

**Lucent Technologies**  
Bell Labs Innovations



# Frame Relay Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000

Product Code: 86020  
Revision 000  
September 2005

---

**Copyright© 2005 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, Data Networking Group 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.** All trademarks and service marks specified herein are owned by their respective companies.

**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.....	iv
Reading Path.....	v
How to Use This Guide.....	viii
What's New in This Guide.....	x
Conventions.....	xi
Related Documents.....	xii
Lucent.....	xii
Third Party.....	xiii
Using the Navis EMS-CBGX Online Help.....	xiv
Ordering Printed Manuals Online.....	xv
Customer Comments.....	xv
Technical Support.....	xv

## Chapter 1

### Overview

Logical Ports.....	1-2
Trunks.....	1-2
PVCs.....	1-3
Offnet Circuits.....	1-3
Ethernet Virtual Circuits (EVCs).....	1-3
Layer2 Virtual Private Networks.....	1-3
Fault Tolerant PVCs.....	1-4
Resilient LMI.....	1-4
SVCs.....	1-4
Closed User Groups.....	1-4
Port Security Screening.....	1-4

## Chapter 2

### Frame Relay Services

About Frame Relay Logical Ports.....	2-2
Logical Port Types.....	2-2
Using Fault-Tolerant PVCs.....	2-4
Using Resilient LMI PVCs.....	2-4
Using Frame Relay OPTimum Trunks.....	2-5
Congestion Control.....	2-5

Closed-Loop Congestion Control and Congestion States .....	2-5
Link State Updates .....	2-6
Congestion Parameters .....	2-7
Threshold Parameters .....	2-7
Maximum Threshold Values .....	2-8
Default Congestion Level Values .....	2-9
Congestion Control on the 4-Port Channelized T1 Module .....	2-11
Congestion Control on the 4-Port Channelized E1 Module .....	2-12
Congestion Control on the 32-Port Channelized T1/E1 FR/IP Module .....	2-13
Congestion Threshold Example (32-Port Channelized T1/E1 FR/IP Module) .....	2-14
Maximum Mono-Class and Multi-Class Congestion Thresholds .....	2-14
Default Mono-Class and Multi-Class Congestion Thresholds .....	2-15
Congestion Control on the 6-Port Channelized DS3/1/0 Frame Relay I/O Module .....	2-17
Algorithms .....	2-17
Logical Port Congestion Thresholds for TAQL and Simpler Algorithms .....	2-20
Frame TS0 Thresholds .....	2-21
CLLM Congestion Notification .....	2-22
About CLLM .....	2-22
CLLM Threshold States .....	2-23
CLLM Messages .....	2-23
Priority Frame Quality of Service (QoS) .....	2-24
Using a T1/E1 Card .....	2-24
Administrative Tasks .....	2-25
Using Templates .....	2-25
Modifying Switch Configuration Attributes .....	2-26
Non-Disruptive Logical Port and Trunk Attributes (CBX Only) .....	2-27
Deleting Frame Relay Logical Ports .....	2-28
Deleting Circuits .....	2-28
Deleting Trunks .....	2-29
Deleting Management or Multicast DLCIs .....	2-30
Deleting the Logical Port .....	2-32

## Chapter 3      **Configuring Frame Relay LPorts**

Working with Frame Relay LPorts .....	3-2
Accessing LPorts in the Switch Tab .....	3-3
Adding a Frame Relay LPort .....	3-5
Modifying a Frame Relay LPort .....	3-7
Defining Frame Relay UNI DCE/DTE or NNI LPorts .....	3-10
Defining the Service Type and LPort Type .....	3-10
Setting Frame Relay LPort Attributes .....	3-11
General Attributes for Frame Relay LPorts .....	3-12
Administrative Attributes for Frame Relay LPorts .....	3-15
FRF.19 Attributes for Frame Relay LPorts .....	3-21
Congestion Control Attributes (VFR-NRT only) for Frame Relay LPorts .....	3-24



Priority Frame Attributes for Logical Ports.....	3-29
QoS Attributes for Logical Ports .....	3-31
MLFR LPort Bind Attributes for Logical Ports.....	3-33
Link Management Attributes for Logical Ports.....	3-34
MLFR Configuration Attributes for Logical Ports .....	3-38
Trap Control Attributes for Logical Ports.....	3-40
Configuring Logical Ports for Use With SVCs .....	3-42
General Attributes for SVCs .....	3-43
Setting SVC Priorities.....	3-45
Setting SVC QoS Attributes .....	3-46
Setting Traffic Descriptor Limits.....	3-47
Signaling Attributes for SVCs.....	3-49
Setting SVC Signaling Tuning Attributes .....	3-50
Address Attributes for SVCs.....	3-52
Connection ID Attributes for SVCs .....	3-56
CUG Attributes for SVCs.....	3-56
Defining Frame Relay OPTimum PVC Trunk Logical Ports.....	3-58
About DLCI Numbers.....	3-58
Defining the OPTimum PVC Trunk .....	3-59
Defining Encapsulation FRAD, Direct Line Trunk, and PPP Logical Ports .....	3-60
Completing the PPP Logical Port Configuration .....	3-62
Defining Authentication Attributes .....	3-62
Defining Point-to-Point Options for a PPP LPort.....	3-64
Defining Multilink Frame Relay (MLFR) Trunks (B-STDX).....	3-65
About MLFR .....	3-65
ML Member Logical Ports and MLFR Trunk Bundle Logical Ports.....	3-66
MLFR Logical Port Configuration Process.....	3-67
Defining MLFR Trunk Bundle Logical Ports .....	3-67
Defining ML Member Logical Ports.....	3-69
Logical Port Configuration Considerations for CBX 500	
4-Port Channelized DS3/1 and DS3/1/0 Modules .....	3-71
Logical Port Limits for Channelized DS3/1 and DS3/1/0 Modules.....	3-71
FIFO Block Allocation.....	3-71
Example 1: FIFO Block (Over Allocation Limits).....	3-72
Example 2: FIFO Block (Within Allocation Limits).....	3-72
Calculating FIFO Blocks.....	3-72
Using the get lport MIB Command .....	3-72
Determining Time Slot Positions.....	3-73
Using the FIFO Conversion Table.....	3-74

## Chapter 4      **Configuring Trunks**

About Trunks .....	4-1
Trunk Oversubscription Factor .....	4-2
OSPF Trunk Administrative Cost .....	4-3
Configuring Minimum-hop Paths.....	4-3
Link Trunk Protocol .....	4-3
Trunk Delay .....	4-4
Keep-alive Threshold.....	4-4

Static and Dynamic Delay .....	4-4
Trunk Backup .....	4-5
Working with Trunks .....	4-6
Adding a Trunk .....	4-7
Modifying Trunks.....	4-14
Viewing and Configuring PVCs.....	4-16
Configuring Trunk Backup .....	4-16
Using the Automatic Trunk Backup Feature.....	4-16
Switching Over to a Backup Trunk.....	4-17
Activating or Terminating a Backup Trunk Manually .....	4-17

## **Chapter 5 Configuring Multilink Frame Relay (MLFR) UNI/NNI Bundles**

About MLFR UNI/NNI .....	5-1
MLFR Overview .....	5-2
MLFR UNI/NNI Bundle Logical Ports.....	5-2
ML Member Logical Ports .....	5-3
Total Number of MLFR Bundles .....	5-4
MLFR Features for 4-Port Channelized DS3/1 and DS3/1/0 FR/IP and 32-Port Channelized T1/E1 FR/IP Modules .....	5-4
MLFR Features for 6-Port Channelized DS3/1/0 Frame Relay I/O Modules.....	5-6
Differential Delay .....	5-6
Administrative Tasks .....	5-8
Configuring MLFR UNI/NNI Bundle Logical Ports .....	5-8
Defining the Bundle Logical Port.....	5-9
Defining ML Member Logical Ports .....	5-11
Binding and Unbinding ML Members to MLFR Bundle Logical Ports.....	5-14
Configuring MLFR on the 6-Port Channelized DS3/1/0 Module .....	5-18
Defining an MLFR Logical Port.....	5-18
Modifying Member LPorts .....	5-23
Configuring a Logical Port for a Layer2 VPN and Customer .....	5-25
Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint.....	5-26

## **Chapter 6 Configuring Multilink Point-to-Point Protocol Bundles**

About MLPPP .....	6-1
Overview .....	6-1
MLPPP Links .....	6-2
MLPPP Bundles .....	6-2
MLPPP Features.....	6-4
Supported Protocols .....	6-5
Point-to-Point Protocol .....	6-5
Link Control Protocol .....	6-5
IP Control Protocol .....	6-5
Bridging Control Protocol .....	6-6
Fragmentation and Reassembly.....	6-6
Fragmentation Strategy.....	6-6
Administrative Tasks .....	6-7

Defining MLPPP Logical Ports.....	6-8
Setting MLPPP LPort Attributes.....	6-8
Setting Point-to-Point Attributes .....	6-9
Configuring the MLPPP Bundle .....	6-12
Configuring PVCs With an MLPPP Bundle LPort Endpoint .....	6-14

## Chapter 7      **Configuring Permanent Virtual Circuits (PVCs)**

About Permanent Virtual Circuits (PVCs) .....	7-2
Reliable Scalable Circuit.....	7-2
PVC Endpoint Rules .....	7-3
PVC Establishment Rate Control.....	7-4
VC Overload Control and PVC Establishment Rate Control .....	7-4
VC Overload Control .....	7-5
About VC Overload Control.....	7-5
About Overload Severity Levels.....	7-6
Rate Enforcement .....	7-6
Graceful Discard.....	7-7
Rate Enforcement Schemes .....	7-8
About DLCI Numbers.....	7-8
Working with PVCs.....	7-9
Accessing PVCs Using Navis EMS-CBGX.....	7-9
Defining a Point-to-Point Circuit Connection.....	7-11
Administrative Attributes for PVCs .....	7-14
Traffic Type Attributes for PVCs and Redirect PVCs .....	7-18
User Preference Attributes for PVCs and Redirect PVCs .....	7-21
Accounting Attributes for PVCs.....	7-27
Path Attributes for PVCs .....	7-28
Manually-Defining the Circuit Path.....	7-28
Working with Redirect PVC Connections.....	7-30
Accessing Redirect PVCs Using Navis EMS-CBGX .....	7-31
Defining a Redirect PVC Connection .....	7-33
Administrative Attributes for Redirect PVCs.....	7-34
Setting the Redirect PVC Delay Timer .....	7-38
Working with Multicast DLCIs .....	7-39
Multicast DLCI Member Limits.....	7-39
Multicast DLCI Member Limits for B-STDX Modules.....	7-39
Multicast DLCI Member Limits for CBX Modules .....	7-40
Adding a New Multicast DLCI .....	7-42
Managing Circuits.....	7-43
Moving Circuits.....	7-43
Moving Circuit Endpoint from an LPort instance .....	7-44
Moving Circuit Endpoint from a Circuit instance .....	7-46
Using Templates to Define Circuits .....	7-48
Deleting Circuits.....	7-50

## Chapter 8      **Configuring Offnet Circuits**

Supported Modules .....	8-2
About Offnet Circuits (SPVCs) .....	8-2

	Frame Relay Offnet Circuit Scalability .....	8-3
	Using PVC/PVP Termination .....	8-3
	Specifying the Target Select Type .....	8-4
	Defining a Point-to-Point Offnet Circuit Connection .....	8-5
	Selecting an Endpoint From a Switch.....	8-6
	Selecting an Endpoint From a Physical Port .....	8-7
	Selecting the Terminating Endpoint Address .....	8-8
	Configuring Offnet Circuit Parameters .....	8-10
	Administrative Attributes .....	8-10
	Traffic Type Attributes .....	8-14
	User Preference Attributes.....	8-20
	Accounting Attributes.....	8-24
	Path Attributes .....	8-27
	FRF.5 Attributes .....	8-29
	Restarting an OffNet Circuit.....	8-30
<b>Chapter 9</b>	<b>Configuring Ethernet Virtual Circuits (EVCs)</b>	
	Prerequisites.....	9-2
	Adding or Modifying EVCs.....	9-2
	Administrative Attributes .....	9-6
	Traffic Type Attributes.....	9-11
	User Preference Attributes .....	9-17
	Path Attributes.....	9-20
<b>Chapter 10</b>	<b>Configuring Layer2 Virtual Private Networks (VPNs)</b>	
	About Layer2 VPNs.....	10-2
	Configuring a Layer2 VPN.....	10-3
	Creating a Layer2 VPN .....	10-4
	Adding Customers to a Layer2 VPN.....	10-5
	Assigning Logical Ports to a Layer2 VPN .....	10-6
	Using the Layer2 VPN/Customer View Feature .....	10-8
	Configuring a PVC for Layer2 VPN .....	10-9
<b>Chapter 11</b>	<b>Configuring Management Paths</b>	
	Overview .....	11-1
	Using Management PVCs.....	11-2
	Defining Physical Port Attributes.....	11-3
	Defining a Frame Relay UNI Logical Port .....	11-4
	Defining a Standard or Redirect MPVC Connection .....	11-5
	Using Management DLCIs .....	11-7
	Defining the Management Path .....	11-9
<b>Chapter 12</b>	<b>Configuring Fault-tolerant PVCs</b>	
	Configuration Procedure .....	12-1
	Creating a Primary Port .....	12-2
	Creating a Backup Port .....	12-4
	Activating a Backup Binding Port.....	12-4

---

	Returning the Primary Logical Port to Service.....	12-6
<b>Chapter 13</b>	<b>Configuring Resilient LMI</b>	
	Configuration Overview .....	13-1
	About RLMIs .....	13-2
	Resilient LMI Terms .....	13-2
	Configuration Guidelines .....	13-3
	Resilient LMI Configuration Procedure.....	13-4
	Creating Service Names.....	13-5
	Configuring the RLMI Switchover Mode.....	13-8
<b>Chapter 14</b>	<b>Configuring Switched Virtual Circuit (SVC) Parameters</b>	
	Configuration Overview .....	14-2
	About Address Formats.....	14-2
	About Route Determination .....	14-3
	About Network ID Addressing.....	14-5
	I/O Modules for SVC Frame Relay Service.....	14-6
	Administrative Tasks .....	14-6
	Managing SVCs .....	14-7
	Configuring Node Prefixes.....	14-7
	Configuring Port Prefixes.....	14-11
	Defining Default Routes for Network-to-Network Connections .....	14-15
	Configuring Port Addresses .....	14-16
	Defining Network IDs.....	14-20
<b>Chapter 15</b>	<b>Closed User Groups</b>	
	Configuration Overview .....	15-1
	About Closed User Groups (CUGs).....	15-1
	About CUG Member Rules.....	15-2
	Defining Incoming and Outgoing Access.....	15-2
	Developing Closed User Groups.....	15-3
	Using CUGs in the Network.....	15-4
	Configured Addresses and CUG Membership .....	15-5
	Administrative Tasks .....	15-6
	Defining CUG Members .....	15-6
	Defining a CUG.....	15-8
<b>Chapter 16</b>	<b>Port Security Screening</b>	
	Configuration Overview .....	16-1
	About Port Security Screening.....	16-2
	Implementing Port Security Screening.....	16-2
	Default Screens .....	16-2
	Security Screens.....	16-4
	Port Security Screening Sample Configuration .....	16-5
	Administrative Tasks .....	16-7
	Creating Port Security Screen Definitions .....	16-8
	Assigning Security Screens to Logical Ports .....	16-10

**Appendix A    Reliable Scalable Circuit**

Circuit Add Errors..... A-2  
Circuit Modify Errors ..... A-4  
Circuit Delete Errors ..... A-5

**Appendix B    OSPF Name Aggregation**

About OSPF Name Aggregation ..... B-1  
    OSPF Names ..... B-1  
    Name Limitations ..... B-2  
Using OSPF Name Aggregation..... B-2  
    Sample Network Scenario ..... B-2  
        Port-level Name Aggregation ..... B-3  
        Switch-level Name Aggregation..... B-4  
Network Hierarchical Addressing Plans ..... B-4  
Monitoring Network OSPF Name Activity ..... B-6  
    Viewing OSPF Names at the Network Level..... B-6  
    Viewing OSPF Names at the Switch Level..... B-7  
    Viewing OSPF Names at the Card Level..... B-9

**Appendix C    Priority Routing**

About Priority Routing ..... C-1  
    Network Convergence Time ..... C-2  
    Specifying Routing Priorities ..... C-2  
    Using Restricted Priority Routing ..... C-3  
Routing Priority Rules ..... C-4  
    Circuit Provisioning ..... C-4  
    Trunk-failure Recovery ..... C-4  
    Balance Rerouting ..... C-5  
    Interoperability with Previous Releases ..... C-5  
Priority Routing and Path Cost ..... C-5  
    Priority Routing and Path Cost Example ..... C-6  
    Restricted Priority Routing and Path Cost Example ..... C-6

**Appendix D    Customer Names**

Adding Customer Names ..... D-1  
Associating a Logical Port with a Customer Name ..... D-3  
Using the Layer2 Customer/VPN View Feature ..... D-4

**Abbreviations and Acronyms**

Abbreviations ..... Acronyms-1  
Acronyms ..... Acronyms-3

**Index**

# List of Figures

Figure 2-1.	Congestion Control Tab for 32-Port Channelized T1/E1 Module	2-14
Figure 2-2.	Add LPort Using a Template	2-26
Figure 2-3.	Deleting a Circuit Based on LPort	2-29
Figure 2-4.	Deleting a Trunk Based on LPort	2-30
Figure 2-5.	Deleting a Multicast DLCIs Based on LPort	2-31
Figure 2-6.	Deleting a Management DLCIs Based on LPort	2-32
Figure 2-7.	Deleting a LPort	2-33
Figure 3-1.	Logical Ports in the Cards Node	3-2
Figure 3-2.	Logical Ports in the LPorts Node	3-3
Figure 3-3.	Managing Logical Ports in the Switch Tab	3-4
Figure 3-4.	Adding a Logical Port	3-5
Figure 3-5.	Add Logical Port Dialog Box	3-6
Figure 3-6.	Modifying a Logical Port	3-7
Figure 3-7.	Modify Logical Port Dialog Box	3-9
Figure 3-8.	Add/Modify Logical Port: General Tab	3-12
Figure 3-9.	Add/Modify Logical Port: Administrative Tab	3-15
Figure 3-10.	Channel Allocation Fields for T1/E1 Logical Ports	3-19
Figure 3-11.	Adding Logical Ports on Channelized DS3/1/0 FR Modules	3-20
Figure 3-12.	Channel Allocation Fields for DS3 Logical Ports	3-21
Figure 3-13.	Add/Modify Logical Port: FRF.19 Tab	3-21
Figure 3-14.	Add/Modify Logical Port: Congestion Control Tab	3-24
Figure 3-15.	Add/Modify Logical Port: Priority Frame Tab	3-29
Figure 3-16.	Add/Modify Logical Port: QoS Tab	3-31
Figure 3-17.	Add/Modify Logical Port: MLFR LPort Bind Tab	3-33
Figure 3-18.	Add/Modify Logical Port: Link Management Tab (UNI NNI)	3-34
Figure 3-19.	Add/Modify Logical Port: MLFR Configuration Tab	3-38
Figure 3-20.	Add/Modify Logical Port: Trap Control Tab	3-40
Figure 3-21.	Configuring LPort SVC Parameters in the Switch Tab	3-42
Figure 3-22.	Configure SVC Dialog Box: General Tab	3-43
Figure 3-23.	SVC TD Limits Dialog Box	3-47
Figure 3-24.	Configure SVC Dialog Box: Signaling Tab	3-49
Figure 3-25.	SVC Signaling Tuning Dialog Box	3-50
Figure 3-26.	Configure SVC Dialog Box: Address Tab	3-52
Figure 3-27.	Configure SVC Dialog Box: Connection ID Tab	3-56
Figure 3-28.	Configure SVC Dialog Box: CUG Tab	3-56
Figure 3-29.	Configuring PPP Authentications	3-63
Figure 3-30.	Add PPP Authentication Domain Dialog Box	3-63
Figure 3-31.	Add Authentication Domain Dialog Box	3-64
Figure 3-32.	Add/Modify Logical Port: Point-to-Point Tab	3-64
Figure 3-33.	Multilink Frame Relay Unit (MFRU)	3-66
Figure 3-34.	Adding a Trunk Bundle LPort	3-67
Figure 3-35.	Add/Modify Logical Port Dialog Box: Member Bind Tab	3-68
Figure 3-36.	Adding a ML Member Logical Port on a Channelized Card	3-69
Figure 3-37.	Add/Modify Logical Port Dialog Box: MLFR LPort Bind Tab	3-70



---

Figure 3-38.	MLFR Logical Port Selection Dialog Box .....	3-70
Figure 4-1.	Trunk Delay – OSPF Metric and Keep-alive Messaging .....	4-4
Figure 4-2.	Adding a Trunk.....	4-7
Figure 4-3.	Add Trunk Dialog Box: Administrative Tab.....	4-8
Figure 4-4.	Select Trunk Endpoints Dialog Box .....	4-8
Figure 4-5.	Add Trunk Dialog Box: Primary Options Tab .....	4-13
Figure 4-6.	Modifying a Trunk.....	4-15
Figure 4-7.	Modify Trunk Dialog Box .....	4-15
Figure 4-8.	Modifying PVCs.....	4-16
Figure 4-9.	Backup Options Tab and Select Primary Trunk Dialog Box .....	4-17
Figure 4-10.	Activating or Terminating a Backup Trunk.....	4-18
Figure 5-1.	Multilink Frame Relay Unit (MFRU).....	5-2
Figure 5-2.	Navigation Panel: Add LPorts .....	5-9
Figure 5-3.	Add Logical Port Dialog Box .....	5-9
Figure 5-4.	Adding a ML Member LPort on a Channelized DS3 Module.....	5-12
Figure 5-5.	Navigation Panel: Add LPorts .....	5-12
Figure 5-6.	Add Logical Port Dialog Box .....	5-13
Figure 5-7.	Navigation Panel: Modify Logical Port.....	5-15
Figure 5-8.	Modify Logical Port Dialog Box.....	5-16
Figure 5-9.	MLFR Logical Port Selection Dialog Box .....	5-16
Figure 5-10.	Modifying an MLFR Bundle Logical Port .....	5-17
Figure 5-11.	Modify Logical Port Dialog Box: Member Bind Tab .....	5-17
Figure 5-12.	Navigation Panel: Add LPorts .....	5-19
Figure 5-13.	Add Logical Port Dialog Box .....	5-19
Figure 5-14.	Add/Modify Logical Port: MLFR Configuration Tab.....	5-20
Figure 5-15.	Modifying a Member LPort.....	5-24
Figure 5-16.	Modify Logical LPort Dialog Box .....	5-24
Figure 5-17.	Assigning a Logical Port to an L2 VPN or Customer .....	5-25
Figure 5-18.	Choose VPN / Policy Dialog Box .....	5-25
Figure 5-19.	Add/Modify PVC: User Preference Tab.....	5-26
Figure 6-1.	Network Diagram for MLPPP Applications.....	6-2
Figure 6-2.	Data Flow Diagram.....	6-4
Figure 6-3.	Add Logical Port Dialog Box .....	6-8
Figure 6-4.	Add Logical Port: Point-to-Point Tab.....	6-10
Figure 6-5.	Add Logical Port: Member Bind Tab.....	6-13
Figure 6-6.	Add PVC Dialog Box .....	6-14
Figure 6-7.	Select Endpoints Dialog Box.....	6-15
Figure 6-8.	Select Endpoints MLPPP Bundle and FR UNI DTE.....	6-16
Figure 6-9.	Select Endpoints MLPPP Bundle and FR NNI .....	6-17
Figure 6-10.	Select Endpoints MLPPP Bundle and Direct ATM UNI DTE.....	6-18
Figure 6-11.	Add PVC Dialog Box .....	6-19
Figure 7-1.	Navigation Panel: PVCs Node.....	7-9
Figure 7-2.	Navigation Panel: Circuits Node .....	7-10
Figure 7-3.	Add PVC Dialog Box .....	7-11
Figure 7-4.	Select Endpoints Dialog Box.....	7-12
Figure 7-5.	Add PVC Dialog Box: Administrative Tab.....	7-14
Figure 7-6.	Add PVC Dialog Box: Traffic Type Tab .....	7-18
Figure 7-7.	Add PVC Dialog Box: User Preference Tab .....	7-21



Figure 7-8.	Add PVC Dialog Box: Accounting Tab .....	7-27
Figure 7-9.	Add PVC Dialog Box: Path Tab.....	7-28
Figure 7-10.	Add/Modify PVC Dialog Box: Path Tab.....	7-29
Figure 7-11.	Define Path Dialog Box.....	7-29
Figure 7-12.	Right-Clicking on the Redirect PVCs Node.....	7-31
Figure 7-13.	Navigation Panel: Redirect PVCs.....	7-32
Figure 7-14.	Select Endpoints Dialog Box.....	7-33
Figure 7-15.	Add Redirect PVC Dialog Box: Administrative Tab .....	7-34
Figure 7-16.	Adding a Multicast DLCI.....	7-42
Figure 7-17.	Add Multicast DLCI Dialog Box .....	7-42
Figure 7-18.	Moving a Circuit Endpoint from an LPort instance .....	7-44
Figure 7-19.	Select Endpoints Dialog Box.....	7-45
Figure 7-20.	Move Circuit Endpoint Dialog Box.....	7-46
Figure 7-21.	Moving a Circuit Endpoint .....	7-47
Figure 7-22.	Select Endpoints Dialog Box.....	7-47
Figure 7-23.	Move Circuit Endpoint Dialog Box.....	7-48
Figure 7-24.	Adding a PVC Based on a Template .....	7-49
Figure 7-25.	Choose Template Dialog Box.....	7-49
Figure 8-1.	Navigation Panel: Offnet Circuits node.....	8-6
Figure 8-2.	Offnet Endpoints Selection dialog box.....	8-8
Figure 8-3.	Add OffNet Circuit: Administrative Tab.....	8-10
Figure 8-4.	Add OffNet Circuit: Traffic Type Tab .....	8-14
Figure 8-5.	Add OffNet Circuit: User Preference Tab .....	8-20
Figure 8-6.	Add OffNet Circuit: Accounting Tab .....	8-24
Figure 8-7.	Add OffNet Circuit: Path Tab.....	8-27
Figure 8-8.	Define Path dialog box .....	8-27
Figure 8-9.	Add OffNet Circuit: FRF.5 Tab.....	8-29
Figure 9-1.	Add PVC Dialog Box .....	9-3
Figure 9-2.	Select Endpoints Dialog Box.....	9-4
Figure 9-3.	Select Endpoints Dialog Box (for Redirect PVC) .....	9-5
Figure 9-4.	Offnet Endpoint Selection Dialog Box.....	9-5
Figure 9-5.	Add PVC: Administrative Tab .....	9-6
Figure 9-6.	Add PVC: Traffic Type Tab.....	9-11
Figure 9-7.	Add PVC: User Preference Tab.....	9-17
Figure 9-8.	Add PVC: Path Tab .....	9-20
Figure 10-1.	Layer2 VPN Restrictive Mode Example .....	10-2
Figure 10-2.	Layer2 VPN Inclusive Mode Example.....	10-3
Figure 10-3.	Adding a VPN.....	10-4
Figure 10-4.	Add VPN Dialog Box .....	10-5
Figure 10-5.	Adding a VNN Customer .....	10-5
Figure 10-6.	Add Customer Dialog Box .....	10-6
Figure 10-7.	Assigning a Logical Port to a Layer 2 VPN / Customer Name ....	10-7
Figure 10-8.	Choose VPN / Policy Dialog Box .....	10-7
Figure 10-9.	Selecting the L2 VPN/VNN Customer for a Network .....	10-8
Figure 10-10.	Select Layer2 Customer/VPN View Dialog Box .....	10-8
Figure 10-11.	Assigning a Logical Port to a Layer 2 VPN / Customer Name ....	10-9
Figure 10-12.	Choose VPN / Policy Dialog Box .....	10-10
Figure 11-1.	Modifying a Physical Port .....	11-3

Figure 11-2.	Adding Logical Ports .....	11-4
Figure 11-3.	Right-Clicking on the PVCs Node .....	11-5
Figure 11-4.	Add PVC Dialog Box .....	11-5
Figure 11-5.	Select Endpoints Dialog Box .....	11-6
Figure 11-6.	Adding a Management DLCI .....	11-8
Figure 11-7.	Add Management DLCI Dialog Box.....	11-8
Figure 11-8.	Adding a Management Path.....	11-9
Figure 11-9.	Add NMS Path Dialog Box .....	11-9
Figure 12-1.	Adding a Service Name .....	12-3
Figure 12-2.	Add RNNI/UNI Service Name Dialog Box .....	12-3
Figure 12-3.	Modifying a Service Name .....	12-4
Figure 12-4.	Modify Service Name Dialog Box .....	12-5
Figure 12-5.	Select Backup LPort Dialog Box.....	12-5
Figure 13-1.	Adding a Service Name .....	13-5
Figure 13-2.	Add RLMI Service Name Dialog Box .....	13-6
Figure 13-3.	Select Backup LPort Dialog Box.....	13-7
Figure 13-4.	Modifying a Service Name .....	13-8
Figure 13-5.	Modify Service Name Dialog Box .....	13-8
Figure 14-1.	Adding and Modifying SVCs by Logical Port or Switch.....	14-7
Figure 14-2.	Adding a Node Prefix .....	14-8
Figure 14-3.	Add SVC Node Prefix Dialog Box.....	14-8
Figure 14-4.	Adding a Port Prefix .....	14-12
Figure 14-5.	Add SVC Port Prefix Dialog Box.....	14-12
Figure 14-6.	Adding a Port Prefix .....	14-15
Figure 14-7.	Add SVC Port Prefix Dialog Box.....	14-16
Figure 14-8.	Adding a Port Address.....	14-17
Figure 14-9.	Add SVC Port Address Dialog Box .....	14-17
Figure 14-10.	Adding a Network ID .....	14-20
Figure 14-11.	Add Network ID Dialog Box.....	14-20
Figure 15-1.	Implementing CUGs .....	15-4
Figure 15-2.	Defining a CUG Member .....	15-7
Figure 15-3.	Add CUG Member Dialog Box.....	15-7
Figure 15-4.	Defining a CUG .....	15-9
Figure 15-5.	Add CUG Dialog Box .....	15-9
Figure 16-1.	Adding a Security Screen .....	16-8
Figure 16-2.	Add Security Screen Dialog Box.....	16-8
Figure 16-3.	Assigning a Security Screen to a Logical Port .....	16-10
Figure 16-4.	Activate and Assign Security Screen: Default Screen Tab .....	16-11
Figure 16-5.	Activate and Assign Security Screen: Assigned Screens Tab ....	16-12
Figure B-1.	Sample Network Addressing Scenario .....	B-2
Figure B-3.	Sample Network Showing Port and Network Prefixes.....	B-5
Figure D-1.	Adding a VNN Customer .....	D-2
Figure D-2.	Add Customer Dialog Box .....	D-2
Figure 4-3.	Assigning a Logical Port to a Layer 2 VPN / Customer Name .....	D-3
Figure 4-4.	Choose VPN / Policy Dialog Box .....	D-3
Figure D-5.	Select Layer2 Customer VPN View Dialog Box .....	D-4

## List of Tables

Table 2-1.	Frame Relay Logical Port Types .....	2-2
Table 2-2.	Congested and Ingress Switch Behavior .....	2-6
Table 2-3.	Congestion Parameters .....	2-7
Table 2-4.	Maximum Mono-Class and Multi-Class (VFR-NRT) Thresholds ..	2-8
Table 2-5.	Default Congestion Level Thresholds per Card Type .....	2-10
Table 2-6.	4-Port Channelized T1 Default Thresholds .....	2-11
Table 2-7.	4-Port Channelized E1 Default Thresholds .....	2-12
Table 2-8.	32-Port Channelized T1/E1 FR/IP Maximum Thresholds .....	2-15
Table 2-9.	32-Port Channelized T1/E1 FR/IP Default Thresholds .....	2-16
Table 2-10.	WRED Congestion Threshold Values .....	2-18
Table 2-11.	WRED Congestion Threshold Values .....	2-19
Table 2-12.	Default Mono-Class and Multi-Class Thresholds (TAQL) .....	2-20
Table 2-13.	Frame TS0 Thresholds.....	2-21
Table 2-14.	QoS Class of Service Descriptions .....	2-24
Table 2-15.	T1/E1 I/O Module QoS Class of Service Guidelines .....	2-24
Table 2-16.	Default QoS Values for Frame Relay Logical Ports .....	2-25
Table 2-17.	Non-Disruptive Logical Port and Trunk Attributes.....	2-27
Table 3-1.	Frame Relay Logical Port Configurations.....	3-6
Table 3-2.	Service Type and Logical Port Type (UNI-DCE).....	3-10
Table 3-3.	Add/Modify Logical Port: General Tab .....	3-13
Table 3-4.	Add/Modify Logical Port: Administrative Tab .....	3-16
Table 3-5.	Add/Modify Logical Port: FRF.19 Tab .....	3-22
Table 3-6.	Add/Modify Logical Port: Congestion Control Tab.....	3-25
Table 3-7.	Add/Modify Logical Port: Priority Frame Tab.....	3-30
Table 3-8.	Add/Modify Logical Port: QoS Tab .....	3-32
Table 3-9.	Add/Modify Logical Port: Link Management Tab.....	3-34
Table 3-10.	Add/Modify Logical Port: MLFR Configuration Tab.....	3-38
Table 3-11.	Add/Modify Logical Port: Trap Control Tab .....	3-41
Table 3-12.	Configure SVC Dialog Box: General Tab.....	3-44
Table 3-13.	Configure SVC Dialog Box: General Tab Priorities Settings .....	3-45
Table 3-14.	TD Limits Dialog Box .....	3-48
Table 3-15.	Configure SVC Dialog Box: Signaling Tab .....	3-49
Table 3-16.	SVC Signaling Tuning Dialog Box .....	3-50
Table 3-17.	Configure SVC Dialog Box: Address Tab .....	3-53
Table 3-18.	Configure SVC Dialog Box: Connection ID Tab.....	3-56
Table 3-19.	Configure SVC Dialog Box: CUG Tab .....	3-57
Table 3-20.	DLCI Number Guidelines.....	3-58
Table 3-21.	Add Logical Port Type (OPTimum PVC Trunk) .....	3-59
Table 3-22.	Add Logical Port Type (Other).....	3-61
Table 3-23.	Add PPP Authentication Domain Dialog Box.....	3-63
Table 3-24.	Add/Modify Logical Port: Point-to-Point Tab .....	3-65
Table 3-25.	FIFO Blocks for Fractional T1s.....	3-71
Table 3-26.	FIFO Conversion Table .....	3-74
Table 4-1.	Add Trunk Dialog Box: Administrative Tab.....	4-9

Table 4-2.	Add Trunk Dialog Box: Primary Options Tab .....	4-13
Table 5-1.	Total number of MLFR bundles .....	5-4
Table 5-2.	Add Logical Port Type Dialog Box.....	5-10
Table 5-3.	ML Member and MLFR Bundle LPort Bindings .....	5-13
Table 5-4.	Add Logical Port Type Dialog Box Fields .....	5-20
Table 5-5.	MLFR Configuration Tab.....	5-21
Table 5-6.	User Preference Tab: Error Recovery Settings.....	5-27
Table 6-1.	Add/Modify Logical Port: Point-to-Point Tab .....	6-10
Table 7-1.	PVC Endpoint Rules.....	7-3
Table 7-2.	Rate Enforcement and Discard Policy .....	7-7
Table 7-3.	Rate Enforcement Schemes .....	7-8
Table 7-4.	DLCI Number Guidelines.....	7-8
Table 7-5.	Logical Port Endpoints for Circuits.....	7-12
Table 7-6.	Add PVC Dialog Box: Administrative Tab.....	7-14
Table 7-7.	Add PVC Dialog Box: Traffic Type Tab .....	7-19
Table 7-8.	Add PVC Dialog Box: User Preference Tab .....	7-21
Table 7-9.	Add Redirect PVC Dialog Box: Administrative Tab .....	7-35
Table 7-10.	Multicast DLCI Member Limits (B-STDx Modules).....	7-40
Table 7-11.	Forwarding Engine Support on CBX IOM2 Modules.....	7-40
Table 7-12.	Multicast DLCI Member Limits (CBX Modules).....	7-41
Table 8-1.	Offnet Circuit Frame Relay Module Support .....	8-2
Table 8-2.	OffNet Circuit Target Select Type .....	8-4
Table 8-3.	Address Formats and Address Components .....	8-9
Table 8-4.	Add OffNet Circuits: Administrative Tab .....	8-11
Table 8-5.	Allowable QoS Classes.....	8-15
Table 8-6.	Add OffNet Circuit: Traffic Type Tab .....	8-16
Table 8-7.	Add OffNet Circuit: User Preference Tab .....	8-21
Table 8-8.	Add OffNet Circuit: Accounting Tab .....	8-24
Table 8-9.	Add OffNet Circuit: FRF.5 Tab.....	8-29
Table 9-1.	Add PVC: Administrative Tab .....	9-7
Table 9-2.	Add PVC: Traffic Type Tab .....	9-12
Table 9-3.	Add PVC: User Preference Tab.....	9-18
Table 13-1.	Resilient LMI Terms.....	13-2
Table 14-1.	E.164 Node Prefix, Port Prefix, and Port Address Example .....	14-4
Table 14-2.	Routing by Called Party Address Example .....	14-4
Table 14-3.	Frame Relay SVC Modules .....	14-6
Table 14-4.	Add SVC Node Prefix Dialog Box.....	14-9
Table 14-5.	Add SVC Port Prefix Dialog Box.....	14-12
Table 14-6.	Add SVC Port Address Dialog Box .....	14-17
Table 14-7.	Add Network ID Dialog Box.....	14-21
Table 15-1.	ICB/OCB Attributes and Member Rules.....	15-4
Table 15-2.	Configured Address and Corresponding CUG Membership.....	15-5
Table 15-3.	Add SVC CUG Member Dialog Box .....	15-7
Table 16-1.	Default Screens .....	16-3
Table 16-2.	Security Screens.....	16-5
Table 16-3.	Add Security Screen Dialog Box.....	16-9
Table 16-4.	Activate and Assign Security Screen Dialog Box .....	16-11
Table A-1.	Errors Encountered During Circuit Add Procedure.....	A-3

Table A-2.	Errors Encountered During Circuit Modify Procedure .....	A-4
Table A-3.	Errors Encountered During Circuit Delete Procedure .....	A-6
Table B-2.	Address Routing Requirements for Sample Network .....	B-3



# About This Guide

The *Frame Relay Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000* is a task-oriented guide that describes, step-by-step, the process for using Navis EMS-CBGX to configure Frame Relay services in a Lucent switch network. Specifically, this guide describes how to configure logical ports, trunks, permanent virtual circuits (PVCs), soft permanent virtual circuits (SPVCs) or Offnet Circuits, and switched virtual circuits (SVCs) to support Frame Relay services on either a CBX 3500<sup>®</sup>, CBX 500<sup>®</sup>, or B-STDX 9000<sup>®</sup> switch. This guide also explains how to configure a variety of features that enhance the Frame Relay service platform, including virtual private networks, closed user groups, and port security screening.

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

- Navis EMS-CBGX, Release 10.00.01.00 or greater
- CBX 3500 Multiservice Edge switch software Release 10.00.01.00 or greater
- CBX 500 Multiservice WAN switch software Release 10.00.01.00 or greater
- Prior supported releases of B-STDX 9000 Multiservice WAN switch software as noted in the Interoperability section of the Navis EMS-CBGX Software Release Notice (SRN).



---

**Note** – This document describes Navis EMS-CBGX IP Services functions in several chapters. References to Navis EMS-CBGX IP Services are valid only for the following switch software releases: B-STDX 06.05.02.xx and CBX 03.05.02.xx.

---

## What You Need to Know

As a reader of this guide, you should be familiar with UNIX and HP OpenView. You should also know about relational databases to properly maintain Sybase, which is used by Navis EMS-CBGX.

This guide assumes you have already installed the Lucent switch hardware, NMS, and switch software. See the “[Related Documents](#)” section 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.

Before you begin to configure Frame Relay services, see the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* to configure processors, I/O cards, and physical ports.



---

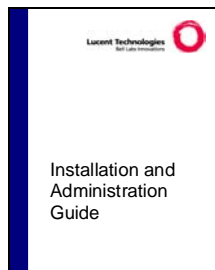
## Reading Path

This section describes all of the documents that support the Navis<sup>®</sup> EMS-CBGX and switch software.

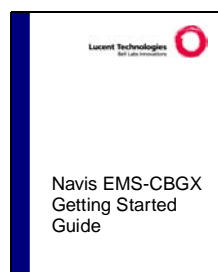
Read the following documents to install and operate Navis EMS-CBGX Release 10.00.01.00 or greater and the associated switch software. Be sure to review the accompanying SRNs for any changes not included in these guides.



These guides describe how to install and set up the switch hardware, replace hardware modules, and interpret LED indicators.

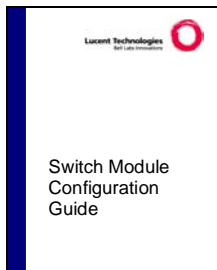


This guide describes prerequisite tasks, hardware and software requirements, and instructions for installing and upgrading Solaris and Navis EMS-CBGX on the NMS.

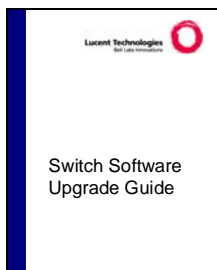


This guide describes how to start the Navis EMS-CBGX client on Windows and Solaris. It also provides a description of the Navis EMS-CBGX window components, how to access network and map configuration options, how to configure and manage Lucent switches and instructions for customizing Navis EMS-CBGX.

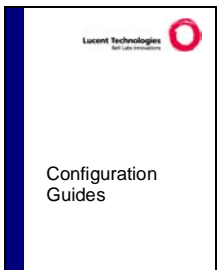




This guide describes the processor and input/output modules on each switch platform, and how to configure physical ports, timing, and other attributes through Navis EMS-CBGX.

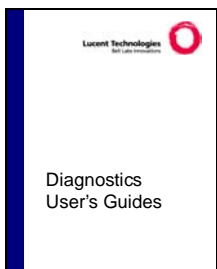


This guide describes procedures for upgrading a Lucent switch to the current release.



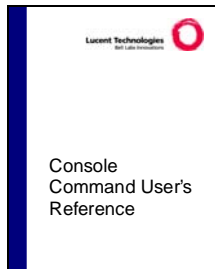
The following guides describe how to configure wide area network (WAN) services on the supported switch platforms:

- *Frame Relay Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000*
- *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*
- *IP Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000*



This guide describes how to monitor and diagnose problems in your Navis EMS-CBGX switch network.





This guide contains reference lists and describes the switch console commands.

## 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 to understand before you configure Frame Relay logical ports.
Chapter 3	Configuring Frame Relay logical ports on B-STDX and CBX switches.
Chapter 4	Configuring Frame Relay trunks to enable switches to pass data and exchange internal control messages.
Chapter 5	Configuring Multilink Frame Relay (MLFR) user-to-network interface and network-to-network interface (UNI/NNI) bundles on the 4-Port Channelized DS3/1 and DS3/1/0 Frame Relay/Internet Protocol (FR/IP) modules, the 6-Port Channelized DS3/1/0 Frame Relay module, and the 32-Port Channelized T1/E1 FR/IP module.
Chapter 6	Configuring Multilink Point-to-Point Protocol (MLPPP). This chapter describes the configuration of MLPPP bundles on a 32-Port Channelized T1/E1 Frame Relay module.
Chapter 7	Configuring Frame Relay PVCs, including Point-to-Point Protocol. This chapter also explains how to configure redirect PVCs and multicast DLCI, and how to define PVC between Frame Relay and Gigabit Ethernet modules.
Chapter 8	Configuring Offnet Circuits. This chapter explains how to configure a Point-to-Point Offnet circuit and also how to restart an Offnet circuit.
Chapter 9	Adding or modifying Ethernet Virtual Circuit between Frame Relay and Gigabit Ethernet modules.
Chapter 10	Configuring your Frame Relay services to provide Layer2 VPNs.
Chapter 11	Configuring management PVC and management DLCI connection paths between the NMS or IP host that you use to access the switch network.
Chapter 12	Configuring fault tolerant (Resilient UNI/NNI) PVC services to provide backup services should a logical port endpoint fail.
Chapter 13	Configuring Resilient Link Management Interface (RLMI) services to provide preferred and backup logical ports. If the primary port fails, an automatic switchover to the backup port occurs.
Chapter 14	Configuring Frame Relay SVCs.
Chapter 15	Closed User Groups (CUGs) that enable you to divide all network users into logically linked groups of users.

Read	To Learn About
Chapter 16	Using Port Security Screening to allow/disallow incoming/outgoing calls.
Appendix A	Reliable Scalable Circuit error messages and corrective actions.
Appendix B	Using OSPF name aggregation to minimize memory consumption when you provision addresses for SVC connections across network switches.
Appendix C	Explains the use of circuit priority routing for PVCs and SVCs.
Appendix D	Using the Customer Names feature to assign logical ports to a specific customer. You can then use the customer name as a filter when viewing logical ports in a network.

## What's New in This Guide

This guide describes the following new product features in Navis EMS-CBGX Release 10.00.01.00 and includes the following changes and enhancements:

<b>Feature or Enhancement</b>	<b>Description</b>
<b>New Features in This Release</b>	
Support for Multilink Point-to-Point Protocol	Navis EMS-CBGX supports 32-Port Channelized T1/E1 Frame Relay module.
Support for group-wise resource partitioning	Navis EMS-CBGX supports group-wise resource partitioning for specific modules.
Support for 2-Port ULC Gigabit Ethernet module	Navis EMS-CBGX supports 2-Port ULC Gigabit Ethernet module on CBX 3500. It also supports configuration of Ethernet Virtual Circuits (EVCs) and Virtual LAN (VLAN).
Small Packet Size support for 32-Port Channelized T1/E1 module	Navis EMS-CBGX provides the Frame Threshold values to define the Small Packet Size for 32-Port Channelized T1/E1 module on CBX 500 and CBX 3500. The Frame Threshold values provide the fixed memory size and number of frames that are handled by the device.
Support for Policy Routing	Navis EMS-CBGX supports Policy Routing for CBX 500 and CBX 3500. Policy Routing enables you to associate policy constraint to a circuit.

