, 8-22
SVC addresses, 9-12 to 9-14, 15-26 to 15-35
trunk coloring environment variable, 7-33
trunks, 7-20
Deleting
logical ports, 2-24
PMP circuits, 8-86
PVCs, 8-87
trunks, 2-25
Determining
FCP profile values, D-2
Direct trunk logical ports, 2-9
defining, 3-9
Direction (DIR) indicator, 5-9
Discard mechanisms
CLP1, 5-18
EPD, 5-18
PPD, 5-18
Discard/Congestion mapping, 4-33, 4-48
DLCI, *see* data link connection identifier
Domain Specific Part, 14-5
Downloading
buffer threshold tables, 6-5
rate profile tables, 6-5
DS0 channels
assigning to ATM logical ports, 4-16
DS3 IOM minimum cell rate (MCR) class, D-4 to D-7
DTE, *see* data terminal equipment

E

E.164 addresses
AESA format, 14-6
AESA port prefixes, 15-17
AESA SVC addresses, 15-34
translating, 3-69
E1 logical ports
assigning TS0 channels, 4-16
Early packet discard (EPD), 5-18, 6-15
support, 8-37
Egress address translation
disabling, 3-68
tunnel option, 3-68
End system identifier (ESI)
automatically assigning, 15-26
byte assignments, 15-26
definition, 14-5
End-to-End Delay
for PVC routing, 8-28, 8-51
threshold for PVC routing, 8-14, 8-21, 8-67
EPD, *see* early packet discard
ESI, *see* end system identifier
Excess burst size (Be), 8-54
Explicit forward congestion indication (EFCI)
bit check, 6-8
threshold, 6-9
Explicit forward congestion indicator (EFCI)
mapping, 8-59
Extended QoS parameters, 8-38
External device object
adding, 7-45
External interface
configuring, 7-50
External route aggregates
VNN OSPF, 7-60
External trunk
adding, 7-52
configuring, 7-44
described, 7-44

F

Failure trap threshold
for SVCs, 3-60
Fast Inter-card APS 1+1
GX 550 PNNI interworking with PSAX 4500, 20-12
configuring, 7-39
overview, 7-8
supported modules, 7-8
Fault tolerant PVCs
activating a backup port, 12-4, 12-6
configuring circuits for, 8-23
configuring logical ports for, 12-1 to 12-4
defining the service name bindings, 12-4
for UNI DCE logical ports, 3-15, 4-15, 4-39
FCP, *see* ATM Flow Control Processor
Flooding, of LSAs
standard, 7-66
VNN OSPF optimized, 7-66 to 7-69
Flow Control Processor, *see* ATM Flow Control Processor
Frame discard, 3-70, 8-37
Frame Relay to ATM interworking
configuring circuits for, 8-41
Frame Relay to ATM Network Interworking (FRF.5)
offnet PVCs over PNNI, 20-52
overview, 8-42
Frame Relay to ATM Service Interworking (FRF.8)
overview, 8-41
traffic parameter conversion, 8-47
Frame Relay-to-PNNI interworking, 20-21
Frame User-to-Network Interface (FUNI)
described, 4-8
Frequently asked questions, ATM Flow Control Processor (FCP), 6-11 to 6-14
FUNI, *see* Frame User-to-Network Interface

G

Gateway addresses
setting for port prefixes, 15-21
Generating cells, 5-6
BCM cells, 5-11
CCRM cells, 5-9
Global thresholds

CLP0+1, 5-16
congestion, 5-16
discard, 5-16
Graceful discard, 8-46

H

High-Order Domain-Specific Part (HO-DSP), 14-5

I

I/O modules
for ATM, 4-7
ICD, *see* international country designator
ICR, *see* Initial Cell Rate
IDI, *see* initial domain identifier
Idle VC factor, 5-13
IE sig overide mask, 3-61
ILMI, *see* Interim Link Management Interface
IMA groups
minimum cell rate (MCR) class, D-18
Ingress address translation
disabling, 3-69
tunnelling option, 3-69
Initial Cell Rate (ICR)
constant, 5-13, 5-15, 6-4
Initial domain identifier (IDI), 14-4
Initial domain part (IDP), 14-4
Interim Link Management Interface (ILMI)
DTE prefix screen mode, 3-30
effect on port behavior, 2-4
eligible prefixes, 14-8
enabling support, 3-29
loss threshold, 2-4, 3-29, 4-26
polling period, 2-4, 3-29, 4-26
VCC trap support, 2-5, 3-29, 4-26
VCI for polling, 3-29, 4-26
VPI for polling, 3-29, 4-26
International country designator (ICD)
address format, 14-6
port prefixes, 15-16
SVC addresses, 15-32
Intra-card APS, 7-6

K

Keep Alive threshold
configuring, 7-23
overview, 7-3

L

Layer2 VPN, 11-1
Leaf Initiated Join (LIJ), 2-3, 20-15
Least OSPF delay, 8-28
Link state advertisements
Name LSA suppression, 7-70
VNN OSPF optimized flooding, 7-66 to 7-69
Link Trunk Protocol
overview, 7-3
LMI Profile ID, 8-51
Load balancing
for SVCs, 3-60
Load Rate Profile Table Dialog Box, 6-6
Local
gateway address
setting, 15-21
Local congestion threshold, 5-16
Local discard threshold, 5-16
Logical ports
configuring fault tolerant PVCs, 12-1 to 12-4
configuring RLMI, 1-3, 13-1
defining, 3-9
deleting, 2-24, 3-5
ID for T1 and E1 modules, 4-14
modifying, 3-5
non-disruptive attributes, 2-22
service class, 4-22
specifying SVC VPI/VCI range, 3-13
types of (B-STDX), 4-2
types of (CBX/GX), 2-2
viewing screen assignments, 19-15
Loopback status
for management DLCIs, 8-14, 8-21, 20-57
for PVCs, 8-65
Loss threshold
ILMI, 2-4, 3-29, 4-26

M

Management
  PVCs, 9-3
  trunks, 7-17
  VPI/VCIs, 9-8 to 9-10
Management DLCIs
  loopback, 8-14, 8-21, 20-57
Management Permanent Virtual Circuit (MPVC), 9-3
  configuring, 9-4
Management redirect PVC
  defined, 9-2
Management Soft Permanent Virtual Circuit (MSPVC), 9-2
  configuring, 9-11
  described, 9-11
  in PNNI environment, 9-11
Management VPI/VCI
  defined, 9-2
Maximum burst size (MBS)
  definition of, 10-6
  for ATM UNI DS3/E3, 4-32
  PVCs, 8-31, 8-56, 8-81, 10-11
Maximum cell delay variation
  OPTimum trunks, 3-17, 4-30
MBS, *see* maximum burst size
MCR, *see* minimum cell rate
Minimum Cell Rate (MCR)
  class
    DS1 (T1) configuration, D-8
    IMA group configuration, D-18
  class parameters, D-4 to D-17
    OC-12c/STM-4 IOM, D-14 to D-17
    OC-3c/STM-1 IOM, D-10 to D-13
  guarantee, 5-3
  traffic descriptor type, 8-31, 8-56
Modifying trunks, 7-15
Moving circuits, 8-73 to 8-74
MPVC, *see* Management Permanent Virtual Circuit
MSPVC, *see* Management Soft Permanent Virtual Circuit
Multicast cells, 5-20
Multicast rate, 6-4
Multiple OSPF area support, 7-16, 7-23, 15-11
Multiple trunks
  displaying, 7-32
Multipoint VCCs
  and OPTimum trunks, 4-31, 4-32

N

Name summary LSAs
  suppressing, 7-70
Native E.164
  port prefixes, 15-14
  SVC addresses, 15-31
  translating addresses to E.164 AESA, 3-69
Net overflow
  configuring
    for ATM logical ports (B-STDX), 4-39
    for circuits, 8-27
    for point-to-multipoint circuits, 8-82
    for UNI ports, 3-15
Network ID addressing
  overview, 14-17
Network Parameter Control (NPC)
  NNI logical ports, 3-25
Network prefix, 14-9
Networks
  tunneling through, 3-68
Network-to-Network Interface (NNI) logical ports
  configuring, 3-9
  NPC function, 3-25
  overview, 2-9
NNI DLCI, 8-51
NNI, *see* Network-to-Network Interface logical ports
No Increase (NI) bit, 5-7, 5-9
Node link BW factor (%), 20-32, 20-43
Node prefixes
  configuring, 15-2 to 15-10
  ILMI-eligible, 14-8
  using for call screening, 3-55
Non-disruptive logical port and trunk attributes, 2-22
NPC, *see* Network Parameter Control
Number of valid bits in VPI/VCI