---

## Conventions

This guide uses the following conventions, when applicable:

Convention	Indicates	Example
Courier Regular	System output, filenames, and command names.	Please wait...
< <i>Courier Bold Italics</i> >	Variable text input; user supplies a value.	Enter <cdrompath>/docs/ atmcfg.pdf to display...
< <i>Courier Italics</i> >	Variable text output.	<cdrompath>/docs/ atmcfg.pdf
<b>Courier Bold</b>	User input.	> <b>show ospf names</b>
Menu ⇒ Option	A selection from a menu.	Actions ⇒ Monitor
<i>Italics</i>	Book titles, new terms, and emphasized text.	<i>Frame Relay Services Configuration Guide</i>
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

- *CBX 3500 Multiservice Edge Switch Hardware Installation Guide* (Product Code: 80253)
- *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)
- *Navis EMS-CBGX Release 10.00.01.00 Getting Started Guide* (Product Code: 86019)
- *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* (Product Code: 80263)
- *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* (Product Code: 80260)
- *IP Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000* (Product Code: 80264)
- *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* (Product Code: 80262)
- *Console Command User's Reference for CBX 3500, CBX 500, GX 550, and B-STDX 9000* (Product Code: 86021)
- *Switch Software Upgrade Guide for CBX 3500, CBX 500, and GX 550* (Product code 80265)
- *Navis EMS-CBGX Release 10.00.01.00 Installation and Administration Guide* (Product Code: 86018)
- *NavisXtend Statistics Server Release 10.00.01.00 User's Guide* (Product Code: 86017)
- *NavisXtend Accounting Server Release 10.00.01.00 Administrator's Guide* (Product Code: 86024)
- *NavisXtend Provisioning Server Release 10.00.01.00 User's Guide* (Product Code: 86013)
- *NavisXtend Provisioning Server Release 10.00.01.00 Object Attribute Definitions User's Reference* (Product Code: 86014)



- *NavisXtend Provisioning Server Release 10.00.01.00 Command Line Interface User's Reference* (Product Code: 86015)
- *NavisXtend Provisioning Server Release 10.00.01.00 Error Codes User's Reference* (Product Code: 86016)
- *NavisXtend Provisioning Server Release 10.00.01.00 C++ API User's Reference* (Product Code: 86027)
- *NavisXtend Fault Server Release 10.00.01.00 User's Guide* (Product Code: 86025)
- *NavisXtend Database Standby Server Release 10.00.01.00 User's Guide* (Product Code: 86026)
- *NavisXtend Provisioning Server Legacy C API Reference* (Product Code: 80163)
- *Navis EMS-CBGX TMF 814 Adapter Implementation Reference* (Product Code: 86022)
- *Navis EMS-CBGX TMF 814 Adapter Installation and Administration Guide* (Product Code: 86023)

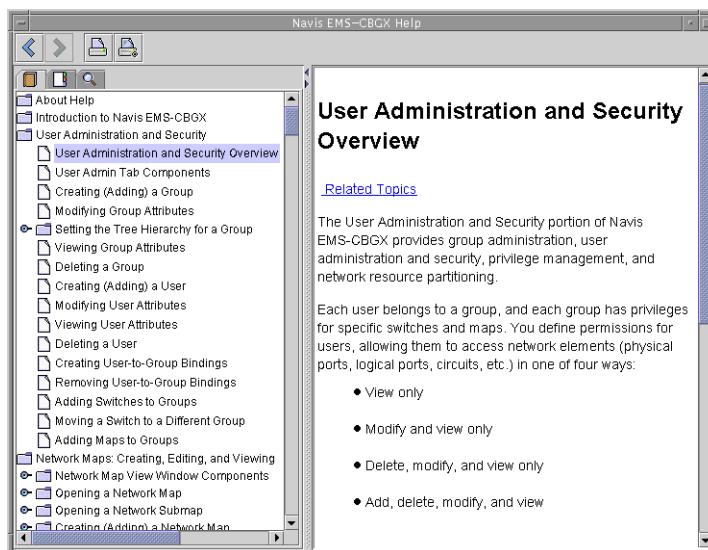
All manuals for the Data Networking Group and the *Master Glossary* are available on the CBX and GX Release 10.00.01.00 Customer Documentation CD-ROM (Product Code: 80267 Rev 000).

## Third Party

- *Solaris 9 Advanced Installation Guide*
- *Solaris 9 (SPARC Platform Edition) Release Notes*
- *Solaris 9 Sun Hardware Platform Guide*
- *Installation Guide Sybase Adaptive Server™ Enterprise on Sun Solaris*

## Using the Navis EMS-CBGX Online Help

Navis EMS-CBGX Online Help provides comprehensive procedures and field descriptions designed to support you in using the Navis EMS-CBGX interface.



You can open the help system in two ways:

- **Help buttons in dialog boxes** — Information about a particular dialog box can be accessed by choosing the Help button in that dialog box.
- **Help menus** — The help system can be opened by selecting Help Topics from the Help menu in the Navis EMS-CBGX window or by selecting Console from the Help menu in the Console window.

When help is open, the following methods of navigation are available:

- **Table of Contents tab** — Displays the table of contents in the left pane. Click on a topic name to display the topic's contents in the right pane. If a topic in the table of contents has subtopics, an expand symbol is displayed to the left of the topic. To list the subtopics, click on the expand symbol.
- **Index tab** — Displays the index entries in the left pane. Click on an index entry to display the referenced contents in the right pane.
- **Search tab** — Displays the Find field and search results. To search for a specific word or words within the help, enter the words in the Find field and then press the Enter key. The files that contain the words are listed below the Find field. Click on the file name to display the file in the right pane. The words in the file that match the search will be highlighted in blue.
- **Back and Forward buttons** — Displays information that was previously in the right pane. Back and forward are relative to the initial sequence in which pieces of information were displayed.

## Ordering Printed Manuals Online

You can order Data Networking Group 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](mailto:cspubs@lucent.com).

## 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>



# Overview

This chapter gives an overview of the information described in this guide.

Some chapters provide information about Frame Relay network basics such as logical ports, trunks, and PVCs; other chapters explain how to configure optional features such as Layer2 virtual private networks (VPNs) and closed user groups (CUGs).

This chapter contains the following sections:

- “Logical Ports” on page 1-2
- “Trunks” on page 1-2
- “PVCs” on page 1-3
- “Offnet Circuits” on page 1-3
- “Ethernet Virtual Circuits (EVCs)” on page 1-3
- “Layer2 Virtual Private Networks” on page 1-3
- “Fault Tolerant PVCs” on page 1-4
- “Resilient LMI” on page 1-4
- “SVCs” on page 1-4
- “Closed User Groups” on page 1-4
- “Port Security Screening” on page 1-4

## Logical Ports

The following chapters describe Frame Relay logical ports:

- **Chapter 2** provides an overview of Frame Relay logical port types and features. Read this chapter to learn about congestion control, Consolidated Link Layer Management (CLLM) notification, and Priority Frame Quality of Service (QoS).
- **Chapter 3** describes how to configure the following types of Frame Relay logical ports on a Lucent switch: UNI DCE/DTE, NNI, OPTimum PVC, FRAD, Direct Line Trunk, Point-to-Point Protocol (PPP) according to RFC 1490, and Multilink Frame Relay (MLFR) Multilink (ML) Member. This chapter also describes how to configure logical ports for use with Frame Relay switched virtual circuits (SVCs).
- **Chapter 5** describes how to define MLFR user-to-network interface/network-to-network interface (UNI/NNI) bundles on the 4-Port Channelized DS3/1 and DS3/1/0 Frame Relay/Internet Protocol (FR/IP) input/output modules (IOM), and 32-Port Channelized T1/E1 FR/IP modules.
- **Chapter 6** describes how to configure the MLPPP bundles on the 32-Port Channelized T1/E1 Frame Relay module.
- **Appendix D** describes how to associate logical ports with a specific customer name.

## Trunks

**Chapter 4** provides an overview of trunks and describes how to configure backup trunks and add the trunk-line connection. You can configure the following types of Frame Relay trunks:

- Frame Relay direct line
- Frame Relay OPTimum PVC
- MLFR direct line
- External

For information about these trunk types, review the trunk logical port descriptions in **Chapter 2** and **Chapter 3**.

---

## PVCs

The following chapters describe permanent virtual circuits (PVCs):

- **Chapter 7** provides an overview of PVC features such as rate enforcement and describes how to configure PVCs, specifically standard Frame Relay point-to-point PVCs and redirect PVCs that have three endpoints. This chapter also describes how to configure multicast data link connection identifiers (DLCIs).



**Note** – For information on configuring Frame Relay-to-ATM Service Interworking (FRF.8) and Frame Relay-to-ATM Network Interworking (FRF.5) circuits, see the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

---

- **Chapter 11** describes how to configure a management path between the NMS or Internet Protocol (IP) host to access the switch network. Use this chapter to configure management PVCs, redirect management PVCs, and management DLCIs.
- **Appendix C** provides an overview of priority routing concepts relevant to PVCs.

## Offnet Circuits

**Chapter 8** explains Offnet Circuits (or SPVCs) and its features for the Frame Relay module. It also provides procedures to define a Point-to-Point Offnet circuit, and restart an Offnet circuit.

## Ethernet Virtual Circuits (EVCs)

**Chapter 9** describes how to define or modify an Ethernet Virtual Circuit between Frame Relay and Gigabit Ethernet modules.

## Layer2 Virtual Private Networks

**Chapter 10** describes a Layer2 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.



**Note** – Layer2 VPNs were known in previous releases as Virtual Network Navigator (VNN) VPNs.

---

## 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 DCE, UNI DTE, or FR NNI 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.

## Resilient LMI

**Chapter 13** describes an optional logical port feature called Resilient Link Management Interface (RLMI). An RLMI configuration enables a pair of Frame Relay UNI or NNI logical ports to serve as preferred and backup ports. If the primary port fails, a switchover to the backup port occurs. The switchover is automatic unless you specify otherwise.

## SVCs

**Chapter 14** provides an overview of SVC concepts, such as address formats, node prefixes, and network ID addressing. This chapter also describes how to configure SVC node and port prefixes and port addresses for each address format.

**Appendix C** provides an overview of priority routing concepts relevant to SVCs.

## Closed User Groups

**Chapter 15** describes 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 network users, allowing only those users who are members of the CUG to set up calls to each other.

## Port Security Screening

**Chapter 16** describes Port Security Screening, which 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 allow or disallow incoming and outgoing SVCs.



# Frame Relay Services

This chapter describes Lucent Frame Relay networking services as defined by their logical port types.

This chapter contains:

- “About Frame Relay Logical Ports” on page 2-2
- “Congestion Control” on page 2-5
- “CLLM Congestion Notification” on page 2-22
- “Frame TS0 Thresholds” on page 2-21
- “Priority Frame Quality of Service (QoS)” on page 2-24
- “Administrative Tasks” on page 2-25

## About Frame Relay Logical Ports

A single physical port contains one or more logical port configurations. The logical port differs from the physical port configuration. A physical port parameters specify only clocking and clock speeds; whereas a logical port definition specifies how each channel is to communicate with the attached equipment.

For example, a logical port configured as a Frame Relay User Network Interface-Data Communication Equipment (UNI-DCE) port acts as the network for link management purposes. This UNI port may be physically set to provide clocking (defined as Data Communications Equipment or DCE) or no clocking (defined as Data Terminal Equipment or DTE).

Navis EMS-CBGX enables you to add, modify, or delete logical port configurations for a specified physical port. The logical port configuration defines the link management protocol used, the amount of bandwidth allocated, and the individual link timer parameters. See [Chapter 3, “Configuring Frame Relay LPorts”](#) for more information.

## Logical Port Types

[Table 2-1](#) lists and describes the different types of Frame Relay logical ports.

**Table 2-1. Frame Relay Logical Port Types**

<b>UNI - DCE</b>	<b>LPort Type:</b> Frame Relay User-to-network interface - Data communications equipment (UNI-DCE) <b>PPort Config:</b> Frame Relay UNI - DCE <b>Description:</b> Performs link management and expects a Frame Relay DTE device to be attached. Frame Relay DTE devices refer to those user devices that perform the LMI/DTE and F or B protocols, such as routers, bridges, cluster controllers, and front-end processors, or packetized voice and video.
<b>UNI-DTE</b>	<b>LPort Type:</b> Frame Relay User-to-network interface - Data terminal equipment (UNI-DTE) <b>PPort Config:</b> Frame Relay UNI-DTE <b>Description:</b> Specified for link management. Select this option to connect to a Frame Relay DCE (network switch) where the Lucent switch acts as the DTE. You can also use this logical port type as the link between two Lucent switches when configuring a Frame Relay OPTimum trunk on the same physical port.

**Table 2-1. Frame Relay Logical Port Types (Continued)**

<b>NNI</b>	<p><b>LPort Type:</b> Frame Relay Network-to-Network Interface (NNI)</p> <p><b>PPort Config:</b> NNI</p> <p><b>Description:</b> Functions according to the Frame Relay Forum NNI Specification. NNI enables two different switches or networks to connect together using a standard protocol. The NNI port performs both the DTE and DCE Link Management Interface (LMI) function. You can also use this port as the link between two Lucent switches when configuring a Frame Relay OPTimum trunk on the same physical port.</p>
<b>OPTimum PVC Trunk</b>	<p><b>LPort Type:</b> Frame Relay OPTimum PVC Trunk</p> <p><b>PPort Config:</b> Switch-to-switch Lucent trunk through a Frame Relay public data network (PDN)</p> <p><b>Description:</b> Known as Open Packet Trunking (OPTimum trunk). You must first configure either a UNI-DTE feeder or a Frame Relay NNI logical port on the same physical port to enable link management between the two connections.</p>
<b>Encapsulation FRAD</b>	<p><b>LPort Type:</b> Encapsulation Frame Relay Assembler Disassembler (FRAD)</p> <p><b>PPort Config:</b> Frame Relay encapsulation/ deencapsulation for high-level datalink control (HDLC) and Synchronous Data Link Control (SDLC)-based protocols</p> <p><b>Description:</b> Encapsulates traffic entering the network and deencapsulates it upon exiting the network. This configuration enables you to establish a single circuit between any FRAD port and another non trunk port. The incoming HDLC/SDLC frames must have a start and end flag (hexadecimal '7E') and a 16-bit cyclic redundancy check (CRC 16). The remainder of the frame is transparent to the switch.</p>
<b>Direct Line Trunk</b>	<p><b>LPort Type:</b> Direct Line Trunk</p> <p><b>PPort Config:</b> Trunk connection to another Lucent switch</p> <p><b>Description:</b> Performs Frame Relay functions when the trunk connection carries traffic destined for other switches in the network using Lucent's trunk protocol.</p>

**Table 2-1. Frame Relay Logical Port Types (Continued)**

<b>PPP</b>	<b>LPort Type:</b> Point-to-Point Protocol (PPP) <b>PPort Config:</b> PPP according to RFC 1490 <b>Description:</b> Enables a PPP DTE device to communicate with another DTE device configured for Frame Relay and encapsulating multi-protocols, according to the RFC 1490 Specification. This configuration enables you to establish a single circuit between the two devices. The switch performs the PPP Link Control Protocol (LCP) and Network Control Protocol (NCP) and translates PPP encapsulation into the RFC 1490 encapsulation.
<b>MLFR</b>	<b>LPort Type:</b> Multilink (ML) Member <b>PPort Config:</b> Multilink Frame Relay <b>Description:</b> Aggregates available bandwidth on a set of Frame Relay logical links between two networking devices. The aggregated links, collectively referred to as the Multilink Frame Relay Unit (MFRU), can be thought of as a single logical link. The MFRU provides a single logical link between the router and the Frame Relay switch.

## Using Fault-Tolerant PVCs

You can configure Frame Relay UNI DCE, UNI DTE, and NNI logical ports for backup service by implementing a fault tolerant PVC configuration. A fault tolerant PVC configuration enables a logical port to serve as a backup for any number of active UNI and/or NNI ports. If the primary port fails, you can activate the backup port using Navis EMS-CBGX.

See [Chapter 12, “Configuring Fault-tolerant PVCs,”](#) for more information.

## Using Resilient LMI PVCs

You can configure Frame Relay logical ports for backup service by implementing a Resilient LMI (RLMI) PVC configuration. An RLMI configuration enables a pair of UNI or NNI logical ports to serve as preferred and backup ports. If the primary port fails, the switchover to the backup port occurs based on the switchover configuration.

See [Chapter 13, “Configuring Resilient LMI,”](#) for more information.

## Using Frame Relay OPTimum Trunks

A Frame Relay OPTimum trunk creates a switch-to-switch Lucent trunk through a public data network (PDN) into another Lucent Frame Relay network. This configuration maintains the Lucent header. The Lucent OPTimum trunk feature allows private enterprise networks to purchase lower-cost, public-carrier services as the trunk between two Lucent switches instead of using a more expensive leased line.

See [“Defining Frame Relay OPTimum PVC Trunk Logical Ports”](#) on page 3-58 for configuration information.

## Congestion Control

Congestion control enables you to configure threshold values for each logical port. The congestion control parameters determine how the switch responds to frames and enable you to configure discard thresholds for red and amber frames.

As data travels through the network and is queued for transmit, the switch checks each transmit queue’s state for congestion and monitors the behavior of each PVC. The switch marks each PVC as having either “good” or “bad” behavior, based on the configured congestion commitment.

When congestion occurs on a link, the switch sets the forward explicit congestion notification (FECN) bit on packets traveling in the direction of the congestion and the backward explicit congestion notification (BECN) bit on packets traveling in the opposite direction of the congestion.

## Closed-Loop Congestion Control and Congestion States

Closed-loop congestion control reduces the rate of excess data during congested periods. The reduction in excess data is in relation to ill-behaved connections, and proportional to the configured Excess Burst Size (*Be*) value of the PVC.

Using Open Shortest Path First (OSPF), the congestion state of the trunk is communicated to all switches in the network. The ingress switch uses this information to reduce the flow of excess data into the network. You can enable or disable the closed-loop congestion control feature for each logical port in the Congestion Control attributes for logical ports. The default is “Off” (closed-loop congestion control disabled). Select “OSPF-based” to enable closed-loop congestion control. See [“Congestion Control Attributes \(VFR-NRT only\) for Frame Relay LPorts”](#) on page 3-24 for additional configuration information.

To implement closed-loop congestion control on a logical port, enable this feature on both the UNI ports and trunk end-points.

When we define a Frame Relay circuit with both the endpoints as Frame Relay, then the following congestion states are available:

- Mild
- Severe
- Absolute

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

**Table 2-2. Congested and Ingress Switch Behavior**

<b>Congestion State</b>	<b>Ingress Switch Be Reduction</b>	<b>Discarded by Congested Switch</b>	<b>FECN/BECN Marked</b>
Light-mild	Percent reduction for mild (Pm%) of Excess Burst Size (Be) of bad PVCs	Bad red frames	Bad PVCs
Heavy-mild	Pm% of Be of all PVCs	All red frames	Bad PVCs
Light-severe	Percent reduction for severe (Ps%) of Be of bad PVCs Pm% of Be of other PVCs	All red and bad amber frames	All PVCs
Heavy-severe	Ps% of Be of all PVCs	All red and amber frames	All PVCs
Light-absolute	100% of Be of bad PVCs Ps% of Be of other PVCs	All red, amber, and bad frames	All PVCs
Heavy-absolute	100% of Be of all PVCs	All red, amber and green frames	All PVCs

Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for details on congestion states available for 2-Port ULC Gigabit Ethernet module.

## Link State Updates

In switches that contain trunks, the OSPF agent in the switch monitors the congestion state of the trunk every  $N$  seconds. If one or more trunks become congested, OSPF sends a link state update (LSU) to all other switches in the network. When the switches receive the LSU, OSPF updates its routing table with the new congestion state. Similarly, if a trunk moves out of a congested state and remains non-congested for  $N_c$  seconds, OSPF sends an LSU to all switches in the network.

You can configure  $N$  (check interval) and  $N_c$  (clear delay) time intervals. The default value for  $N$  is 1 second and default value for  $N_c$  is 3 seconds.

## Congestion Parameters

Table 2-3 lists the congestion parameters that you configure for each logical port.

**Table 2-3. Congestion Parameters**

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

## Threshold Parameters

You can configure the following congestion threshold parameters for each logical port in the Congestion Control tab of the Modify Logical Port dialog box:

- The mild, normal, severe, and absolute congestion threshold parameters when one of the endpoints is Gigabit Ethernet in a Frame Relay circuit.
- The mild, severe, and absolute congestion threshold parameters when both the endpoints are Frame Relay or one of the endpoints is ATM in a Frame Relay circuit.

You change the existing (default) values for the threshold parameters by modifying the logical port congestion control attributes. When you configure the congestion thresholds, you set the threshold values incrementally.

For example, if congestion level is set at 175 for a mild threshold, the severe threshold must be greater than the mild threshold (say, 200), and the absolute threshold must be greater than the severe threshold (say, 225). These numbers represent the amount of frame traffic in terms of 56-byte buffers that are queued for transmission.

The 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 services.

See the following topics:

- [“Priority Frame Attributes for Logical Ports” on page 3-29](#) for information about configuring mono- and multi-class services.
- [Table 2-14 on page 2-24](#) for descriptions of QoS classes of service.

## Maximum Threshold Values

Table 2-4 lists the maximum mono-class and multi-class (VFR-NRT) service threshold values for each type of card.

**Table 2-4. Maximum Mono-Class and Multi-Class (VFR-NRT) Thresholds**

Card Type		Mono Class		Multi Class	
		56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
8-Port UIO	Port speed ≤ 2048 Kbps	5450	305200	2800	156800
	Port speed > 2048 and ≤ 4096 Kbps			5600	313600
	Port speed > 4096 and ≤ 8192 Kbps			11200	627200
10-Port DSX		4668	261408	2080	116480
4-Port Channelized T1		225 <sup>1</sup>	12600	225 <sup>3</sup>	12600
4-Port Channelized E1		174 <sup>1</sup>	9744	180 <sup>4</sup>	10080
4-Port Unchannelized T1		5408	302848	1600	89600
4-Port Unchannelized E1		5408	302848	1600	89600
12-Port Unchannelized E1		1922	107632	2069	115864
2-Port HSSI		23632	1323392	22400	1254400
1-Port ATM UNI		60799	3404744	54504	3052224
1-Port Channelized DS3		1922	107632	2069	115864
1-Port Channelized DS3/1/0 <sup>2</sup>	1-3 DS0s per LPort	600	33600	600	33600
	4-24 DS0s per LPort	1922	107632	1922	107632
4-Port Channelized DS3/1 FR/IP for CBX 500		2224	124544	1112	62272
4-Port Channelized DS3/1/0 FR/IP for CBX 500	1 DS0 per LPort	424	23747	212	11872
	2-3 DS0s per LPort	656	36736	328	18368
	4-7 DS0s per LPort	916	51296	458	25648
	8-16 DS0s per LPort	1248	69888	624	34944
	17-24 DS0s per LPort	2224	124544	1112	62272



**Table 2-4. Maximum Mono-Class and Multi-Class (VFR-NRT) Thresholds**

Card Type	Mono Class		Multi Class	
	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
6-Port DS3 FR/IP for CBX 500	9325 x 2	1044400	9325	522200
8-Port DS3 FR/IP for CBX 500	9325 x 2	1044400	9325	522200

<sup>1</sup> For 4-Port Channelized T1 and 4-Port Channelized E1 cards, if **n** DS0/TS0s are assigned per logical port, the maximum value allowed on the number of buffers is **n** × 225 (T1 card) and **n** × 174 (E1 card).

<sup>2</sup> The 1-Port Channelized DS3/1/0 is supported *only* on B-STDx switches that are running switch software Release 04.04.00.00 or greater.

<sup>3</sup> For 4-Port Channelized T1 cards, if the number of DS0s assigned per logical port is greater than or equal to 4 and less than or equal to 10, the maximum value allowed on the number of buffers is  $(225 * n \text{ DS0s} - 406)/2$ . If the number of DS0s assigned is greater than 10, the maximum value allowed is  $(225 * n \text{ DS0s} - 534)/2$ .

<sup>4</sup> For 4-Port Channelized E1 cards, if the number of TS0s assigned per logical port is greater than or equal to 4 and less than or equal to 15, the maximum value allowed on the number of buffers is  $(180 * n \text{ TS0s} - 342)/2$ . If the number of TS0s assigned is greater than 15, the maximum value allowed is  $(180 * n \text{ TS0s} - 534)/2$ .



**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.

### Default Congestion Level Values

Table 2-5 lists the default congestion level values for the ATM, HSSI, UIO, 10-Port DSX, Unchannelized T1/E1, Channelized DS3, Unchannelized 12-Port E1, Channelized DS3/1/0, and CBX DS3 FR/IP cards.



**Note** – For B-STDx and CBX DS3 FR/IP cards, all threshold values are by the number of 56-byte buffers.

**Table 2-5. Default Congestion Level Thresholds per Card Type**

Card Type	Class	Mild		Severe		Absolute	
		56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
ATM and HSSI	Both	4268	239008	8535	477960	17070	955920
UIO, 10-Port DSX, Unchannelized T1/E1	Both	225	12600	294	16464	588	32928
Unchannelized 12-Port E1	Both	480	26880	961	53816	1922	107632
Channelized DS3	Both	480	26880	961	53816	1922	107632
CBX DS3 FR/IP	Mono	2000 x 2	224000	4000 x 2	448000	8000 x 2	896000
	Multi	2000	112000	4000	224000	8000	448000
CBX 8-Port Subrate DS3 FR/IP	Mono	2000 x 2	224000	4000 x 2	448000	8000 x 2	896000
	Multi	2000	112000	4000	224000	8000	448000
Channelized CBX DS3/1 FR/IP	Mono	540	30240	1080	60480	2160	120960
	Multi	270	15120	540	30240	1080	60480
Channelized DS3/1/0							
• 1-3 DS0s per LPort	Both	300	16800	450	25200	600	33600
• 4-24 DS0s per LPort	Both	480	26880	961	53816	1922	107632
Channelized DS3/1/0 FR/IP							
• 1 DS0 per LPort	Mono	100	5600	200	11200	400	22400
	Multi	50	2800	100	5600	200	11200
• 2-3 DS0s per LPort	Mono	156	8736	312	17472	624	34944
	Multi	78	4368	156	8736	312	17472
• 4-7 DS0s per LPort	Mono	216	12096	432	24192	864	48384
	Multi	108	6048	216	12096	432	24192
• 8-16 DS0s per LPort	Mono	296	16576	592	33152	1184	66304
	Multi	148	8288	296	16576	592	33152
• 17-24 DS0s per LPort	Mono	540	30240	1080	60480	2160	120960
	Multi	270	15120	540	30240	1080	60480

## Congestion Control on the 4-Port Channelized T1 Module

**Table 2-6** lists the default values for a 4-Port Channelized T1 card configured for mono-class or multi-class (VFR-NRT) service. The threshold default values vary depending on the number of DS0s you assign to each logical port. For example, if you assign each DS0 to one channel on a 4-Port Channelized T1 card, you can assign a maximum of 225 (56-byte) buffers to each logical port.

**Table 2-6. 4-Port Channelized T1 Default Thresholds**

Class	DS0s/ Channels	Mild		Severe		Absolute	
		56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
Mono	1	175	9800	200	11200	225	12600
	2	225	12600	294	16464	450	25200
	>2	225	12600	294	16464	588	32928
Multi	4	175	9800	200	11200	247	13832
	5	225	12600	294	16464	359	20104
	6	225	12600	294	16464	472	26432
	7	225	1260	294	16464	584	13832
	≥8	225	12600	294	16464	588	32928

## Congestion Control on the 4-Port Channelized E1 Module

**Table 2-7** lists the default values for a 4-Port Channelized E1 card configured for mono-class or multi-class (VFR-NRT) service. The threshold default values vary depending on the number of TS0s you assign to each logical port. For example, if you assign each TS0 to one channel on a 4-Port Channelized E1 card, you can assign a maximum of 174 (56-byte) buffers to each logical port.

**Table 2-7. 4-Port Channelized E1 Default Thresholds**

Class	DS0s/ Channels	Mild		Severe		Absolute	
		56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
Mono	1	150	8400	165	9240	174	9744
	2	225	12600	294	16464	340	19040
	3	225	12600	294	16464	520	29120
	>3	225	12600	294	16464	588	32928
Multi	4	150	8400	165	9240	189	10584
	5	165	9240	225	10584	279	15624
	6	225	12600	294	16464	369	29664
	7	225	12600	294	16464	459	25704
	8	225	12600	294	16464	549	30744
	≥9	225	12600	294	16464	588	32928

## Congestion Control on the 32-Port Channelized T1/E1 FR/IP Module

For logical ports configured on the 32-Port Channelized T1/E1 Frame Relay/Internet Protocol FR/IP input/output module (IOM), the maximum and default congestion threshold values vary according to both of the following:

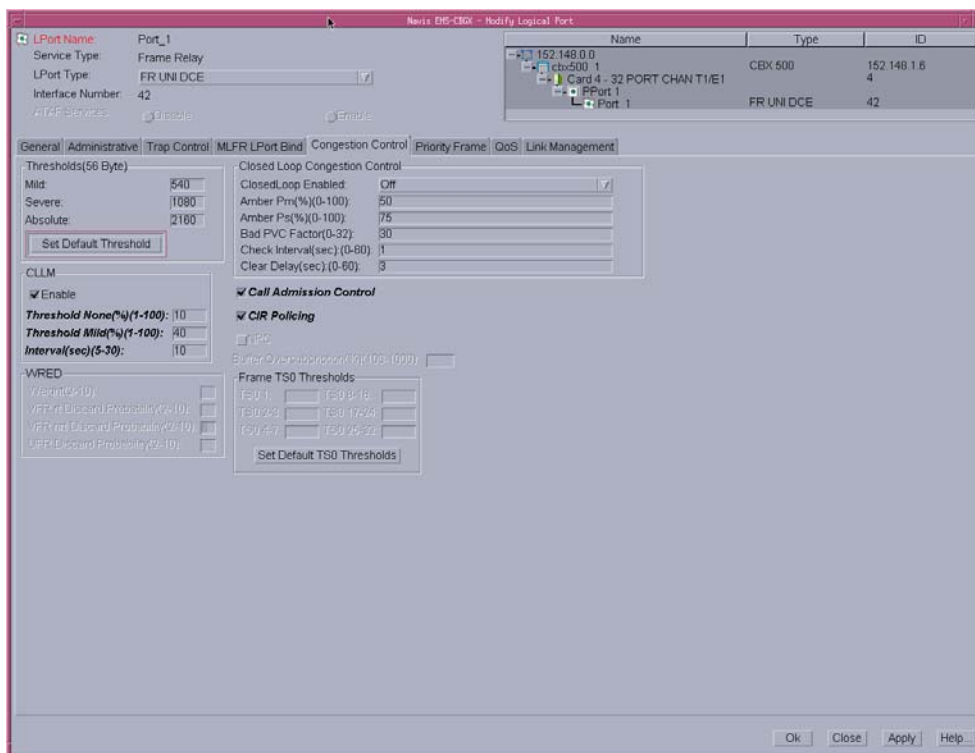
- **Number of channels assigned** — The congestion threshold values depend on the number of DS0 channels (for modules configured in T1 mode) or TS0 channels (for modules configured in E1 mode) assigned to the logical port. The maximum and default threshold values increase as the number of channels assigned to the logical port increases. See [“Assigning Channels to LPorts on Channelized T1/E1 Modules” on page 3-18](#) for more information.
- **Service class configured** — You can configure congestion thresholds for both mono-class and Priority Frame Quality of Service (QoS) multi-class (VFR-NRT) services.

See the following topics:

- [“Priority Frame Quality of Service \(QoS\)” on page 2-24](#) for information on QoS classes.
- [“Priority Frame Attributes for Logical Ports” on page 3-29](#) to configure these attributes.

## Congestion Threshold Example (32-Port Channelized T1/E1 FR/IP Module)

When you configure the congestion thresholds, you set the mild, severe, and absolute threshold values incrementally as explained in the example.



**Figure 2-1. Congestion Control Tab for 32-Port Channelized T1/E1 Module**

Figure 2-1 is an example to understand the mild, severe, and absolute congestion threshold values that you might set for a 32-Port Channelized T1/E1 module. In the example, the mild congestion threshold percentage is less than the severe threshold percentage. Likewise, the severe threshold percentage is less than the absolute threshold percentage. These numbers represent the amount of frame traffic in terms of 56-byte buffers that are queued for transmission.

### Maximum Mono-Class and Multi-Class Congestion Thresholds

Table 2-8 lists the maximum congestion thresholds for a 32-Port Channelized T1/E1 FR/IP IOM configured for mono-class service and multi-class (VFR-NRT) service.

The maximum congestion threshold value varies depending on the number of DS0 or TSO channels assigned to the logical port.

For example:

- Using mono-class service, if you assign ten channels to a logical port, then the absolute congestion threshold you configure must not exceed 1248 (56-byte) buffers.
- Using multi-class service, if you assign 18 channels to a logical port, the absolute congestion threshold you configure must not exceed 868 (56-byte) buffers.

**Table 2-8. 32-Port Channelized T1/E1 FR/IP Maximum Thresholds**

DS0/TS0 Channels Per LPort	Mono-Class		Multi-Class (VFR-NRT)	
	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
1	424	23744	212	11872
2 - 3	656	36736	328	18368
4 - 7	916	51296	458	25648
8 - 16	1248	69888	624	34944
17 - 24	1736	97216	868	48608
25 - 32 (TS0 channels only)	2224	124544	1112	62272

### Default Mono-Class and Multi-Class Congestion Thresholds

Table 2-9 lists the default mild, severe, and absolute congestion thresholds for a 32-Port Channelized T1/E1 FR/IP IOM configured for mono-class or multi-class (VFR-NRT) service. The congestion threshold values vary depending on the number of DS0 or TS0 channels assigned to the logical port.



**Note** – When you complete the Congestion Control fields to configure the mild, severe, and absolute congestion thresholds for a logical port, make sure you enter the values as the number of 56-byte buffers, *not* as the number of bytes.

**Table 2-9. 32-Port Channelized T1/E1 FR/IP Default Thresholds**

Class	DS0s/ Channels	Congestion Level					
		Mild		Severe		Absolute	
		56-Byte Buffers	Bytes	56-Byte Buffers	Bytes	56-Byte Buffers	Bytes
Mono	1	100	5600	200	11200	400	22400
	2-3	156	8736	312	17472	624	34944
	4-7	216	12096	432	24192	864	48384
	8-16	296	16576	592	33152	1184	66304
	17-24	420	23520	840	47040	1680	94080
	25-32	540	30240	1080	60480	2160	120960
Multi	1	50	2800	100	5600	200	11200
	2-3	78	4368	156	8736	312	17472
	4-7	108	6048	216	12096	432	24192
	8-16	148	8288	296	16576	592	33152
	17-24	210	11760	420	23520	840	47040
	25-32	270	15120	540	30240	1080	60480



## Congestion Control on the 6-Port Channelized DS3/1/0 Frame Relay I/O Module

This section describes the congestion control algorithms supported by the 6-Port Channelized DS3/1/0 Frame Relay I/O Module.

### Algorithms

The 6-Port Channelized DS3/1/0 Frame Relay I/O Module supports the following types of congestion control algorithms:

- **Simpler algorithms based on the actual queue length (for VFR-RT, UFR, and mono-class):** To enable this algorithm, select `TAQL` in the `Congestion Control` field in the `Add Logical Port` dialog box.
- **Time-average queue length (TAQL) (for VFR-NRT):** To enable this algorithm, select `TAQL` in the `Congestion Control` field in the `Add Logical Port` dialog box.
- **Weighted Random Early Detection (WRED):** This is applicable to all the classes, including mono-class. To enable this algorithm, select `WRED` in the `Congestion Control` field in the `Add Logical Port` dialog box.

### Simpler Algorithms

When you select `TAQL` for VFR-RT, UFR, or mono-class, the actual queue length is used in the algorithm, rather than the `TAQL`. You also define three congestion thresholds to indicate the mild, severe, and absolute congestion states, and the actual queue length is compared with these thresholds to determine which frames will be dropped. [Table 2-2](#) lists the discarded frames for various queue states.

### TAQL

When you selects `TAQL` for VFR-NRT, you also defined three congestion thresholds to indicate the mild, severe, and absolute congestion states. The software further subdivides the three thresholds.

The `TAQL` value is calculated and compared with these thresholds to determine which frames will be dropped. [Table 2-2 on page 2-6](#) lists the discarded frames for various queue states.

The `TAQL` is calculated as follows:

- On each frame arrival, you have the queue length  $Qlen(i)$ .
- For each set of 32 frame arrivals, the average queue length for the period is calculated as:

$$AQL(j) = (Qlen(1) + Qlen(2) + \dots + Qlen(32)) / 32.$$

- The `TAQL` of the current period  $n$  is:

$$TAQL(n) = (TAQL(n-1) + AQL(n)) / 2.$$

The advantage of using TAQL to perform early congestion detection is that it enables the system to tolerate bursty traffic. Since the TAQL builds up slowly, bursts of traffic can be accommodated.

However, because the TAQL value takes a while to come down, it may cause some unnecessary traffic discards for steady non-bursty traffic because of a delayed reaction to the real queue status. This problem is more serious for Zero CIR applications (best effort). In these cases, all the frames are either Amber or Red and they are the discard targets of lower congestion states (Mild and Severe).

### **WRED**

WRED is a congestion avoidance mechanism that takes advantage of congestion control mechanism of TCP. By randomly dropping packets prior to periods of high congestion, WRED informs the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared. WRED reduces the chance of waves of congestion followed by periods of under-utilization of the transmission link. This under-utilization occurs because multiple TCP hosts reduce their transmission rates.

WRED compares the average queue size to two thresholds: a minimum threshold and a maximum threshold. The WRED calculates the average queue size using a low-pass filter with an exponential weighted moving average. You can define the weight factor.

- When the average queue size is less than or equal to the minimum threshold, no packets are dropped, and when the average queue size is greater than the maximum threshold, all packets are dropped. You define a discard probability value to assign to packets when the average queue size is at the maximum threshold. When the average queue size is between the minimum and the maximum thresholds, the discard probability assigned to each arriving packet increases linearly up to the discard probability at the maximum threshold.

**Table 2-10** lists the WRED Congestion Threshold values for Mono-Class.

**Table 2-10. WRED Congestion Threshold Values**

<b>NMS Default Values</b>				
<b>Mono-class</b>				
<b>LPort Capacity</b>	<b>Default Mild</b>	<b>Default Severe</b>	<b>Default Absolute</b>	<b>Maximum Buffers</b>
1 DS0	26	52	104	120
2-3 DS0	39	78	156	178
4-7 DS0	64	128	256	295
8-12 DS0	116	232	464	528

**Table 2-10. WRED Congestion Threshold Values**

NMS Default Values				
Mono-class				
LPort Capacity	Default Mild	Default Severe	Default Absolute	Maximum Buffers
13-18 DS0	180	360	720	820
19-24 DS0	321	642	1284	1462
25-32 DS0	429	858	1716	1950

Table 2-11 lists the WRED Congestion Threshold values for Multi-Class.

**Table 2-11. WRED Congestion Threshold Values**

NMS Default Values				
Multi-class				
LPort Capacity	Default Mild	Default Severe	Default Absolute	Maximum Buffers
1 DS0	9	18	36	45
2-3 DS0	14	28	56	67
4-7 DS0	24	48	96	112
8-12 DS0	44	88	176	200
13-18 DS0	68	136	272	311
19-24 DS0	122	244	488	555
25-32 DS0	162	324	648	740

## Logical Port Congestion Thresholds for TAQL and Simpler Algorithms

The mild, severe, and absolute threshold default values and maximum values for an LPort depend on the LPort capacity. [Table 2-12](#) provides these values for mono-class and multi-class. The default values are displayed on the mild, severe and absolute threshold fields and the user inputs are checked against the maximum allowed values.

[Table 2-12](#) lists the default Mono-Class and Multi-Class Threshold values.

**Table 2-12. Default Mono-Class and Multi-Class Thresholds (TAQL)**

Class	DS0s per LPort	Mild	Severe	Absolute	Max Buffers
Mono	1	26	52	104	120
	2-3	39	78	156	178
	4-7	64	128	256	295
	8-12	116	232	464	528
	13-18	180	360	720	820
	19-24	321	642	1284	1462
Multi	1	9	18	36	45
	2-3	14	28	56	67
	4-7	24	48	96	112
	8-12	44	88	176	200
	13-18	68	136	272	311
	19-24	122	244	488	555

## Frame TS0 Thresholds

This section describes the Frame TS0 thresholds that are available for Frame Relay UNI DCE and UNI DTE, and NNI.



**Note** – Frame TS0 Thresholds are applicable only to a 32-Port Channelized T1/E1 card.

Table 2-13 lists the available Frame TS0 Thresholds.

**Table 2-13. Frame TS0 Thresholds**

Frame TS0 Threshold	Description
TS0 1	This value is the Frame Threshold value for the LPort with 1 TS0. Its valid range is 1 to 3900 and the default value is 78.
TS0 2-3	This value is the Frame Threshold value for the LPort with 2 to 3 TS0s. Its valid range is 1 to 3900 and the default value is 110.
TS0 4-7	This value is the Frame Threshold value for the LPort with 4 to 7 TS0s. Its valid range is 1 to 3900 and the default value is 149.
TS0 8-16	This value is the Frame Threshold value for the LPort with 8 to 16 TS0s. Its valid range is 1 to 3900 and the default value is 208.
TS0 17-24	This value is the Frame Threshold value for the LPort with 17 to 24 TS0s. Its valid range is 1 to 3900 and the default value is 267.
TS0 25-32	This value is the Frame Threshold value for the LPort with 25 to 32 TS0s. Its valid range is 1 to 3900 and the default value is 50.

## CLLM Congestion Notification

Consolidated Link Layer Management (CLLM) congestion notification occurs with increases in network traffic load. Network congestion occurs when the traffic attempting to pass is greater than the available bandwidth. When a Frame Relay network reaches its congestion point, frames are discarded until congestion is alleviated.

The following types of congestion control are used to manage Frame Relay data transport:

- **Implicit Congestion** — Involves certain events available in the data link layer to detect the frame loss.
- **Explicit Congestion** — Involves the following types of notification:
  - Forward Explicit Congestion Notification (FECN) or Backward Explicit Congestion Notification (BECN) – Flow control is built into the Frame Relay address in the form of FECN and BECN bits.
  - Consolidated Link Layer Management (CLLM) – One DLCI address (1007) is reserved exclusively for transmitting congestion notification.

### About CLLM

You can enable or disable CLLM on any Frame Relay UNI or NNI port. The CLLM mechanism applies to PVCs only. The IOM2 and IOM6 modules support CLLM only for UNI/NNI LPorts. The switch reserves DLCI address 1007 exclusively for transmitting congestion notification messages to the user device. The CLLM message:

- Is sent periodically to the customer premise equipment (CPE) or network access device until congestion is alleviated.
- Notifies users of congestion activity outside the conventional framing structure.
- Contains a list of DLCIs that correspond to the congested Frame Relay bearer connections.
- Supports up to a maximum of 127 DLCIs. You can configure the time duration between each consecutive message.



**Note** – If you are already using DLCI 1007, then you must delete the PVC and assign a new DLCI number.

---

## CLLM Threshold States

The configurable parameters, CLLMThresholdNone and CLLMThresholdMild, determine the virtual circuit (VC) congestion threshold type and congestion state. These parameters represent a percentage of BECN frames received since the last CLLM message. The following guidelines determine the VC congestion threshold:

- **Not congested** — The percentage of BECN frames received on any VC on the logical port does not exceed the configured CLLMThresholdNone.
- **Mild congested state** — The percentage of BECN frames received on any VC on the logical port exceeds the configured CLLMThresholdNone but does not exceed the configured CLLMThresholdMild.
- **Absolute congested state** — The percentage of BECN frames received on any VC on the logical port exceeds the configured CLLMThresholdMild.

See [“Congestion Control Attributes \(VFR-NRT only\) for Frame Relay LPorts”](#) on [page 3-24](#) for information about setting CLLM attributes.

## CLLM Messages

Based on the congestion threshold state, there are two types of CLLM messages:

- **Absolute CLLM** — Contains a list of all VCs that are in absolute congested state.
- **Mild CLLM** — Contains a list of all VCs that are in mild congested state.

For example, in a network having two VCs on a Frame Relay UNI port with one VC in absolute congested state and the other VC in mild congested state, the absolute congested state is reported in absolute CLLM frame and the other VC is reported in mild CLLM frame.

## Priority Frame Quality of Service (QoS)

The Priority Frame Quality of Service (QoS) feature enables you to configure “Frame Relay-like service classes” on Frame Relay logical ports.

You must set the logical port service class type to “multi-class” to enable Priority Frame QoS. By default, all service classes are not selected. You can use the Set QoS Parameters option to set QoS parameters. See “[QoS Attributes for Logical Ports](#)” on [page 3-31](#) for information about setting the multi-class service type and QoS parameters.

When you set the QoS service class, you can use the values listed in [Table 2-16](#), or modify these settings.



**Note** – For Channelized T1/E1 cards and the Channelized DS3/1/0, configuring QoS on fewer than four DS0/TS0s provides a modified service because of the lack of buffers.

[Table 2-14](#) briefly describes each class of service.

**Table 2-14. QoS Class of Service Descriptions**

Field	Description
Variable Frame Rate (VFR) Real Time	Used for special delay-sensitive applications, such as packet voice, which require low delay between endpoints.
Variable Frame Rate Non-Real Time (VFR-NRT)	Handles transfer of data streams with a committed information rate over a pre-established connection. This service provides low data loss but no delay guarantee.
Unspecified Frame Rate (UFR)	Primarily used for LAN traffic. The CPE should compensate for any delay or lost traffic.

## Using a T1/E1 Card

If you are configuring QoS Class of Service on a T1/E1 card, use the guidelines described in [Table 2-15](#).