UNI logical ports, 2-11, 3-27, 4-24

O

OAM, *see* Operations, Administration, and Maintenance alarms
OC-12c/STM-4 I/O module (CBX)
  minimum cell rate (MCR) class, D-14 to D-17
OC-12c/STM-4 Phy module (GX 550)
  minimum cell rate (MCR) class, D-14 to D-17
OC-3c/STM-1 Phy module (GX 550)
  minimum cell rate (MCR) class, D-10 to D-13
Octet formats, 14-6
Offnet PVC over PNNI
  adding, 20-58
  configuring, 20-59
  overview, 20-52
Open Shortest Path First
  defining OSPF external route aggregates, 7-64
  defining VNN area aggregates, 7-57, 7-61, 7-64
  defining VNN external route aggregates, 7-60
  defining VNN virtual links, 7-59
  LSA flooding
    about, 7-66
    VNN OSPF optimized, 7-66 to 7-69
Open Shortest Path First (OSPF)
  area support, 7-16, 7-23
  bypassing on PVCs, 8-69 to 8-72
Operational status
  fail reason status codes, 8-12
Operations, Administration, and Maintenance (OAM) alarms
  enabling on PVCs, 8-34
  enabling on UNI ports, 3-31, 4-26
  timer threshold, 3-31, 4-26
OPTimum cell trunks
  configuring for B-STDX, 4-28
  maximum cell delay variation, 4-30
  multipoint VCCs, 4-31, 4-32
OPTimum frame trunks
  configuring for B-STDX, 4-37
  specifying VPI for, 4-37
OPTimum trunks, 2-7
  defining for CBX/GX, 3-9
  maximum cell delay variation, 3-17
  PMP circuit leafs on, 8-85
  vpi range, 3-38
OSPF
  area support, 15-11
  console commands, G-7
  name
    aggregation, G-1
      with a network hierarchical addressing plan, G-5
    limitations, G-2
Overload Severity, 8-7
Oversubscription, 2-18 to 2-19, 3-46
Overview
  ATM Flow Control Processor (FCP) configuration, 6-2

P

Partial packet discard (PPD), 5-18
  support, 8-37
PCR, *see* peak cell rate
Peak cell rate (PCR)
  definition of, 10-5
  PVCs, 8-31, 8-56, 8-81, 10-10
Permanent virtual circuit (PVC)
  adding, 8-22 to 8-40
  administrative cost, 8-28, 8-51
  bypassing OSPF, 8-69 to 8-72
  configuring
    fault tolerance, 8-23
    priority routing, 8-33, 8-59
  CS/IWU shaper, 8-32
  defining a new connection, 8-22 to 8-40
  deleting, 8-87
  EFCI mapping, 8-59
  enabling
    OAM alarms on, 8-34
    reroute balance, 8-33, 8-59
    UPC function on, 8-35, 8-61
  endpoint creation rules, 8-4
  FCP discard, 8-34, 8-60
  frame discard, 8-37
  frame relay to ATM interworking, 8-41