**Table 2-15. T1/E1 I/O Module QoS Class of Service Guidelines**

Number of DS0/TS0s	Number of allowed QoS Class of Service Combinations
1-3	1 one-class with VFR-NRT characteristics
4 or more	All valid traffic class combinations



Table 2-16 describes the QoS values for Frame Relay logical ports.

**Table 2-16. Default QoS Values for Frame Relay Logical Ports**

Service Type	Bandwidth Allocation	Routing Metric	Oversubscription Factor
VFR-RT	Dynamic	Admin Cost	100%
VFR-NRT	Dynamic	Admin Cost	100%
UFR	Dynamic	Admin Cost	100%

## Administrative Tasks

This section describes the following administrative tasks:

- [“Using Templates” on page 2-25](#)
- [“Modifying Switch Configuration Attributes” on page 2-26](#)
- [“Deleting Frame Relay Logical Ports” on page 2-28](#)

### Using Templates

After you define a logical port configuration and save it as a template, you can define a new logical port using the same parameters.

To define a logical port from a template, perform the following tasks:

1. In the `Switch` tab, expand the node for the PPort, subport, channel, card, or IMA group to which you want to add an LPort.
2. Right-click the `LPorts` node.

3. From the popup menu, select Add LPort Using Template.

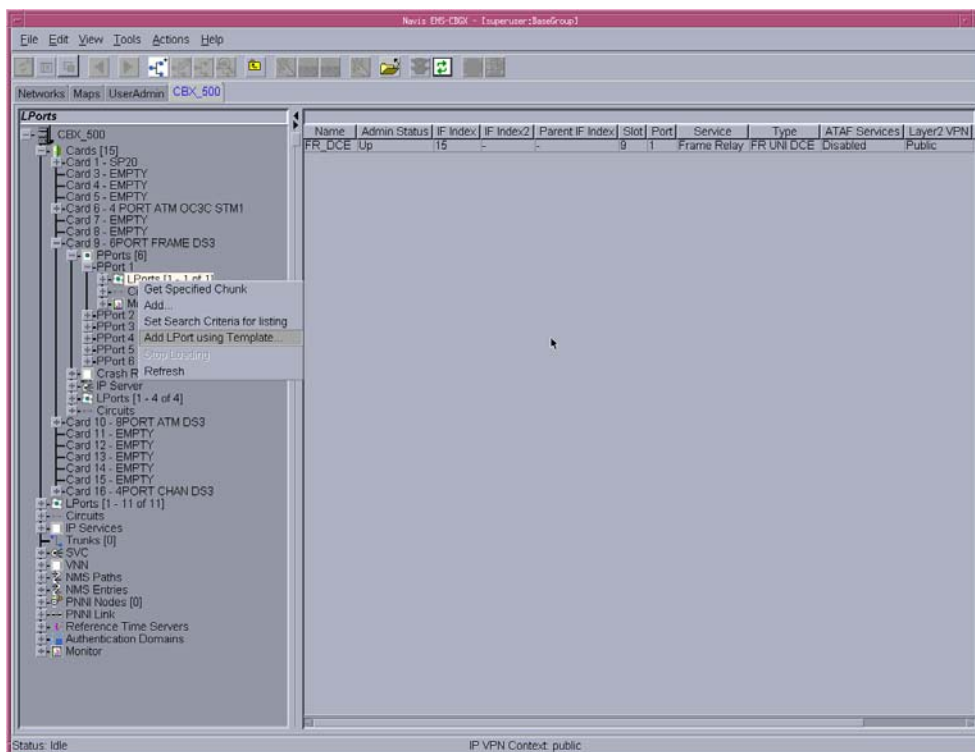


Figure 2-2. Add LPort Using a Template

4. In the Choose Template dialog box, the templates that are applicable for the card type in which the LPort is being created are listed. Select a template and then choose OK.



**Note** – You can define logical port templates for creating bulk (multiple) logical ports on the B-STDx and CBX Channelized DS3/1/0 FR/IP modules. For information about the Bulk LPort feature, refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000*.

## Modifying Switch Configuration Attributes

When you modify CBX 500 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. Refer to the *Navis EMS-CBGX Getting Started Guide* for information about using PRAM features.

## Non-Disruptive Logical Port and Trunk Attributes (CBX Only)

Certain logical port and trunk attributes are defined as *non-disruptive*. When you modify any of these attributes on CBX 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 in Navis EMS-CBGX dialog boxes. **Table 2-17** 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 2-17. Non-Disruptive Logical Port and Trunk Attributes**

Attribute	See
Net Overflow	<b>“General Attributes for Frame Relay LPorts” on page 3-12</b>
Redirect PVC Delay Time	<b>“General Attributes for Frame Relay LPorts” on page 3-12</b> <b>“Defining a Redirect PVC Connection” on page 7-33</b>
Call Admission Control	<b>“Congestion Control Attributes (VFR-NRT only) for Frame Relay LPorts” on page 3-24</b>
CLLM Interval (sec) CLLM Thrhld None (%) CLLM Thrhld Mild (%)	<b>“Congestion Control Attributes (VFR-NRT only) for Frame Relay LPorts” on page 3-24</b>
LMI Update Delay	<b>“Link Management Attributes for Logical Ports” on page 3-34</b>
CIR Policing Enabled	<b>“Link Management Attributes for Logical Ports” on page 3-34</b>
RLMI Max Full Status Attempts	<b>“Link Management Attributes for Logical Ports” on page 3-34</b>
Hold Down Timer (0..255)	<b>“General Attributes for SVCs” on page 3-43</b>
Trunk Admin Cost	<b>“Adding a Trunk” on page 4-7</b>
Subscription Factor (%)	<b>“Adding a Trunk” on page 4-7</b>
Area ID	<b>“Adding a Trunk” on page 4-7</b>
Customer Name	<b>“Assigning Logical Ports to a Layer2 VPN” on page 10-6</b> <b>“Adding Customer Names” on page D-1</b>

## Deleting Frame Relay Logical Ports

Before you can delete a Frame Relay logical port, verify that the following conditions are met:

- No circuit uses this logical port as an endpoint.
- No trunk is defined that uses this logical port as an endpoint.
- No management DLCI or multicast DLCI exists on this port.
- This logical port is not defined as the feeder (FR UNI DTE/NNI) for an existing OPTimum PVC trunk logical port.
- If the MLFR trunk bundle logical port is an endpoint of a trunk, you can delete all but one logical port binding.
- No network ID exists on this logical port.



**Note** – Unless a logical port has a loopback status of “None”, do not attempt to delete the logical port. Refer to the *Switch Diagnostics User’s Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for information about loopback testing.

---

If any of the conditions mentioned above exist for the logical port you want to delete, then you must first delete them in the following order:

- Circuits
- Trunks
- Management or multicast DLCIs
- Logical port

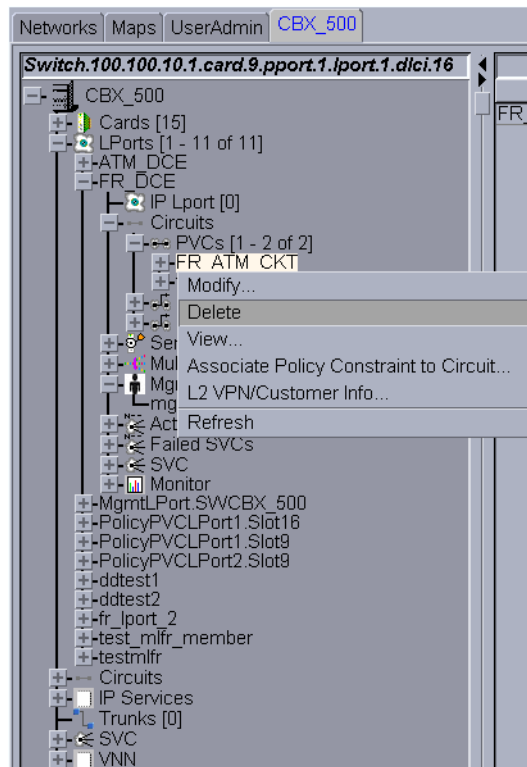
### Deleting Circuits

In the Switch tab, you can either delete circuits by expanding the Circuits node to display all circuits configured on the switch, or you can view and delete only circuits associated with a specific LPort.

To delete a circuit associated with an LPort, perform the following tasks:

1. In the Switch tab, expand the LPorts node, then expand the node for the LPort you are working with.

2. Expand the `Circuits` node, then expand the node for the type of circuit you want to delete.



**Figure 2-3. Deleting a Circuit Based on LPort**

3. Right-click the circuit you want to delete.
4. From the popup menu, select `Delete`. On your confirmation, the selected LPort is deleted.

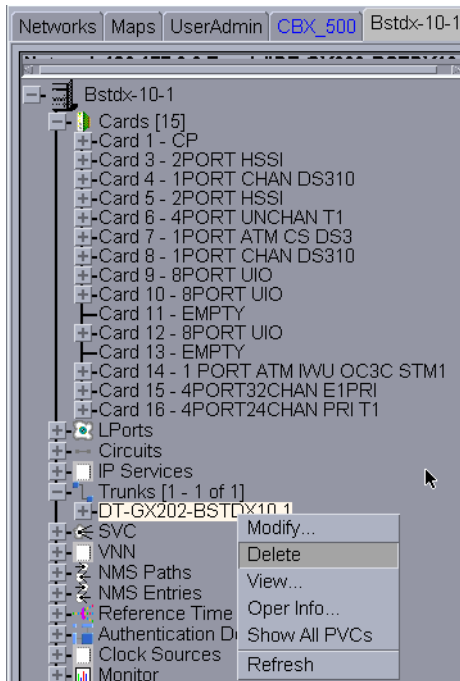
## Deleting Trunks

In the `Switch` tab, you can either delete trunks by expanding the `Trunks` node to display all trunks configured on the switch, or you can view and delete only trunks associated with a specific LPort.

To delete a trunk, perform the following tasks:

1. In the `Switch` tab, expand the `LPorts` node, then expand the node for the LPort you are working with.
2. Expand the `Trunks` node.

3. Right-click the trunk you want to delete.



**Figure 2-4. Deleting a Trunk Based on LPort**

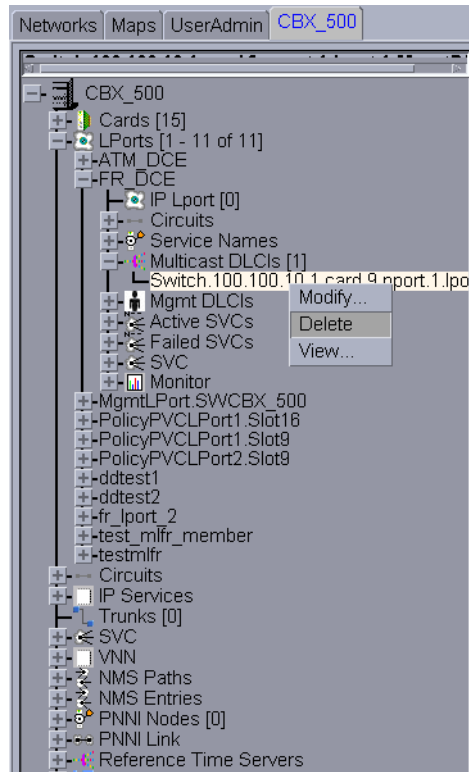
4. From the popup menu, select `Delete`. On your confirmation, the selected trunk is deleted.

## Deleting Management or Multicast DLCIs

To delete management or multicast DLCIs, perform the following tasks:

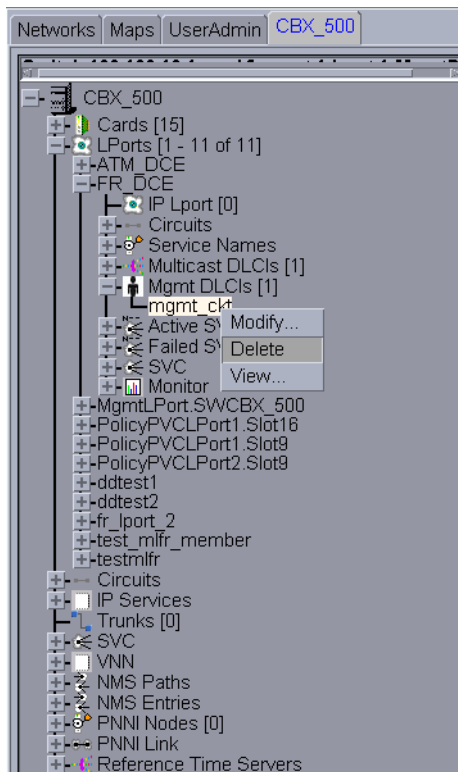
1. In the `Switch` tab, expand the `LPorts` node, then expand the node for the LPort you are working with.
2. Expand the `Multicast DLCIs` or `Management DLCIs` node, then right-click the DLCI you want to delete.

The Multicast DLCIs dialog box is displayed (Figure 2-5).



**Figure 2-5. Deleting a Multicast DLCIs Based on LPort**

The Management DLCIs dialog box is displayed (Figure 2-6).



**Figure 2-6. Deleting a Management DLCIs Based on LPort**

3. From the popup menu, select **Delete**. On your confirmation, the selected Multicast DLCI or Management DLCI is deleted.

## Deleting the Logical Port

In the Switch tab, you can either delete logical ports by expanding the LPorts node to display all logical ports configured on the switch, or you can view and delete logical ports based on card.



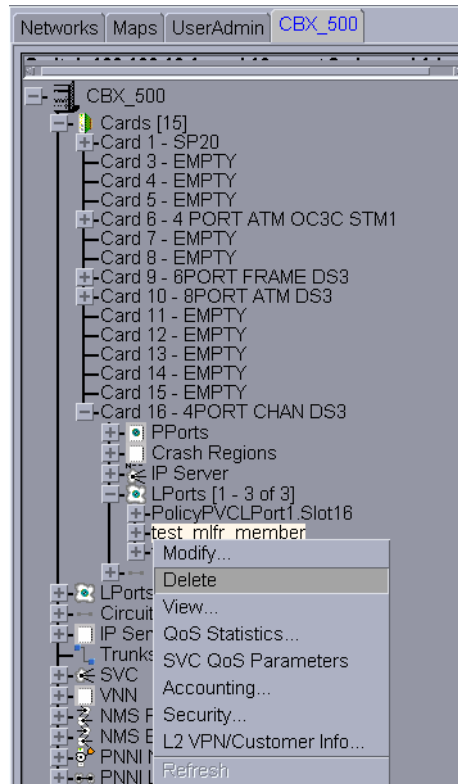
**Note** – When you delete logical ports:

- Make sure this logical port is not the UNI DTE or NNI logical port used as the feeder for a Frame Relay OPTimum trunk. You first need to take the OPTimum trunk out of service, or first define another feeder, before you can delete this logical port.
  - If the MLFR trunk bundle logical port is an endpoint of a trunk, you can delete all but one logical port binding. The system displays a warning message if deleting a logical port binding will cause the trunk endpoints to have a different number of logical ports.
-



To delete an LPort based on card, perform the following tasks:

1. In the Switch tab, expand the Cards node, then expand the node for the card you are working with.
2. Expand the LPorts node, then right-click the LPort you want to delete.



**Figure 2-7. Deleting a LPort**

3. From the popup menu, select Delete. Make sure the Loopback for the LPort is “NONE”. On your confirmation, the selected LPort is deleted.



## Configuring Frame Relay LPorts

This chapter provides instructions for configuring Frame Relay logical ports on a CBX or B-STDX switch. See [Chapter 2, “Frame Relay Services,”](#) for an overview of Lucent’s Frame Relay logical port services.



---

**Note** – If you are configuring 4-Port Channelized DS3/1 and DS3/1/0 modules on the CBX 500 switch, see [“Logical Port Configuration Considerations for CBX 500 4-Port Channelized DS3/1 and DS3/1/0 Modules”](#) on page 3-71 for more information.

---

This chapter contains:

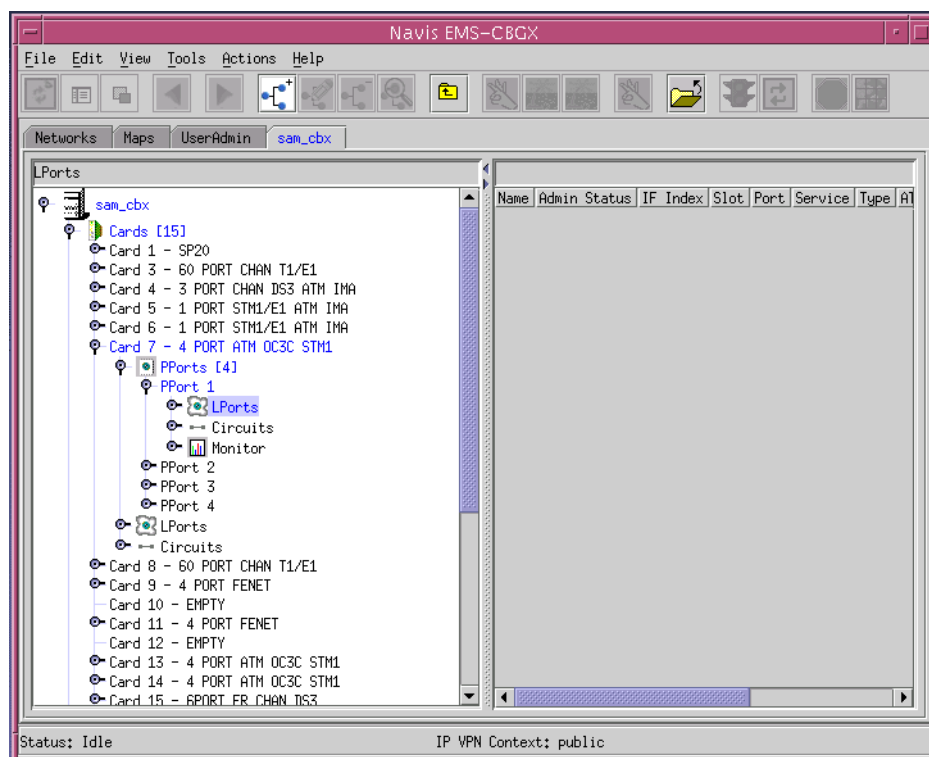
- [“Working with Frame Relay LPorts”](#) on page 3-2
- [“Defining Frame Relay UNI DCE/DTE or NNI LPorts”](#) on page 3-10
- [“Assigning Channels to LPorts on Channelized T1/E1 Modules”](#) on page 3-18
- [“Configuring Logical Ports for Use With SVCs”](#) on page 3-42
- [“Defining Frame Relay OPTimum PVC Trunk Logical Ports”](#) on page 3-58
- [“Defining Encapsulation FRAD, Direct Line Trunk, and PPP Logical Ports”](#) on page 3-60
- [“Defining Multilink Frame Relay \(MLFR\) Trunks \(B-STDX\)”](#) on page 3-65
- [“Logical Port Configuration Considerations for CBX 500 4-Port Channelized DS3/1 and DS3/1/0 Modules”](#) on page 3-71

## Working with Frame Relay LPorts

Manage logical ports through the Switch tab of Navis EMS-CBGX, by expanding either the Cards or LPorts nodes.

- **Using the Cards node**

Create a new logical port by choosing the Cards node, and selecting the card and physical port upon which you want to create the logical port. See [“Defining Frame Relay UNI DCE/DTE or NNI LPorts”](#) on page 3-10.



**Figure 3-1. Logical Ports in the Cards Node**

- **Using the LPorts node**

View or modify existing logical ports by choosing the LPorts node in the Switch tab, or choosing the Cards node to view logical ports based on card and physical port. See [“Modifying a Frame Relay LPort”](#) on page 3-7.

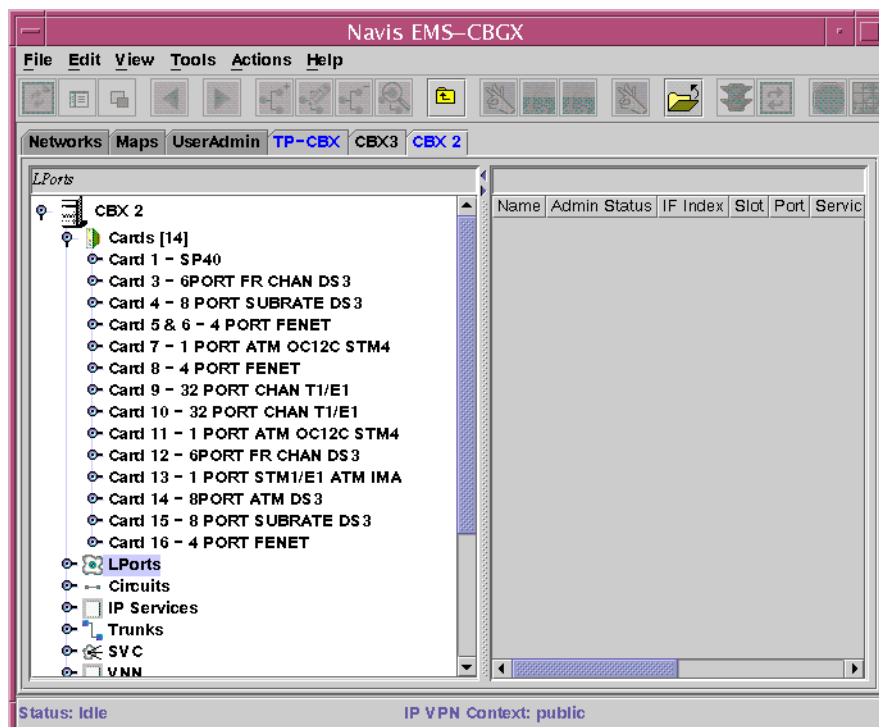


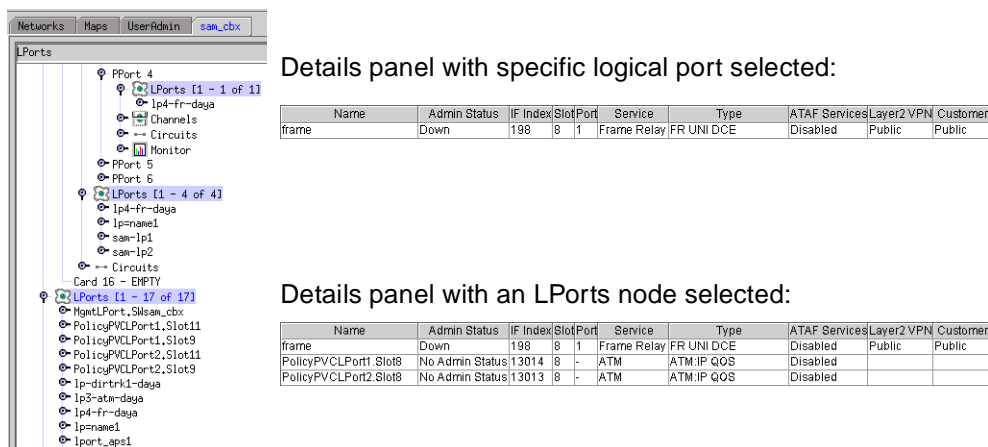
Figure 3-2. Logical Ports in the LPorts Node

## Accessing LPorts in the Switch Tab

To access the Switch tab:

1. Log in to Navis EMS-CBGX.
2. In the Networks tab, expand the network node, then expand the Switches node.
3. Double-click on the switch to which you want to add a logical port.

The Switch tab is displayed. You can access LPort nodes and expand them as shown in [Figure 3-3](#).



**Figure 3-3. Managing Logical Ports in the Switch Tab**

[Figure 3-3](#) demonstrates how you can find the same logical port by expanding either the Cards or LPorts node, and shows the function of the Details panel on the right-hand side of the window, based on your selection in the navigation tree.

When you select an LPorts node or a specific port on the left-hand side of the Navis EMS-CBGX window, the detail panel displays:

- **Name** — Unique alphanumeric name that identifies the logical port.
- **Admin Status** — Administrative state of the port as Up or Down.
- **IF Index** — Interface number of the logical port.
- **Slot/Port** — Slot and port numbers of the PPort on which the LPort is configured.
- **Service** — Service type of the selected logical port (for example, Frame Relay)
- **Type** — The logical port type, such as FR UNI DCE or FR UNI DTE.
- **ATAF Services** — Indicates whether the ATM Test Access Function (ATAF) is enabled or disabled on the logical port.
- **Layer2 VPN** — Name of the Layer2 virtual private network (VPN) to which this logical port belongs. See [Chapter 10, “Configuring Layer2 Virtual Private Networks \(VPNs\),”](#) for more information.
- **Customer** — Name of the customer to which this logical port is dedicated. The default name is Public.

## Adding a Frame Relay LPort

To create a new Frame Relay logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, right-click on the LPorts node and select Add from the popup menu.

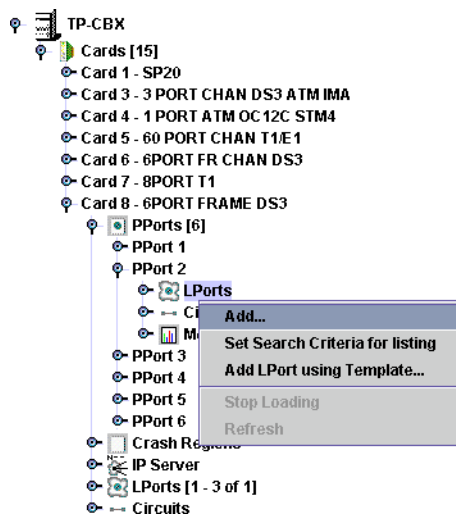
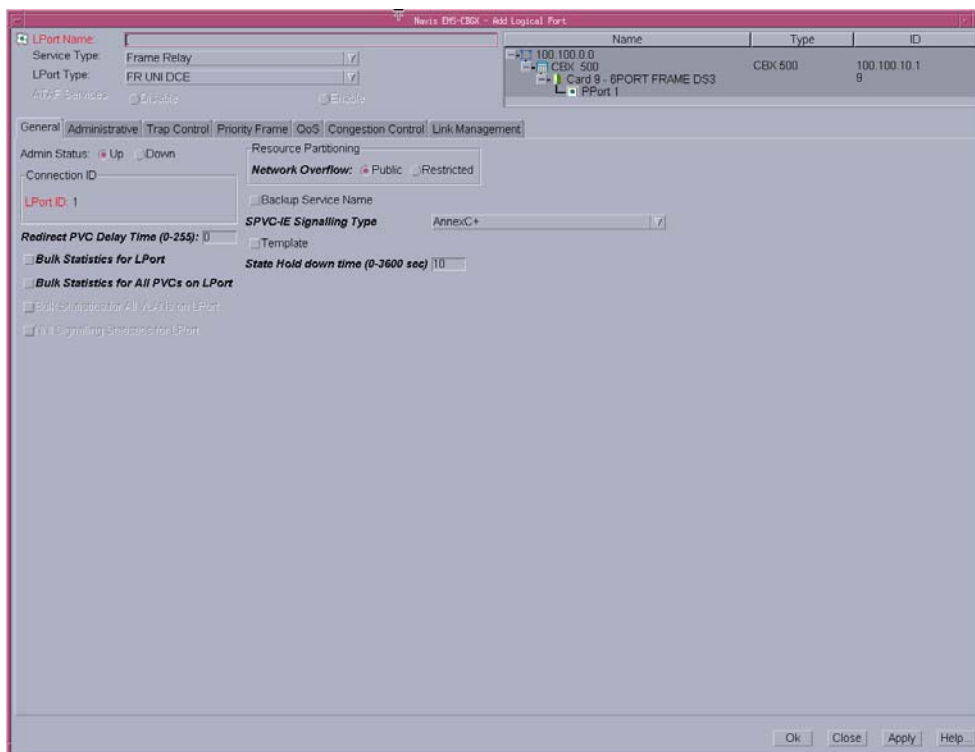


Figure 3-4. Adding a Logical Port

The Add Logical Port dialog box (Figure 3-5) is displayed.



**Figure 3-5. Add Logical Port Dialog Box**

4. Define the logical port type, and use the tabs in the Add Logical Port dialog box to configure the Frame Relay logical port. See Table 3-1 for references to information about configuring specific types of Frame Relay logical ports.

**Table 3-1. Frame Relay Logical Port Configurations**

Service Type	Logical Port Type	See...
Frame Relay	FR UNI-DCE	"Defining Frame Relay UNI DCE/DTE or NNI LPorts" on page 3-10
	FR UNI-DTE	
	FR UNI-NNI	
	Frame Relay OPTimum Trunk	"Defining Frame Relay OPTimum PVC Trunk Logical Ports" on page 3-58
Others	Direct Line Trunk, Encapsulation FRAD, Point-to-Point Protocol	"Defining Encapsulation FRAD, Direct Line Trunk, and PPP Logical Ports" on page 3-60
	ML Member	"Defining ML Member Logical Ports" on page 3-69

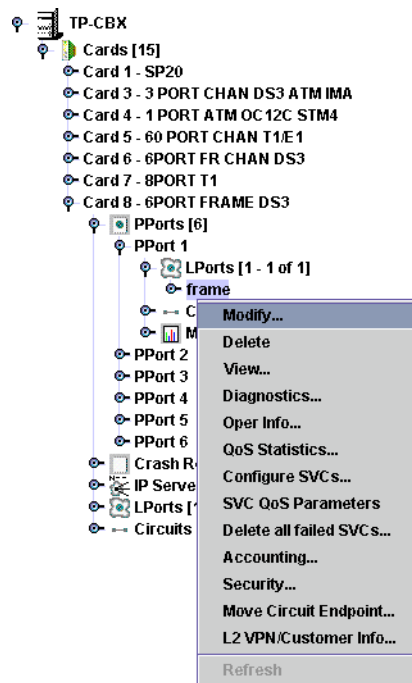


5. When you have configured the logical port, click OK.
6. Optionally, perform the following configuration tasks:
  - To configure this logical port for a specific Layer2 VPN and customer, see [“Assigning Logical Ports to a Layer2 VPN”](#) on page 10-6.
  - If you plan to configure SVC addresses for this logical port, continue with the instructions in [“Configuring Logical Ports for Use With SVCs”](#) on page 3-42.

## Modifying a Frame Relay LPort

To modify an existing logical port:

1. In the Switch tab, expand the LPorts node.
2. Right-click on the LPort you want to configure, as shown in [Figure 3-6](#).



**Figure 3-6. Modifying a Logical Port**

When you right-click on a logical port, the following commands are available from the popup menu:

- **Modify** — Displays the Modify Logical Port dialog box which enables you to configure the LPort. See [“Setting Frame Relay LPort Attributes”](#) on page 3-11.
- **Delete** — Deletes the LPort.
- **View** — Enables you to view the LPort without modifying the configuration.

- **Diagnostics** — Enables you to run diagnostics on the LPort. Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- **Oper Info** — Displays the View LPort Operational Status dialog box, which enables you to check the operating state of the LPort. Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- **QoS Statistics** — Enables you to view LPort Quality of Service (QoS) statistics. Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- **Configure SVCs** — Displays the Configure SVC dialog box, which enables you to manage SVCs. See [“Configuring Logical Ports for Use With SVCs” on page 3-42](#).
- **SVC QoS Parameters** — Enables you to view LPort SVC Quality of Service (QoS) statistics. Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- **Delete all failed SVCs** — Clears the list of failed SVCs for the LPort. View the list by expanding the LPort node and expanding the Failed SVCs node.
- **Accounting** — Enables you to configure NavisXtend Accounting Server parameters. For more information about the Accounting Server, refer to the *NavisXtend Accounting Server Administrator's Guide*.
- **Security** — Enables you to create screens that protect your network from unauthorized SVC access. To configure screen assignments for port security screening, see [Chapter 16, “Port Security Screening.”](#)
- **Move Circuit Endpoint** — Enables you to move circuit endpoints between LPorts. See [“Moving Circuits” on page 7-43](#).
- **L2 VPN / Customer Info** — Enables you to assign the LPort to a Layer 2 VPN or customer name. See [Chapter 10, “Configuring Layer2 Virtual Private Networks \(VPNs\),”](#) for more information.

3. Select Modify from the popup menu.

The Modify Logical Port dialog box (Figure 3-7) is displayed.

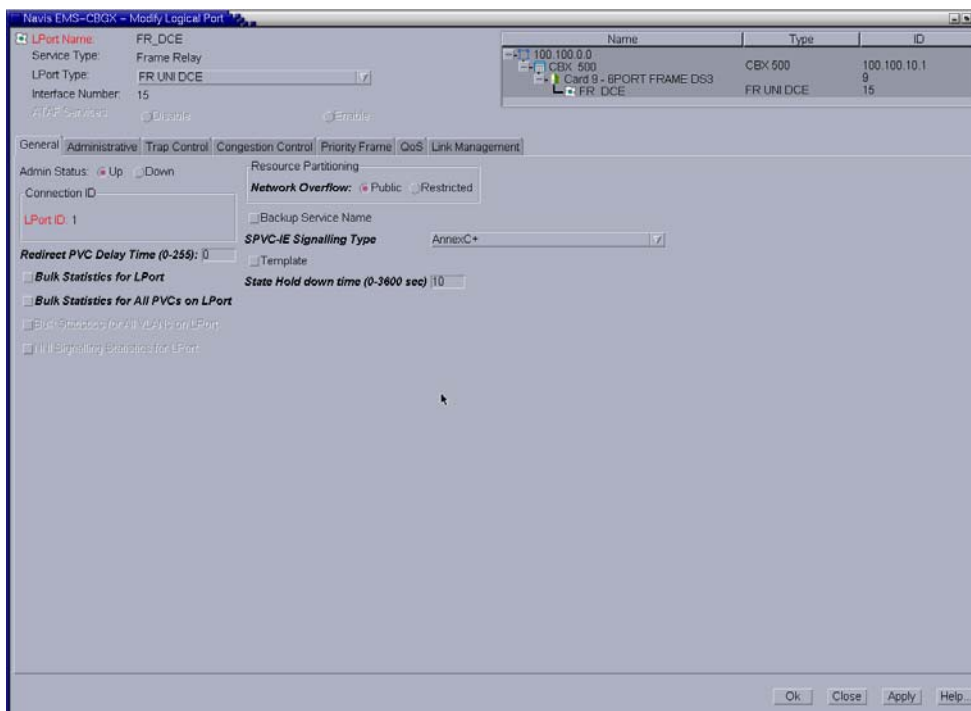


Figure 3-7. Modify Logical Port Dialog Box

4. Use the tabs in the Add Logical Port dialog box to configure the Frame Relay logical port. See Table 3-1 for references to information about configuring specific types of Frame Relay logical ports.
5. When you have configured the logical port, click OK.
6. Optionally, perform the following configuration tasks:
  - To configure this logical port for a specific Layer2 VPN and customer, see “Assigning Logical Ports to a Layer2 VPN” on page 10-6.
  - If you plan to configure SVC addresses for this logical port, continue with the instructions in “Configuring Logical Ports for Use With SVCs” on page 3-42.

## Defining Frame Relay UNI DCE/DTE or NNI LPorts

Defining a Frame Relay UNI DCE/DTE or NNI logical port involves:

1. “Defining the Service Type and LPort Type” on page 3-10
2. “Setting Frame Relay LPort Attributes” on page 3-11
3. “Assigning Channels to LPorts on Channelized T1/E1 Modules” on page 3-18

### Defining the Service Type and LPort Type

To define a Frame Relay UNI DCE, UNI DTE, or NNI logical port in the Add Logical Port dialog box (Figure 3-5 on page 3-6), complete the fields described in Table 3-2.

**Table 3-2. Service Type and Logical Port Type (UNI-DCE)**

Element	Description
Service Type	Select Frame Relay.
LPort Type	Select either FR UNI DCE, FR UNI DTE, or FR NNI.  Resilient local management interface (RLMI) Master logical ports must be either FR UNI DTE or FR NNI. RLMI Slave logical ports must be either FR UNI DCE or FR NNI. For more information about RLMI, see Chapter 13, “Configuring Resilient LMI.”
LPort ID <i>(4-Port Channelized T1, E1, and 32-Port Channelized T1/E1 FR/IP modules only)</i>	Enter a number that uniquely identifies this logical port on the physical port. <ul style="list-style-type: none"> <li>• For a 4-Port Channelized T1 module, enter a number 1 - 24.</li> <li>• For a 4-Port Channelized E1 module, enter a number 1 - 30.</li> <li>• For a 32-Port Channelized T1/E1 FR/IP module, the number you specify depends on the operation mode (T1 or E1) selected in the Modify Card dialog box, as follows:                             <ul style="list-style-type: none"> <li>– <b>T1 mode</b> – If the module is configured in T1 mode, enter a number between 1 and 24 for the 24 DS0 channels available per physical port in T1 Mode.</li> <li>– <b>E1 mode</b> – If the module is configured in E1 mode, enter a number between 1 and 31 for the 30 TS0 channels available per physical port in E1 Mode. Refer to the <i>Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i> for more information on setting the operation mode on the Modify Card dialog box.</li> </ul> </li> </ul> For all other modules, the LPort ID is a read-only field that automatically defaults to 1.

When you have configured the service type and LPort type, continue by setting attributes for a the service type and LPort type you selected.

## Setting Frame Relay LPort Attributes

When you define a new logical port, the Add Logical Port dialog box (Figure 3-5) displays a series of tabs that enable you to set attributes for the logical port. The following tabs are displayed:

- **General** — Sets general logical port parameters such as the admin state. See [“General Attributes for Frame Relay LPorts” on page 3-12](#).
- **Administrative** — Sets admin-related parameters including bandwidth parameters. See [“Administrative Attributes for Frame Relay LPorts” on page 3-15](#) and [“Assigning Channels to LPorts on Channelized T1/E1 Modules” on page 3-18](#).
- **FRF.19** — Enables you to configure the Frame Relay OAM (FRF.19) features supported by the 6-Port Channelized DS3/1/0 Frame Relay I/O Module. See [“FRF.19 Attributes for Frame Relay LPorts” on page 3-21](#).
- **Congestion Control** — Sets the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network. See [“Congestion Control Attributes \(VFR-NRT only\) for Frame Relay LPorts” on page 3-24](#).
- **Priority Frame** — Sets the logical port service class and transmit schedule mode. See [“Priority Frame Attributes for Logical Ports” on page 3-29](#).
- **QoS** — Sets the bandwidth and routing metrics (if applicable) for the various traffic service classes. By setting logical port QoS parameters, you can allocate bandwidth for PVCs and SVCs based on their QoS services on a logical port. See [“QoS Attributes for Logical Ports” on page 3-31](#).
- **MLFR LPort Bind** — Enables you to bind an ML Member logical port to an MLFR UNI/NNI bundle logical port. See [“MLFR LPort Bind Attributes for Logical Ports” on page 3-33](#).
- **Link Management** — Sets the link management protocol used in the network and the local management interface (LMI) update delay and error thresholds. See [“Link Management Attributes for Logical Ports” on page 3-34](#).
- **MLFR Configuration** — Configures MultiLink Frame Relay (MLFR) attributes for MLFR logical ports on 6-Port Channelized DS3/1/0 Frame Relay modules. See [“MLFR Configuration Attributes for Logical Ports” on page 3-38](#).
- **Trap Control** — Sets the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port. The supported logical port types are different for each I/O module. See [“Trap Control Attributes for Logical Ports” on page 3-40](#).

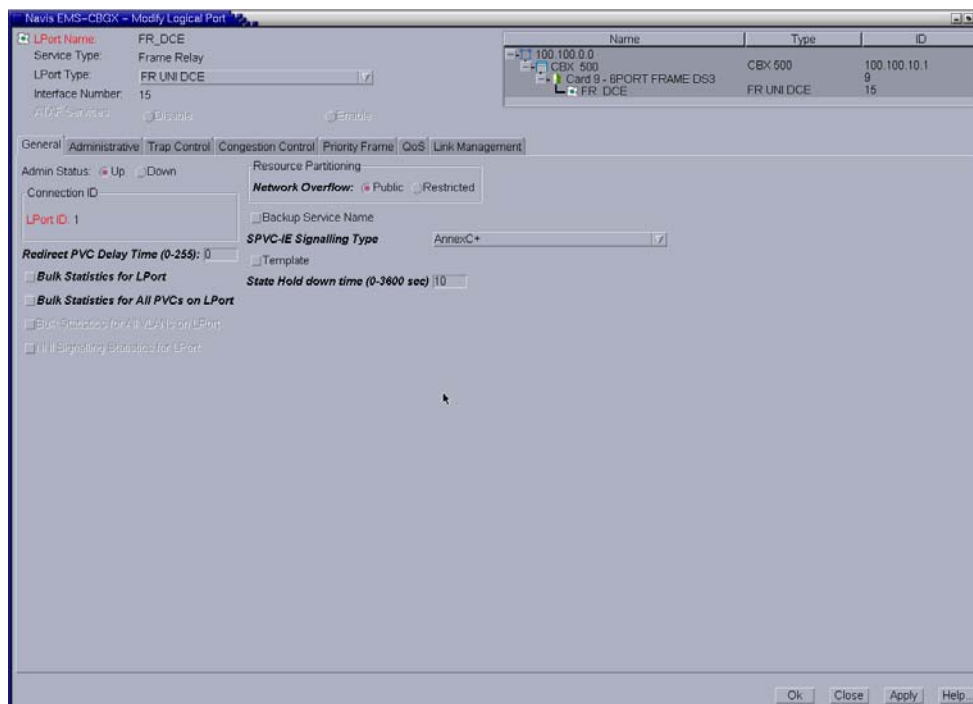


**Note** – If you are configuring a Multilink (ML) Member logical port that you will bind to a Multilink Frame Relay (MLFR) UNI/NNI bundle logical port, you must select Disable in the Link Mgmt Protocol field to disable link management for this logical port. For more information, see [Chapter 5, “Configuring Multilink Frame Relay \(MLFR\) UNI/NNI Bundles.”](#)

This section explains how to set all attributes except SVC attributes. For information about setting SVC attributes, see [“Configuring Logical Ports for Use With SVCs” on page 3-42.](#)

## General Attributes for Frame Relay LPorts

The General tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-8.](#)



**Figure 3-8. Add/Modify Logical Port: General Tab**

**Table 3-3** describes the fields and controls in the General tab.

**Table 3-3. Add/Modify Logical Port: General Tab**

Element	Description
Admin Status	<p>Set the Admin Status as follows:</p> <ul style="list-style-type: none"> <li>• <i>Up</i> – (default) Activates the port.</li> <li>• <i>Down</i> – Saves the configuration in the database without activating the port or takes the port offline to run diagnostics.</li> </ul> <p><i>Note: 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.</i></p>
LPort ID	<p>Displays a valid ID for the logical port in a range from 1-24. The LPort Type must not be MLFR Trunk Bundle. The default value is one. There is no default for the 32 Port T1/E1 card or for the 1 Port Channelized 3-1-0 card.</p>
Redirect PVC Delay Time	<p>Enter a value between 0-255 seconds. The 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).</p> <p>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 switchover between a working <i>redirect</i> 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.</p> <p><i>Note: Changing the value for this attribute does not admin down the logical port.</i></p> <p>For more information about redirect PVCs, see <a href="#">Chapter 7, “Configuring Permanent Virtual Circuits (PVCs).”</a></p>
Bulk Statistics for LPort	<p>Enables statistics collection from the logical port by the NavisXtend Statistics Server. To collect statistics at the logical port level, Bulk Statistics must also be enabled at the switch level. Clear the check box (default) to disable statistics collection.</p> <p><i>Note: Bulk Statistics is not supported on the 1-Port ATM IWU OC-3c/STM-1 card.</i></p>
Bulk Statistics for All PVCs on LPort	<p>Enables statistics collection for PVCs on the logical port. To collect statistics on circuits, you must also enable Bulk Statistics on each individual circuit. The default is Disable.</p> <p><i>Note: Bulk Statistics is not supported on the 1-Port ATM IWU OC-3c/STM-1 card.</i></p>

**Table 3-3. Add/Modify Logical Port: General Tab (Continued)**

Element	Description
Network Overflow	<p>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. To assign this logical port to a specific Layer2 VPN and customer, see <a href="#">Chapter 10, “Configuring Layer2 Virtual Private Networks (VPNs).”</a></p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Public</i> – (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).</li> <li>• <i>Restricted</i> – 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.</li> </ul> <p><i>Note: Changing the value for this attribute does not admin down the logical port.</i></p>
Backup Service Names	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Fault-tolerant PVC only</i> – Select Yes to configure a logical port for backup service. The default is No. For more information, see <a href="#">Chapter 12, “Configuring Fault-tolerant PVCs.”</a></li> <li>• <i>Primary or Backup RLMI Port only</i> – Select Yes to configure this port as the RLMI backup port. Select No to configure this port as the RLMI primary port. For more information about RLMI, see <a href="#">Chapter 13, “Configuring Resilient LMI.”</a></li> </ul> <p><i>Note: When an RLMI backup port is not in use, the port is idle and does not use network resources.</i></p>
SPVC IE Signaling Type	<p>This feature enables you to specify one of two different SPVC signaling options at the logical port level:</p> <ul style="list-style-type: none"> <li>• <i>AnnexC+</i> (default) - This option indicates that the SPVC-IE signalling first attempt will be accomplished with the PNNI 1.0 Annex C based SPVC signalling. If the call is rejected with the release cause of #88 (Incompatible destination), the signalling will retry the same path using Addendum af-cs-0127 SPVC-IE support. (The destination must be a FR interface.)</li> <li>• <i>Addendum127</i> - This option indicates that the SPVC-IE signalling is always based on Addendum af-cs-0127 SPVC-IE support. The SPVC-IE signalling option is specified as part of the Administrative Options when configuring the logical port.</li> </ul>

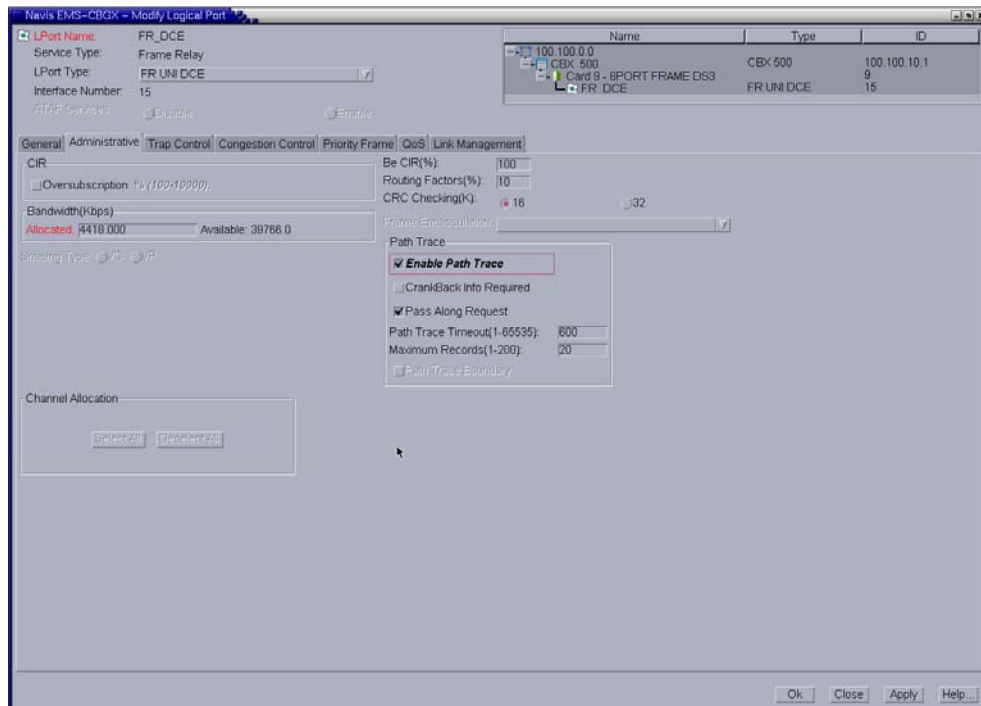


**Table 3-3. Add/Modify Logical Port: General Tab (Continued)**

Element	Description
Template	Saves these settings as a template to configure another logical port with similar options. To create a template, enable the <i>Template</i> field. The default is disabled. See “Using Templates” on page 2-25 for more information.
State Hold Down Time	Name LSAs will be advertised only if the logical port state remains “Down” for the specified minimum time. Enter a number of seconds (0-3600) for the minimum time. The default is 10 seconds.

### Administrative Attributes for Frame Relay LPorts

The Administrative tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-9](#).



**Figure 3-9. Add/Modify Logical Port: Administrative Tab**

[Table 3-4](#) describes the fields and controls in the Administrative tab.

**Table 3-4. Add/Modify Logical Port: Administrative Tab**

Element	Description
CIR Oversubscription %	<p>Enables bandwidth subscription. The default value is disabled. If you enable the setting, you must also specify a value in the Oversubscription percentage field. If you disable the setting, you will not receive notification when oversubscription occurs on the port. If you enabled Oversubscription, enter the subscription percentage. The default is 100%.</p>
Bandwidth	<p>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.</p> <p>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:</p> <p><i>Physical port clock speed: 1536 Kbps</i>  <i>Logical port UNI-DTE/NNI Feeder Bandwidth: 56 Kbps</i>  <i>Logical port Frame Relay Trunk Bandwidth: 1480 Kbps</i></p> <p>This sample configuration allocates a PDN trunk with 1480 Kbps bandwidth between two Lucent switches, each attached to a PDN network.</p>
Be CIR (%)	<p>Enter a value between 0-100 percent. This value represents the UNI bandwidth percentage on all configured zero CIR circuits. The default is 100 percent.</p>
Routing Factors (%)	<p>Enter a value between 0-100 percent. This value represents the routing factor percentage on all rate enforcement circuits. The default is 10 percent.</p>
CRC Checking (HSSI and CBX 6-Port DS3 modules, only)	<p>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.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>CRC 16</i> - Data will be checked in 4K frames.</li> <li>• <i>CRC 32</i> - Data will be checked in 8K frames.</li> <li>• <i>PassThru</i> - Guarantees that any corruption of the frame by Lucent switches will be detected and discarded by the end user as an invalid CRC frame. This feature is disabled by default. For information about enabling this feature, refer to the <i>Navis EMS-CBGX Getting Started Guide</i>.</li> </ul>

**Table 3-4. Add/Modify Logical Port: Administrative Tab**

Element	Description
Path Trace	<p>Path Trace enables you to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network. You can configure a logical port so all circuits that either come into, or originate on, this logical port are traced. This is the only way to trace SVCs and calls from a B-STDX 9000 switch.</p> <ul style="list-style-type: none"> <li>• <b>Enable Path Trace</b> – Enable or disable the path trace feature for circuits that pass through this LPort. Select Enabled to enable path trace or Disabled (default) if you do not want to have path trace enabled.</li> <li>• <b>Crankback Info Required</b> – Enable or disable collection of crankback information. Select Yes to instruct the switch to collect and maintain the crankback information, that is, information about dynamic rerouting of call setups around failed nodes or links (or links with insufficient resources) on the traced path. If No (default) is selected, crankback information will not be collected.</li> <li>• <b>Pass Along Request</b> – Enable or disable pass along request for this path trace. Select Yes (default) to have the path trace continue through nodes that do not support the path trace feature. This may cause the trace results to contain some gaps between successive entries of logical nodes and logical ports traversed by this connection or party. Select No to cause the path trace to terminate at any switch that does not support the path trace feature. A partial path trace will be returned.</li> <li>• <b>Path Trace Timeout (sec)</b> – Enter a number of seconds (0-65535) for which you want the trace results to be maintained in the switch. The default is ten minutes (600 seconds).</li> <li>• <b>Maximum Records</b> – Specify how many trace records can be present for this LPort. The default is 20.</li> </ul> <p>For information about configuring path tracing at the circuit level, see <b>“Administrative Attributes for PVCs”</b> on page 7-14. For more information about how path tracing works, refer to the <i>Switch Diagnostics User’s Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i>.</p>

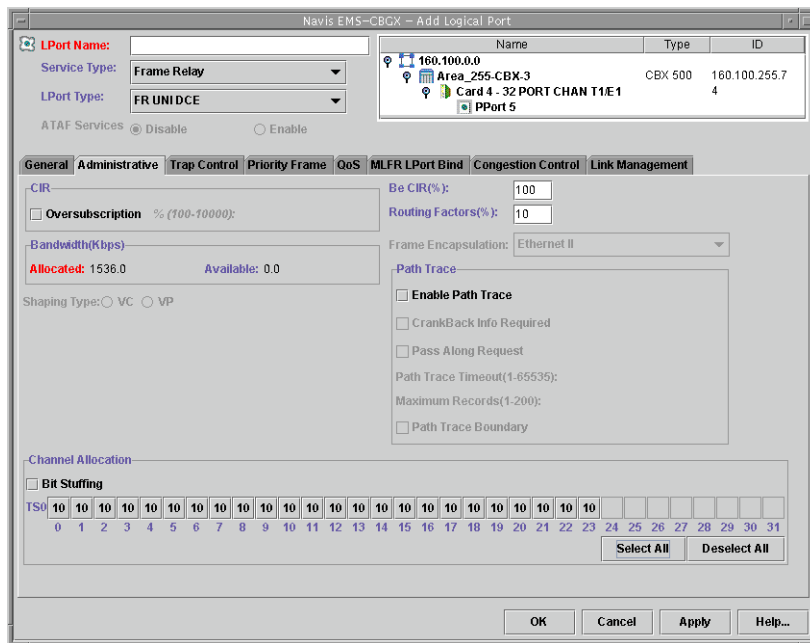
**Table 3-4. Add/Modify Logical Port: Administrative Tab**

Element	Description
Channel Allocation (4-Port Channelized T1/E1, 32-Port Channelized T1/E1 FR/IP, and 6-Port Channelized DS3/1/0 Frame Relay I/O modules)	<p>If you are configuring a 4-Port Channelized T1/E1, 32-Port Channelized T1/E1 FR/IP, or 6-Port Channelized DS3/1/0 Frame Relay I/O module, specify the DS0 (for T1) or TS0 (for E1) channel(s) assigned to the logical port.</p> <p>The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel to remove the X. You can select/deselect channels by using the Channel Allocation editing buttons.</p> <p><b>Note:</b> <i>The logical port bandwidth either increases or decreases 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.</i></p> <p>For more information on assigning channels to logical ports, see <a href="#">“Assigning Channels to LPorts on Channelized T1/E1 Modules”</a> on page 3-18.</p>

### ***Assigning Channels to LPorts on Channelized T1/E1 Modules***

If you are configuring a 4-Port Channelized T1/E1 or 32-Port Channelized T1/E1 FR/IP module, the Administrative tab of the Add Logical Port dialog box enables you to specify the DS0 (for T1) or TS0 (for E1) channel(s) assigned to the logical port.

When you configure Administrative attributes for a logical port, you can assign one or more channels to the logical port, as shown in **Figure 3-10**.



**Figure 3-10. Channel Allocation Fields for T1/E1 Logical Ports**

The logical port ID number appears in the box (channel) you select. To deselect DS0 channels, click on the channel. You can select/deselect channels by using the Channel Allocation editing buttons.



**Note** – The logical port bandwidth either increases or decreases 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.

The type and number of channels you can assign depends on the operation mode (T1 or E1) selected for the module in the Modify Card dialog box, as follows:

- **T1 mode** — If the module is configured in T1 mode, you can assign up to twenty-four 64-KB DS0 channels with a maximum total bandwidth of 1536 Kbps.
- **E1 mode** — If the module is configured in E1 mode, you can assign up to thirty 64-KB TS0 channels with a maximum total bandwidth of 1920 Kbps.

If you choose a Link Framing setting in the Modify PPort dialog box that enables time slot 16 (TS16), you can also use channel 16 to send data on a 32-Port Channelized T1/E1 FR/IP IOM configured in E1 mode.

For more information about this dialog box and setting the Link Framing parameter, and for information on selecting the operation mode in the Modify Card dialog box, refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

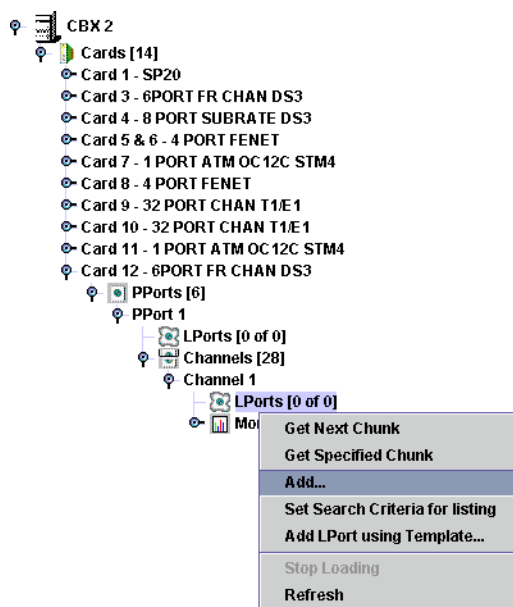
### **Assigning LPorts on Channelized DS3/1/0 FR Modules**

If you are configuring a 6-Port Channelized DS3/1/0 Frame Relay I/O module, the Administrative tab of the Add Logical Port dialog box enables you to specify the DS0 channels assigned to the logical port.

For more information about configuring physical ports and channels on the 6-Port Channelized DS3/1/0 Frame Relay I/O module, refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

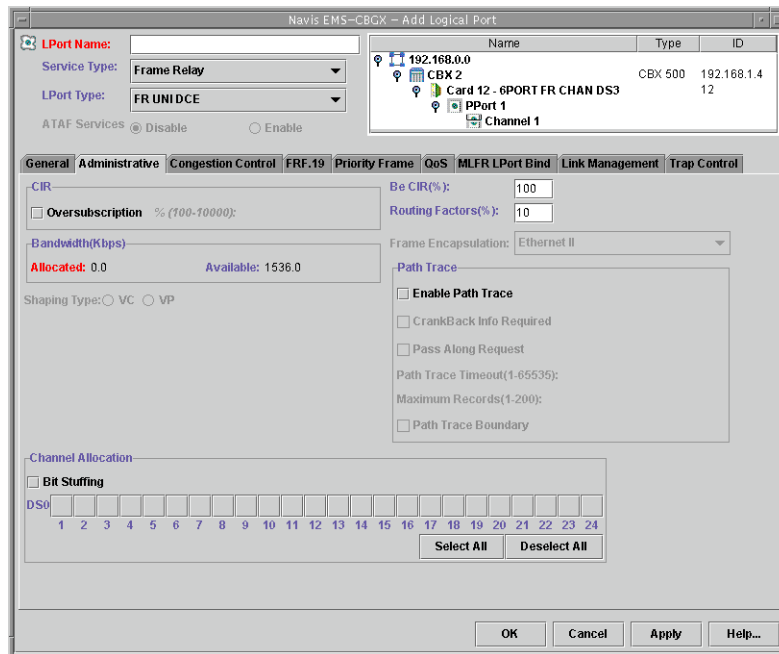
To add a logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module.
2. Expand the PPorts node, and expand the node for the physical port you want to configure.
3. Expand the Channels node, and expand the node for the channel you want to configure.
4. Under the node for the channel, right-click on the LPorts node and select Add from the popup menu, as shown in [Figure 3-11](#).



**Figure 3-11. Adding Logical Ports on Channelized DS3/1/0 FR Modules**

When you configure the logical port, the Administrative attributes enable you to assign one or more channels to the logical port, as shown in [Figure 3-12](#).



**Figure 3-12. Channel Allocation Fields for DS3 Logical Ports**

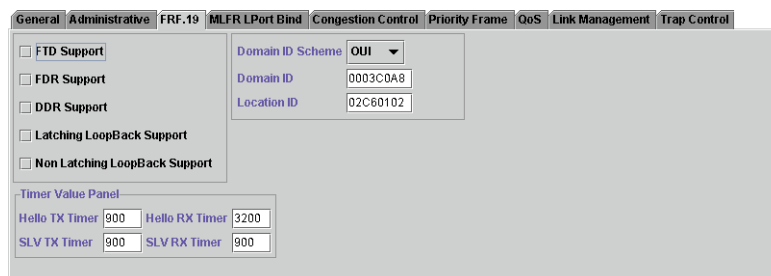
The logical port bandwidth either increases or decreases depending on the number of channels you select or deselect. You can configure other logical ports with different attributes on other DS0 channels on this same physical port.

### FRF.19 Attributes for Frame Relay LPorts

The 6-Port Channelized DS3/1/0 Frame Relay I/O Module supports the Frame Relay OAM (operations, administration, and maintenance) protocol (FRF.19).

For more information about Frame Relay OAM, refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000*.

The FRF.19 tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-13](#).



**Figure 3-13. Add/Modify Logical Port: FRF.19 Tab**

Table 3-5 describes the fields and controls in the FRF.19 tab.

**Table 3-5. Add/Modify Logical Port: FRF.19 Tab**

Element	Description
FTD Support	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Enabled</i> — This MP supports FTD measurements.</li> <li>• <i>Disabled</i>— This MP does not support FTD measurements.</li> </ul> FTD measurements can be made only if both the near end and far end MPs for a Frame Relay OAM test have FTD enabled.
FDR Support	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Enabled</i> — This MP supports FDR measurements.</li> <li>• <i>Disabled</i>— This MP does not support FDR measurements.</li> </ul> FDR measurements can be made only if both the near end and far end MPs for a Frame Relay OAM test have FDR enabled.
DDR Support	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Enabled</i> — This MP supports DDR measurements.</li> <li>• <i>Disabled</i>— This MP does not support DDR measurements.</li> </ul> DDR measurements can be made only if both the near end and far end MPs for a Frame Relay OAM test have DDR enabled.
Latching Loopback	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Enabled</i> — This MP supports latching loopbacks.</li> <li>• <i>Disabled</i>— This MP does not support latching loopbacks.</li> </ul>
Non Latching Loopback	Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Enabled</i> — This MP supports non-latching loopbacks.</li> <li>• <i>Disabled</i>— This MP does not support non-latching loopbacks.</li> </ul>
Domain ID Scheme	Select one of the following schemes for the domain ID: <ul style="list-style-type: none"> <li>• <i>OUI</i> — (Organizationally Unique Identifier) The format is a zero byte followed by a 3-octet OUI, which is administered by the IEEE.</li> <li>• <i>IPv4</i> (default) — The format is the network portion of a public IPv4 address block owned by the service provider.</li> <li>• <i>X.121</i> — The format is X.121 DNIC, as defined in X.76, padded on the left with zeros to fill 8 octets, and then BCD-encoded into 4 octets.</li> <li>• <i>E.164</i> — The format is the E.164 Network Identification Field of the Transit Network ID, as defined in X.76, padded on the left with zeros to fill 8 octets, and then BCD-encoded into 4 octets.</li> </ul>



**Table 3-5. Add/Modify Logical Port: FRF.19 Tab (Continued)**

Element	Description
Domain ID	Enter a value for the domain ID. Use the format you chose in the Domain ID Scheme field. By default, the Domain ID value is the first two octets of the switch IP address. If MPs are in different networks, the default value cannot be used.
Location ID	Displays the default Location ID. The default Location ID for a logical port is a combination of the least significant two octets of the switch IP address and the interface number of the logical port.  The Location ID for all MPs within an administrative domain must be unique. When the administrative domain is formed by multiple Lucent networks or a Lucent and a non-Lucent network, the default values for the Location IDs might not be unique. In this case, use the Modify Logical Port dialog box to change default Location IDs.
Hello TX Timer	Enter the length of time (in seconds) between the transmission of Hello messages from the MP. The minimum value is 15 and the maximum value is 3600. The default value is 900.
Hello RX Timer	Enter the maximum length of time (in seconds) that may pass between the reception of consecutive Hello messages from a peer MP. If this time is exceeded, it is assumed that the peer MP is no longer advertising its presence. The Frame Relay OAM measurements with that peer are discontinued until the next Hello message is received. The minimum value is 60 and the maximum value is 14400. The default value is 3200.
SLV TX Timer	Enter the length of time (in seconds) between the transmission of service verification messages from the MP to a peer MP. The minimum value is 15 and the maximum value is 36000. The default value is 900 seconds.
SLV RX Timer	Enter the maximum length of time (in seconds) that may pass between the reception of a service verification message (FDR and DDR) from a MP peer and the reception of the next verification message (FDR and DDR) from the same peer. If the next service verification message is received within this time limit, the parameters are recorded, the FDR and DDR are calculated, and the timer is restarted. If the next service verification message is received after this time limit, the received parameters are recorded as initial values and the timer is restarted. The minimum value is 15 and the maximum value is 36000. The default value is 900.

## Congestion Control Attributes (VFR-NRT only) for Frame Relay LPorts

The Congestion Control tab of the Add/Modify Logical Port dialog box is shown in Figure 3-14. See “Congestion Control” on page 2-5 for more information.

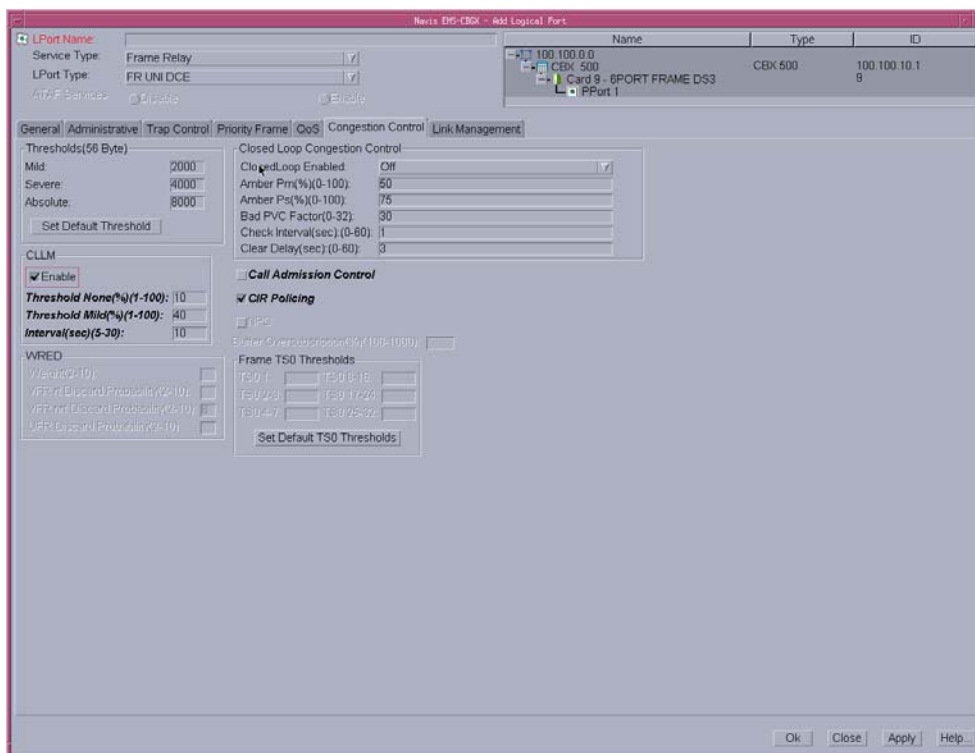


Figure 3-14. Add/Modify Logical Port: Congestion Control Tab



**Note** – Do not exceed the maximum threshold value for each card type (see Table 2-4 on page 2-8, and Table 2-8 on page 2-15 for more information). The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.



**Note** – For 4-Port Channelized T1/E1 cards, if  $n$  DS0/TSOs are assigned per logical port, the maximum value allowed on the number of buffers is  $n \times 225$  (T1) and  $n \times 174$  (E1).

Table 3-6 describes the fields and controls in the Congestion Control tab.

**Table 3-6. Add/Modify Logical Port: Congestion Control Tab**

Element	Description
Thresholds (%)	<p>Accept the defaults or enter values for the mild, normal, severe, and absolute threshold fields as defined in <a href="#">Table 2-4 on page 2-8</a> through <a href="#">Table 2-9 on page 2-16</a>.</p> <p><i>Note: When setting threshold parameters:</i></p> <ul style="list-style-type: none"> <li>• Do not exceed the maximum threshold value for each card type (see <a href="#">Table 2-4 on page 2-8</a> for more information). The absolute congestion threshold cannot be greater than the maximum value allowed for each logical port.</li> <li>• If you are setting threshold parameters on a T1/E1 card, the default values will not appear until you set the bit stuffing and bandwidth allocation. See <a href="#">Table 2-4 on page 2-8</a> for more information.</li> <li>• For 4-Port Channelized T1/E1 cards, if <i>n</i> DS0s are assigned per logical port, the maximum value allowed on the number of buffers is <i>n</i> x 225 (T1) and <i>n</i> x 174 (E1).</li> <li>• The Normal threshold is available if Service Type is Gigabit Ethernet.</li> </ul>
CLLM	<p><i>Note: Changing the values for the threshold or interval attributes does not admin down the logical port.</i></p> <p>For more information about these fields, see “<a href="#">CLLM Threshold States</a>” on page 2-23.</p> <ul style="list-style-type: none"> <li>• Enable Set the admin state to enable or disable CLLM notification on this logical port. <ul style="list-style-type: none"> <li>– <i>Enable</i> – Enables CLLM notification.</li> <li>– <i>Disable</i> – (default) Disables CLLM notification.</li> </ul> </li> <li>• Threshold None (%) Displays the threshold percentage value (between 1-100) of BECN frames received on any VC on this port. The default value is 10.</li> <li>• Threshold Mild (%) Displays the threshold percentage value (between 1-100) of BECN frames received on any VC on this port. The default value is 40. The value for the Mild threshold must be equal to or greater than the value for the None threshold.</li> <li>• Interval (sec) Determines the time duration (in seconds) between two consecutive CLLM messages sent on the logical port. The CLLM message is sent as long as at least one VC on this logical port remains in a congested state. Enter a value between 5 and 30 seconds. The default value is 10 seconds.</li> </ul>

**Table 3-6. Add/Modify Logical Port: Congestion Control Tab (Continued)**

Element	Description
Closed Loop Congestion Control	<p>The following settings are available:</p> <ul style="list-style-type: none"> <li>• <b>ClosedLoop Enabled</b> Set the congestion control parameters. This field enables/disables OSPF closed-loop congestion control for each logical port. For more information see <b>“Closed-Loop Congestion Control and Congestion States”</b> on page 2-5. Options include:                             <ul style="list-style-type: none"> <li>– <i>Off</i> – (default) Disables closed-loop congestion.</li> <li>– <i>OSPF-based</i> – Enables closed-loop congestion.</li> </ul> </li> <li>• <b>Amber Pm (%)</b> Controls the reduction percentage of Be when mild congestion occurs. Enter a Pm% value. The default is 50%.</li> <li>• <b>Amber Ps (%)</b> Controls the reduction percentage of Be when severe congestion occurs. Enter a Ps% value. The default is 75%.</li> <li>• <b>Bad PVC Factor</b> Enter a value between 0-32. The default is 30. Determines the threshold for “bad” PVC detection. The following example shows the relationship between the “bad” PVC factor and threshold.</li> </ul> $\text{Threshold} = \frac{Bc + (Be/2)}{2^{(32-Fb)}}$ <p><i>Note: If you select simple as the rate enforcement scheme, this feature is disabled.</i></p> <ul style="list-style-type: none"> <li>• <b>Check Interval (sec)</b> Determines the number of seconds in which the switch monitors the trunk’s congestion on the port. Enter an interval. The default is 1 second.</li> <li>• <b>Clear Delay (sec)</b> Determines the number of seconds in which the switch monitors the trunk’s non-congestion state. Enter a value. The default is 3 seconds.</li> </ul>

**Table 3-6. Add/Modify Logical Port: Congestion Control Tab (Continued)**

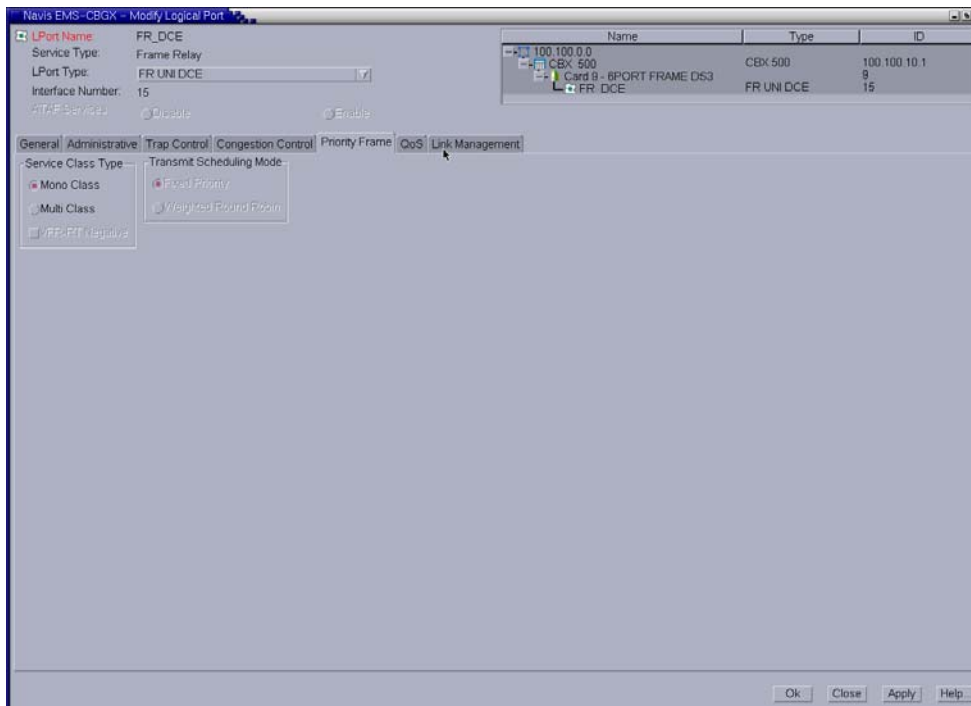
Element	Description
Call Admission Control	<p>When enabled, the port rejects a circuit creation request if there is not enough available bandwidth on that logical port.</p> <p>When disabled (default), the port attempts to create a circuit even if there is not enough available bandwidth on that logical port. For information about Bandwidth Allocation, see <a href="#">Table 3-8, “Add/Modify Logical Port: QoS Tab,”</a> on page 3-32.</p> <p><i>Note: If you disable Call Admission Control on a UNI logical port, you are effectively disabling the Call Master Connection Admission Control (CAC) function on that logical port.</i></p> <p>Changing the value for this attribute does not admin down the logical port.</p>
CIR Policing	<p>Enables or disables frame committed information rate (CIR) policing.</p> <ul style="list-style-type: none"> <li>• <i>Enabled</i> – (default) When a circuit exceeds the established CIR, the Discard Eligible (DE) bit in the Frame Relay header is set <i>on</i> for incoming frames that exceed the CIR.</li> <li>• <i>Disabled</i> – The DE bit is not changed for incoming frames.</li> </ul> <p><i>Note: Whenever the network is congested, frames with the DE bit set on are discarded first.</i></p> <p>Changing the value for this attribute does not admin down the logical port.</p>
NPC	<p>Enables or disables the Network Parameter Control (NPC) function (NNI only):</p> <ul style="list-style-type: none"> <li>• <i>Enabled</i> – Enables the NPC function, which is an aid for inter-network communication. Frames that do not conform to the traffic parameters are dropped or tagged as they come into the port.</li> <li>• <i>Disabled</i> – Disables the NPC function. All traffic, including non-conforming traffic, passes through the port.</li> </ul>
Buffer Oversubscription	<p>For the 6-Port Channelized DS3/1/0 Frame Relay card, 8-Port Subrate DS3 card and 32-Port Channelized E1 card configures the oversubscription factor (100 – 1000) for the buffers allocated for this LPort. The default is 100.</p>

**Table 3-6. Add/Modify Logical Port: Congestion Control Tab (Continued)**

Element	Description
WRED	<p>For the 6-Port Channelized DS3/1/0 Frame Relay card, configures Weighted Random Early Discard (WRED) parameters for VFR rt, VFR nrt, and UFR.</p> <ul style="list-style-type: none"> <li>• <b>Weight</b> If WRED is selected in the Congestion Control Algorithm field, determines the weight factor of the low-pass filter that calculates the WRED average queue size. Enter a positive integer from 2 to 10. This value represent a negative power of 2.</li> <li>• <b>VFR rt / VFR nrt / UFR Discard Probability</b> If WRED is selected in the Congestion Control Algorithm field, determines the packet drop probability when the average queue length is at the maximum threshold. Enter a positive integer from 2 to 10. This value represents a negative power of 2.</li> </ul> <p>For more information, see <a href="#">“Congestion Control on the 6-Port Channelized DS3/1/0 Frame Relay I/O Module”</a> on page 2-17.</p>
<b>Frame TS0 Thresholds</b>	
TS0 1	<p>Enter a value in the range 1 to 3900. The default value is 78. This value is the Frame Threshold value for the LPort with 1 TS0.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
TS0 2-3	<p>Enter a value in the range 1 to 3900. The default value is 110. This value is the Frame Threshold value for the LPort with 2 to 3 TS0s.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
TS0 4-7	<p>Enter a value in the range 1 to 3900. The default value is 149. This value is the Frame Threshold value for the LPort with 4 to 7 TS0s.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
TS0 8-16	<p>Enter a value in the range 1 to 3900. The default value is 208. This value is the Frame Threshold value for the LPort with 8 to 16 TS0s.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
TS0 17-24	<p>Enter a value in the range 1 to 3900. The default value is 267. This value is the Frame Threshold value for the LPort with 17 to 24 TS0s.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
TS0 25-32	<p>Enter a value in the range 1 to 3900. The default value is 50. This value is the Frame Threshold value for the LPort with 25 to 32 TS0s.</p> <p><b>Note:</b> <i>Applicable only to a 32-Port T1/E1 card.</i></p>
Set Default TSO Thresholds	<p>Click <i>Set Default TSO Thresholds</i> to set the default values for the thresholds.</p>

## Priority Frame Attributes for Logical Ports

The Priority Frame tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-15](#). See [“Priority Frame Quality of Service \(QoS\)”](#) on [page 2-24](#) for more information.



**Figure 3-15. Add/Modify Logical Port: Priority Frame Tab**

[Table 3-7](#) describes the fields and controls in the Priority Frame tab.

**Table 3-7. Add/Modify Logical Port: Priority Frame Tab**

Element	Description
Service Class Type	<p>Select the service class type for this logical port. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Mono-class</i> – Transmits all circuits using VFR-NRT characteristics.</li> <li>• <i>Multi-class</i> – Enables Frame Relay QoS and supports all QoS classes. The multi-class setting default transmit scheduling mode is “Fixed Priority.”</li> <li>• <i>VFR-RT Negative - (Trunk Logical Port types only)</i> The VFR-RT Negative field is available when you select the Multi-Class LPort Service Class type. Select one of the following options:                             <ul style="list-style-type: none"> <li>– <i>Disabled</i> – (default) VFR-RT PVCs from the failed trunk may not reroute and remain down; however, existing trunk bandwidth and service remain stable.</li> <li>– <i>Enabled</i> – The trunk can be oversubscribed. This option is useful when a trunk has failed, and PVCs must be rerouted to a new trunk. In this event, trunk bandwidth can become negative and delay commitments are not guaranteed, but PVCs stay up.</li> </ul> </li> </ul>
Transmit Scheduling Mode	<p>The transmit scheduling mode is available when you select Multi-class in the LPort Service Class Type field. This mode determines the transmission scheduling method to schedule transmission among the three service class types (VFR-RT, VFR-NRT, and UFR). Select the transmit scheduling mode. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Fixed Priority</i> (default) – This scheme is a fixed scheduling policy. Transmit scheduling is according to strict priority in the following order:                             <ol style="list-style-type: none"> <li>1. CFR</li> <li>2. VFR-RT</li> <li>3. VFR-NRT</li> <li>4. UFR</li> </ol> <p>With this policy, the high priority control and VFR-RT traffic are always serviced before lower priority traffic.</p> </li> <li>• <i>Weighted Round Robin</i> – CFR traffic is scheduled first, and then VFR-RT and VFR-NRT traffic is scheduled using a weighted round robin algorithm. When there is no traffic queued for CFR, VFR-RT or VFR-NRT, then UFR traffic will be transmitted. A best effort attempt is made for UFR traffic, which has the lowest priority. For information about bandwidth allocation for the UFR service class, see <a href="#">Table 3-8, “Add/Modify Logical Port: QoS Tab,” on page 3-32.</a></li> </ul>



## QoS Attributes for Logical Ports

The Add Logical Port dialog box QoS tab enables you to configure logical port Quality of Service (QoS) parameters. You can also configure SVC QoS parameters to determine the percentage of logical port bandwidth allocated to SVCs.

- Logical port QoS parameters
 

Available when you select the Multi-class LPort Service Class type (see [“Priority Frame Attributes for Logical Ports” on page 3-29](#)). To review QoS parameters and, if necessary, modify these defaults, refer to the instructions in this section.
- SVC QoS parameters
 

Enables you to set the percentage of bandwidth available for SVCs for each available class of service. To set the SVC QoS parameters, see [“Setting SVC QoS Attributes” on page 3-46](#).

This section describes how to set the logical port Quality of Service (QoS) parameters. These parameters enable you to specify the bandwidth and routing metrics (if applicable) for the various traffic service classes. By setting logical port QoS Parameters, you can allocate bandwidth for PVCs and SVCs based on their QoS services on a logical port. To limit the percentage of logical port bandwidth of SVC services, continue to [“Setting SVC QoS Attributes” on page 3-46](#).

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 may display negative bandwidth.

The service class bandwidth allocation values you enter in the QoS tab of the Add/Modify Logical Port dialog box work in conjunction with the values you enter in the Configure SVC dialog box (see [“Setting SVC QoS Attributes” on page 3-46](#)).

To set the QoS Parameters:

1. In the Add Logical Port dialog box, select the Priority Frame tab (see [“Priority Frame Attributes for Logical Ports” on page 3-29](#)), and then select the Multi-class LPort Service Class type.
2. Complete the fields described in [Table 3-7 on page 3-30](#).
3. In the Add Logical Port, select the QoS tab ([Figure 3-16](#)).

Class	Bandwidth Allocation	Fixed At %	Routing Metric	Oversubscription...
CBR/CFR	Dynamic	0	Admin Cost	100
VBR/VFR (RT)	Dynamic	0	Admin Cost	100
VBR/VFR (NRT)	Dynamic	0	Admin Cost	100
ABR/UBR	Dynamic	0	Admin Cost	100

**Figure 3-16. Add/Modify Logical Port: QoS Tab**

4. Complete the required fields described in [Table 3-8](#) for each service class.

Table 3-8 describes the fields and controls in the QoS tab.

**Table 3-8. Add/Modify Logical Port: QoS Tab**

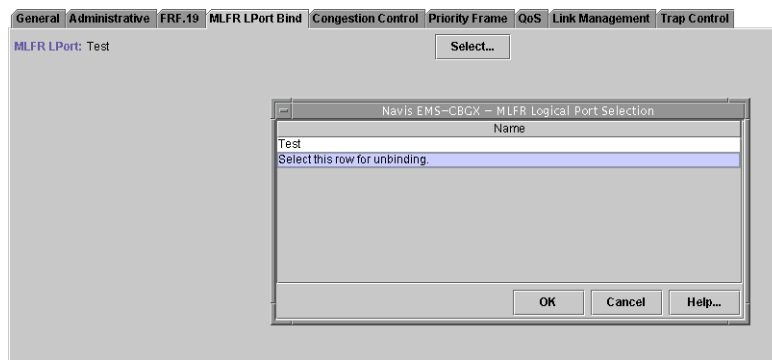
Element	Description
Bandwidth Allocation	<p>Enables you to assign bandwidth allocation values to each QoS service class. Bandwidth allocation applies only if Call Master Admission Control (CAC) is enabled during logical port configuration.</p> <p>Options include:</p> <ul style="list-style-type: none"> <li>• <i>Dynamic</i> – Enables 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.</li> <li>• <i>Fixed</i> – Specifies the percentage of bandwidth you want to reserve for the circuits of 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. When you set the VFR service class bandwidth to <i>Fixed</i>, you are specifying the maximum bandwidth to reserve for the circuits of this type of traffic. If the network requests a circuit that exceeds the fixed value, the circuit cannot be created.</li> </ul> <p>If you have service classes set to Dynamic, any remaining bandwidth percentage will be allocated to the circuits of those service classes as needed. For example, if UFR is Fixed at 55%, and the VFR classes are set to Dynamic, the bandwidth value assigned to UFR will be allocated to those circuits as requested until it cannot accommodate further UFR circuits. The remaining 45% of bandwidth will be dynamically allocated among the circuits of the two VFR service classes.</p> <p><i>Note: If VFR traffic is allowed to exceed its CIR, there is a possibility that UFR traffic will be discarded. UFR traffic is a best effort service, and cannot be guaranteed.</i></p>
Routing Metric	<p>Select a Routing Metric for each class of service. Routing metrics apply only if the port is configured as a UNI DCE or UNI DTE logical port. Options include:</p> <ul style="list-style-type: none"> <li>• <i>End-to-End Delay</i> – Measures the static delay of the logical port, which consists of both propagation and transmission delay. It is measured when the port initially comes up. It does not include queuing delays, and therefore does not account for port congestion.</li> <li>• <i>Admin Cost</i> – Measures the Administrative Cost associated with the logical port.</li> </ul> <p><i>Note: Changing the value for this attribute does not admin down the logical port.</i></p>

**Table 3-8. Add/Modify Logical Port: QoS Tab (Continued)**

Element	Description
Oversubscription (%) <i>(Optional)</i>	<p>Specify the Oversubscription percentage for each class of service (except CFR, which is set to 100% and cannot be modified). This value must be between 100% and 1000%.</p> <p>In general, you can leave these values set to 100%, since the Call Master Connection Admission Control (CAC) algorithm ensures that you can pack circuits on a port without losing data or Quality of Service. If, however, after monitoring your network, you determine that users of a particular service class are reserving more bandwidth than they are actually using, you can adjust the oversubscription values to suit your needs. By doing so, however, you may adversely impact the Quality of Service for this and lower-priority service classes.</p> <p><i>Note: Changing the value for this attribute does not admin down the logical port.</i></p>

### MLFR LPort Bind Attributes for Logical Ports

The MLFR LPort Bind tab enables you to bind an ML Member logical port to an MLFR UNI/NNI bundle logical port. To reduce bandwidth on the MLFR UNI/NNI bundle, you can also unbind ML Member logical ports from the MLFR UNI/NNI bundle logical port.

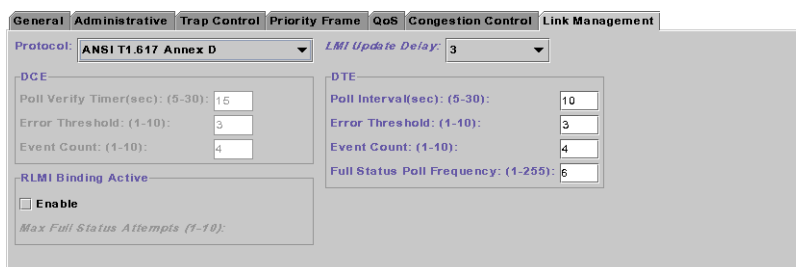


**Figure 3-17. Add/Modify Logical Port: MLFR LPort Bind Tab**

Click on the Select button to select an MLFR logical port or to unbind the MLFR member logical port from the bundle.

## Link Management Attributes for Logical Ports

The Link Management tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-18](#).



**Figure 3-18. Add/Modify Logical Port: Link Management Tab (UNI NNI)**

[Table 3-9](#) describes the fields and controls in the Link Management tab.

**Table 3-9. Add/Modify Logical Port: Link Management Tab**

Element	Description
Protocol	<p>Select the link management protocol that represents the type of Frame Relay implementation used in your network. Options include:</p> <ul style="list-style-type: none"> <li><i>ANSI T1.617 Annex D</i> – (default) The network uses DLCI 0 for link management.</li> <li><i>LMI Rev1</i> – The network uses DLCI 1023 for link management.</li> <li><i>CCITT Q.933 Annex A</i> – For international standard (European) use only. The network uses DLCI 0 for link management.</li> <li><i>Auto Detect</i> – Use this option only if the attached CPE provides the link management protocol. This logical port can then automatically detect which protocol is in use.</li> <li><i>Disabled</i> – Use this option only if the attached CPE does not support link management or if you need to disable link management for troubleshooting purposes. If you disable this option (LMI), you cannot enable RLMI.</li> </ul>

**Table 3-9. Add/Modify Logical Port: Link Management Tab**

Element	Description
DCE Poll Verify Timer (sec) <i>(DCE and NNI only)</i>	<p>Set the poll verify timer (in seconds). This field specifies the value of the T392 timer, which sets the length of time the network waits between status inquiry messages. If the network does not receive a status inquiry message within the specified number of seconds, the network records an error. The default value is 15 seconds.</p> <p><i>Note: The attached CPE must be set to a value that is less than the DCE (DTE) Poll Verify Timer.</i></p> <p>Increase this value if the DTE or DCE device has a poll frequency that is greater than or equal to the DCE or DTE Poll Verify Timer. Decrease this value if the DTE's or DCE's poll frequency is less than or equal to one-half that of the DCE or DTE Poll Verify Timer.</p>
DCE Error Threshold	<p>Specify an error threshold. This parameter is used with the DCE Event Count (N393) parameter. The Local Management protocol monitors the specified number of events for the DCE Event Count. If the number of events found in error exceeds the specified DCE Error Threshold, the link is declared inactive. The default value is 3.</p>
DCE Event Count	<p>Specify the number of events in a sliding window of events monitored by the network. An event is the receipt of a valid or invalid status inquiry message, or the expiration of the T392 timer.</p> <p>For example, use the default DCE Error Threshold value of 3 and the default DCE Event Count value of 4. If three (N392) of the last four (N393) events are found in error, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.</p> <p><i>Note: The DCE Error Threshold and the DCE 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.</i></p>

**Table 3-9. Add/Modify Logical Port: Link Management Tab**

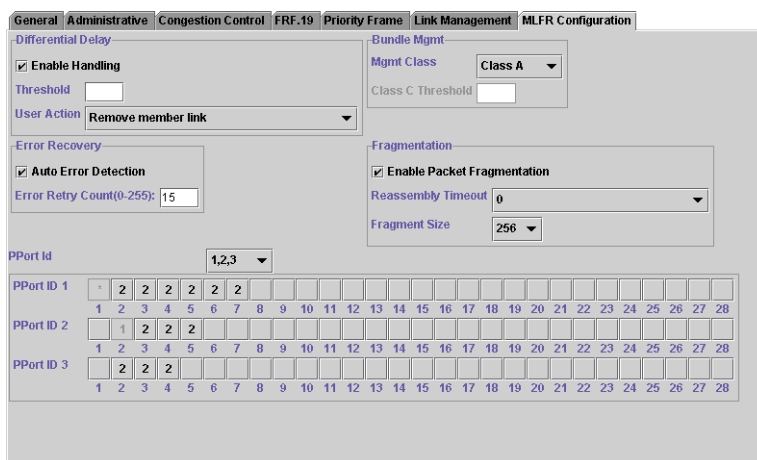
Element	Description
RLMI Binding Active	<p>Enables or disables the resilient LMI administrative state.</p> <ul style="list-style-type: none"> <li>• <i>Disabled</i> – (default) Disables RLMI.</li> <li>• <i>Enabled</i> – Enables RLMI. If you enable RLMI on a Frame Relay UNI DTE or NNI port, you can configure the RLMI Max Full Status Attempts. If you enable this option (RLMI), you cannot disable LMI.</li> </ul> <p><i>Note:</i> You cannot disable RLMI or delete a logical port if the logical port is configured in an RLMI service name binding. If the logical port is configured as a member of a “Master” RLMI service name binding, you can change the logical port type to Frame Relay UNI DTE or NNI. If the logical port is configured as a member of a “Slave” RLMI service name binding, you can change the logical port type to Frame Relay UNI DCE or NNI.</p> <p>For more information about RLMI, see <a href="#">Chapter 13, “Configuring Resilient LMI.”</a></p>
Max Full Status Attempts	<p>This field appears when the RLMI Admin Status field is set to Enabled, Select the number of RLMI full status enquiry attempts used to bring up the working interface. Enter a value greater than zero. The default is 3 attempts.</p> <p><i>Note:</i> Changing the value for this attribute does not admin down the logical port.</p> <p>For more information about RLMI, see <a href="#">Chapter 13, “Configuring Resilient LMI.”</a></p>
LMI Update Delay	<p>Set a timer from 1 to 9 seconds to enable asynchronous LMI updates. The default is 3 seconds.</p> <p>When you set this timer, the switch sends a signal (known as an <i>event</i>) to notify other network equipment (CPE) when a circuit on this logical port goes up or down. The specified time interval creates a buffer. If the circuit recovers within this period of time, no event is issued.</p> <ul style="list-style-type: none"> <li>• If you choose No Updates, the switch does not send a signal to the CPE.</li> <li>• If you choose No Delay, the switch sends an update immediately to the CPE.</li> </ul> <p>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.</p> <p><i>Note:</i> Changing the value for this attribute does not admin down the logical port.</p>
DTE Poll Interval (sec)	<p>Specify the number of seconds between the transmission of Status Enquiry messages. The default is 10 seconds.</p>

**Table 3-9. Add/Modify Logical Port: Link Management Tab**

Element	Description
DTE Error Threshold	Specify an error threshold. This parameter is used with the DTE Event 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. An event is the receipt of a valid or invalid status inquiry message, or the expiration of the T392 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 found in error, the link is declared inactive. The link remains inactive until the network receives four consecutive error-free events.  <i>Note: The DTE Error Threshold and the 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.</i>
DTE Full Status Poll Frequency	Specify the number of polling cycles between full Status Enquiry messages. The default is 6 seconds.