GX provisioning guidelines, 8-2
manually defining circuit path, 8-69 to 8-72
MBS, 8-31, 8-56, 8-81, 10-11
MCR, 8-31, 8-56
moving, 8-73 to 8-74
PCR, 8-31, 8-56, 8-81, 10-10
priority for PMP circuits, 8-82
routing thresholds, 8-28
routing with end-to-end delay, 8-28, 8-51
SCR, 8-31, 8-56, 8-81, 10-10
specifying traffic descriptor, 8-30
templates, 8-87
VCI, 8-9, 8-25, 8-81
VPI, 8-9, 8-25, 8-65, 8-80
Per-VC queuing, 5-16
PMP circuits, *see* point-to-multipoint circuits
PNNI Features
PNNI Reroute Load Balancing, 20-22
Resilient UNI/APS Resilient UNI, 20-25
PNNI Name Translation, 7-71
PNNI Reroute Load Balancing, 20-22 to 20-24
criteria, 20-22
defining reroute tuning parameters, 20-23
PNNI reroute time tuning
reroute count, 20-23, 20-24
reroute delay, 20-23, 20-24
reroute ratio, 20-23
PNNI Resilient UNI/APS Resilient UNI, 20-25 to 20-26
PNNI, *see* private network-to-network interface
Point-to-multipoint (PMP) circuits
adding leafs to, 8-84 to 8-85
configuring, 8-75 to 8-87
root, 8-79
deleting
leafs, 8-86
root, 8-86
enabling reroute balance on, 8-82
on OPTimum trunks, 8-85
specifying circuit priority, 8-82
Polling
for ILMI, 2-4, 3-29
VCI, 3-29, 4-26
VPI, 3-29, 4-26
Polling period
ILMI, 4-26
Port
addresses
using for call screening, 3-55
prefixes
configuring, 15-13 to 15-23
custom AESA, 15-19
DCC, 15-16
defining a default route, 15-23
E.164 AESA, 15-17
ICD, 15-16
ILMI-eligible, 14-8
native E.164, 15-14
setting gateway addresses, 15-21
security screening
activating, 19-13
assigning screens, 19-11 to 19-13
creating security screens, 19-8 to 19-10
defined, 1-5, 19-1
screen addresses, 19-3
viewing screen assignments, 19-15
PPD, *see* Partial packet discard
Prefix screen mode
UNI DTE ports, 3-30
Priority frame
configuring for ATM logical ports, 4-22
Priority routing, E-1
configuring PVCs, 8-33, 8-59
for SVCs, 3-61, 3-64
Private net overflow
configuring, 8-66
Private network-to-network interface (PNNI)
configuring PNNI routing, 20-27
connecting a PNNI network, 9-2
external name, 15-11
Frame Relay-to-PNNI interworking, 20-21
GX 550 Fast APS 1+1 PNNI interworking with PSAX 4500, 7-8, 7-39, 20-12
hierarchical organization, 20-7
holdoff timer, 3-36
importing exterior addresses, 20-17
Lucent ATM SPVC node prefix, 20-15
name translation, 7-71
Native E.164 address advertisement, 20-18
organizational scope, 15-4

PNNI administrative weight, 7-41, 20-13, 20-45
PNNI link line connection
defining, 20-48
status colors, 20-50
PNNI MIB, 7-48
PNNI/VNN gateway support, 20-17
PNNI/VNN OSPF call interworking, 20-17
RCC traffic descriptors, 10-17
routing protocol, 20-7
signaling overview, 20-14
supported features, 20-2
suppress PNNI advertisement, 15-12
trap support, 20-66
UBR load balancing, 20-14
using management SPVCs, 9-11
Protocol timers
Q.93B signaling, 3-34
Proxy signaling
overview, 3-12, 16-1
PSA, 16-3
PSC, 16-3
PVC Establishment Rate Control, 8-5
with VC Overload Control disabled, 8-5
with VC Overload Control enabled, 8-5
PVC Manager Revision
for a trunk, 7-19
PVC redirect, 8-15
PVC, *see* permanent virtual circuit

Q

Q.93B signaling, 3-33 to 3-36
maximum restarts, 3-34
protocol timers, 3-34
Q.SAAL
thresholds, 3-35
QoS, *see* Quality of Service
Quality of Service (QoS)
configuring on UNI ports, 3-44
for SVCs, 3-47
parameters, 8-53
setting for logical ports, 3-44 to 3-46

R

Rate Decrease Factor (RDF), 5-14
Rate enforcement, 8-45
Rate Increase Factor (RIF), 5-14
Rate profile tables, 6-5
description of, 5-15
determining values, D-2
Rate Decrease Exponent (RDE), 5-15
Rate Increase Exponent (RIE), 5-15
Redirect PVCs
described, 8-15
Reject delay, 3-61
Reliable Scalable Circuit
described, 8-8
error messages, F-1
Remote gateway address
setting, 15-21
Reroute time tuning
enabling on PMP circuits, 8-82
enabling on PVCs, 8-33, 8-59
Resilient Link Management Interface (RLMI)
configuring logical ports for, 1-3, 13-1
Resilient UNI
with APS, 12-8
Resilient UNI/APS Resilient UNI over PNNI, 20-25 to 20-26
Resilient UNI/NNI, 12-1
Restricted priority routing, 3-63, 8-33, E-3
RFC 1483 to 1490, 8-58
RFC 1490 to 1483, 8-58
RLMI, *see* Resilient Link Management Interface
RM cells
generation, 5-6
Routing determination
SVCs, 14-10
Routing metrics, 3-46
administrative cost, 3-46
cell delay variation, 3-46

S

Scope
configuring PNNI organizational scope, 15-4
SCR, *see* sustainable cell rate

Security screens, 19-8 to 19-10
Selectable statistics, 3-42, 8-39
Selective Discard (CLP1), 5-18
Selector (SEL), 14-5
Service name bindings
  defining, 12-4
Set All VNN Optimized Flooding Dialog Box, 7-68
Set ATM FCP Attributes Dialog Box, 6-7
Set attributes option menu
  for ATM logical ports, 4-10
Set Switch Tuning dialog box, 20-23
Shaper
  with CS/IWU PVC endpoints, 8-32
Show all circuits on trunk, 7-15
Signaling tuning parameters, 3-33 to 3-36
  UNI logical ports, 3-23
Static ARP entry
  defining, 8-16
Status indicators
  PNNI link line connection, 20-50
  trunks, 7-33
Subnet routing for Management VPI/VCI
  defined, 9-2
Sustainable cell rate (SCR)
  definition of, 10-5
  for ATM direct and OPTimum cell trunks, 4-32
  PVCs, 8-31, 8-56, 8-81, 10-10
SVC VPI/VCI range, 3-13
SVC, *see* switched virtual circuit
Switched virtual circuits (SVCs)
  address registration, 14-8
  addresses
    DCC, 15-32
    E.164 AESA, 15-34
    ICD, 15-32
    native E.164, 15-31
    user part, 15-39
  anycast formats, 14-2
  automatic assignment of ESI bytes, 15-26
  Calling Party Insertion Mode, 3-53
  configuring
    node prefixes, 15-2 to 15-10
    port prefixes, 15-13 to 15-23
  defining
    addresses, 9-12 to 9-14, 15-26 to 15-35
    call screening, 3-55
  defining attributes, 3-50
  failure trap threshold, 3-60
  hold down timer, 3-60
  load balancing, 3-60
  overview, 14-1
  routing determination, 14-10
  tunneling, 3-68
  user part, 15-39

T

T1 logical ports
  assigning DS0, 4-16
T1 modules (CBX)
  minimum cell rate (MCR) class, D-8 to D-9
Tables
  buffer threshold, 6-5
  rate profile, 6-5
Tagging, 10-6
Technical, xliii
Templates
  for ATM logical ports, 2-21, 3-5
  for circuits, 8-11, 8-66, 8-87
  for SPVCs, 17-6
Terminating cells, 5-6
  BCM cells, 5-12
  CCRM cells, 5-9
Thresholds
  buffer, 6-5
  CLP+1, 6-9
  CLP0+1, 6-9
  EFCI, 6-9
  FCP UBR back pressure, 6-10
  FCP VBR back pressure, 6-9
  Global Discard buffer, 6-9
  Multicast Discard, 6-4
Traffic descriptors
  best effort option, 10-6
  description of, 10-5 to 10-8, B-1 to B-4
  PCR CLP=0+1, Best Effort, B-4
  PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1, B-8

PCR CLP=0+1, SCR CLP=0, MBS CLP=0, B-4
PCR CLP=0+1, SCR CLP=0, MBS CLP=0, Tagging, B-6
PCR CLP=0, PCR CLP=0+1, B-2
PCR CLP=0, PCR CLP=0+1, Tagging, B-3
specifying for PVCs, 8-30
tagging option, 10-6
Traffic shaping
configuring, 5-16
description of, 5-15
Transmit scheduling, 4-22
Trunk backup
for B-STDX, 7-12
with APS and Fast APS 1+1, 7-34
Trunk hold down time, 7-18, 7-24
Trunk logical ports
for ATM, 4-3, 4-4
Trunks
administrative cost, 7-2, 7-23, 8-14, 8-20, 8-66
coloring
defining environment variable, 7-33
configuring, 7-1
management trunks, 7-17
creating trunk lines, 7-27
defining, 7-20
deleting, 2-25, 7-15
displaying
multiple trunks, 7-32
managing trunks, 7-31
modifying, 7-15
non-disruptive attributes, 2-22
PVC Manager revision, 7-19
show all circuits on, 7-15
status, 7-19
status colors, 7-33
submap window, 7-32
TS0 channels
for ATM logical ports, 4-16
Tuning
defining circuit reroute parameters, 20-23
See also PNNI reroute time tuning
Tunneling through networks, 3-68