## MLFR Configuration Attributes for Logical Ports

The MLFR Configuration tab configures MultiLink Frame Relay (MLFR) attributes for MLFR logical ports on 6-Port Channelized DS3/1/0 Frame Relay modules. The MLFR Configuration tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-19](#).



**Figure 3-19. Add/Modify Logical Port: MLFR Configuration Tab**

[Table 3-10](#) describes the fields and controls in the MLFR Configuration tab.

**Table 3-10. Add/Modify Logical Port: MLFR Configuration Tab**

Element	Description
<b>Differential Delay</b>	
Handling	This field enables/disables differential delay monitoring. For more information see <a href="#">“Differential Delay”</a> on page 5-6. Options include: <ul style="list-style-type: none"> <li><i>Disable</i> – (default) Disables differential delay monitoring.</li> <li><i>Enable</i> – Enables differential delay monitoring.</li> </ul>
Threshold	Enter the threshold, in milliseconds, that the differential delay must exceed before the user action is taken on the member link.



**Table 3-10. Add/Modify Logical Port: MLFR Configuration Tab (Continued)**

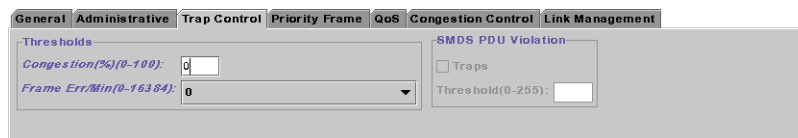
Element	Description
User Action	<p>This field appears when Handling is set to Enable. Determines the action that will be taken on a member link when the differential delay for the member exceeds the threshold. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Remove member link</i> – (default) The link is taken out of service.</li> <li>• <i>Stop member link traffic and restore</i> – The link stops transmitting outgoing traffic, and resumes transmitting traffic when the delay has been corrected.</li> <li>• <i>Stop member link traffic but do not restore</i> – The link stops transmitting outgoing traffic, but does not resume transmission of traffic when the delay has been corrected.</li> <li>• <i>No action</i> – No action on the link is taken when the threshold is exceeded. (SNMP traps are still generated when the threshold is exceeded).</li> </ul>
<b>Bundle Management</b>	
Mgmt Class	<p>Determines how the MLFR bundle operational status will be set if individual member links are inactive. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Class A</i>– (default) The MLFR bundle is up as long as at least one of its members is active and operational.</li> <li>• <i>Class B</i>– The MLFR bundle is up only if all of its members are active and operational.</li> <li>• <i>Class C</i>– The MLFR bundle is up as long as a minimum number of its members are active and operational. You specify this minimum value in the Class C Threshold field.</li> </ul>
Class C Threshold	<p>This field appears when Mgmt is set to Class C. Enter a value for the minimum number of member links that must be active and operational in order for the MLFR bundle to be up.</p>
<b>Fragmentation</b>	
Packet Fragmentation	<p>Packet fragmentation partitions frames into equal lengths before sending data over the MLFR bundle so that member links can be evenly loaded with data. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Disables packet fragmentation.</li> <li>• <i>Enable</i> – Enables packet fragmentation. You specify the fragment size in the Fragment Size field.</li> </ul>
Reassembly Timeout (msec)	<p>Select the length of time that frame fragments in a packet will wait at the destination for missing fragments before the packet is dropped. Values are available from 0 to 140 milliseconds, in increments of 10.</p>

**Table 3-10. Add/Modify Logical Port: MLFR Configuration Tab (Continued)**

Element	Description
Fragment Size	This field appears when Packet fragmentation is set to Enable. Select a value for the length of the fragments into which frames are partitioned. The available choices are 128, 256, and 512.
PPort Channels	Next to each PPort ID appear the DS1 channels that can be bound to the MLFR bundle. Any channels that are already bound to an MLFR bundle display the bundle ID.  To bind a channel to the current MLFR bundle, click on the channel. A maximum of 12 channels can be bound to an MLFR bundle.
<b>Error Recovery</b>	
Auto Error Detection	Auto error detection identifies errors coming into the MLFR bundle logical port, such as lost events, and shuts down the logical port connection.  Select one of the following: <ul style="list-style-type: none"> <li>• <i>Enable</i> – (default) Enables auto error detection.</li> <li>• <i>Disable</i> – Disables auto error detection.</li> </ul> (This setting is overridden at the circuit level by the Auto Error Detection setting for the specific circuit. See “Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint” on page 5-26.)
Error Retry Count	If you enabled Auto Error Detection, specify the number of retries that should be attempted before the connection is shut down. Enter a value between 0 and 255. The default value is 15.  (This setting is overridden at the circuit level by the Error Retry Count setting for the specific circuit. See “Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint” on page 5-26.)

### Trap Control Attributes for Logical Ports

The Trap Control tab of the Add/Modify Logical Port dialog box is shown in [Figure 3-18](#).



**Figure 3-20. Add/Modify Logical Port: Trap Control Tab**

**Table 3-11** describes the fields and controls in the Trap Control tab.

**Table 3-11. Add/Modify Logical Port: Trap Control Tab**

Element	Description
Congestion (%)	<p>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.</p> <p>Adjust the entered value according to how sensitive this port needs to be to network congestion. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Low</i> – Generates a trap at the first sign of congestion.</li> <li>• <i>High</i> – Generates traps for serious network congestion.</li> <li>• <i>Zero</i> – (default) Disables congestion threshold. If you enter zero, no traps are generated for this logical port.</li> </ul>
Frame Err/Min Threshold	<p>Enter a value from 0 to 16384 to configure the threshold of frame errors on this logical port. If the number of frame errors received in one minute exceeds the specified number, a trap is sent to the NMS.</p> <p>Adjust this value according to how sensitive this port needs to be to frame errors. A lower value will make the port sensitive to frame errors. A high value will generate traps when a significant number of frame errors occur within a one-minute period.</p> <p>A value of zero (default) disables this feature, which prevents traps from being generated for this logical port.</p>
SMDS PDU Violation Traps <i>(Frame Relay OPTimum and Direct Trunks only)</i>	<p>Select one of the following options to enable or disable SMDS PDU violation traps. An SMDS PDU violation can be either an SIP 3 SMDS address failure or an invalid DXI2 frame header. These errors signify that incoming frames are bad, indicating problems with the CPE configuration.</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Turns off PDU violation traps.</li> <li>• <i>Enable</i> – Issues traps for PDU violations.</li> </ul> <p>Note: This attribute is available only for Frame Relay Direct line and Frame Relay Optimum trunks on B-STDx switches for cards with SMDS capability.</p>

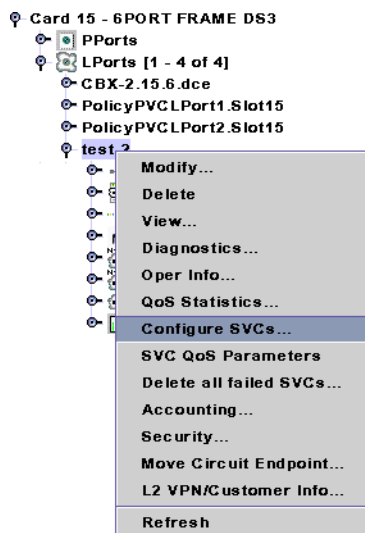
**Table 3-11. Add/Modify Logical Port: Trap Control Tab (Continued)**

Element	Description
SMDS PDU Violation Threshold (0-255)  <i>(Frame Relay OPTimum and Direct Trunks only)</i>	Specify the number of protocol data unit (PDU) violations that can occur before a trap is sent to the NMS. The software increments a counter every time a Switched Multimegabit Data Service (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: <ul style="list-style-type: none"> <li>• <i>Low</i> – Sensitive to SMDS PDU violations.</li> <li>• <i>High</i> – Issue traps only when there is a significant number of SMDS PDU violations.</li> </ul> Note: This attribute is available only for Frame Relay Direct line and Frame Relay Optimum trunks on B-STDx switches for cards with SMDS capability.

## Configuring Logical Ports for Use With SVCs

If you plan to use SVCs in your network, you must perform additional configuration. To set SVC parameters:

1. In the Switch tab, expand either the Cards or LPorts node and locate the node for the logical port you want to configure.
2. Right-click on the LPort node, and select Configure SVCs from the popup menu.



**Figure 3-21. Configuring LPort SVC Parameters in the Switch Tab**

The Configure SVC dialog box (Figure 3-22) is displayed. Refer to the following sections to configure the tabs:

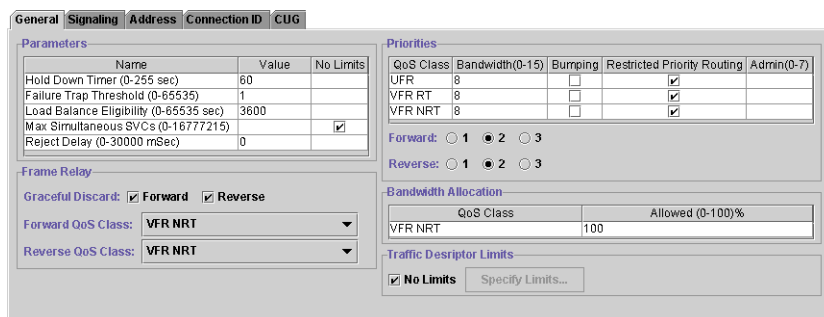
- **“General Attributes for SVCs” on page 3-43**  
 Enables you to configure general parameters, Frame Relay settings, priorities, bandwidth allocation, and traffic descriptor limits.
- **“Signaling Attributes for SVCs” on page 3-49**  
 Enables you to define signaling parameters. The fields on this dialog box also enable you to configure forward and reverse QoS class, graceful discard, signaled parameter defaults, and logical port signaling tuning parameters.
- **“Address Attributes for SVCs” on page 3-52**  
 Enables you to define various SVC screening and handling parameters for each logical port on the switch.
- **“Connection ID Attributes for SVCs” on page 3-56**  
 Enables you to assign the DLCI start and stop values to limit the DLCI range available to SVCs at this logical port.
- **“CUG Attributes for SVCs” on page 3-56**  
 Enables address-based or port-based Closed User Groups (CUGs).

For more information about SVCs, see the following chapters:

- **Chapter 14, “Configuring Switched Virtual Circuit (SVC) Parameters”**
- **Chapter 15, “Closed User Groups”**
- **Chapter 16, “Port Security Screening”**

## General Attributes for SVCs

The General tab enables you to configure general parameters, Frame Relay settings, priorities, bandwidth allocation, and traffic descriptor limits.



**Figure 3-22. Configure SVC Dialog Box: General Tab**

**Table 3-12** describes the parameters in the General tab. Although you can modify the fields in the Parameters section, Lucent recommends you use the default parameters.

**Table 3-12. Configure SVC Dialog Box: General Tab**

Element	Description
Hold Down Timer	<p>Enter the number of seconds to wait before the network initiates call clearing when a trunk has gone down. If you enter 0, the network clears the SVC immediately upon detection of a trunk outage.</p> <p><i>Note: Changing the value for this attribute does not admin down the logical port.</i></p>
Failure Trap Threshold	<p>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.</p> <p>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 expires. If you change the threshold value to 100, it means that to trigger a trap, 100 SVC failures must occur in a 15-minute window. If you enter 0, the switch never generates a failure trap.</p>
Load Balance Eligibility	<p>Enter the number of seconds an SVC must be established before a call 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.</p>
Max Simultaneous SVCs	<p>The maximum number of SVCs allowed on the logical port. Originating and terminating SVCs are summed for this purpose.</p> <p>Enter a value between 0-16777215 or accept the default (no limit).</p>
Reject Delay	<p>Enter the number of milliseconds to wait for a RELEASE PDU after a SETUP PDU has been received. The default value is 30000. The range of values is 0 - 30000.</p>
Graceful Discard	<p><i>Enable</i> (default) or <i>Disable</i> graceful discard for the ingress or egress direction for Frame Relay SVCs originating on this logical port.</p> <p>If you enable Graceful Discard in both directions, the rate enforcement is disabled for all SVCs that originate on the logical port.</p>
Forward QoS Class	<p>Select a QoS class for this logical port. For more information see <a href="#">Table 2-14 on page 2-24</a>. Options include:</p> <ul style="list-style-type: none"> <li>• VFR (Non Real Time) (default)</li> <li>• VFR (Real Time)</li> <li>• UFR</li> </ul>

**Table 3-12. Configure SVC Dialog Box: General Tab (Continued)**

Element	Description
Reverse QoS Class	Select a QoS class for this logical port. For more information see <a href="#">Table 2-14 on page 2-24</a> . Options include: <ul style="list-style-type: none"> <li>• VFR (Non Real Time) (default)</li> <li>• VFR (Real Time)</li> <li>• UFR</li> </ul>
Priorities	Enables you to define priorities for each of the QoS classes. See <a href="#">“Setting SVC Priorities” on page 3-45</a> .
Bandwidth Allocation	Enables you to limit the bandwidth (per SVC category) that a single SVC consumes. See <a href="#">“Setting SVC QoS Attributes” on page 3-46</a> .
Traffic Descriptor Limits	The Traffic Descriptor Limits attributes enable you to configure the VFR-RT and VFR-NRT maximum traffic descriptor values for each service class. See <a href="#">“Setting Traffic Descriptor Limits” on page 3-47</a> .

### Setting SVC Priorities

You can assign bandwidth priority and bumping eligibility to SVCs based on ingress QoS class. The network routes SVCs originating from this logical port according to the SVC ingress QoS class you select. The priorities settings also enable you to assign forward and reverse circuit discard priorities to SVCs that originate on a specific logical port.

For each of the QoS queues, define priorities using the information provided in [Table 3-13](#).

**Table 3-13. Configure SVC Dialog Box: General Tab Priorities Settings**

Element	Description
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 <a href="#">Appendix C, “Priority Routing,”</a> for more information.

**Table 3-13. Configure SVC Dialog Box: General Tab Priorities Settings**

Element	Description
Bumping Eligibility	<p>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.</p> <p>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).</p> <p>Bumping eligibility is valid only for non-real time circuits, based on QoS classes. Real time circuits ignore this setting.</p> <p>See <a href="#">Appendix C, “Priority Routing,”</a> for more information.</p>
Restricted Priority Routing	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enabled</i> – (default) Provision new SVCs at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings.</li> <li>• <i>Disabled</i> – Use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits.</li> </ul> <p>See <a href="#">Appendix C, “Priority Routing,”</a> for more information.</p>
Forward Priority	<p>Specify a value from 1 through 3, where 2 is the default. The value sets the circuit discard priority in the ingress direction for SVCs that originate at this logical port.</p>
Reverse Priority	<p>Specify a value from 1 through 3, where 2 is the default. The value sets the circuit discard priority in the egress direction for SVCs that originate at this logical port.</p>

### Setting SVC QoS Attributes

The SVC QoS feature enables you to limit the percentage of logical port bandwidth that SVCs are allowed to consume. This feature is useful 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 can set the percentage of bandwidth available for SVCs for each available class of service.

The values you enter in the Configure SVC dialog box work in conjunction with the service class bandwidth allocation values you enter in the QoS tab of the Add/Modify Logical Port dialog box (see [“QoS Attributes for Logical Ports” on page 3-31](#)).



In the QoS tab of the Add/Modify Logical Port 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 40% for VFR-NRT (for example), the logical port bandwidth available for SVCs would be a maximum of 40%. You can limit the VFR-NRT bandwidth further by entering an allowed value in the Bandwidth Allocation part of the Configure SVC dialog box (see [Figure 3-22 on page 3-43](#)).

If you accept the default 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 an allowed value lower than 100% in the Bandwidth Allocation settings. For example, if you want to limit VFR-NRT SVCs to 50% of the logical port bandwidth available to VFR-NRT connections, enter 50% in the Allowed (%) field.

The values entered in the Configure SVC dialog box 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 Allowed (%) field (for the appropriate class of service) of the Configure SVC dialog box.

In the General tab, complete the Bandwidth Allocation settings as described in [Table 3-22](#), entering values between 0-100%. The default is 100%.

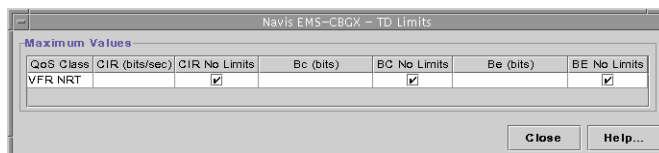
- If you configured the LPort Service Class type as mono-class, enter a percentage value in the VFR-NRT field.
- If you configured the LPort Service Class type as multi-class, enter a percentage value in the VFR-RT, VFR-NRT, and UFR fields.

### Setting Traffic Descriptor Limits

The Traffic Descriptor Limits attributes enable you to configure the VFR-RT and VFR-NRT maximum traffic descriptor values for each service class.

- If you configured the LPort Service Class type as mono-class, enter a value in the VFR-NRT field.
- If you configured the LPort Service Class type as multi-class, enter values in the VFR-RT and VFR-NRT fields.

SVC TD limits qualify SVCs in the ingress and egress direction at this logical port. The No Limits check box is enabled by default. To set limits, disable the No Limits check box and click on the Specify Limits button.



**Figure 3-23. SVC TD Limits Dialog Box**

In the TD Limits dialog box, configure the values as shown in [Table 3-14](#).

**Table 3-14. TD Limits Dialog Box**

Element	Description
<b>SVC Maximum Traffic Descriptors: VFR-RT (multi-class only)</b>	
CIR (bits/sec)	The maximum CIR, in bits per second, that may be signaled for a VFR-RT SVC. This object qualifies the outgoing CIR signaled at this ingress logical port and the incoming CIR signaled at this egress logical port.  Enter a value between 0-2147483647. The default value is “No Limit” (2147483647).
Bc (bits)	The maximum Bc, in bits, that may be signaled for a VFR-RT SVC. This object qualifies the outgoing Bc signaled at this ingress logical port and the incoming Bc signaled at this egress logical port.  Enter a value between 0-2147483647. The default value is “No Limit” (2147483647).
Be (bits)	The maximum Be, in bits, that may be signaled for a VFR-RT SVC. This object qualifies the outgoing Be signaled at this ingress logical port and the incoming Be signaled at this egress logical port.  Enter a value between 0-2147483647. The default value is “No Limit” (2147483647).
<b>SVC Maximum Traffic Descriptors: VFR-NRT (mono-class and multi-class)</b>	
CIR (bits/sec)	The maximum CIR, in bits per second, that may be signaled for a VFR-NRT SVC. This object qualifies the outgoing CIR signaled at this ingress logical port and the incoming CIR signaled at this egress logical port.  Enter a value between 0-2147483647. The default is “No Limit” (2147483647).
Bc (bits)	The maximum Bc, in bits, that may be signaled for a VFR-NRT SVC. This object qualifies the outgoing Bc signaled at this ingress logical port and the incoming Bc signaled at this egress logical port.  Enter a value between 0-2147483647. The default is “No Limit” (2147483647).

**Table 3-14. TD Limits Dialog Box**

Element	Description
Be (bits)	<p>The maximum Be, in bits, that may be signaled for a VFR-NRT SVC. This object qualifies the outgoing Be signaled at this ingress logical port and the incoming Be signaled at this egress logical port.</p> <p>Enter a value between 0-2147483647. The default is “No Limit” (2147483647).</p>

## Signaling Attributes for SVCs

The Signaling tab enables you to configure SVC signaling parameters. You can enable Q.922 signaling for Frame Relay SVCs, and set logical port parameter defaults that the customer premise equipment (CPE) uses when it fails to signal optional parameters (for example, CIR).



**Figure 3-24. Configure SVC Dialog Box: Signaling Tab**

**Table 3-15** describes the parameters in the Signaling tab.

**Table 3-15. Configure SVC Dialog Box: Signaling Tab**

Element	Description
Enable Signaling	<p>Enable Q.922 signaling for Frame Relay SVCs to function on the switch. The default value for this field is Disabled.</p> <p>For more information about Frame Relay SVCs and Q.922 Signaling, see <a href="#">Chapter 14, “Configuring Switched Virtual Circuit (SVC) Parameters.”</a></p>
CIR	<p>Specifies the Committed Information Rate in the ingress and egress directions in case one is not signaled.</p> <p>Enter a value between 0-2047000000. The default is 0.</p>
Bc	<p>Specifies the Committed Burst size in the ingress and egress directions in case one is not signaled.</p> <p>Enter a value between 0-2147483632. The default is 0.</p>

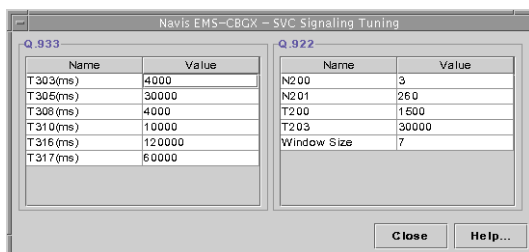
**Table 3-15. Configure SVC Dialog Box: Signaling Tab (Continued)**

Element	Description
Be	Specifies the Excess Burst size in the ingress and egress directions in case one is not signaled. Enter a value between 0-2147483632. The default is 0.
Max Frame Size	Specifies the maximum Frame Mode Information Field (FMIF) size in the ingress and egress directions in case one is not signaled. Enter a value between 0-8192. The default is 8192.
Tuning Parameters	Displays the Set Logical Port Signaling Tuning Parameters dialog box. This dialog box enables you to view defaults and reset signaling protocol timers and counters for a logical port. See <a href="#">“Setting SVC Signaling Tuning Attributes” on page 3-50</a> .

### Setting SVC Signaling Tuning Attributes

To configure SVC signaling tuning parameters, click on the Tuning Parameters button in the Signaling tab of the Configure SVC dialog box.

These tuning parameters enable you to view defaults and reset signaling protocol timers and counters for a logical port. You must set the logical port admin status to Down before you set the tuning parameters.



**Figure 3-25. SVC Signaling Tuning Dialog Box**

**Table 3-16** describes the protocol timer and counter fields in the SVC Signaling Tuning dialog box.

**Table 3-16. SVC Signaling Tuning Dialog Box**

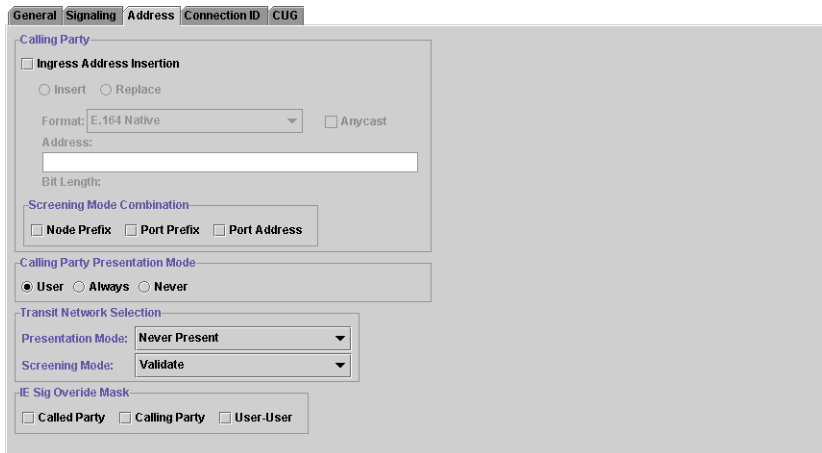
Element	Description
<b>Q.933</b>	
T303 (ms)	How long to wait for a response after a SETUP protocol data unit (PDU) has been sent. The default is 4000ms.
T305 (ms)	How long to wait for a response after a DISCONNECT PDU has been sent. The default is 30000ms.

**Table 3-16. SVC Signaling Tuning Dialog Box (Continued)**

Element	Description
T308 (ms)	How long to wait for a response after a RELEASE PDU has been sent. The default is 4000ms.
T310 (ms)	How long to wait for the next response after a CALL PROCEEDING PDU has been received. The default is 10000ms.
T316 (ms)	How long to wait for a response after a RESTART PDU has been sent. The default is 120000ms.
T317 (ms)	How long to wait for the internal clearing of the call after RESTART PDU has been received. The default is 60000ms.
<b>Q.922</b>	
N200	How many times to retransmit an unacknowledged frame. The default is 3.
N201	The maximum number of octets in an Information field. The default is 260.
T200 (ms)	How long to wait before retransmitting an unacknowledged frame. The default is 1500.
T203 (ms)	The maximum time allowed without frames being exchanged. The default is 30000.
Window Size	The maximum number of sequentially numbered unacknowledged I frames. The default is 7 frames.

## Address Attributes for SVCs

The Address tab enables you to define various SVC screening and handling parameters for each logical port on the switch.



**Figure 3-26. Configure SVC Dialog Box: Address Tab**

Table 3-17 describes the fields and buttons in the Address tab.

**Table 3-17. Configure SVC Dialog Box: Address Tab**

Element	Description
Ingress Address Insertion	<p>Specifies how the logical port handles the calling party address for ingress SVCs.</p> <ul style="list-style-type: none"> <li>• <i>Disabled</i> — The logical port does not insert or replace the calling party address. If you set the Insertion Mode field to Disabled, skip to <b>Calling Party Presentation Mode</b>.</li> <li>• <i>Insert</i> — 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. With this option, the 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.</li> <li>• <i>Replace</i> — When the logical port receives an SVC request and 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. This effectively disables calling party screening, because Calling Party Insertion Address field is always considered valid.</li> </ul> <p><i>Note:</i> For calling party screening to occur, set Insertion Mode to <i>Disabled</i> or <i>Insert</i>.</p> <p>Select the appropriate SVC Port Address Format. See <b>Chapter 14, “Configuring Switched Virtual Circuit (SVC) Parameters,”</b> for information about Native E.164 and X.121 addresses.</p> <p>Note that the calling party insertion address is not used to route calls to this port. To use the calling party insertion address to route calls to this port, configure the address (or a prefix corresponding to the address) on this port. For more information, see <b>“Configuring Port Addresses” on page 14-16.</b></p>

**Table 3-17. Configure SVC Dialog Box: Address Tab (Continued)**

Element	Description
Screening Mode Combination	<p>Select one or more of the Screening Mode options. 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).</p> <ul style="list-style-type: none"> <li>• <i>Node Prefix</i> — Screens the calling party against all of the configured node prefixes. If a match is found, the screen is successful.</li> <li>• <i>Prefix</i> — Screens the calling party against all of the configured port prefixes. If a match is found, the screen is successful.</li> <li>• <i>Address</i> — Screens the calling party against all of the configured port addresses. If a match is found, the screen is successful.</li> </ul> <p><i>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.</i></p>
Calling Party Presentation Mode	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>User</i> — Include the calling party address based on the Presentation Indicator in the SETUP message of the user's SVC request.</li> <li>• <i>Always</i> — Always include the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's SVC request.</li> <li>• <i>Never</i> — Never include the calling party address on outgoing calls, regardless of the Presentation Indicator in the SETUP message of the user's SVC request.</li> </ul>



**Table 3-17. Configure SVC Dialog Box: Address Tab (Continued)**

Element	Description
Transit Network Selection	<p>For the Presentation Mode, select the egress presentation mode for the selected logical port. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Never Present</i> – (default) Never signal TNS in egress SVC requests.</li> <li>• <i>Present Signaled TNS Only</i> – Signal TNS in egress SVC requests only if TNS was signaled by the user in the ingress SVC request.</li> <li>• <i>Signaled or Source Default</i> – 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.</li> </ul> <p><i>Note: Network IDs that do not match the adjacent network ID (see the Adjacent Network field in <a href="#">Table 14-7 on page 14-21</a>) 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 (as if presentation mode were Never).</i></p> <p>For the Screening Mode, select the screening mode for the selected logical port. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Ignore</i> – Ignore the signaled TNS.</li> <li>• <i>Accept</i> – Always accept the signaled TNS.</li> <li>• <i>Validate</i> – (default) Screens the signaled TNS and ignores it if there is no match.</li> </ul>
IE Sig Override Mask	<p>Enter a value to prevent the incoming SVC ATM Adaptation Layer (AAL) information element (IE) parameter from overriding the logical port setting. The default value is 0 (zero). The range of values is 0 - 2147483647 (mask bits).</p>

## Connection ID Attributes for SVCs

The SVC Connection ID Range attributes enable you to configure the DLCI start and stop range for SVC allocation (unless the allocation is for a PVC).



**Figure 3-27. Configure SVC Dialog Box: Connection ID Tab**

**Table 3-18** describes the parameters in the Connection ID tab.

**Table 3-18. Configure SVC Dialog Box: Connection ID Tab**

Element	Description
DLCI Start (16-1006)	The lowest DLCI to be allocated for SVCs, unless otherwise allocated to a PVC. The value must be less than or equal to the DLCI Stop value.  Enter a value between 16-1006. The default is 16.
DLCI Stop (16-1006)	The highest DLCI to be allocated for SVCs, unless otherwise allocated to a PVC. The value must be greater than or equal to the DLCI Start value.  Enter a value between 16-1006. The default is 1006.

## CUG Attributes for SVCs

The CUG tab allows you to enable address-based or port-based Closed User Groups (CUGs). For more information about CUGs, see [Chapter 15, “Closed User Groups.”](#)



**Figure 3-28. Configure SVC Dialog Box: CUG Tab**

**Table 3-19** describes the parameters in the CUG tab.

**Table 3-19. Configure SVC Dialog Box: CUG Tab**

Element	Description
Mode	<p>Allows you to enable address-based or port-based CUG. Select one of the following options</p> <ul style="list-style-type: none"> <li>• <i>Terminate</i> (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.</li> <li>• <i>Disabled</i> – Disables CUG.</li> <li>• <i>Signal</i> – The port signals the port-based CUG interlock code at the FR UNI or NNI.</li> </ul>
Default Type	<p>The type of default CUG configured on this logical port for port-based CUG. Options include:</p> <ul style="list-style-type: none"> <li>• <i>None</i> (default)</li> <li>• <i>E.164</i></li> <li>• <i>DNIC</i></li> <li>• <i>AESA</i></li> </ul>
Incoming Access	<p>Specifies how egress calls from non-CUG users or users of a different CUG are handled. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – Accepts calls from users that do not belong to the same CUG.</li> <li>• <i>Disable</i> – (default) Rejects calls from users that do not belong to the same CUG.</li> </ul>
Outgoing Access	<p>Specifies how ingress calls to non-CUG users or users of a different CUG are handled. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – Allows calls to users that do not belong to the same CUG.</li> <li>• <i>Disable</i> – (default) Blocks calls to users that do not belong to the same CUG.</li> </ul>
Interlock Code	<p>The Interlock Code for the default CUG configured on this logical port. E.164 and DNIC interlock codes are typically 13 numerical digits encoded as T.50 (ASCII) characters; however, interlock code lengths of 1-13 are allowed.</p> <p>AESA interlock codes are typically 24 binary octets where the first 20 resemble an AESA; however, interlock code lengths of 1-24 are allowed.</p>

## Defining Frame Relay OPTimum PVC Trunk Logical Ports

To configure a Frame Relay OPTimum trunk, you must first configure either a UNI-DTE feeder or a Frame Relay NNI logical port on the same physical port.



**Note** – You cannot define a trunk logical port on a 4-Port Channelized T1/E1 module or a 32-Port Channelized T1/E1 FR/IP module.

---

Use the following sequence to configure an OPTimum trunk:

1. Configure the physical port you want to use for the OPTimum trunk (refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*).
2. Configure a Frame Relay DTE or NNI (“**Defining Frame Relay UNI DCE/DTE or NNI LPorts**” on page 3-10) logical port on this physical port, and assign this logical port a minimum amount of bandwidth.
3. Follow the instructions in this section to configure a Frame Relay OPTimum trunk logical port. You can assign all remaining bandwidth to the logical port.

### About DLCI Numbers

A data link connection identifier (DLCI) number is a 10-bit address that identifies PVCs. This DLCI number corresponds to the DLCI number the Frame Relay trunk uses to access the PDN. The PDN recognizes this as a normal PVC carrying user traffic.

Depending on your link management type, use the guidelines in [Table 3-20](#) to define DLCI numbers.

**Table 3-20. DLCI Number Guidelines**

DLCI Number Range	Description
0-15	Reserved
16-991	Available for all link management types
16-1007	Available for LMI Rev 1 only
1008-1023	Reserved

## Defining the OPTimum PVC Trunk

To define a logical port as a Frame Relay OPTimum PVC trunk:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, right-click on the LPorts node and select Add from the popup menu.
4. In the Add Logical Port dialog box (Figure 3-5 on page 3-6), complete the fields described in Table 3-21.

**Table 3-21. Add Logical Port Type (OPTimum PVC Trunk)**

Element	Description
Service Type	Select Frame Relay.
LPort Type	Select FR OPTimum PVC Trunk.
DLCI	Enter a data link connection identifier (DLCI) number that corresponds to the DLCI number the Frame Relay trunk uses to access the PDN. The PDN recognizes this as a normal PVC carrying user traffic. For more information, see “About DLCI Numbers” on page 3-58.

5. In the Add Logical Port dialog box, complete the following tabs:
  - General attributes (see page 3-12)
  - Administrative attributes (see page 3-15)
  - Congestion Control attributes (see page 3-24)



**Note** – Set the congestion control attributes on the feeder logical port only. You cannot define the threshold attributes on the OPTimum trunk logical port.

- Priority Frame attributes (see page 3-29)
  - QoS parameters (see page 3-31)
  - Link Management attributes (see page 3-34)
  - Trap Control attributes (see page 3-40)
6. When you have configured the logical port, click OK.

# Defining Encapsulation FRAD, Direct Line Trunk, and PPP Logical Ports

This section describes how to define the following types of logical ports:

- **Encapsulation FRAD Services** — Configure a logical port to perform Frame Relay encapsulation/de-encapsulation for the HDLC/SDLC-based protocol.



---

**Note** – You cannot define an Encapsulation FRAD logical port type on the 8-Port Subrate DS-3 FR/IP IOM or 6-Port Channelized DS3/1/0 IOM6.

---

- **Direct Line Trunk Services** — Configure the logical port for a trunk connection to another Lucent switch.
- **Point-to-Point Protocol**— Configure the logical port to enable a configured Point-to-Point Protocol (PPP) DTE device to communicate with another DTE device configured for Frame Relay and encapsulating multiprotocols, according to RFC 1490. This configuration enables you to define a single circuit between the two devices. PPP is supported on the following modules:
  - 8-Port Universal IOPA (V.35, X.21)
  - 4-Port Unchannelized T1/E1 IOPA
  - 4-Port Channelized T1/E1 IOPA
  - 10-Port DSX-1 IOPA
  - 2-Port HSSI IOPB
  - 12-Port Unchannelized E1 IOPB
  - 1-Port Channelized DS3 IOPB
  - 1-Port Channelized DS3/1/0 IOPB
  - 4-Port Channelized DS3/1 FR/IP IOM2 and DS3/1/0 FR/IP IOM2
  - 6-Port DS3 FR/IP IOM2
  - 32-Port Channelized T1/E1 FR/IP IOM
  - 6-Port Channelized DS3/1/0 Frame Relay IOM

To define encapsulated FRAD, direct line trunk, and PPP services:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, right-click on the LPorts node and select Add from the popup menu.

4. In the Add Logical Port dialog box (Figure 3-5 on page 3-6), complete the fields described in Table 3-22.

**Table 3-22. Add Logical Port Type (Other)**

Element	Description
Service Type	Select Other.
LPort Type	Select a logical port type from the list.
LPort ID <i>(4-Port Channelized T1, E1, and 32-Port Channelized T1/E1 FR/IP modules only)</i>	<p>For the following modules, enter a number that uniquely identifies this logical port on the physical port. For all other modules, the LPort ID is a read-only field that automatically defaults to 1.</p> <ul style="list-style-type: none"> <li>• For a 4-Port Channelized T1 module, enter a number between 1 and 24.</li> <li>• For a 4-Port Channelized E1 module, enter a number between 1 and 30.</li> <li>• For a 32-Port Channelized T1/E1 FR/IP module, the number you specify depends on the operation mode (T1 or E1) selected in the Modify Card dialog box, as follows: <ul style="list-style-type: none"> <li>– <b>T1 mode</b> – If the module is configured in T1 mode, enter a number between 1 and 24 for the 24 DS0 channels available per physical port in T1 Mode.</li> <li>– <b>E1 mode</b> – If the module is configured in E1 mode, enter a number between 1 and 31 for the 30 TSO channels available per physical port in E1 Mode.</li> </ul> </li> </ul> <p>Refer to the <i>Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i> for more information on setting the operation mode on the Modify Card dialog box.</p>

5. In the Add Logical Port dialog box, complete the following tabs:
  - General attributes (see [page 3-12](#))
  - Administrative attributes (see [page 3-15](#))
  - Congestion Control attributes (see [page 3-24](#))
  - Priority Frame attributes (see [page 3-29](#))
  - Trap Control attributes (see [page 3-40](#))
6. When you have configured the logical port, click OK.

If you are defining PPP logical ports, proceed to the next section, “[Completing the PPP Logical Port Configuration.](#)”

## Completing the PPP Logical Port Configuration

When you configure PPP logical ports, you can define authentication attributes and other options for these ports.

### Defining Authentication Attributes

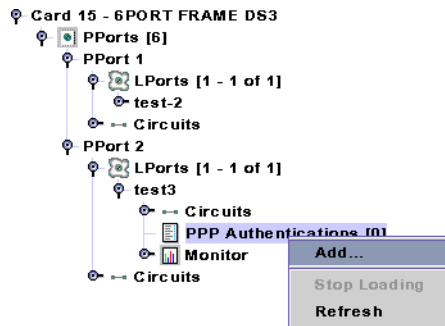
Console authentication is a domain security feature that is handled by the Remote Access Dial-In User Service (RADIUS) protocol. Before you can define authentication attributes for PPP ports, you must add the authentication domain and configure the RADIUS server parameters. For more information about adding an authentication domain, refer to the *Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

To define authentication attributes for the two PPP ports:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, expand the LPorts node.
4. Under the LPorts node, expand the LPort you want to configure.

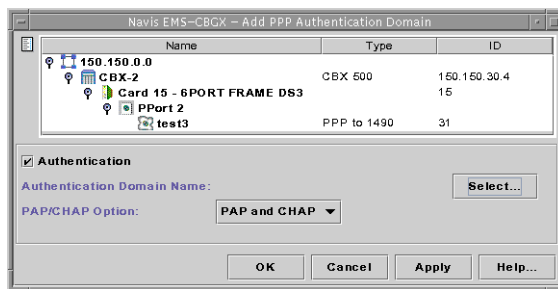


- Right-click on the PPP Authentications class node and select Add from the pop-up menu, as shown in [Figure 3-29](#).



**Figure 3-29. Configuring PPP Authentications**

The Add PPP Authentication Domain dialog box ([Figure 3-30](#)) is displayed.



**Figure 3-30. Add PPP Authentication Domain Dialog Box**

- Fill in the fields described in [Table 3-22](#).

**Table 3-23. Add PPP Authentication Domain Dialog Box**

Element	Description
Authentication	Select Enable to enable the port to authenticate the connection to the RADIUS server. Refer to the <i>Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000</i> for more information about RADIUS.
Authentication Domain Name	Select the Authentication Domain. Each switch that has access to a RADIUS server has an Authentication Domain name. Refer to the <i>Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000</i> for more information about RADIUS.
PAP/CHAP Option	Select PAP only, CHAP only, or PAP & CHAP to establish Password Authentication Protocol, Challenge Handshake Authentication Protocol, or a combination of PAP and CHAP.

7. Click on the Select button.

The PPP Authentication Domain dialog box (Figure 3-31) is displayed.



**Figure 3-31. Add Authentication Domain Dialog Box**

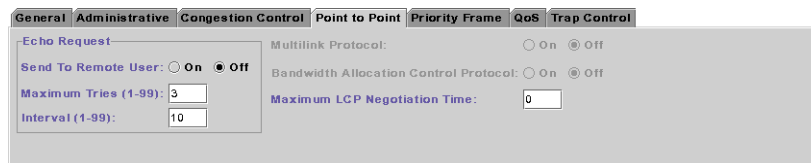
If no authentication domains are available, refer to the *Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for information about adding an authentication domain and configuring the RADIUS server parameters.

8. Select the authentication domain the LPort should use, and click OK.
9. In the Add PPP Authentication Domain dialog box, click OK.

### Defining Point-to-Point Options for a PPP LPort

To define the Point-to-Point options for a PPP logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a PPP logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, expand the LPorts node.
4. Under the LPorts node, right-click on the PPP logical port you want to configure, and select Modify from the popup menu.
5. The Modify Logical Port dialog box (Figure 3-7 on page 3-9) is displayed.
6. In the Point-to-Point tab (Figure 3-32), complete the fields described in Table 3-24.



**Figure 3-32. Add/Modify Logical Port: Point-to-Point Tab**

**Table 3-24. Add/Modify Logical Port: Point-to-Point Tab**

Element	Description
Echo Request Send To Remote User	Select On to send keep-alive packets to the remote user.
Echo Request Maximum Tries	Enter a number from 1 to 99 that represents the maximum number of keep-alive packets sent to the remote user.
Echo Request Interval	Enter a number from 1 to 99 that represents the time interval between each keep-alive packet.
Multilink Protocol Option	This option is not supported in the current software release.
Bandwidth Allocation Control Protocol	Set this value to On if the associated router supports the Bandwidth Allocation Control Protocol (BACP). Refer to the <i>BACP/BAPP Internet Draft</i> for a detailed description of these protocols.
Maximum LCP Negotiation Time	The maximum time interval for the Link Control Protocol (LCP) to negotiate the exchange of packets.

7. When you have configured the logical port, click OK.

## Defining Multilink Frame Relay (MLFR) Trunks (B-STDX)

To define a Multilink Frame Relay (MLFR) trunk, you must first create ML Member logical ports, which are then bound to the MLFR trunk bundle logical port.

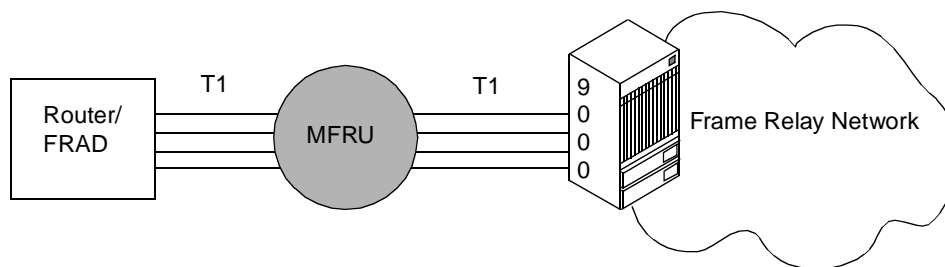


**Note** – For information on how to configure MLFR UNI/NNI bundles on CBX 4-Port Channelized DS3/1, DS3/1/0 FR/IP, and 32-Port Channelized T1/E1 FR/IP modules, see [Chapter 5, “Configuring Multilink Frame Relay \(MLFR\) UNI/NNI Bundles.”](#)

### About MLFR

MLFR is a method of aggregating available bandwidth on a set of Frame Relay logical links between two networking devices. The aggregated links, collectively referred to as the Multilink Frame Relay Unit (MFRU), can be thought of as a single logical link.

As shown in **Figure 3-33**, the MFRU provides a single logical link (with 4\*T1 bandwidth) between the router and the Frame Relay switch.



**Figure 3-33. Multilink Frame Relay Unit (MFRU)**

MLFR is implemented through the encapsulation of Frame Relay packets within a Multipoint-like frame. User and control packets are encapsulated, enabling several logical links to be combined. PVC traffic is automatically distributed across the multiple links. MLFR provides a cost-effective, high-speed service without the need for additional hardware.

MLFR is supported on the following B-STDX modules:

- 8-Port Universal IOPA
- 4-Port Unchannelized T1/E1 IOPA
- 4-Port Channelized T1/E1 IOPA
- 10-Port DSX-1 IOPA
- 2-Port HSSI IOPB
- 12-Port Unchannelized E1 IOPB
- 1-Port Channelized DS3 IOPB
- 1-Port Channelized DS3/1/0 IOPB

## **ML Member Logical Ports and MLFR Trunk Bundle Logical Ports**

ML Member logical ports inherit their configuration from the logical port to which they are bound, therefore you only need to configure the administrative attributes described in **“Administrative Attributes for Frame Relay LPorts”** on page 3-15. The ML Member logical port can be bound to only one MLFR trunk bundle logical port, and the trunk bundle logical port must be on the same card.

A multilink trunk bundle logical port is created at the card level (not the physical port level). A maximum of 32 ML Member logical ports can be bound to an MLFR trunk bundle logical port. You should create the MLFR trunk with each MLFR trunk bundle endpoint containing the same number of bound MLFR logical ports and aggregate bandwidth. The NMS does not enforce this condition.

## MLFR Logical Port Configuration Process

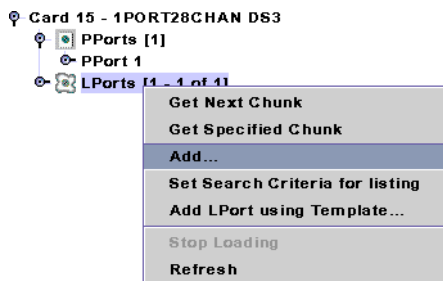
Defining MLFR over trunks involves the following tasks:

1. Creating a MLFR trunk bundle LPort.  
See “[Defining MLFR Trunk Bundle Logical Ports](#)” on page 3-67.
2. Creating ML member LPorts and binding them to the MLFR trunk bundle LPort.  
See “[Defining ML Member Logical Ports](#)” on page 3-69.
3. Create an MLFR direct link trunk between cards using MLFR trunk bundle logical ports as endpoints.  
See “[Adding a Trunk](#)” on page 4-7.

## Defining MLFR Trunk Bundle Logical Ports

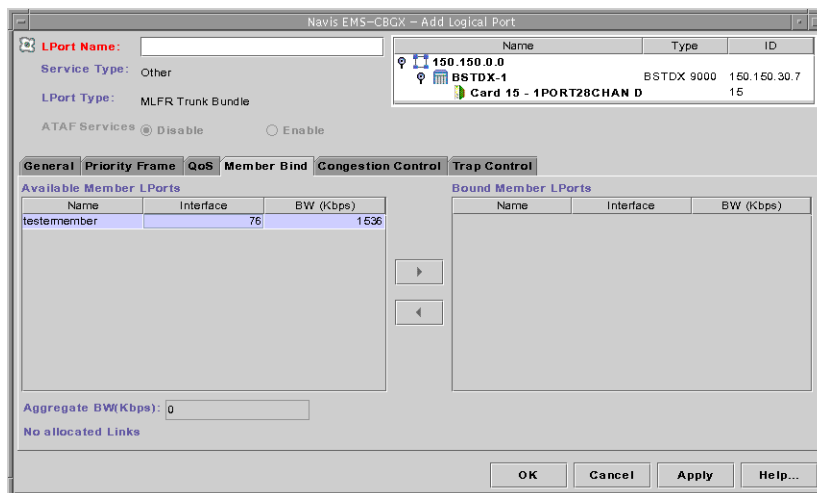
Complete the following steps to define an MLFR trunk bundle logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the physical port on which you want to configure a MLFR trunk bundle logical port.
2. Right-click on the LPorts node, and click Add on the popup menu as shown in [Figure 3-34](#).



**Figure 3-34. Adding a Trunk Bundle LPort**

The Add Logical Port dialog box (Figure 3-35) is displayed.



**Figure 3-35. Add/Modify Logical Port Dialog Box: Member Bind Tab**

3. Make sure the Service Type is configured as Other, and the LPort Type is configured as MLFR Trunk Bundle.
4. Complete the logical port attributes as described in “Setting Frame Relay LPort Attributes” on page 3-11. The bandwidth field for this logical port type is read-only.
5. In the Member Bind tab, you can bind any ML member LPorts that have already been configured. You can bind additional member LPorts later as you configure them.
  - To bind an ML Member logical port to the bundle, select an ML Member logical port from the Available ML Member LPorts list on the left, and click on the right arrow button. The selected logical port is removed from the available list and added to the bound list on the right. The system updates the Aggregate BW (kbps) field to include the bound logical port’s bandwidth.
  - To unbind a bound ML Member logical port from the bundle, select a bound ML Member logical port from the Bound ML Member LPorts list on the right, and click on the left arrow button. The selected logical port is removed from the bound list and added to the available list on the left. The system updates the Aggregate BW (kbps) field to include the deletion of the unbound logical port’s bandwidth from the bundle.
6. Click OK to configure the bundle logical port.

## Defining ML Member Logical Ports

Complete the following steps to define an ML member logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the physical port on which you want to configure a ML member logical port.



**Note** – You define an MLFR bundle logical port at the card level using the LPorts node within the node for the card, rather than the LPorts node for a physical port.

If you are defining ML member logical ports on channelized cards:

- a. Expand the PPort node, and expand the node for the specific physical port.
  - b. Expand the Channels node, and expand the node for the specific channel.
2. Under the node for the card or channel on which you want to configure the ML member logical port, right-click on the LPorts node, and click Add on the popup menu as shown in [Figure 3-36](#).

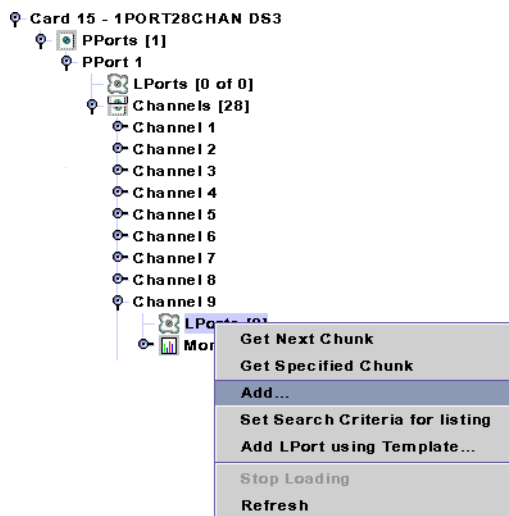
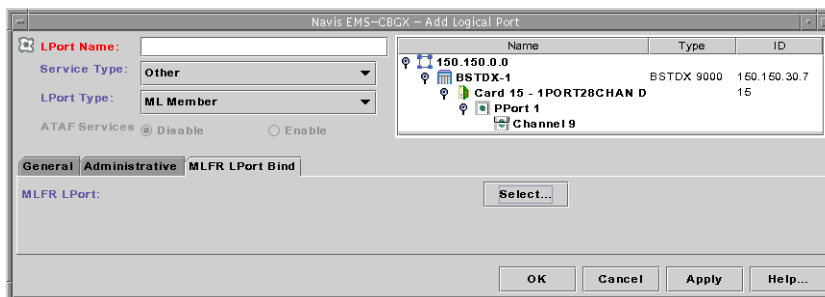


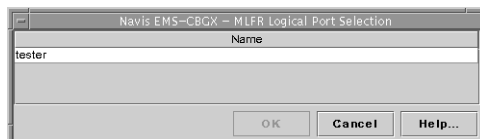
Figure 3-36. Adding a ML Member Logical Port on a Channelized Card

The Add Logical Port dialog box (Figure 3-37) is displayed.



**Figure 3-37. Add/Modify Logical Port Dialog Box: MLFR LPort Bind Tab**

3. Make sure the Service Type is configured as Other, and the LPort Type is configured as ML Member.
4. Complete the logical port attributes as described in “Setting Frame Relay LPort Attributes” on page 3-11. Since an ML Member logical port inherits its configuration from the MLFR trunk bundle logical port to which it is bound, you need to configure only the administrative attributes for the ML Member logical port.
5. In the MLFR LPort Bind tab, click on the Select button and choose the MLFR logical port to which you want to bind this ML member logical port, then click OK.



**Figure 3-38. MLFR Logical Port Selection Dialog Box**

The MLFR LPort Bind tab displays the MLFR LPort to which the member will be bound.

6. Click OK to configure and bind the ML member logical port.



## Logical Port Configuration Considerations for CBX 500 4-Port Channelized DS3/1 and DS3/1/0 Modules

This section describes logical port configuration considerations for 4-Port Channelized DS3/1 and DS3/1/0 modules on the CBX switch.

### Logical Port Limits for Channelized DS3/1 and DS3/1/0 Modules

The LPort limits for the Channelized DS3/1 and DS3/1/0 modules are as follows:

- **DS3/1 logical port capability** — Allows up to 112 logical ports per card with a maximum of 28 logical ports per physical port. Note that when configuring Multilink Frame Relay (MLFR) bundle LPorts or IP LPorts, the LPort and IP port limit per physical port is 108 (12 bundles of 8 LPorts).
- **DS3/1/0 logical port capability** — Allows up to 1024 logical ports per card with
  - 128 logical ports available on physical ports 1 and 2.
  - 384 logical ports available on physical ports 3 and 4.

These numbers may vary by release, see the Software Release Notice (SRN) for your version of the CBX switch software for the most up-to-date information.

### FIFO Block Allocation

When configuring LPorts on 4-Port Channelized DS3/1 and DS3/1/0 PPorts, the number of First-In First-Out (FIFO) blocks on these LPorts *cannot* exceed the parameter listed in the release notes for the software running on your switch. This limitation holds true even if the LPort limits on each of these PPorts have not been reached.

FIFO blocks are allocated as follows:

- DS0 = 3 FIFO blocks
- DS1 = 12 FIFO blocks

The FIFO blocks for Fractional T1s are allocated based on the total number of DS0s configured. The FIFO values are as follows:

**Table 3-25. FIFO Blocks for Fractional T1s**

DS0s	FIFOs
1 to 2	3
3 to 6	4
7 to 13	6

**Table 3-25. FIFO Blocks for Fractional T1s**

DS0s	FIFOs
14 to 18	8
19 to 22	10
23 to 24	12

Lucent recommends that you calculate the number of FIFO blocks that will be used before configuring DS1 and DS0 channels on PPort 1 and PPort 2 of the 4-Port Channelized DS3/1 and DS3/1/0 modules.

**Example 1: FIFO Block (Over Allocation Limits)**

If you configure the following on PPort 1:

- 4 channels, each with 24 DS0 LPorts, for a total of 96 LPorts and 288 FIFO blocks (96 LPorts \* 3 FIFO blocks = 288)
- 24 channels, each with 1 DS1 LPort, for a total of 24 LPorts and 288 FIFO blocks (24 LPorts \* 12 FIFO blocks = 288)

you will have configured 120 LPorts and used 576 FIFO blocks.

**Example 2: FIFO Block (Within Allocation Limits)**

If you configure the following on PPort 1:

- 120 DS0 LPorts with 360 FIFO blocks (120 LPorts \* 3 FIFO blocks = 360)
- 8 DS1 LPorts with 96 FIFO (8 LPorts \* 12 FIFO blocks = 96)

you will have configured 128 LPorts and used 456 FIFO blocks.

## Calculating FIFO Blocks

To calculate FIFO blocks, perform the tasks in the following sections:

- [“Using the get lport MIB Command” on page 3-72](#)
- [“Determining Time Slot Positions” on page 3-73](#)
- [“Using the FIFO Conversion Table” on page 3-74](#)

**Using the get lport MIB Command**

You can use the following MIB command to calculate the FIFO blocks allocated to each LPort interface:

```
get lport.1.1.8.<interface #>
```

The following is a sample of this command's output:

```
Switch name> get lport.1.1.8.151
1.3.6.1.4.1.277.1.5.1.1.8.151 = 00F00000 (OctetString)
```

The MIB command output shows the total number of time slots (DS0s) assigned to the LPort interface in Hex format (for example, 00F00000).

### Determining Time Slot Positions

For Channelized DS3/1 and DS3/1/0 modules, the 24 time slots (DS0s) are divided into 6 groups called positions. These positions each contain 4 binary sets.

Using the MIB command output of 00F00000, the following example shows that DS0s are only configured in position 6:

Output	0	0	F	0	0	0	0	0
Time Slot Positions	x	x	6	5	4	3	2	1

When the output for a time slot position is “0” (zero), no DS0s have been configured for that position.



**Note** – The time slot positions marked with an “x” are not used for the Channelized DS3/1 and DS3/1/0 modules.

Based on this information, you must look up the Hex Value in [Table 3-26](#) for “F” to determine the number of DS0s and FIFO blocks configured for the LPort interface.

### Multiple Time Slot Positions

If the MIB command result shows DS0s assigned in multiple positions, you have to first determine the actual number of DS0s.

Using the MIB command output of 0020001E, the following example shows that DS0s are configured in position 6, 2, and 1.

Output	0	0	2	0	0	0	1	E
Time Slot Positions	x	x	6	5	4	3	2	1

Based on this information, you must look up the Hex Value in [Table 3-26 on page 3-74](#) for each of the time slots (with a number or letter other than “0”) to determine the number of DS0s and FIFO blocks configured for the LPort interface.

### Using the FIFO Conversion Table

With [Table 3-26](#), you can use the Hex number returned by the MIB command to calculate the FIFO blocks:

**Table 3-26. FIFO Conversion Table**

Hex Value	DS0s	FIFOs
0	0	0
1	1	3
2	1	3
3	2	3
4	1	3
5	2	3
6	2	3
7	3	4
8	1	3
9	2	3
A	2	3
B	3	4
C	2	3
D	3	4
E	3	4
F	4	4

***FIFO Conversion Table Examples***

For the MIB command output of 00F00000, the “F” Hex value denotes that of 4 DS0s are configured that use 4 FIFO blocks.

For the MIB command output of 0020001E, the Hex values from position 6, 2, and 1 (which are 2, 1, and E) make for a total of 5 DS0s configured. Using the information in **“FIFO Block Allocation” on page 3-71**, when 5 DS0s are configured, 4 FIFO blocks are used.

## **Configuring Frame Relay LPorts**

*Logical Port Configuration Considerations for CBX 500 4-Port Channelized DS3/1 and DS3/1/0 Modules*

---

# Configuring Trunks

A Lucent trunk enables two Lucent switches to pass data to each other and exchange internal control messages. This chapter describes how to configure a trunk in a Lucent switch network.

This chapter contains:

- [“About Trunks” on page 4-1](#)
- [“Working with Trunks” on page 4-6](#)
- [“Configuring Trunk Backup” on page 4-16](#)

## About Trunks

A Lucent trunk is the communications circuit between two switches. The trunk provides the means for two Lucent switches to pass data to each other and exchange internal control messages such as Open Shortest Path First (OSPF), Simple Network Management Protocol (SNMP) and others.

This section describes several parameters that you need to understand to better manage trunk traffic in a Lucent switch network. These parameters include:

- **Trunk oversubscription factor** — The trunk oversubscription factor enables you to oversubscribe a trunk; that is, configure more circuits to a trunk than can be supported at one time. Oversubscription assumes that due to the bursty nature of network traffic, not all circuits on the trunk are operating at the committed information rate (CIR) at the same time. Therefore, trunk bandwidth should remain sufficient.
- **OSPF trunk administrative cost** — The trunk administrative cost enables you to assign a cost value for the trunk. When multiple trunks are available, a circuit uses the trunk with the lowest administrative cost.
- **Link Trunk Protocol** — Using Link Trunk Protocol (LTP), switches communicate by exchanging keep-alive (KA) control frames. The exchange of KA control frames can be used to measure trunk delay in the network.

- **Trunk backup option** — The trunk backup option enables you to set up one or more backup trunks to replace a primary trunk. If a Lucent switch trunk line fails or needs maintenance, you can reroute permanent virtual circuits (PVCs) from the primary trunk to the backup trunk.



**Note** – For more information on configuring Virtual Network Navigator (VNN) OSPF routing over Lucent trunks, refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

---

## Trunk Oversubscription Factor

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

The routing for PVCs is determined by either an OSPF algorithm or by the network administrator (if you manually define the circuit path). Each time a PVC attempts to come up, OSPF reserves bandwidth equal to the CIR of the PVC on the trunk with the shortest path. The amount of reserved bandwidth is deducted from the available virtual bandwidth pool. The formula used to determine virtual bandwidth is only used for allocating the initial path for the PVC. The system periodically reviews each PVC to optimize network resources according to the reroute-tuning parameters (refer to the *Navis EMS-CBGX Getting Started Guide*).

OSPF uses two formulas to determine the available virtual bandwidth value:

**Formula 1:** This formula determines the initial value of the available virtual bandwidth, where V represents the trunk oversubscription factor:

$$\text{Initial Value} = 0.95 (\text{configured bandwidth}) \times V(\%)$$

**Formula 2:** **Available Virtual Bandwidth = Initial Value – (Sum of PVC CIR)**



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

---

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



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

## OSPF Trunk Administrative Cost

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

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

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

### Configuring Minimum-hop Paths

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

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

## Link Trunk Protocol

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

## Trunk Delay

Figure 4-1 illustrates the process of keep-alive frames used to measure trunk delay. When Switch A sends a KA request to Switch B, a time stamp is put into the KA request frame. When Switch B receives the KA request, it sends a KA reply to Switch A. Switch A receives the KA reply and calculates the round-trip delay from Switch A to Switch B.

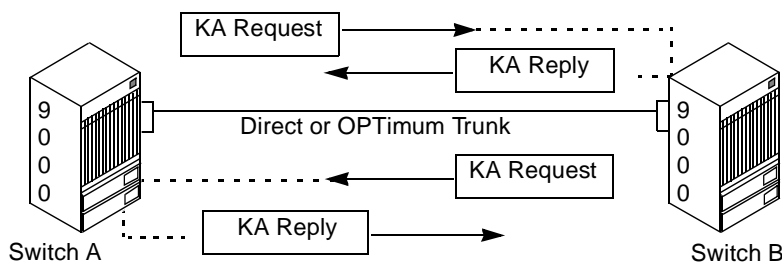


Figure 4-1. Trunk Delay – OSPF Metric and Keep-alive Messaging

## Keep-alive Threshold

The Keep Alive Threshold field in the Add/Modify Trunk dialog box (Figure 4-3 on page 4-8) 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 in the Add/Modify Trunk dialog box (Figure 4-3 on page 4-8) 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 change such that the dynamic delay changes, this value may differ from the static delay.

If you use the Add/Modify Trunk dialog box (Figure 4-3 on page 4-8) 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 value.



---

**Note** – Static delay is a non-disruptive trunk attribute, which means that modifying its value does *not* bring down the trunk or its associated logical port. See “[Working with Trunks](#)” on page 4-6 for more information.

---

To modify the static delay value:

1. In the Networks tab, expand the network node, then expand the Switches node.
2. Double-click on the switch to which you want to add a logical port.

The Switch tab is displayed. You can access trunk nodes and expand them as shown in [Figure 4-2 on page 4-7](#).

3. Expand the Trunks node.
4. Select a trunk and choose Modify from the popup menu. The system displays a Modify Trunk dialog box similar to the one shown in [Figure 4-7 on page 4-15](#).
5. Edit the static delay value.
6. 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.

## Trunk Backup

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

You define a backup trunk in the Add Trunk dialog box ([Figure 4-5 on page 4-13](#)). A backup trunk can have a total bandwidth that is less than that of the primary trunk. To avoid congestion, you can configure multiple backup trunks to back up a single primary trunk. The switch allows you to define up to eight backup trunks for a single primary trunk.

After you configure the primary and backup trunk(s), you can configure the primary trunk to automatically back up upon failure. If a trunk line requires maintenance, you can manually initiate and terminate a trunk backup.

For more information, see “[Configuring Trunk Backup](#)” on page 4-16.

## Working with Trunks

Perform the following steps to configure a Lucent trunk:

1. Configure a Direct Line Trunk logical port type on both switches. See one of the following sections:
  - “[Defining Frame Relay OPTimum PVC Trunk Logical Ports](#)” on page 3-58
  - “[Defining Encapsulation FRAD, Direct Line Trunk, and PPP Logical Ports](#)” on page 3-60 (describes Direct Line Trunk)
2. Define a trunk configuration between the two switches.

This section contains:

- “[Adding a Trunk](#)” on page 4-7
- “[Modifying Trunks](#)” on page 4-14
- “[Viewing and Configuring PVCs](#)” on page 4-16
- “[Viewing and Configuring PVCs](#)” on page 4-16



**Note** – Certain trunk attributes are defined as *non-disruptive*. Non-disruptive attributes appear in *italicized* text in Navis EMS-CBGX dialog boxes.

When you modify any of these attributes, the NMS sends the appropriate SNMP SET commands to the switch without bringing down the trunk and its associated logical port. Switch Parameter Random Access Memory (PRAM) and the NMS database are synchronized automatically, without interrupting network traffic.

When you modify any attributes other than non-disruptive attributes, the NMS will bring down the trunk and its associated logical port.

See “[Modifying Switch Configuration Attributes](#)” on page 2-26 for more information about non-disruptive trunk attributes.

---



**Note** – Refer to the *Navis EMS-CBGX Installation and Administration Guide* for information on group-wise resource partitioning.

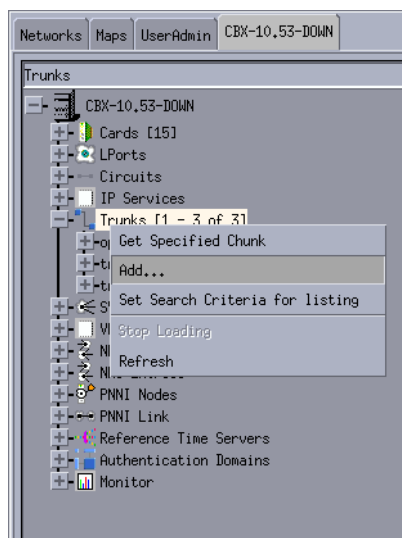
## Adding a Trunk

To add a trunk, perform the following tasks:

1. In the Networks tab, expand the network node, then expand the Switches node.
2. Double-click on the switch to which you want to add a logical port.

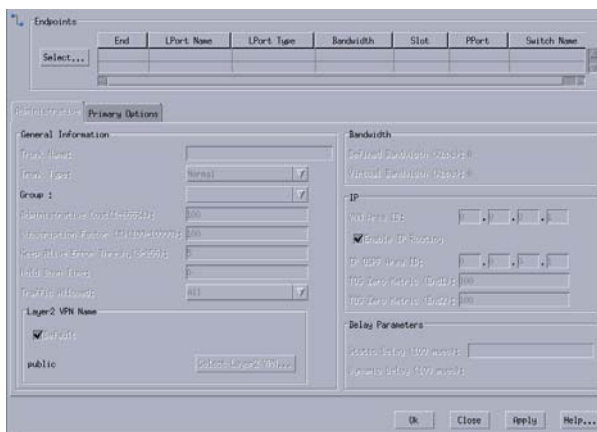
The Switch tab is displayed.

3. Right-click on the Trunks node, and select Add from the popup menu as shown in [Figure 4-2](#).



**Figure 4-2.** Adding a Trunk

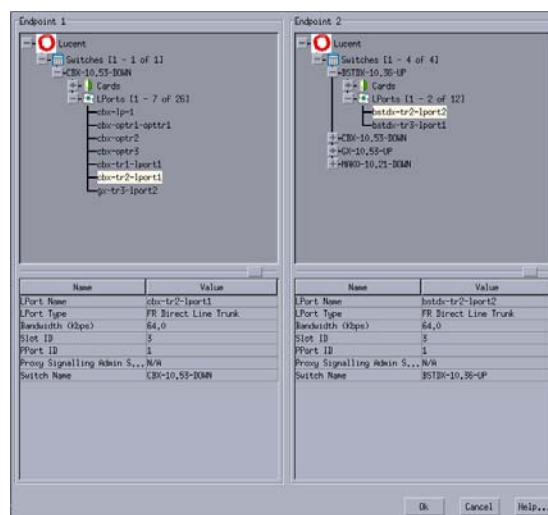
The Add Trunk dialog box (Figure 4-3) is displayed.



**Figure 4-3. Add Trunk Dialog Box: Administrative Tab**

- In the Endpoints section, click on the Select button to choose two logical ports which will be the trunk endpoints.

The Select Trunk Endpoints dialog box (Figure 4-4) is displayed.



**Figure 4-4. Select Trunk Endpoints Dialog Box**

Select the logical ports for Endpoint 1 and Endpoint 2. Endpoint 2 must be of the same trunk logical port type as Endpoint 1. The types are as follows:

- Frame Relay OPTimum Trunk
- Other: Direct Line Trunk
- ATM: Direct Trunk (refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000*)



**Note** – For the 32-Port Channelized T1/E1 FR/IP IOM, the logical port type must be Direct Line Trunk for both logical ports.

- ATM OPTimum Frame Trunk (refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*)
- ATM OPTimum Cell Trunk (refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*)
- MLFR Direct Line Trunk. (This field also displays the ifnum, physical port number, and I/O slot (number) in which the module resides.)

For non-MLFR trunks, review the LPort Bandwidth field for each endpoint to make sure the bandwidth is identical.



**Note** – When you configure a trunk between logical ports on two different 32-Port Channelized T1/E1 FR/IP IOMs, make sure both modules are set to the same operation mode (T1 or E1). You *cannot* configure a trunk between a logical port on a 32-Port Channelized T1/E1 FR/IP IOM set to T1 Mode and a logical port on a 32-Port Channelized T1/E1 FR/IP IOM set to E1 Mode. (For information about setting the operation mode, refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.)

5. Choose OK. The Add Trunk dialog box (**Figure 4-3**) appears, displaying the parameters for both switches in the trunk configuration.
6. Complete the Administrative fields described in **Table 4-1**.

**Table 4-1. Add Trunk Dialog Box: Administrative Tab**

Element	Description
Endpoints	<p>Displays information about the trunk endpoints, and enables you to use the Select button to choose trunk endpoints.</p> <ul style="list-style-type: none"> <li>• LPort Name: Displays the logical port name at each endpoint of the trunk.</li> <li>• LPort Type: Displays the configured logical port type.</li> <li>• Bandwidth: The amount of defined bandwidth, in Kbps, configured on the endpoint.</li> <li>• Slot: Displays the slot number where the I/O module containing the selected port is installed.</li> <li>• Port: Displays the physical port ID number on which the logical port is configured.</li> <li>• Switch Name: The name of the switch on which the endpoint resides.</li> </ul>

**Table 4-1. Add Trunk Dialog Box: Administrative Tab (Continued)**

Element	Description
Trunk Name	Enter a unique alphanumeric name to identify the trunk.
Trunk Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Normal</i> — (default) Indicates that it is a common trunk.</li> <li>• <i>Primary</i> — Indicates that the trunk has a backup for fault tolerance. If selected, you must configure the Primary Options tab. See <a href="#">step 7 on page 4-13</a>.</li> <li>• <i>Backup</i> — Indicates that it is a backup trunk to which traffic will be diverted if the primary trunk fails. See <a href="#">“Using the Automatic Trunk Backup Feature” on page 4-16</a> to configure a backup trunk.</li> </ul> <p><i>Note: This parameter is not supported on trunks between CBX and B-STDX switches.</i></p>
Group	<p>Select a group to which you want to associate the trunk. The trunk can belong to any group or to the BaseGroup.</p> <p>Refer to the <i>Navis EMS-CBGX Installation and Administration Guide</i> for a detailed information on group-wise resource partitioning.</p>
Administrative Cost	<p>Enter a value between 1 and 65534 to define the cost of using this trunk for a virtual circuit when a virtual circuit is being dynamically created on the switch. The default value is 100. The lower the administrative cost of the path, the more likely OSPF will select it for circuit traffic. For a detailed explanation of this parameter, <a href="#">“OSPF Trunk Administrative Cost” on page 4-3</a>.</p> <p><i>Note: When you increase or decrease the administrative cost of a trunk, the reroute tuning parameters control the rate at which the switch adds or removes circuits from the trunk. Refer to the Getting Started User’s Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000 for information about reroute tuning. You cannot use trunk admin cost to force a trunk down.</i></p>
Subscription Factor (%)	<p>The trunk oversubscription factor percentage enables you to optimize the aggregate CIR you can configure on the trunk, by allowing you to over subscribe the trunk. The bandwidth on a trunk is reserved at runtime, based on the configured CIR value of the PVCs that traverse that trunk. For example, you can set this factor to 200% to produce a virtual bandwidth that is two times greater than the defined bandwidth.</p> <p>For a detailed explanation of this parameter, see <a href="#">“Trunk Oversubscription Factor” on page 4-2</a>.</p> <p><i>Note: Setting a oversubscription percentage may impact traffic throughput and services on the network.</i></p> <p><i>Note: You cannot oversubscribe an ATM Direct Trunk.</i></p>



**Table 4-1. Add Trunk Dialog Box: Administrative Tab (Continued)**

Element	Description
Keep Alive Error Thresh	<p>Configure the keep-alive threshold for a value between 3 and 255 seconds. The default is 5 seconds. For a detailed explanation of this parameter, see <a href="#">“Keep-alive Threshold” on page 4-4</a>.</p> <p><i>Note:</i> If you are running different switch code versions in your network (for example, Version 4.1 and Version 4.2), you must accept the default value of 5 seconds.</p> <p><i>Note:</i> Service is disrupted if you change this value after the trunk is online.</p>
Hold Down Time	<p>Accept the default value (0), or enter a value between 0 and 65535 (seconds). The Hold Down Time field enables you to configure the time delay (in seconds) before link state advertisements (LSAs) are generated when a trunk recovery takes effect on the network. This feature reduces the number of LSAs caused by rapid changes in trunk status.</p> <p><i>Note:</i> 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.</p>
Traffic Allowed	<p>Specify one of the following options to designate the type of traffic allowed on this trunk:</p> <ul style="list-style-type: none"> <li>• <i>All</i> – (default) The trunk can carry network management traffic, user traffic, and OSPF address distribution.</li> <li>• <i>Mgt Only</i> – The trunk can carry <i>only</i> network management traffic, such as SNMP communication between a switch and the NMS.</li> <li>• <i>Mgt &amp; User</i> – The trunk can carry network management traffic and user traffic.</li> </ul> <p><i>Note:</i> To calculate the most efficient route for network management traffic, OSPF uses Trunk Admin Cost. OSPF ignores trunk bandwidth when it selects the best path or a route for management traffic. Management traffic can use a negative bandwidth trunk.</p>
Layer 2 VPN Name	<p>Displays and enables you to select the Layer2 virtual private network (VPN) name. This field displays <i>Public</i> if the trunk is not dedicated to a specific Layer2 VPN.</p> <p><i>Note:</i> Layer2 VPNs were referred to in previous software versions as Virtual Network Navigator (VNN) VPNs.</p> <p>For more information about Layer2 VPNs, see <a href="#">Chapter 10, “Configuring Layer2 Virtual Private Networks (VPNs).”</a></p>
Defined Bandwidth	<p>Displays the amount of bandwidth, in Kbps, for the selected trunk line.</p>

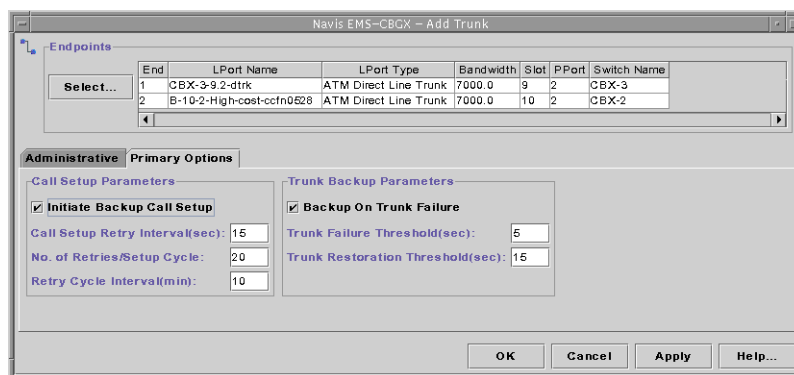
**Table 4-1. Add Trunk Dialog Box: Administrative Tab (Continued)**

Element	Description
Virtual Bandwidth	Displays the amount of virtual bandwidth in Kbps.
IP Area ID	<p>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.</p> <p>If a trunk is in Area 1 and the OSPF Backwards Compatibility option, which is set through Lucent IP services, is set to Yes, external routes are not advertised across the link.</p> <p><i>Note: Area 1 is reserved for Lucent switches. For a detailed description of OSPF areas, and how to use IP Services to configure multiple OSPF areas, refer to the IP Services Configuration Guide for CBX 3500, CBX 500 and B-STDX 9000.</i></p> <p><i>Note: Changing the value for this attribute does not bring down the trunk or its associated logical port.</i></p>
Enable IP Routing	Enable or disable IP routing for the trunk. If disabled, the trunk is reserved for use by Virtual Network Navigator. For more information about IP routing, refer to the <i>IP Services Configuration Guide for CBX 500 and B-STDX 9000</i> .
Trunk IP Area ID	Enter the OSPF Area ID used by IP Services. For more information about Lucent IP services, refer to the <i>IP Services Configuration Guide for CBX 500 and B-STDX 9000</i> .
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.
Static Delay	<p>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 changes state 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 this field, see the instructions in <a href="#">“Static and Dynamic Delay” on page 4-4</a>.</p> <p><i>Note: Changing the value for this attribute does not bring down the trunk or its associated logical port.</i></p>

**Table 4-1. Add Trunk Dialog Box: Administrative Tab (Continued)**

Element	Description
Dynamic Delay	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 can differ from the static delay.

7. (Optional) If you selected *Primary* as the Trunk Type, the system displays the Primary Options tab shown in [Figure 4-5](#).



**Figure 4-5. Add Trunk Dialog Box: Primary Options Tab**

8. Complete the fields described in [Table 4-2](#), or accept the default parameters.

**Table 4-2. Add Trunk Dialog Box: Primary Options Tab**

Element	Description
Initiate Backup Call Setup	Choose Yes (default) to initiate a backup call.
Call Setup Retry Interval	Specify the number of seconds between each retry during a given call retry cycle. The default is 15 seconds.  For example, if your system performs 5 retries for each retry cycle and the wait between each retry cycle is 10 minutes, you might want to perform each retry at every 2-minute interval. Therefore, you would set the Call setup retry Interval to 120 seconds.
No. of Retries/Setup Cycle	Specify the number of retries per interval. The default is 20 retries.
Retry Cycle Interval	Specify a retry interval in minutes. The default is 10 minutes.

**Table 4-2. Add Trunk Dialog Box: Primary Options Tab (Continued)**

Element	Description
Backup on Trunk Failure	Enable (default) or disable trunk backup. If you enable trunk backup, the system automatically uses the backup trunk if the primary trunk fails. If you choose Disabled, the automatic trunk backup option is not used.
Trunk Failure Threshold	If you enabled trunk backup by setting Backup on the Trunk Failure field to <i>Enabled</i> , specify the number of seconds the system will wait before switching over to the backup trunk when the primary trunk fails. The default value is 5 seconds.
Trunk Restoration Threshold	If you enabled trunk backup by setting Backup on the Trunk Failure field to <i>Enabled</i> , specify the number of seconds the system will wait for the primary trunk to become functional before resuming use of the primary trunk. The default value is 15 seconds. If the primary trunk is out of service and the backup trunk is in use, the system will not resume use of the primary trunk until it has been restored for the period of time you specify. The purpose of this field is to prevent a switchover to a primary trunk that has only been temporarily restored.

9. When you complete the Add Trunk dialog box fields, click OK.

## Modifying Trunks

To modify a trunk:

1. In the Switch tab, expand the Trunks node.
2. Right-click on the trunk you want to configure.

When you modify a trunk, the following menu options are available:

- **Modify** — Enables you to configure an existing trunk using the Modify Trunk dialog box (Figure 4-7).
- **Delete** — Deletes an existing trunk.
- **View** — Enables you to view the configuration of an existing trunk in read-only mode.
- **Oper Info** — Displays the View Trunk Operational Information dialog box. For more information, refer to the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.
- **OAM** — Enables you to perform OAM loopback tests. For more information, refer to the *B-STDX, CBX, and GX Switch Diagnostics User's Guide*.

- To configure the trunk, select Modify from the popup menu as shown in Figure 4-6.

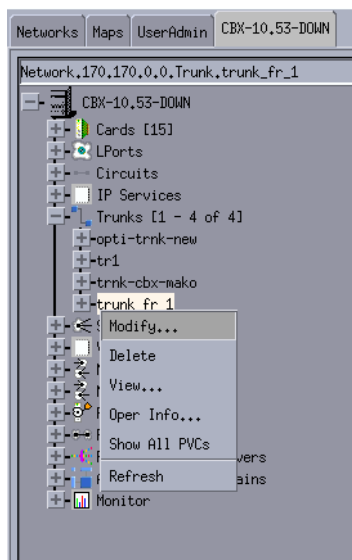


Figure 4-6. Modifying a Trunk

The Modify Trunk dialog box (Figure 4-7) is displayed.

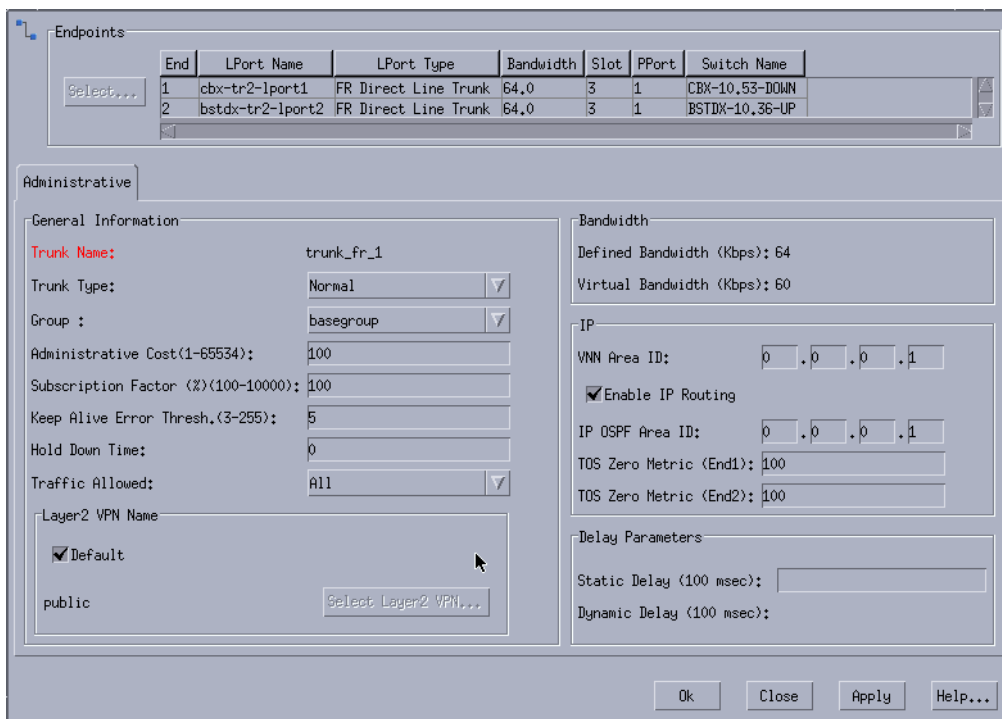


Figure 4-7. Modify Trunk Dialog Box

For information about the fields and buttons in the Add/Modify Trunk dialog box, see [Table 4-1 on page 4-9](#).

## Viewing and Configuring PVCs

Expanding the node for an existing trunk enables you to access the PVCs node, which contains the PVCs that traverse the selected trunk. This dialog box also provides logical port descriptions for each PVC endpoint.

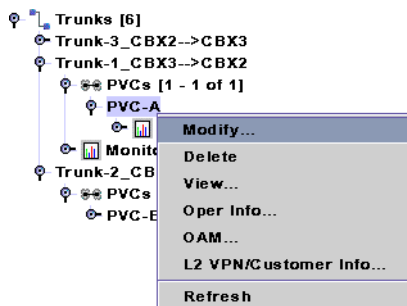


Figure 4-8. Modifying PVCs



**Note** – This function only works when both switches at either end of the trunk are running B-STDX 8000/9000 Release 06.00.xx.xx or later, CBX 500 Release 03.00.xx.xx or later.

For more information about modifying PVCs, see [Chapter 7, “Configuring Permanent Virtual Circuits \(PVCs\)”](#).

## Configuring Trunk Backup

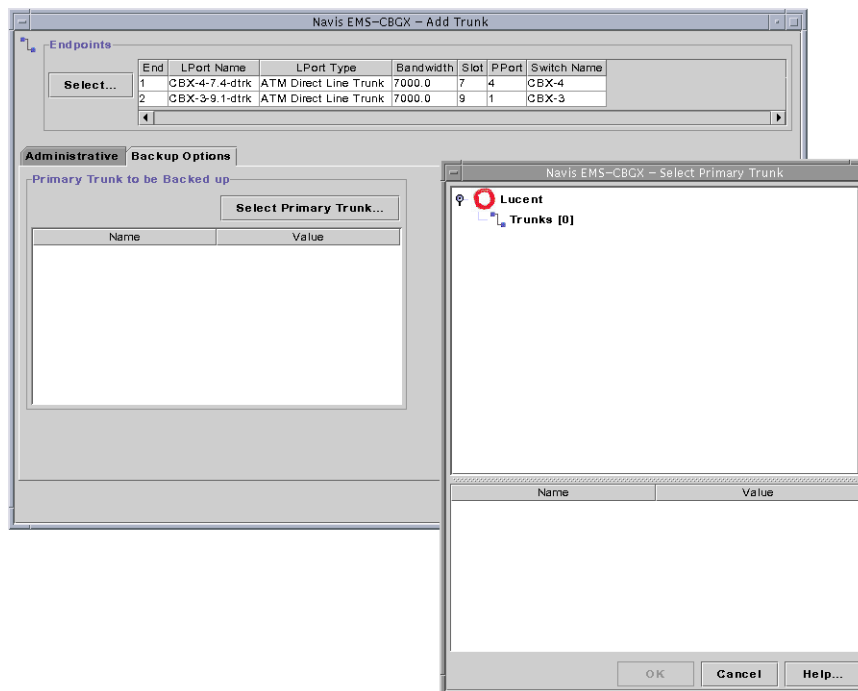
This section describes how to configure automatic trunk backup, or override the values for automatic trunk backup by using the manual trunk backup feature.

### Using the Automatic Trunk Backup Feature

To use the automatic trunk backup feature:

1. Define a trunk that has a Trunk Type of *Primary*. See [“Adding a Trunk” on page 4-7](#).
2. Specify values for all of the fields in the Primary Options tab described in [Table 4-2 on page 4-13](#). Specify a value of *Yes* in the Initiate Backup Call Setup field on the Add Trunk dialog box.
3. Specify a value of *Enabled* in the Backup on Trunk Failure field on the Add Trunk dialog box.

- Define from one to eight trunks that have a Trunk Type of Backup. When you select Backup in the Trunk Type field on the Add Trunk dialog box, the Backup Options tab is displayed (see [Figure 4-9](#)).



**Figure 4-9. Backup Options Tab and Select Primary Trunk Dialog Box**

- For each trunk with a Trunk Type of Backup, click the Select Primary Trunk button in the Backup Options tab, then select the name of the primary trunk specified in [step 1](#).
- Select the name of the switch that initiates the backup call setup for the trunk.

## Switching Over to a Backup Trunk

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

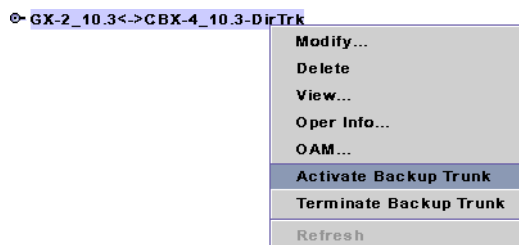
- The system switches over to the backup trunk after the trunk is out of service for the amount of time specified for the primary trunk in the Trunk failure threshold field ([Table 4-2](#)).
- The system resumes use of the primary trunk after it is in service for the period of time specified in the Trunk restoration threshold field ([Table 4-2](#)).

## Activating or Terminating a Backup Trunk Manually

You can override the values for automatic trunk backup by using the manual trunk backup feature.

To activate or terminate a backup trunk manually:

1. In the Switch tab, expand the Trunks node.
2. Right-click on the node for the primary trunk and choose one of the following commands as shown in **Figure 4-10**:
  - Choose Activate Backup Trunk to initiate the manual backup.
  - Choose Terminate Backup Trunk to end the manual backup.



**Figure 4-10. Activating or Terminating a Backup Trunk**



# Configuring Multilink Frame Relay (MLFR) UNI/NNI Bundles

This chapter describes how to define Multilink Frame Relay (MLFR) User-to-Network Interface/Network-to-Network Interface (UNI/NNI) bundles on the 4-Port Channelized DS3/1 and DS3/1/0 Frame Relay/Internet Protocol (FR/IP) modules, the 6-Port Channelized DS3/1/0 Frame Relay module, and the 32-Port Channelized T1/E1 FR/IP IOM.

This chapter contains:

- [“About MLFR UNI/NNI” on page 5-1](#)
- [“Administrative Tasks” on page 5-8](#)

## About MLFR UNI/NNI

This section describes the implementation of MLFR UNI/NNI supported on the following modules:

- 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules
- 6-Port Channelized DS3/1/0 Frame Relay module
- 32-Port Channelized T1/E1 FR/IP module

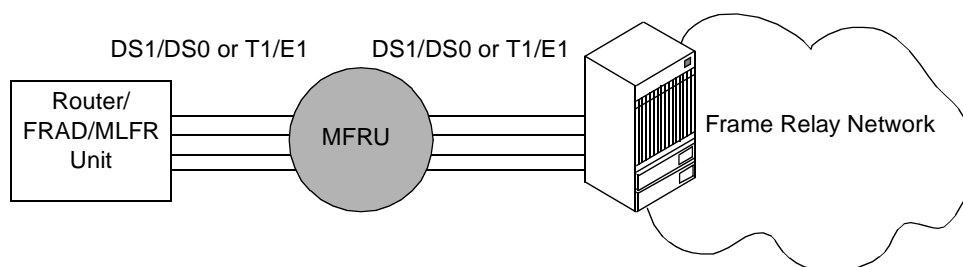
The following topics are covered:

- [“MLFR Overview” on page 5-2](#)
- [“MLFR UNI/NNI Bundle Logical Ports” on page 5-2](#)
- [“ML Member Logical Ports” on page 5-3](#)
- [“MLFR Features for 4-Port Channelized DS3/1 and DS3/1/0 FR/IP and 32-Port Channelized T1/E1 FR/IP Modules” on page 5-4](#)
- [“MLFR Features for 6-Port Channelized DS3/1/0 Frame Relay I/O Modules” on page 5-6](#)

The implementation is based on the Frame Relay Forum (FRF) *Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16)*.

## MLFR Overview

Multilink Frame Relay (MLFR) is a method of aggregating available bandwidth on a set of Frame Relay logical links between two networking devices. The aggregated links, collectively referred to as the Multilink Frame Relay Unit (MFRU), can be thought of as a single logical link. As shown in [Figure 5-1](#), the MFRU provides a single logical link (with 4\*DS1/DS0 bandwidth for 4-Port DS3 modules or 4\*T1/E1 bandwidth for 32-Port T1/E1 modules) between the router or Frame Relay access device (FRAD) and the Frame Relay switch.



**Figure 5-1. Multilink Frame Relay Unit (MFRU)**

MLFR is implemented through the encapsulation of Frame Relay packets within a multipoint-like frame. User packets and control packets are encapsulated, enabling several logical links to be combined. Permanent virtual circuit (PVC) traffic is automatically distributed across the multiple links. MLFR provides a cost-effective and high-speed service without the need for additional hardware.