U

UBR, *see* Unspecified bit rate
UNI, *see* user-to-network interface
Unspecified bit rate (UBR), 10-4
back-pressure threshold, 6-10
traffic managed by FCP, 6-4
UPC, *see* Usage Parameter Control
Usage Parameter Control (UPC)
enabling on PVCs, 8-35, 8-61
UNI logical ports, 3-24
User parts
SVC addresses, 15-39
User-to-network interface (UNI) logical ports
bandwidth policing, 4-25
B-STDX, 4-14 to 4-50
number of valid bits in VPI/VCI, 4-24
CBX/GX
bandwidth, 3-16
policing, 3-24
configuring, 3-10
DCE, 2-2
defining, 3-9
ILMI effect on, 2-4
maximum VPIs, 2-12
number of valid bits in VPI/VCI, 2-11, 3-27
UPC function, 3-24
maximum VCIs, 2-12

V

Variable bit rate-real time/non-real time (VBR-RT/NRT)
back-pressure threshold, 6-9
traffic managed by FCP, 6-4
VC Overload Control, 8-6 to 8-7
PVC Establishment Rate Control, 8-5
VCC, *see* virtual channel connection
VCI, *see* virtual channel identifier
Virtual channel connection (VCC)
specifying, 8-27
SPVCs, 17-12, 17-17
Virtual channel identifier (VCI), 2-11 to 2-13, 3-27, 4-5, 4-24

defined for interworking PVCs, 8-41
for ATM logical ports, 2-11
for GX 550, 8-2
for PVCs, 8-9, 8-25, 8-81
setting for ATM circuits, 8-49
setting valid bits, 4-5
Virtual channels
maximum allowed on UNI port, 2-12
on GX 550 BIO modules, 8-2
Virtual connection, 3-22
Virtual Network Navigator
external route aggregates, 7-60
Name LSA suppression
about, 7-70
enabling and disabling, 7-70, 20-28
OSPF optimized flooding
about, 7-66, 7-67
enabling and disabling, 7-68
interoperability, 7-68
monitoring, 7-69
Virtual path connection (VPC)
configuring the OPTimum Trunk for, 2-8
specifying, 8-27
SPVCs, 17-12, 17-17
Virtual path identifier (VPI), 2-7, 2-11 to 2-13, 3-27, 4-5, 4-24
for ATM logical ports, 2-11
for GX 550, 8-2
for PVCs, 8-9, 8-25, 8-65, 8-80
OPTimum frame trunks, 4-37
setting for ATM circuits, 8-49
setting valid bits, 4-5
Virtual paths
maximum allowed on UNI port, 2-12
Virtual Private Network (VPN)
assigning
circuits, 8-20
configuring, 11-4, H-1
configuring the trunk, 7-24
Layer2, 11-1
overview, 11-1
Virtual UNI logical ports
configuring, 3-49
defined, 2-10
VP shaping
configuring for B-STDX, 4-6, 4-30
configuring on CBX, 3-16
for virtual UNI logical ports, 3-19 to 3-20
VPC, *see* virtual path connection
VPCI addressing
for proxy signaling, 16-3
setting the VPCI table, 16-5
VPI, *see* virtual path identifier
VPN, *see* Virtual Private Network

B-STDX, CBX, and GX ATM Services Configuration Guide
Customer Comments

Please take time to fill out this questionnaire so that we can do our best to meet your documentation needs. Then fax or e-mail your comments to our Technical Publications Dept. Your opinions are of great value to us!

FAX: (978) 692-1510 (Attn: Tech Pubs)
E-MAIL: cspubs@lucent.com

Cut Here

- What tasks did you perform using this guide? _____
- Did you install the hardware/software? _____
- If you were having trouble performing a task, were you able to find the information you needed? Was the index useful? _____
- Were the examples and illustrations helpful for performing tasks? If not, how can they be improved? _____
- Was there any information you needed that was not in the manual? If so, how can we best deliver that information to you? _____
- What did you like/not like about the manual? _____
- Do you have any other comments about the manual? _____

Page	Description of Error

Name _____ Company _____

Mailing Address _____

Phone _____ E-mail address _____

Fax No. _____