## MLFR UNI/NNI Bundle Logical Ports

An MLFR UNI/NNI bundle logical port is an aggregation of individual Frame Relay logical ports (referred to as ML Member logical ports). The advantages of using an MLFR UNI/NNI bundle logical port are:

- Consolidates the bandwidth of several low-capacity links to emulate a single physical link.
- Provides Frame Relay UNI and NNI services over the bundle link.
- Avoids a single point of failure.
- Uses regular Frame Relay logical ports (FR UNI DCE, FR UNI DTE, or FR NNI) as ML Member logical ports, with the addition of an associated bundle ID.
- Provides a flexible way to add or reduce bandwidth on the MLFR bundle link by binding or unbinding ML Member logical ports.

See [“Administrative Tasks” on page 5-8](#) for MLFR LPort configuration information.

## ML Member Logical Ports

An ML Member logical port is a Frame Relay UNI DCE, UNI DTE, or NNI logical port that is bound to the MLFR UNI/NNI bundle logical port. Binding the ML Member logical port to the MLFR bundle logical port associates a bundle ID with the ML Member logical port.

The ML Member logical ports have the following restrictions:

- You can bind an ML Member logical port to only *one* MLFR UNI/NNI bundle logical port.
- The ML Member logical port and MLFR UNI/NNI bundle logical port *must* be on the same I/O module.
- The 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules and the 32-Port Channelized T1/E1 FR/IP module each support a single forwarding engine. The ML Member logical ports bound to the same MLFR UNI/NNI bundle logical port *must* be on this forwarding engine.

See [“Multicast DLCI Member Limits” on page 7-39](#) for more information on forwarding engine support for CBX Frame Relay modules.

- The logical port type of the ML Member *must* correspond to the logical port type of the MLFR UNI/NNI bundle to which it is bound. For example, you can only bind a Frame Relay UNI DCE logical port to an MLFR UNI DCE bundle logical port. See [Table 5-3 on page 5-13](#) for a list of supported bindings.
- You *must* disable the link management protocol for an ML Member logical port in order to bind it to an MLFR UNI/NNI bundle logical port. See [step 7 on page 5-14](#) for instructions.
- You *cannot* configure the following on an ML Member logical port:
  - Backup or resilience associations
  - Circuits
  - IP logical ports
  - Management DLCIs
- You cannot run PPort diagnostics on MLFR LPorts.
- Setting SVC QoS Parameters is not supported for MLFR UNI/NNI bundle logical ports.
- You *cannot* modify an ML Member logical port while it is bound to an MLFR UNI/NNI bundle logical port.

See [“Defining ML Member Logical Ports” on page 5-11](#) for configuration instructions.

## Total Number of MLFR Bundles

Table 5-1 lists the total number of MLFR bundles for supported modules:

Table 5-1. Total number of MLFR bundles

Module	Total number of regular LPorts	Total number of MLFR bundles
<b>IOM2</b>		
DS3/1	112	30
DS3/1/0	1024	32
<b>IOM6</b>		
DS3/1/0	2046	84
<b>32-Port T1/E1</b>		
T1 mode	768	32
E1 mode with TS16 disabled	960	32
E1 mode with TS16 enabled	992	32

## MLFR Features for 4-Port Channelized DS3/1 and DS3/1/0 FR/IP and 32-Port Channelized T1/E1 FR/IP Modules

Following is a summary of the features for MLFR UNI/NNI bundle logical ports on the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP, and the 32-Port Channelized T1/E1 FR/IP modules:

- You *can* configure a circuit on an MLFR UNI/NNI bundle logical port provided it has at least one bound ML Member logical port. See [Chapter 7, “Configuring Permanent Virtual Circuits \(PVCs\).”](#)
- You *cannot* configure the following on an MLFR UNI/NNI bundle logical port:
  - Backup or resilience associations
  - IP logical ports
  - SVCs
  - Management data link connection identifiers (DLCIs)
  - Congestion control attributes (you configure the congestion control attributes *only* on the ML Member logical ports bound to the MLFR UNI/NNI bundle logical port.)

- The 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, and the 32-Port Channelized T1/E1 FR/IP module support a maximum of 32 MLFR UNI/NNI bundle logical ports per module.
- Lucent recommends that you bind no more than eight ML Member logical ports to each MLFR UNI/NNI bundle logical port on the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, and the 32-Port Channelized T1/E1 FR/IP module.
- You should create the MLFR bundle with each MLFR bundle end point containing the same number of bound MLFR logical ports and aggregate bandwidth (the NMS does not enforce this condition).
- All ML Member logical ports bound to the same MLFR UNI/NNI bundle logical port should be of equal bandwidth.
- On a 4-Port DS3 or 32-Port T1/E1 module, unlike a regular Frame Relay logical port, an MLFR UNI/NNI bundle logical port has no actual physical ports or channels associated with it. When you define an MLFR bundle logical port, it is always created on a “dummy” physical port provided for this purpose.
  - On the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, the MLFR bundle logical port is created on physical port number 6.
  - On the 32-Port Channelized T1/E1 FR/IP module, physical port number 34 serves as the dummy physical port for MLFR bundle logical port creation.
- You must configure identical Priority Frame attributes on the MLFR UNI/NNI bundle logical port and on all of its ML Member logical ports.
- You should configure congestion control attributes only on the ML Member logical ports bound to the MLFR UNI/NNI bundle logical port, and *not* on the MLFR UNI/NNI bundle logical port itself. All ML Member logical ports bound to the same MLFR UNI/NNI bundle logical port should be configured with identical congestion control attributes.



**Note** – When you bind member links to an MLFR bundle LPort, LPort enabled with LMI or an LPort with a PVC endpoint, the LPort is displayed in the Available Member Ports dialog box in the Navis EMS-CBGX Client. While adding an LPort, Navis EMS-CBGX performs a check and displays one of the following error messages:

- Only member LPort with LMI protocol disable can be bound to an MLFR bundle LPort (for LPort enabled with LMI).
  - Cannot use an LPort with Circuit or management DLCI configured as ML member (for Circuit endpoint LPorts).
-

# MLFR Features for 6-Port Channelized DS3/1/0 Frame Relay I/O Modules

Following is a summary of the features for MLFR UNI/NNI bundle logical ports on the 6-Port Channelized DS3/1/0 Frame Relay I/O module:

- Member links are from the DS1 level only.
- The MLFR bundle logical port, its member links, and its member bindings are all configured with a single dialog box.
- MLFR bundle logical ports can be created with member links from PPorts 1, 2, and 3 or from PPorts 4, 5, and 6. An MLFR bundle logical port cannot combine member links from PPorts 1, 2, or 3 with member links from PPorts 4, 5, or 6.
- The maximum number of MLFR bundles on a 6-Port Channelized DS3/1/0 Frame Relay I/O Module is 84. (Maximum of 42 on PPorts 1/2/3 and 42 on PPorts 4/5/6.)
- The maximum number of member links per bundle is 12.
- Congestion control is performed per bundle, not per member link.
- Differential delay handling is supported.
- Fragmentation is supported.
- Buffering occurs per member link.
- The bandwidth of a bundle can be dynamically changed by adding or removing members when the bundle is active.
- The Link Integrity Protocol (LIP) is supported (part of the FRF.16.1 standard).

## Differential Delay

This section describes how the 6-Port Channelized DS3/1/0 Frame Relay I/O Module handles differential delay in MLFR bundles.

### *Member Link Delay Problems*

Each of the member links of an MLFR bundle carries portions of the bundle traffic, and the re-sequencing of the frames at the receiving end depends on the time of frame arrival on each link. The re-sequencing of the frames works best when the member links have similar or no delays on the line. However, delays can occur for various reasons, such as differences in hops and bad lines.

When one of the member links has a significantly higher delay than other members, frames received on the other member links must be buffered because they are waiting for delayed frames to arrive. This will eventually cause the buffers to overflow, leading to datagram loss.

### ***Definition of Differential Delay***

One way to overcome the buffering problem that is caused by member link delay differences is to monitor the delay across every member link. The difference in delay time between any pair of the member links is the *differential delay* between them.

Differential delay is measured by first calculating the round trip delay on each member link. This is done by sending out Hello packets on a periodic basis, and waiting for a Hello Acknowledgment. The time for the round trip is stored.

The round trip delay for a member link is then compared to the round trip delay for the other member links. The difference between the round trip delays for two member links is the differential delay between them.

### ***Managing Differential Delay***

If the differential delay for a member link is greater than a configured threshold value, then one of the following actions is taken:

- Remove the link from the bundle.
- Discontinue traffic on the link.
- Stop member link traffic, and restore traffic when the delay is resolved.
- Stop member link traffic, and do not restore traffic when the delay is resolved.
- Take no action.

When the option to remove the link from the bundle has been configured, no traffic should be sent or received on the link if the differential delay exceeds the threshold. This option is useful when the peer MLFR unit does not support differential delay link removal. The remote end peer notices that the link has been taken out of service and stops using it.

When the option to discontinue traffic on the link has been configured, the link should stop transmitting outgoing traffic if the differential delay exceeds the threshold. The link is still in service and is able to receive incoming traffic and LIP messages. This action is useful when both endpoints discontinue high delay links for outbound traffic. Corrective action can be performed, and the link can be reused after the delay is resolved.

When the option to take no action has been configured, the link will remain in service even when the differential delay exceeds the threshold. This option can potentially cause performance drop due to continued traffic high delay links.

When the differential delay threshold is exceeded by a link, SNMP traps are generated for all three options.

## Administrative Tasks

This section describes how to configure MLFR bundles on the supported modules.

The following configurations are discussed:

- [“Configuring MLFR UNI/NNI Bundle Logical Ports” on page 5-8](#)  
Describes how to configure MLFR bundles on the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, and 32-Port Channelized T1/E1 FR/IP module.
- [“Configuring MLFR on the 6-Port Channelized DS3/1/0 Module” on page 5-18](#)  
Describes how to configure MLFR bundles on the 6-Port Channelized DS3/1/0 Frame Relay module.

To create an MLFR UNI/NNI bundle, you first define an MLFR UNI/NNI bundle logical port. Then you define the regular Frame Relay logical ports and bind them as Multilink (ML) Member logical ports to the MLFR bundle logical port.



**Note** – See [“Defining Multilink Frame Relay \(MLFR\) Trunks \(B-STDx\)” on page 3-65](#) to define an MLFR trunk on B-STDx modules.

---

## Configuring MLFR UNI/NNI Bundle Logical Ports

This section describes the following tasks to configure MLFR UNI/NNI bundle logical ports on the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, and the 32-Port Channelized T1/E1 FR/IP module:

- [“Defining the Bundle Logical Port” on page 5-9](#)
- [“Defining ML Member Logical Ports” on page 5-11](#)
- [“Binding and Unbinding ML Members to MLFR Bundle Logical Ports” on page 5-14](#)



## Defining the Bundle Logical Port

To access the MLFR logical port attributes and functions, perform the following tasks:

1. In the Switch tab, expand the Cards node.
2. Right-click the LPorts node, and select Add on the popup menu (Figure 5-2).

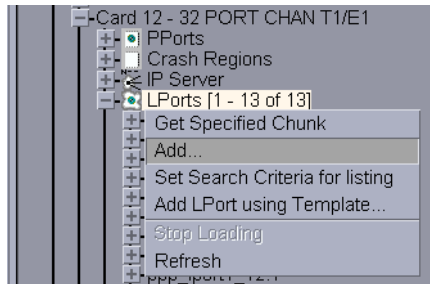


Figure 5-2. Navigation Panel: Add LPorts

The Add Logical Port dialog box is displayed (Figure 5-3).

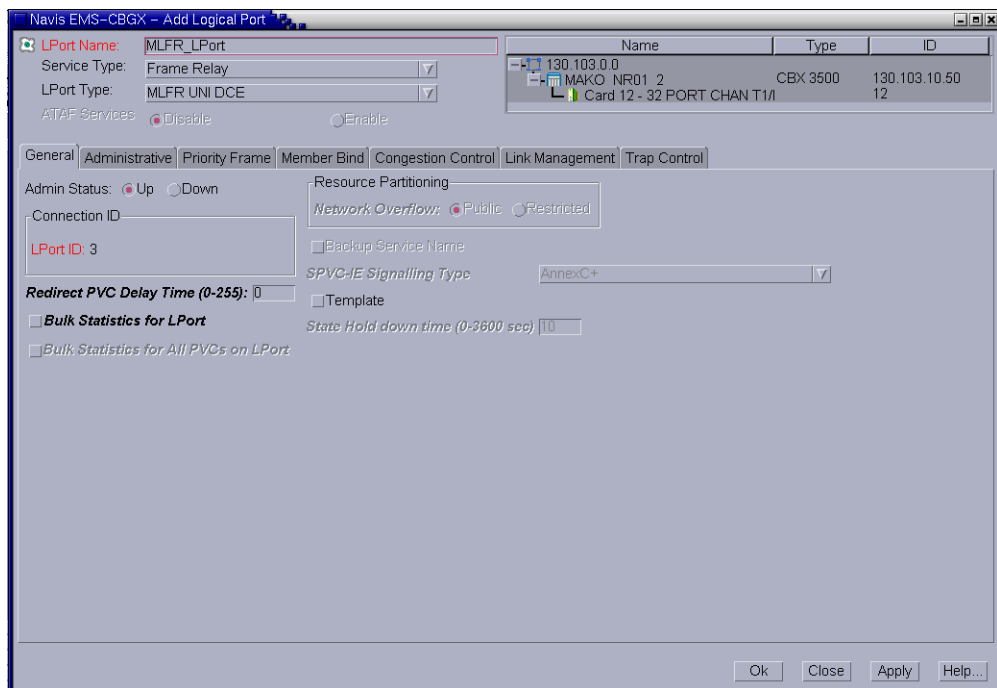


Figure 5-3. Add Logical Port Dialog Box



**Note** – The MLFR bundle logical port is *always* created on PPort number 6 for 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules, and PPort number 34 for the 32-Port Channelized T1/E1 FR/IP module, which are “dummy” PPorts provided for this purpose.

- Complete the dialog box fields described in [Table 5-2](#).

**Table 5-2. Add Logical Port Type Dialog Box**

Element	Description
Service Type	Select <i>Frame Relay</i> .
LPort Type	Select one of the following types for the MLFR bundle logical port: <ul style="list-style-type: none"> <li>• <i>MLFR UNI DCE</i></li> <li>• <i>MLFR UNI DTE</i></li> <li>• <i>MLFR NNI</i></li> </ul> For information about the ML Member logical port types that you can bind to each of these MLFR bundle logical port types, see <a href="#">Table 5-3 on page 5-13</a> .
LPort ID	On 4-Port Channelized DS3/1, DS3/1/0 or 32-Port Channelized T1/E1 FR/IP modules, enter a non-zero number from 1 to 9999 that uniquely identifies this MLFR bundle logical port. The number you enter must be unique among all the MLFR bundle logical ports configured on the IOM.  <b>Note:</b> <i>You can configure a maximum of 32 MLFR UNI/NNI bundle logical ports per module.</i>

- When you define a new MLFR UNI/NNI bundle logical port, the `Add Logical Port` dialog box displays a series of tabs that enable you to configure additional attributes for the MLFR bundle logical port.

See [Chapter 3, “Configuring Frame Relay LPorts”](#) for information about configuring these attributes.

- **General** — Sets general logical port parameters such as the admin state. See [“General Attributes for Frame Relay LPorts” on page 3-12](#).
- **Administrative** — Sets admin-related parameters including net overflow and bandwidth parameters. See [“Administrative Attributes for Frame Relay LPorts” on page 3-15](#).
- **Trap Control** — Sets the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port. The supported logical port types are different for each I/O module. See [“Trap Control Attributes for Logical Ports” on page 3-40](#).
- **Priority Frame** — Sets the logical port service class and transmit schedule mode. See [“Priority Frame Attributes for Logical Ports” on page 3-29](#).



**Note** – You must configure identical Priority Frame attributes on the MLFR UNI/NNI bundle logical port and on all of its ML Member logical ports.

---

- **Member Bind** — In the Member Bind tab, you can bind any ML member LPorts that have already been configured. You can bind additional member LPorts later as you configure them. See “[Binding and Unbinding ML Members to MLFR Bundle Logical Ports](#)” on page 5-14.
  - **Congestion Control** — You cannot configure congestion control attributes for MLFR UNI/NNI bundle logical ports. As a result, the Congestion Control option is not available on the Set Attributes option menu when you are configuring an MLFR UNI/NNI bundle logical port. Instead, you should configure congestion control attributes on the ML Member logical ports that you bind to the MLFR UNI/NNI bundle logical port. See “[Defining ML Member Logical Ports](#)” on page 5-11 for details.
  - **Link Management** — Sets the link management protocol used in the network and the LMI update delay and error thresholds. See “[Link Management Attributes for Logical Ports](#)” on page 3-34.
5. Click OK to configure the bundle logical port.

## Defining ML Member Logical Ports

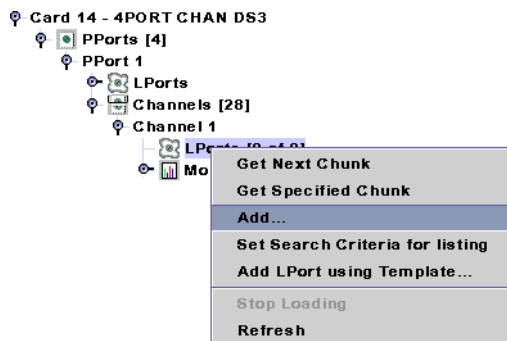
This section describes how to configure ML Member logical ports that you will bind to the MLFR bundle logical port.

An ML Member logical port is a Frame Relay UNI DCE, UNI DTE, or NNI logical port that you bind to the MLFR UNI/NNI bundle logical port. The process for defining an ML Member logical port is the same as the process described in [Chapter 3, “Configuring Frame Relay LPorts,”](#) for defining a standard Frame Relay logical port.

To define an ML Member logical port, perform the following tasks:

1. In the `Switch` tab, expand the `Cards` node and then expand the node for the module that contains the physical port on which you want to configure a MLFR logical port.
2. Use one of the procedures below based on the module you are configuring.  
For the 4-Port Channelized DS3/1 and DS3/1/0 FR/IP modules:
  - a. Expand the `Cards` node, expand the `PPort` node, and expand the node for the specific physical port.
  - b. Expand the `Channels` node, and expand the node for the specific channel on which you want to configure the ML member logical port.

- c. Right-click the LPorts node, and select Add on the popup menu as shown in Figure 5-4.



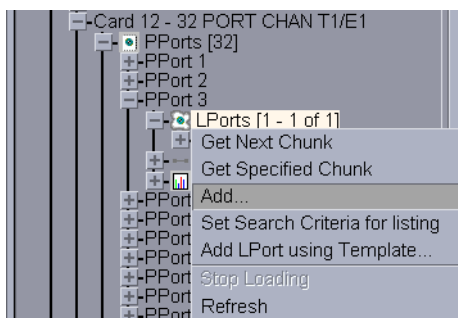
**Figure 5-4. Adding a ML Member LPort on a Channelized DS3 Module**

The Add Logical Port dialog box that is similar to Figure 5-6 on page 5-13 is displayed.

- d. Continue with step 3.

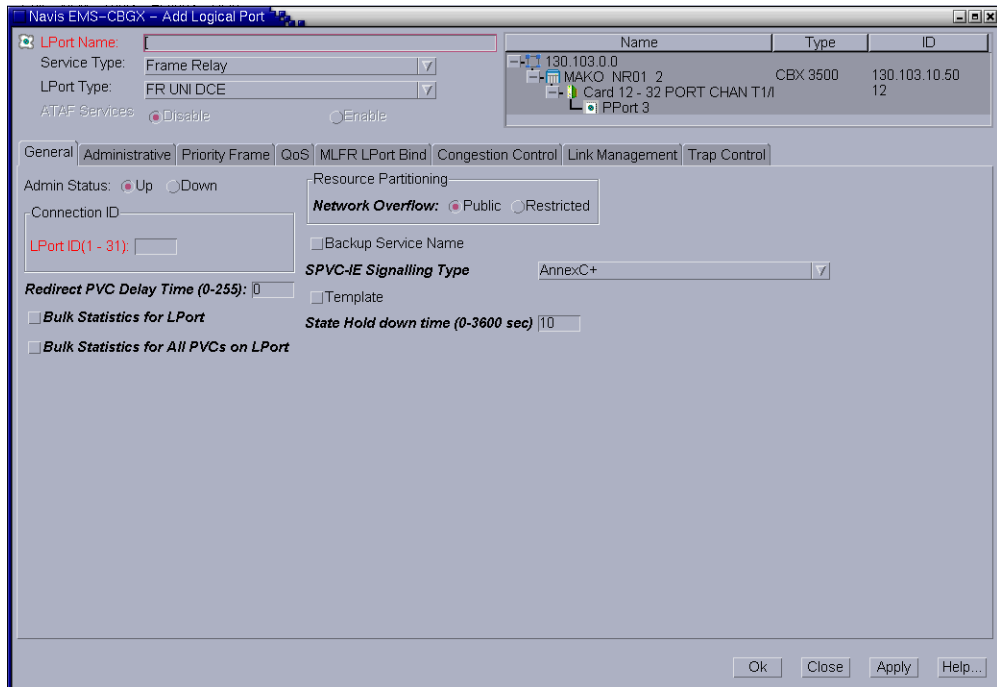
For the 32-Port Channelized T1/E1 FR/IP Modules:

- a. Expand the Cards node, expand the PPort node, and expand the node for the specific physical port.
- b. Right-click the LPorts node, and select Add on the popup menu as shown in Figure 5-5.



**Figure 5-5. Navigation Panel: Add LPorts**

The Add Logical Port dialog box is displayed (Figure 5-6).



**Figure 5-6. Add Logical Port Dialog Box**

- c. Continue with [step 3](#).
3. In the `Service Type` field, select `Frame Relay`.
4. In the `LPort Type` field, select the logical port (LPort) type that corresponds to the MLFR bundle LPort Type to which you want to bind this ML Member, as shown in [Table 5-3](#).

**Table 5-3. ML Member and MLFR Bundle LPort Bindings**

ML Member LPort Type	MLFR Bundle LPort Type
FR UNI DCE	MLFR UNI DCE
FR UNI DTE	MLFR UNI DTE
FR NNI	MLFR NNI

5. In the `LPort ID` field, enter a number that uniquely identifies this logical port on the selected DS1 or T1/E1 channel.

For the 4-Port Channelized DS3/1/0 modules, enter a number in the range 1 to 24 for the 24 DS0 channels available per DS1 channel.

For the 32-Port Channelized T1/E1 FR/IP module, the number you specify depends on the operation mode (T1 or E1) selected for the 32-Port Channelized T1/E1 FR/IP IOM in the `Modify Card` dialog box as follows:

- **T1 Mode** – If the module is configured in T1 mode, then enter a number in the range 1 to 24 for the 24 DS0 channels available per physical port in the T1 mode.
- **E1 Mode** – If the module is configured in E1 mode, then enter a number in the range 1 to 31 for the 30 TS0 channels available per physical port in the E1 mode.

Refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on the `Modify Card` dialog box.

6. Follow the instructions in “**Defining Frame Relay UNI DCE/DTE or NNI LPorts**” on page 3-10 to configure the ML Member logical port.



**Note** – Follow the “**MLFR Features for 4-Port Channelized DS3/1 and DS3/1/0 FR/IP and 32-Port Channelized T1/E1 FR/IP Modules**” on page 5-4 when defining the ML Member logical ports.

7. You *must* disable the link management protocol for an ML Member logical port in order to bind it to an MLFR UNI/NNI bundle logical port, as described in the next section. To disable the ML Member logical port’s link management protocol, follow these steps:
  - a. Display the `Add Logical Port` dialog box or `Modify Logical Port` dialog box for the ML Member logical port.
  - b. In the `Link Management` tab, select `Disabled` in the `Protocol` list box. This disables link management for the ML Member logical port.
8. Click `OK` to save the configuration.

### Binding and Unbinding ML Members to MLFR Bundle Logical Ports

After you define the MLFR bundle logical port and ML Member logical ports, you create the MLFR UNI/NNI bundle by binding one or more ML Member logical ports to the MLFR UNI/NNI bundle logical port. To reduce bandwidth on the MLFR UNI/NNI bundle, you can also unbind ML Member logical ports from the MLFR UNI/NNI bundle logical port.

Observe the following guidelines:

- Lucent recommends that you bind no more than eight ML Member logical ports to each MLFR UNI/NNI bundle logical port that you configure.
- In order to bind an ML Member logical port to an MLFR UNI/NNI bundle logical port, you *must* first disable the link management protocol for the ML Member logical port. See [step 7 on page 5-14](#) for instructions.

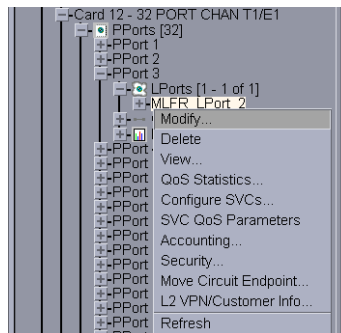
- While an ML Member logical port is bound to an MLFR bundle, you *cannot* modify the ML Member's link management attributes. After you bind the ML Member to the bundle, the Link Management settings in the Modify Logical Port dialog box are unavailable.
- After you unbind an ML Member logical port from an MLFR bundle, you can modify the ML Member's link management attributes. The Link Management settings in the Modify Logical Port dialog box become available.

You can bind ML Member logical ports using the Member Bind tab or the MLFR LPort Bind tab in the Modify Logical Port dialog box.

### **MLFR LPort Bind Tab**

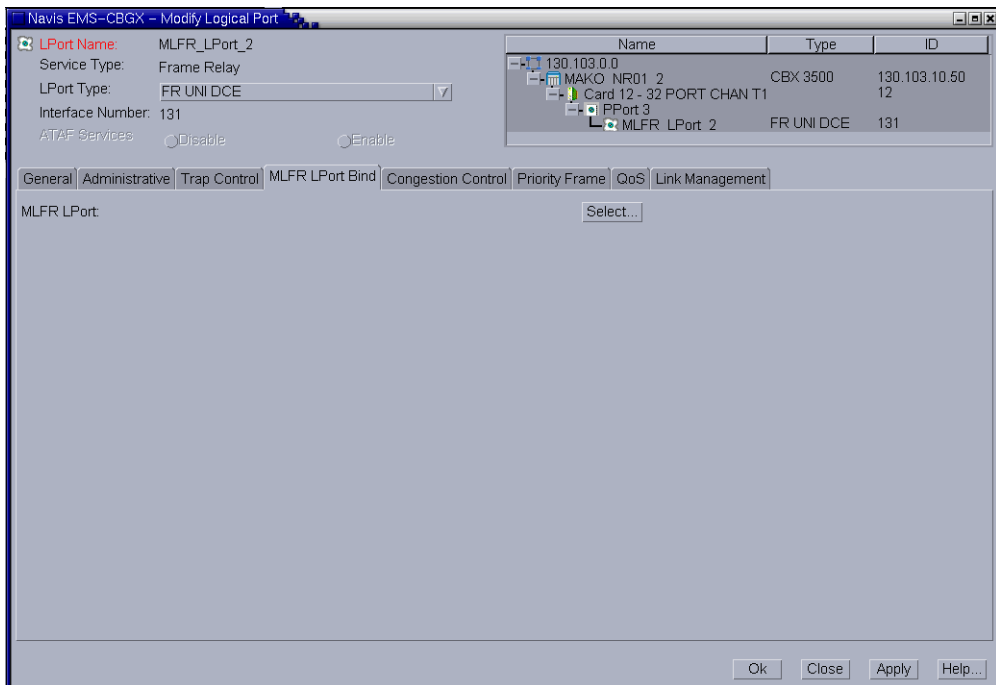
To bind ML Member logical ports to MLFR UNI/NNI bundle logical port, select the MLFR LPort Bind tab for ML Member logical port in the Modify Logical Port dialog box:

1. In the Switch tab, expand the Cards node.
2. Expand the PPorts node, and expand the node for the specific physical port.
3. Expand the LPorts node, and right-click the LPorts instance that want to modify as shown in [Figure 5-7](#).



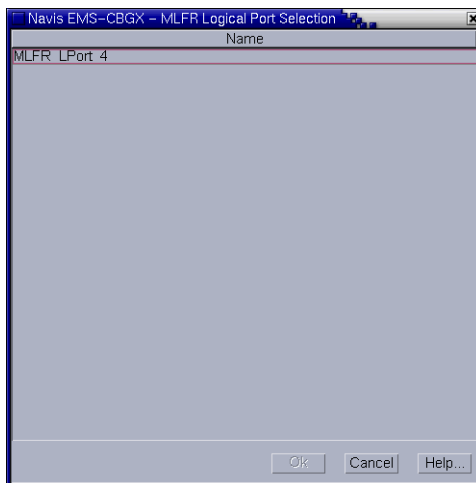
**Figure 5-7. Navigation Panel: Modify Logical Port**

The Modify Logical Port dialog box is displayed (Figure 5-8).



**Figure 5-8. Modify Logical Port Dialog Box**

4. Click Select to view the MLFR Logical Port Selection dialog box (Figure 5-9).



**Figure 5-9. MLFR Logical Port Selection Dialog Box**

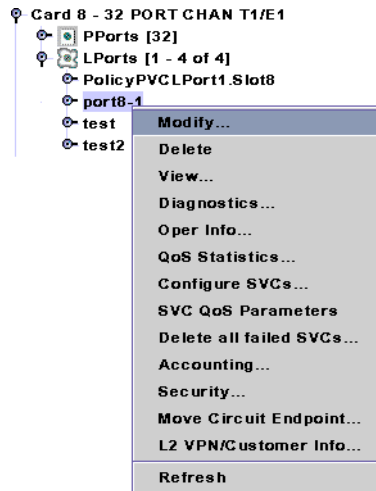
5. Select an MLFR Logical Port, and then click OK to bind the selected MLFR logical port and return to the Modify Logical Port dialog box.
6. Click OK in the Modify Logical Port dialog box to save the modifications.



### Member Bind Tab

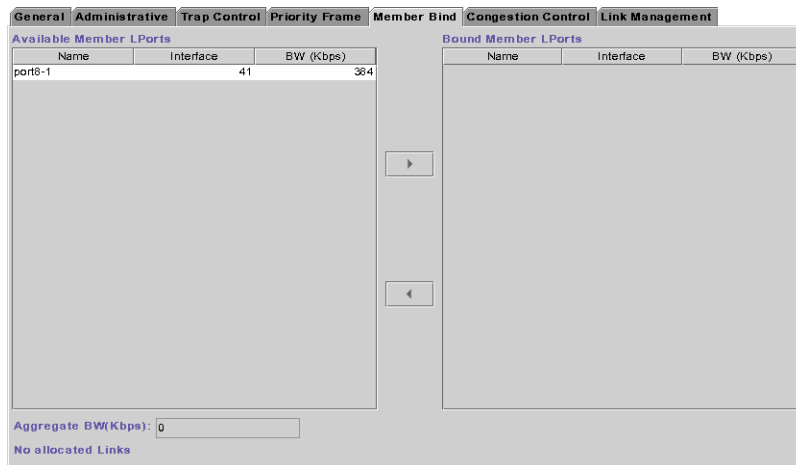
To bind or unbind ML Member logical ports to MLFR UNI/NNI bundle logical port, select the Member Bind tab for MLFR logical port in the Modify Logical Port dialog box:

1. In the Switch tab, expand the Cards node.
2. Expand the LPorts node, and right-click the logical port you want to modify as shown in [Figure 5-10](#).



**Figure 5-10. Modifying an MLFR Bundle Logical Port**

3. In the Modify Logical Port dialog box, click the Member Bind tab ([Figure 5-11](#)).



**Figure 5-11. Modify Logical Port Dialog Box: Member Bind Tab**

In the Member Bind tab, Aggregate BW displays the aggregate bandwidth of all ML member logical ports bound to this MLFR UNI/NNI bundle logical port, expressed in kilobits per second. If no ML members are bound to this MLFR

UNI/NNI bundle logical port, the `Bandwidth` field displays 0 (zero). `Allocated Links` displays the number of links that are allocated for ML member logical ports to bind to this MLFR bundle. For each member logical port, the `BW` column displays the bandwidth of the selected ML Member logical port.

- To bind an ML Member logical port to the MLFR bundle, select an ML Member logical port from the `Available ML Member LPorts` list and choose `Bind`. The selected logical port is removed from the available list and added to the list on the right. The system updates the `Aggregate BW (kbps)` field to include the bandwidth of the bound logical port.

The link management protocol setting *must* be disabled for the ML Member logical port that you are binding to the MLFR bundle. Otherwise, Navis EMS-CBGX will display an error message when you choose `Bind`. For instructions on disabling the link management protocol for an ML Member logical port, see [step 7 on page 5-14](#).

- To unbind a bound ML Member logical port from the MLFR bundle, select a bound ML Member logical port from the `Bound ML Member LPorts` list and choose `Unbind`. The selected logical port is removed from the bound list and added to the available list on the left. The system updates the `Aggregate BW (kbps)` field to include the removal of the bandwidth of the unbound logical port from the bundle.

4. Click `OK` when you have configured the logical port.

## Configuring MLFR on the 6-Port Channelized DS3/1/0 Module

This section describes the following tasks to configure MLFR UNI/NNI bundle logical ports on the 6-Port Channelized DS3/1/0 Frame Relay module:

- [“Defining an MLFR Logical Port” on page 5-18](#)
- [“Configuring a Logical Port for a Layer2 VPN and Customer” on page 5-25](#)
- [“Modifying Member LPorts” on page 5-23](#)
- [“Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint” on page 5-26](#)

### Defining an MLFR Logical Port

To access the MLFR logical port attributes and functions, perform the following tasks:

1. In the `Switch` tab, expand the `Cards` node.

2. Right-click the LPorts node, and click Add on the popup menu as shown in Figure 5-12.

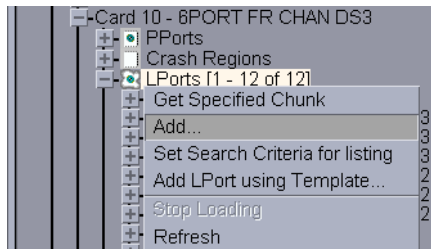


Figure 5-12. Navigation Panel: Add LPorts

The Add Logical Port dialog box is displayed (Figure 5-13).

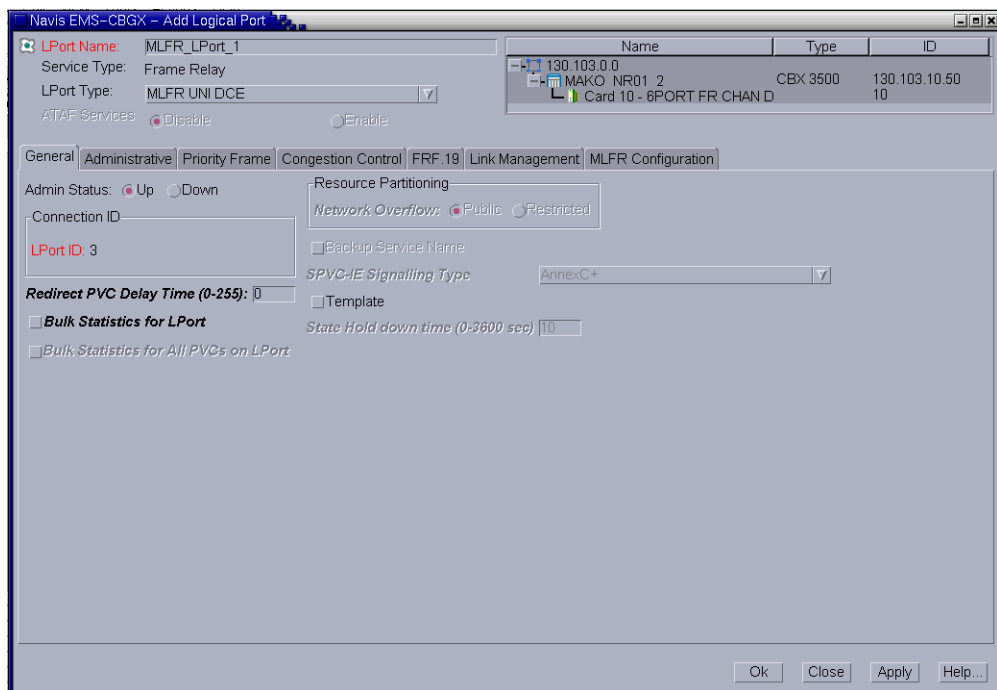


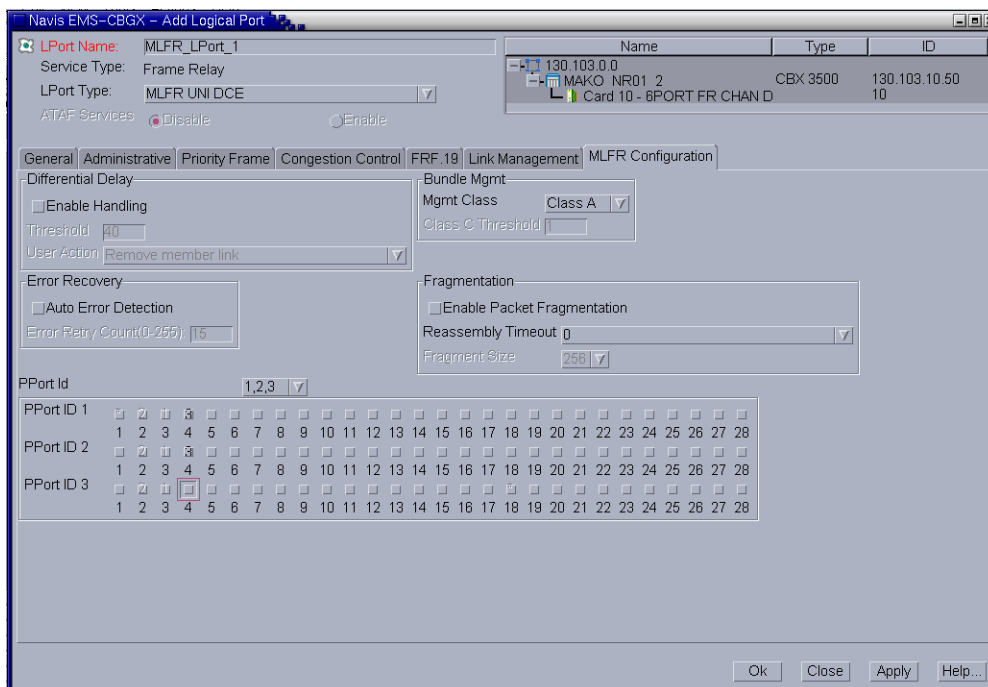
Figure 5-13. Add Logical Port Dialog Box

- In the Add Logical Port dialog box, complete the dialog box fields described in [Table 5-4](#).

**Table 5-4. Add Logical Port Type Dialog Box Fields**

Field	Action/Description
Service Type	<i>Frame Relay</i> is displayed.
LPort Type	Select one of the following types for the MLFR bundle logical port: <ul style="list-style-type: none"> <li>• MLFR UNI DCE</li> <li>• MLFR UNI DTE</li> <li>• MLFR NNI</li> </ul>
LPort ID	Enter a non-zero number from 1 to 99 that uniquely identifies this MLFR bundle logical port. The number you enter must be unique among all the MLFR bundle logical ports configured on the dummy PPort. (An LPort ID used on dummy PPort 8 can be repeated on dummy PPort 9.)  <b>Note:</b> <i>You can configure a maximum of 42 MLFR UNI/NNI bundle logical ports on dummy PPort 8 and 42 MLFR UNI/NNI bundle logical ports on dummy PPort 9.</i>

- Click the MLFR Configuration tab as shown in [Figure 5-14](#).



**Figure 5-14. Add/Modify Logical Port: MLFR Configuration Tab**

5. In the MLFR Configuration tab, set the PPort ID and select channels as follows:
  - Select 1,2,3 to create an MLFR logical port bundle that can include members from PPorts 1, 2, and 3. Displays a dummy PPort ID of 8 in the Navis EMS-CBGX Details panel after creation.
  - Select 4,5,6 to create an MLFR logical port bundle that can include members from PPorts 4, 5, and 6. Displays a dummy PPort ID of 9 in the Navis EMS-CBGX Details panel after creation.

Next to each PPort ID, the DS1 channels that can be bound to the MLFR bundle are displayed. Channels that are already bound to an MLFR bundle appear grayed out, and display the bundle ID.

To bind a channel to the current MLFR bundle, click on the channel. A maximum of 12 channels can be bound to an MLFR bundle.

6. Set other attributes in the MLFR Configuration tab as described in [Table 5-5](#).

**Table 5-5. MLFR Configuration Tab**

Elements	Action/Description
<b>Differential Delay</b>	
Enable Handling	This field enables/disables differential delay monitoring. For more information see <a href="#">“Differential Delay” on page 5-6</a> . Options include: <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Disables differential delay monitoring.</li> <li>• <i>Enable</i> – Enables differential delay monitoring.</li> </ul>
Threshold	Enter the threshold, in milliseconds, that the differential delay must exceed before the user action is taken on the member link.
User Action	This field is displayed when Handling is set to Enable. Determines the action that will be taken on a member link when the differential delay for the member exceeds the threshold. Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Remove member link</i> – (default) The link is taken out of service.</li> <li>• <i>Stop member link traffic and restore</i> – The link stops transmitting outgoing traffic, and resumes transmitting traffic when the delay has been corrected.</li> <li>• <i>Stop member link traffic but do not restore</i> – The link stops transmitting outgoing traffic, but does not resume transmission of traffic when the delay has been corrected.</li> <li>• <i>No action</i> – No action on the link is taken when the threshold is exceeded. (SNMP traps are still generated when the threshold is exceeded).</li> </ul>

**Table 5-5. MLFR Configuration Tab (Continued)**

Elements	Action/Description
<b>Error Recovery</b>	
Auto Error Detection	<p>Auto error detection identifies errors coming into the MLFR bundle logical port, such as lost events, and shuts down the logical port connection. Enabled by default.</p> <p>(This setting is overridden at the circuit level by the Auto Error Detection setting for the specific circuit. See <a href="#">“Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint”</a> on page 5-26.)</p>
Error Retry Count	<p>If you enabled Auto Error Detection, specify the number of retries that should be attempted before the connection is shut down. Enter a value between 0 and 255. The default value is 15.</p> <p>(This setting is overridden at the circuit level by the Error Retry Count setting for the specific circuit. See <a href="#">“Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint”</a> on page 5-26.)</p>
<b>Bundle Mgmt</b>	
Mgmt Class	<p>Determines how the MLFR bundle operational status will be set if individual member links are inactive. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Class A</i>– (default) The MLFR bundle is up as long as at least one of its members is active and operational.</li> <li>• <i>Class B</i>– The MLFR bundle is up only if all of its members are active and operational.</li> <li>• <i>Class C</i>– The MLFR bundle is up as long as a minimum number of its members are active and operational. You specify this minimum value in the Class C Threshold field.</li> </ul>
Class C Threshold	<p>This field is displayed when Mgmt is set to Class C. Enter a value for the minimum number of member links that must be active and operational for the MLFR bundle to be up.</p>

**Table 5-5. MLFR Configuration Tab (Continued)**

Elements	Action/Description
<b>Fragmentation</b>	
Packet Fragmentation	<p>Packet fragmentation partitions frames into equal lengths before sending data over the MLFR bundle so that member links can be evenly loaded with data. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Disables packet fragmentation.</li> <li>• <i>Enable</i> – Enables packet fragmentation. You specify the fragment size in the Fragment Size field.</li> </ul>
Reassembly Time-out (msec)	Select the length of time that frame fragments in a packet will wait at the destination for missing fragments before the packet is dropped. Values are available from 0 to 140 milliseconds, in increments of 10.
Fragment Size	This field is displayed when Packet fragmentation is set to Enable. Select a value for the length of the fragments into which frames are partitioned. The available choices are 128, 256, and 512.

7. Complete other tabs in the Add Logical Port dialog box as described in [Chapter 3, “Configuring Frame Relay LPorts”](#).
8. Click OK to configure the MLFR bundle logical port. Logical ports are automatically created on the channels that you chose to bind.

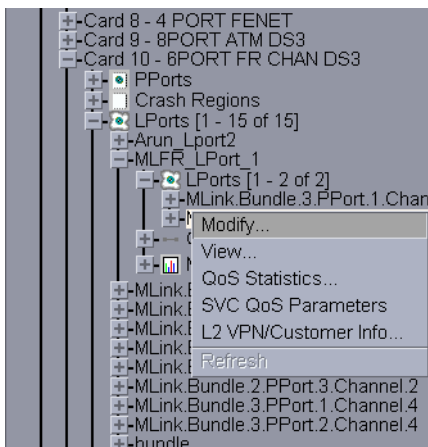
### Modifying Member LPorts

The member LPorts for the MLFR bundle are configured when you create the MLFR bundle. You can modify some attributes for individual members after you have created the MLFR LPort bundle, and bind or unbind members to and from bundles.

To modify a member LPort for a 6-Port Channelized DS3/1/0 Frame Relay module, perform the following tasks:

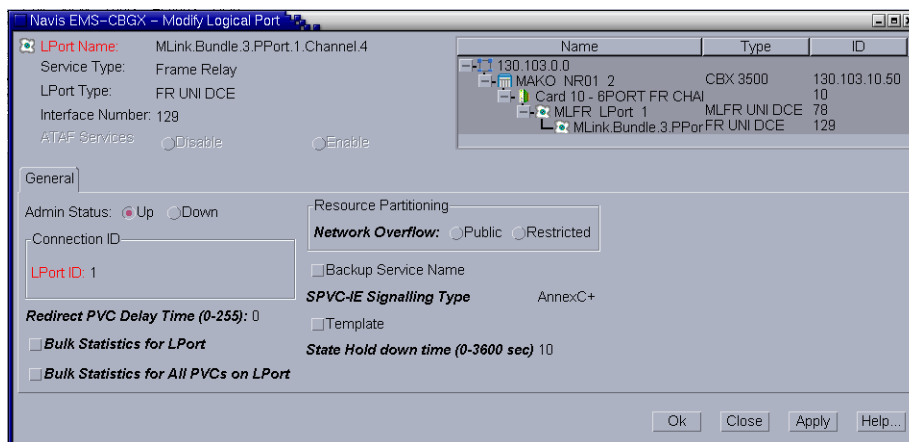
1. In the Cards node, expand the LPort node.
2. Expand the node for the specific DS1 channel that corresponds to the member logical port.

- Expand the LPorts node, and right-click the logical port you want to configure. Then select Modify from the popup menu as shown in Figure 5-15.



**Figure 5-15. Modifying a Member LPort**

The Modify Logical Port dialog box is displayed (Figure 5-16).



**Figure 5-16. Modify Logical LPort Dialog Box**

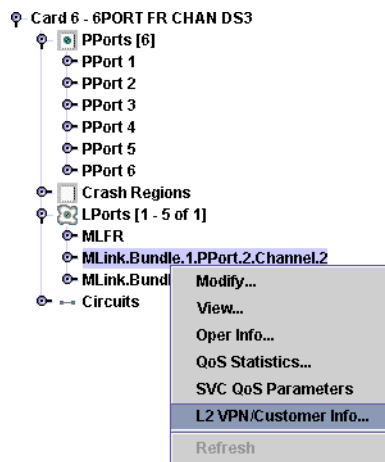
- In the General tab, modify the required fields.
- Click OK to save the modifications.



## Configuring a Logical Port for a Layer2 VPN and Customer

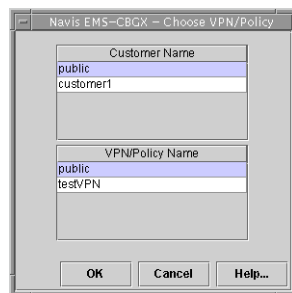
After you configure an MLFR Bundle logical port, use the following steps to dedicate it to a Layer2 VPN and customer.

1. In the `Switch` tab, expand the `Cards` node.
2. Expand the `LPorts` node, and right-click the node for the logical port you want to assign.
3. Select `L2 VPN / Customer Info` from the popup menu, as shown in [Figure 5-17](#).



**Figure 5-17.** Assigning a Logical Port to an L2 VPN or Customer

The `Choose VPN / Policy` dialog box ([Figure 5-18](#)) is displayed.



**Figure 5-18.** Choose VPN / Policy Dialog Box

4. Select the Customer Name and Layer2 VPN Name.



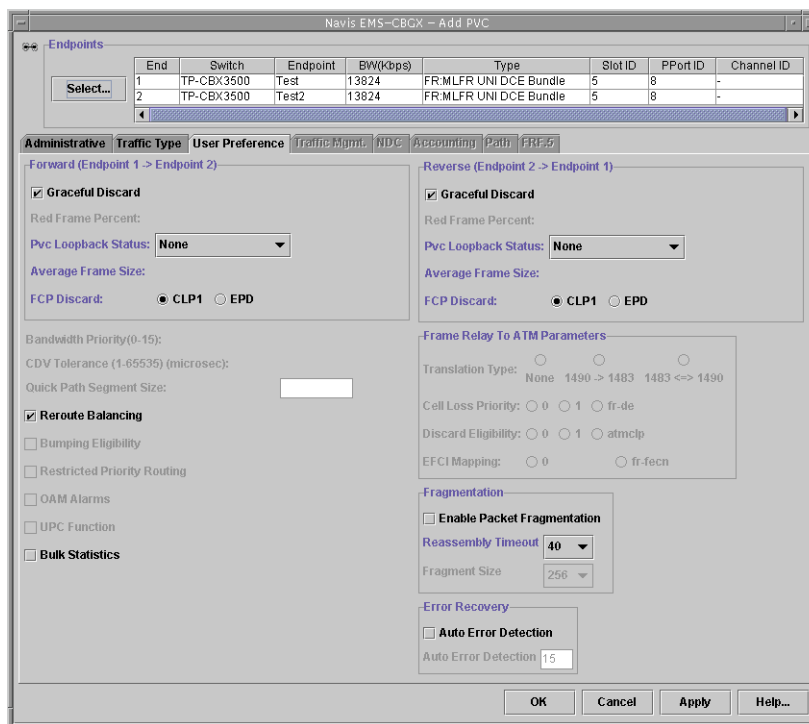
**Note** – Changing the Customer Name does not admin down the logical port.

5. Click `OK`.

## Configuring Circuits With an MLFR UNI/NNI Bundle Logical Port Endpoint

To configure a circuit that has an MLFR UNI/NNI Bundle logical port endpoint on a 6-Port Channelized DS3/1/0 Frame Relay I/O Module, you need to configure an additional set of Error Recovery attributes in the User Preference tab.

1. Follow the instructions in for the type of circuit you want to configure, selecting an MLFR UNI/NNI Bundle logical port as an endpoint.
2. In the `User Preference` tab, complete the Error Recovery fields shown in [Figure 5-19](#) and described in [Table 5-6](#).



**Figure 5-19. Add/Modify PVC: User Preference Tab**

3. Set the Error Recovery attributes in the User Preference tab as described in [Table 5-6](#).

**Table 5-6. User Preference Tab: Error Recovery Settings**

Field	Action
Auto Error Detection	Auto error detection identifies errors coming into the MLFR bundle logical port on the circuit, such as lost events, and shuts down the connection for the circuit. This value overrides the Auto Error Detection setting made at the LPort level.  Select one of the following: <ul style="list-style-type: none"><li>• <i>Enable</i> – Enables auto error detection.</li><li>• <i>Disable</i> – (default) Disables auto error detection.</li></ul>
Error Retry Count	If you enable Auto Error Detection, specify the number of retries that should be attempted before the circuit connection is shut down. Enter a value between 0 and 255. The default value is 15. This value overrides the Error Retry Count setting made at the LPort level.

4. Complete the circuit definition as described in [Chapter 7, “Configuring Permanent Virtual Circuits \(PVCs\)”](#).



# Configuring Multilink Point-to-Point Protocol Bundles

This chapter explains Multilink Point-to-Point Protocol (MLPPP). It describes the configuration of MLPPP bundles on a 32-Port Channelized T1/E1 Frame Relay module.

This chapter contains:

- [“About MLPPP” on page 6-1](#)
- [“Administrative Tasks” on page 6-7](#)

## About MLPPP

This section explains MLPPP links, bundles, and statistics. It also lists the MLPPP-supported protocols. See the following topics:

- [“Overview” on page 6-1](#)
- [“MLPPP Links” on page 6-2](#)
- [“MLPPP Bundles” on page 6-2](#)
- [“MLPPP Features” on page 6-4](#)
- [“Supported Protocols” on page 6-5](#)
- [“Fragmentation and Reassembly” on page 6-6](#)

## Overview

MLPPP is a method of bundling multiple Point-to-Point Protocol (PPP) links to achieve more bandwidth and less latency. The aggregation of links is achieved through a technique called *bundling*. Bundling consolidates one or more physical interfaces into one logical unit. It results in more bandwidth on the bundle port than available on any single link. The bundle interface contains the configuration for the MLPPP bundle and the default PPP link configuration.

Figure 6-1 illustrates the applications of the MLPPP implementation.

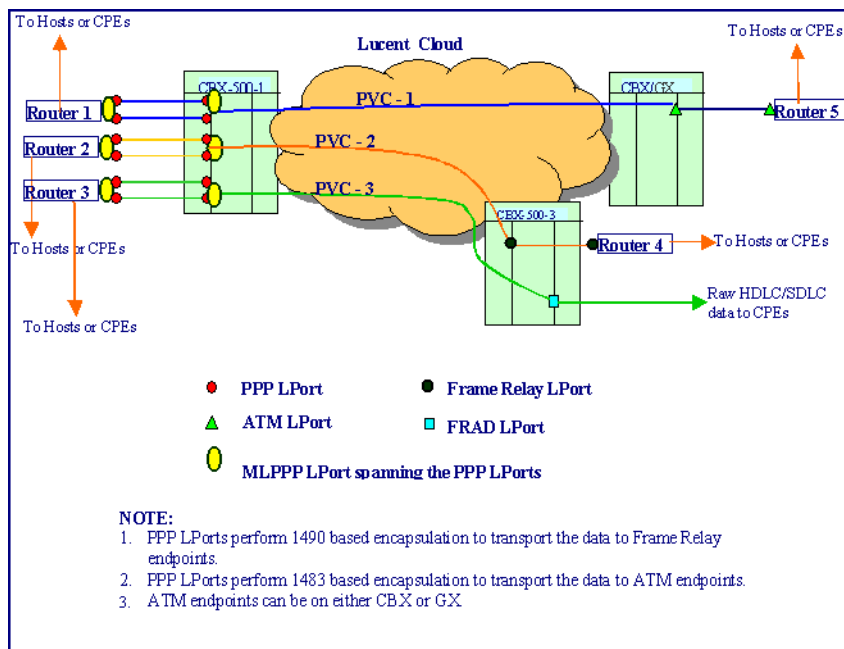


Figure 6-1. Network Diagram for MLPPP Applications



**Note** – MLPPP does not support IP LPort configuration on the MLPPP LPorts.

## MLPPP Links

An MLPPP bundle is a virtual LPort on a card. One or more PPP LPorts of the same card can be attached to this bundle. All the PPP links attached to a bundle form the MLPPP link and the bundle LPort represents an endpoint of the MLPPP link. You can bind one or more PPP links to the bundle interface. This action causes the PPP link to be added in the member list of the bundle object. The PPP links and the bundle interface belong to the same card for binding.

## MLPPP Bundles

You can configure the MLPPP bundles through Navis EMS-CBGX. The MLPPP bundle interfaces are defined at the card level on a 32-Port T1/E1 Frame Relay module. This bundle interface contains the configuration of the MLPPP bundle and the default PPP link configuration. By provisioning an MLPPP bundle interface, a new interface of the MLPPP type and a bundle object are created.

You can bind one or more PPP links to the bundle interface. This causes the PPP link to be added in the member list of bundle objects. The PPP links and the bundle interface belong to the same card for binding.

After the first PPP link is established with LCP set to the Opened state, Network Control Protocols (NCPs) move to the Establishment state at the bundle level. MLPPP requires that LCP protocols are exchanged per link basis. The BCP, IPCP, and BACP Network Control Protocols are exchanged at bundle level.

Bundle objects negotiate NCPs using the member PPP links that have the LCP state set to Opened. The member links are used to transmit and receive the NCP packets. The NCP packets are processed in the context of the bundle. The response to a request type NCP packet need not use the same PPP link.

After establishing the relevant NCP, data flows with multilink headers. If fragmentation is enabled, then the packets will be fragmented, and the fragments are sent as per the fragmentation criterion. The received fragments are buffered to collect all the fragments between the Being and End bits to form a complete packet. These complete packets are sent out on the other of PVC in a sequence. See [“Fragmentation Strategy” on page 6-6](#).

The data packets transmitted over the active member links are assigned an ascending sequence number. This sequence number is encoded in the MLPPP header of the packet and it is a 24-bit rolling number that starts from zero. It is used to guarantee the order of the packet delivery at the receiving system.

The data packets, either non-fragmented singleton packets or fragments of a packet, are distributed across all member links such that the load on all member links is balanced.

Figure 6-2 illustrates the data flow of different packets within the system.

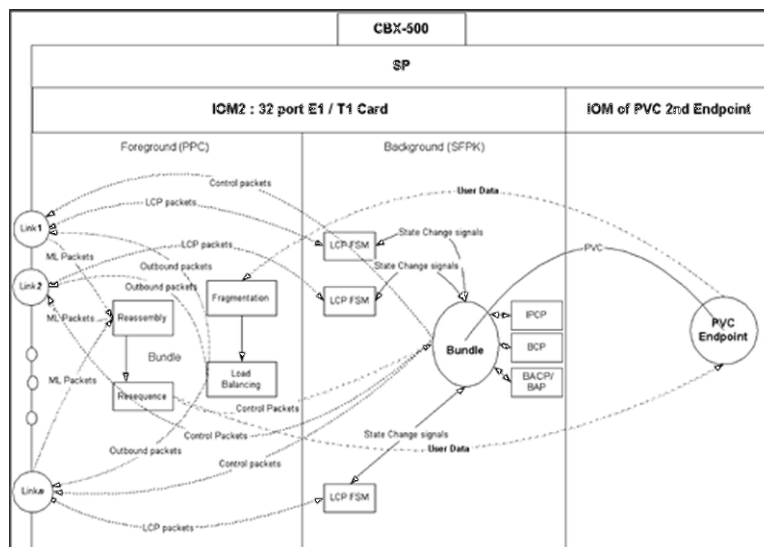


Figure 6-2. Data Flow Diagram

This implementation maintains the LCP, IPCP, and BCP states at the foreground processor of the IOM2 module. When these states are set to Opened, then, only the respective user data flow will be allowed.



**Note** – In Figure 6-2, for simplicity, both the endpoints of PVC are on the same switch. However, the endpoints of PVC can be defined on different switches.

## MLPPP Features

MLPPP supports the following features:

- Statistics and bulk statistics for the supported PVCs
- LPort-level statistics for the MLPPP LPort
- Eventlog mechanism
- Alarms and traps
- Packet fragmentation and reassembly

Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on alarms, eventlog, and LPort statistics summary.



## Supported Protocols

This section describes the MLPPP-supported protocols. The following protocols are defined:

- “Point-to-Point Protocol” on page 6-5
- “Link Control Protocol” on page 6-5
- “IP Control Protocol” on page 6-5
- “Bridging Control Protocol” on page 6-6

### Point-to-Point Protocol

Point-to-Point Protocol (PPP) provides a standard method for transporting multiprotocol datagrams over Point-to-Point links. PPP has three main components:

- A method for encapsulating multi-protocol datagrams.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

### Link Control Protocol

The Link Control Protocol (LCP) is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common mis-configuration errors, and terminate the link. The optional facilities provided are authenticating the identity of its peer on the link, and determining the link failures.

In order to establish communications over a Point-to-Point link, each end of the PPP link sends LCP packets to configure and test the data link. After the link has been established, the peer can be authenticated. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs such as an inactivity timer expires or network administrator intervention.

### IP Control Protocol

The IP Control Protocol (IPCP) is responsible for configuring, enabling, and disabling the IP protocol modules on both ends of the Point-to-Point link. IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPCP packets received before this phase are discarded.

### Bridging Control Protocol

The Bridging Control Protocol (BCP) is configured, enabled, and disabled on both ends of the Point-to-Point link. BCP uses the same packet exchange mechanism as the Link Control Protocol. BCP packets are not exchanged until PPP reaches the Network-Layer Protocol phase. BCP packets received before this phase are discarded.

## Fragmentation and Reassembly

Fragmentation is the process by which a large packet is broken into multiple smaller fragments for simultaneous transmission across multiple links of an MLPPP bundle.

Reassembly is the process by which the destination router reassembles the fragments into the original packets. Use MLPPP fragmentation and reassembly to reduce transmission latency. You can configure fragmentation and reassembly for all current member links in an MLPPP bundle.

### Fragmentation Strategy

You can enable or disable the Fragmentation option on the IOM2 MLPPP bundles.

When you disable the Fragmentation option on the bundle, then:

- The packets received from the other (Frame Relay/ATM/FRAD) endpoint of PVC are checked for MRRU and MRU size.
  - If MRRU is more than the received packet length, and the bundle has a member link with MRU more than the packet length, then the packet will be transmitted on that member link with the Begin and End bits set in an MLPPP header.
  - If either MRRU is less than packet length or no member link exists with MRU higher than packet length, then the received packet will be discarded at bundle interfaces.
- When the packets received from peer indicate that they are fragmented (both the Begin and End bits are not set in the same packet), then fragmented packets are discarded, and the expected sequence numbers on those links are updated.
- When the complete packets are received from peer, the packets are verified if the NCPs are Open and the particular packet type is allowed or not. If verifications are valid, then the packet passes through the necessary header format conversions and transmitted out of the other PVC endpoint.

When you enable the Fragmentation option, then:

- The packets received from the other (Frame Relay/ATM/FRAD) endpoint of PVC are checked for MRRU and MRU size.
  - If the packet length is more than MRRU size, then the packet is dropped.
  - The segment size is calculated per link as least of configured fragment size (bundle level parameter) and peer MRU of the link. If the segment size member link is more than packet size, then the packet sent out to peer as complete packet with the Begin and End bits set in an MLPPP header.
  - If the segment size is less than packet length, then the packet segmented and sent out using the available member links.
- When complete packets are received from peer, these packets will be verified if the NCPs are Open and the particular packet type is allowed or not. If verifications are valid, then the packet will go through necessary header format conversions and transmitted out of other PVC endpoint.
- When the packets received from peer indicate that they are fragmented (both the Begin and End bits not set in the same packet), these packets or segments will be in a reassembly buffer queue, and checked for completeness. If the segment completes a packet, the completed packet will be delivered to the other end of PVC after verifying the NCP state, packet type, and necessary header format conversions.

## Administrative Tasks

The following sections describe how to configure MLPPP bundles on a 32-Port T1/E1 Frame Relay module:

- [“Defining MLPPP Logical Ports” on page 6-8](#)
- [“Setting MLPPP LPort Attributes” on page 6-8](#)
- [“Configuring the MLPPP Bundle” on page 6-12](#)
- [“Configuring PVCs With an MLPPP Bundle LPort Endpoint” on page 6-14](#)

## Defining MLPPP Logical Ports

To define an MLPPP LPort, perform the following tasks:

1. In the Switch tab, expand the Cards node and then select the 32-Port T1/E1 FR module.
2. Right-click the LPorts node of the selected card and then select Add. The Add Logical Port dialog box is displayed (Figure 6-3).

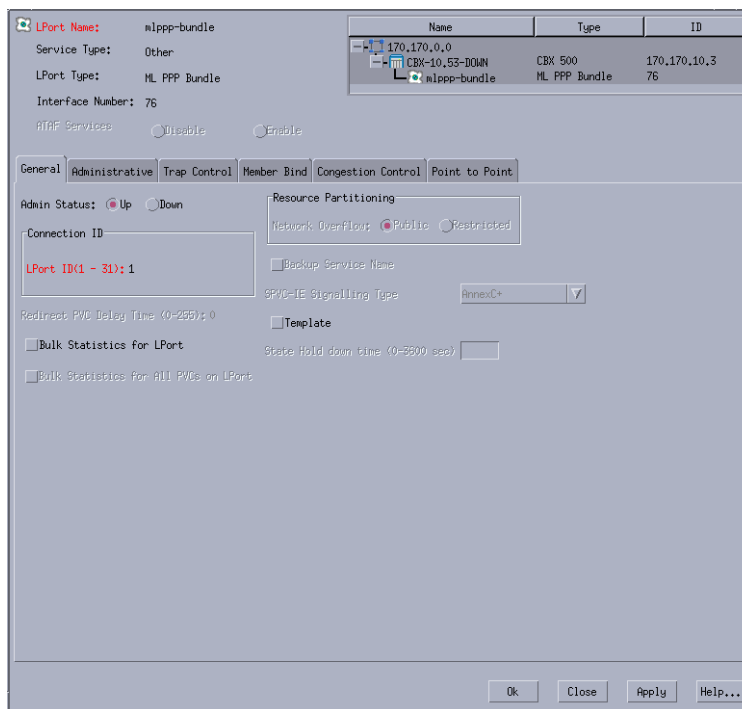


Figure 6-3. Add Logical Port Dialog Box

3. Select Service Type as Other.
4. Select LPort Type as MLPPP Bundle.
5. Continue with “Setting MLPPP LPort Attributes” on page 6-8.

## Setting MLPPP LPort Attributes

When you define a new MLPPP logical port, the Add Logical Port dialog box (Figure 6-3 on page 6-8) displays a series of tabs that enable you to set attributes for the logical port. The following tabs are displayed:

- **General** - Set the general logical port parameters such as Admin Status. See “General Attributes for Frame Relay LPorts” on page 3-12.
- **Administrative** - Set the admin-related parameters including Bandwidth parameters. See “Administrative Attributes for Frame Relay LPorts” on page 3-15.

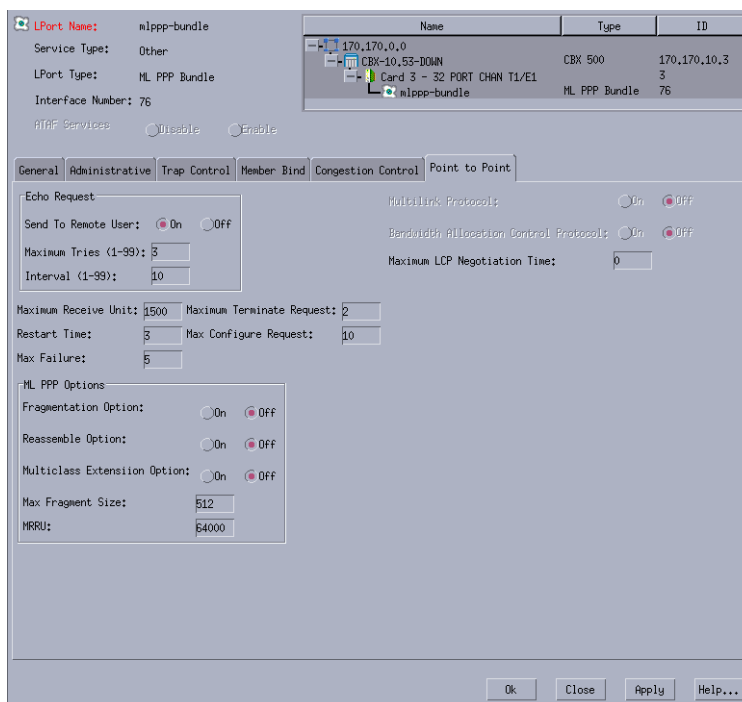
- **Trap Control** - Set the congestion threshold percentage in which traps are generated and the number of frame errors per minute for each logical port. The supported logical port types are different for each I/O module. See [“Trap Control Attributes for Logical Ports” on page 3-40](#).
- **Member Bind** - Bind any ML member LPorts that have already been configured. You can also bind additional member LPorts later. See [“Binding and Unbinding ML Members to MLFR Bundle Logical Ports” on page 5-14](#).
- **Congestion Control** - Set the threshold parameters (mild, severe, and absolute) that determine how the switch responds to congestion in the network. See [“Congestion Control Attributes \(VFR-NRT only\) for Frame Relay LPorts” on page 3-24](#).
- **Point-to-Point** - See [“Setting Point-to-Point Attributes” on page 6-9](#).

### Setting Point-to-Point Attributes

To set the attributes on the Point-to-Point tab, perform the following tasks:

1. In the `Switch` tab, expand the `Cards` node and then select the `32-Port T1/E1 FR` module.
2. Right-click the `LPorts` node of the selected card and then select `Add`. The `Add Logical Port` dialog box is displayed ([Figure 6-3 on page 6-8](#)).

3. Select the **Point-to-Point** tab. The **Point-to-Point** tab of the Add Logical Port dialog box is shown in **Figure 6-3** on page 6-8.



**Figure 6-4. Add Logical Port: Point-to-Point Tab**

4. Complete the fields in the **Point-to-Point** tab as described in **Table 6-1**.

**Table 6-1. Add/Modify Logical Port: Point-to-Point Tab**

Element	Description
<b>Echo Request</b>	
Send to Remote User	Select <i>On</i> (default) or <i>Off</i> to send the echo request to the remote user.
Maximum Tries	Enter a value in the range of 1 to 99 for the maximum echo request tries. The default value is three tries.
Interval	Enter a value in the range of 1 to 99 for the interval. The default value is 10 seconds.  If this option is given, then an LCP echo-request frame is send to the peer every n seconds, where n is the interval value. This option can be used with the LCP echo failure option to detect that the peer is no longer connected.
Maximum LCP Negotiation Time	Enter the LCP negotiation time.

**Table 6-1. Add/Modify Logical Port: Point-to-Point Tab (Continued)**

Element	Description
Maximum Receive Unit	<p>Enter the negotiated maximum receive unit for the local and remote (peer) side of the link. The default value is 1500 bytes.</p> <p>MRU is the maximum length of the PPP Information field, a system wants to receive, which includes Padding, but not including Protocol field.</p> <p>You can configure this parameter on PPP links. IOM2 supports MRU values from 1500 to 64000 bytes with default value 1500 octets. However, the peer can indicate a different value for its MRU in the Configure-Request. If the configured MRU value is more than 1500, then the Configure-Request contains the MRU option to negotiate higher MRU value to peer.</p>
Maximum Terminate Request	<p>Enter the maximum number of terminate requests. The default value is three times.</p> <p>The maximum terminate request indicates the number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond.</p>
Restart Time	<p>Enter the LCP restart interval (retransmission timeout). The default value is three seconds.</p> <p>LCP Finite State Machine (FSM) uses the Restart timer to time transmissions of Configure-Request and Terminate-Request packets. Expiration of the Restart timer causes a Timeout event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.</p>
Max Failure	<p>Enter the maximum number of Configure-Nak packets sent without sending a Configure-Ack before assuming that configuration is not converging. The default value is five tries.</p>
<b>MLPPP Options</b>	
Fragmentation Option	<p>Select <i>On</i> or <i>Off</i> (default) to enable fragmentation. If this option is selected, then a large packet is broken up into multiple smaller fragments for simultaneous transmission across multiple links of an MLPPP bundle.</p>
Reassemble Option	<p>Select <i>On</i> or <i>Off</i> (default) to enable reassemble. If this option is selected, then the destination router reassembles the fragments into the original packets.</p>
Multiclass Extension Option	<p>Select <i>On</i> or <i>Off</i> (default) to enable multiclass extension. If this option is selected, then the extension enables multiple classes of service using MLPPP.</p>
Max Fragment Size	<p>Enter the maximum fragment size. The default value is 512 bytes.</p>

**Table 6-1. Add/Modify Logical Port: Point-to-Point Tab (Continued)**

Element	Description
MRRU	Enter the maximum receive reconstructed unit (MRRU) for the local and remote (peer) side of the link. The default value is 64000 bytes.  MRRU specifies the maximum number of octets in the Information fields of reassembled packets. You can configure this parameter per bundle. IOM2 supports MRRU value up to 64000 bytes, and it can be configured to a minimum of 1500 bytes, with default value 64000 bytes.

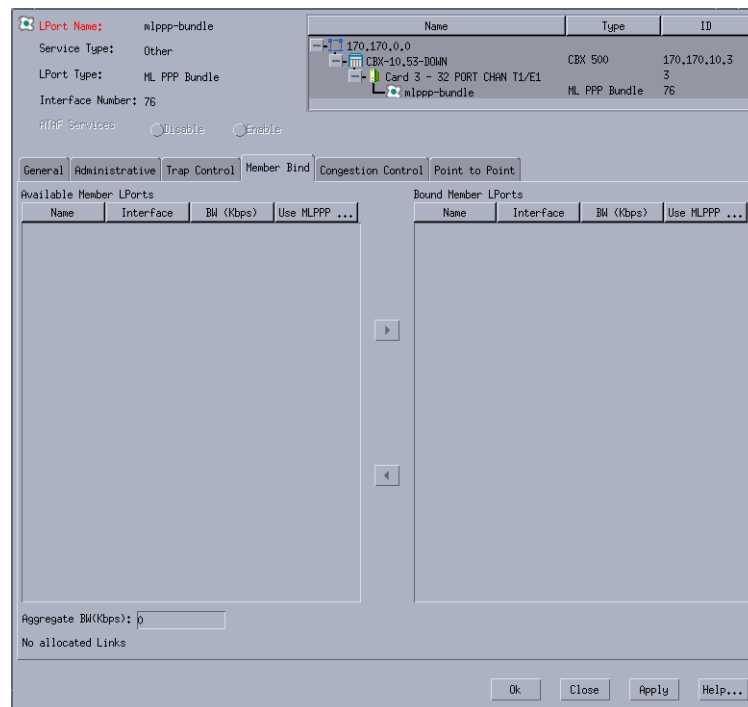
## Configuring the MLPPP Bundle

You can configure the MLPPP Bundle LPorts by binding or unbinding one or more Point-to-Point Protocol (PPP) LPorts to it. To configure the MLPPP bundle, perform the following tasks:

1. In the `Switch` tab, expand the `Cards` node and then select the `32-Port T1/E1 FR` module.
2. Right-click the `LPorts` node of the selected card and then select `Add`. The `Add Logical Port` dialog box is displayed ([Figure 6-3 on page 6-8](#)).



3. Select the Member Bind tab to bind or unbind the PPP LPorts. The Member Bind tab of the Add Logical Port dialog box is shown in **Figure 6-3 on page 6-8**.



**Figure 6-5. Add Logical Port: Member Bind Tab**

4. To bind an MLPPP Bundle LPort, perform the following tasks:
  - a. Select a Member LPort from the Available Member LPorts list.
  - b. Click the right-arrow button. The selected logical port is added to the Bound Member LPorts list. The system updates the Aggregate BW field to include the bandwidth of the bound logical port.
5. To unbind an MLPPP Bundle LPort, perform the following tasks:
  - a. Select a bound Member LPort from the Bound Member LPorts list.
  - b. Click the left-arrow button. The selected logical port is removed from the Bound Member LPorts list and then added to the Available Member LPorts list on the left. Navis EMS-CBGX updates the Aggregate BW field to include the deletion of the bandwidth of the unbound logical port from the bundle.



**Note** – A maximum of eight PPP LPorts can be bound to any Bundle LPort.

## Configuring PVCs With an MLPPP Bundle LPort Endpoint

To configure PVC between an MLPPP Bundle LPort and a Frame Relay LPort, perform the following tasks:

1. In the Switch tab, expand the `Cards` node and then select the `32-Port T1/E1 FR` module.
2. Expand the `Circuits` node defined in the MLPPP LPort.
3. Right-click the `PVCs` node and then select `Add`. The `Add PVC` dialog box is displayed (Figure 6-6).

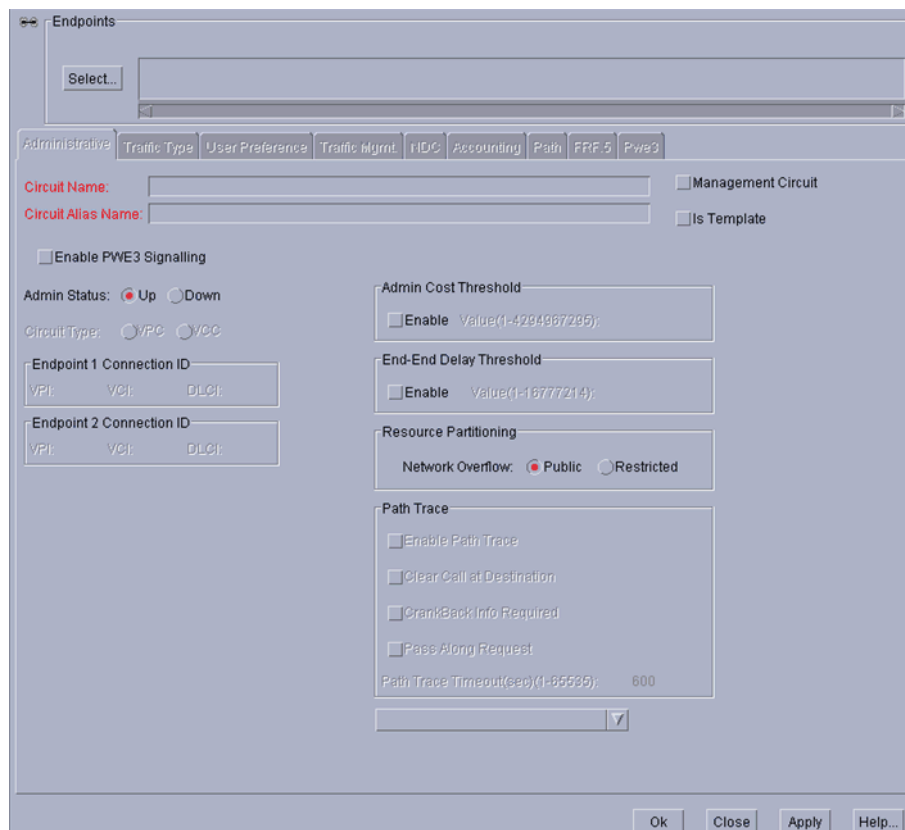
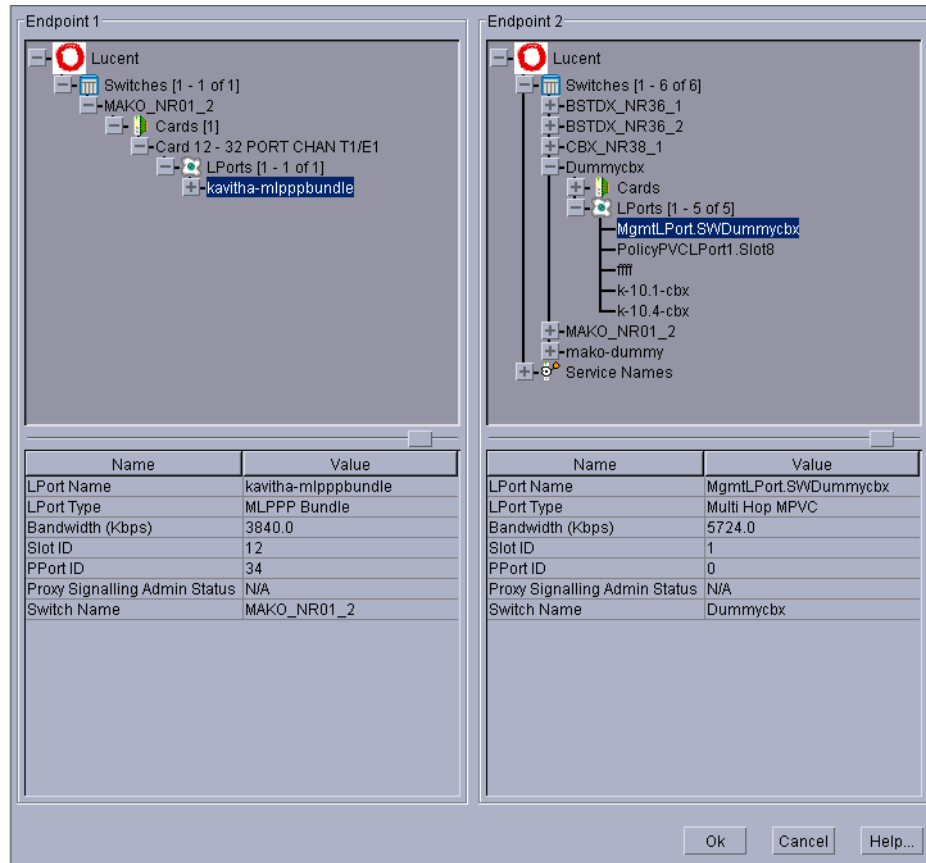


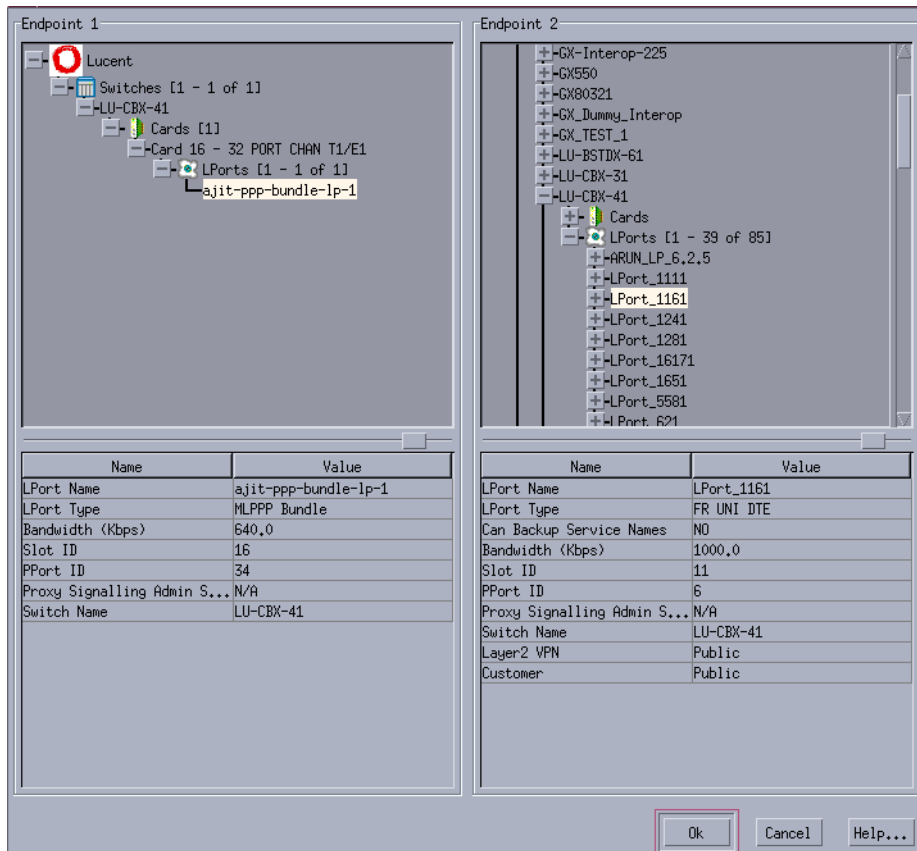
Figure 6-6. Add PVC Dialog Box

4. Click Select to view the Select Endpoints dialog box (Figure 6-7).



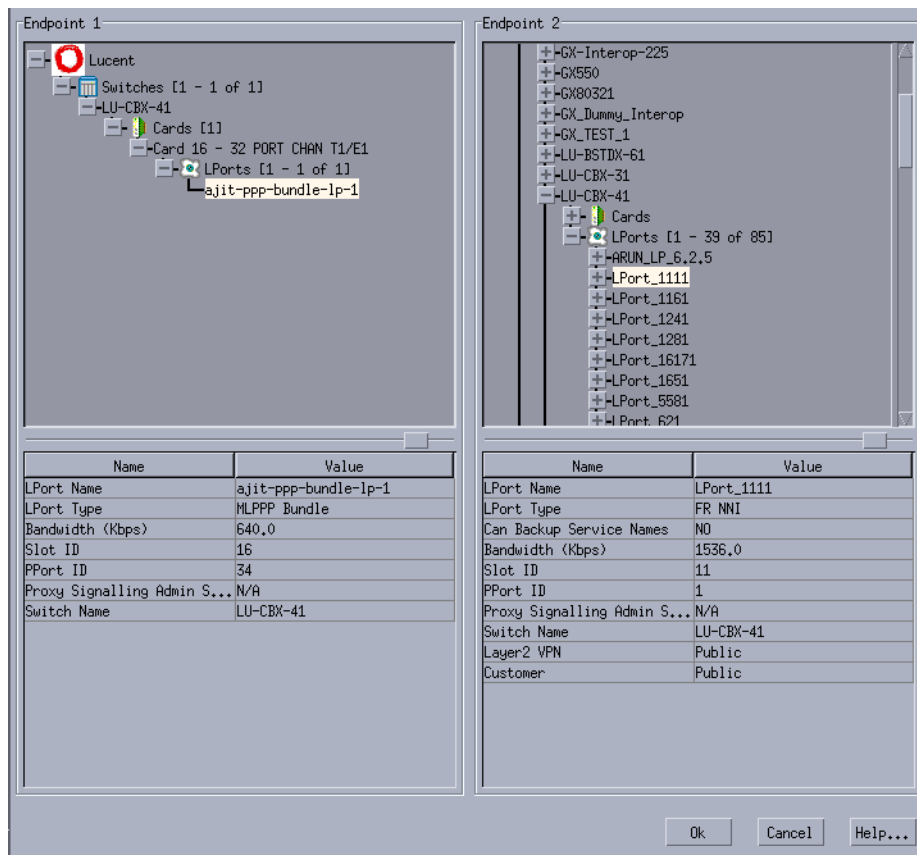
**Figure 6-7. Select Endpoints Dialog Box**

A few sample selections of endpoints are illustrated. See [Figure 6-8 on page 6-16](#) for selecting one endpoint as an MLPPP Bundle and the other endpoint as Frame Relay UNI DTE.



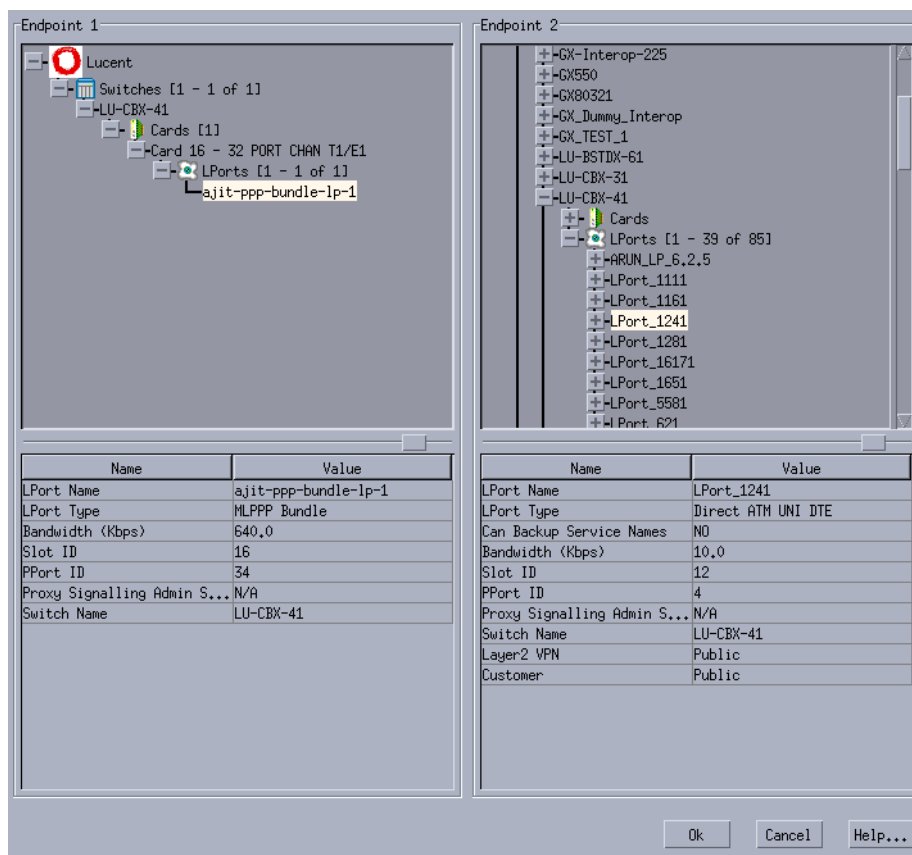
**Figure 6-8. Select Endpoints MLPPP Bundle and FR UNI DTE**

See [Figure 6-9 on page 6-17](#) for selecting one endpoint as an MLPPP Bundle and the other endpoint as Frame Relay NNI.



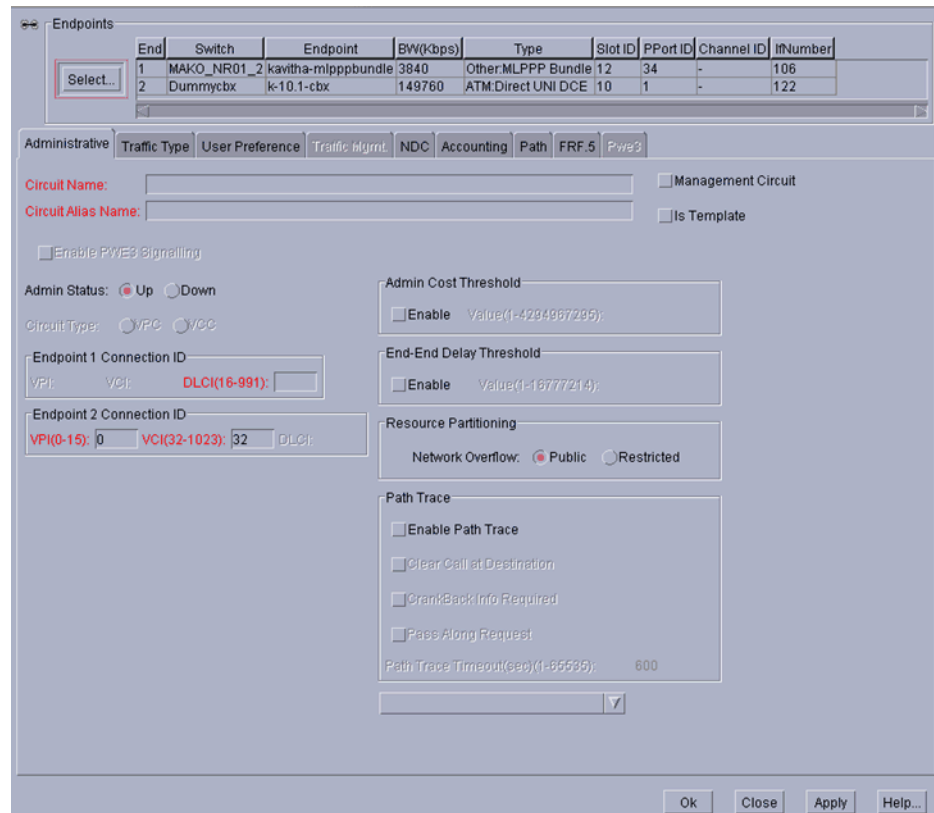
**Figure 6-9. Select Endpoints MLPPP Bundle and FR NNI**

See [Figure 6-10 on page 6-18](#) for selecting one endpoint as an MLPPP Bundle and the other endpoint as Direct ATM UNI DTE.



**Figure 6-10. Select Endpoints MLPPP Bundle and Direct ATM UNI DTE**

5. Define a circuit between an MLPPP Bundle LPort and the other endpoint such as Frame Relay UNI DCE/DTE, Frame Relay NNI, Direct ATM UNI DCE/DTE, or Direct ATM NNI (Figure 6-11).



**Figure 6-11. Add PVC Dialog Box**

6. Click OK to complete the selection of circuit endpoints, and then return to the Add PVC dialog box.
7. Complete the circuit definition as described in Chapter 7, “Configuring Permanent Virtual Circuits (PVCs).”



**Note** – Additional information to be noted:

- The PVC connection to an MLPPP interface is treated as having Priority Frame disabled.
- You cannot define PVC between an MLPPP interface and a Service Name Binding.
- You cannot define PVC between an MLPPP interface and another MLPPP or PPP interface.
- You cannot define SPVC on an MLPPP interface.
- You cannot have more than one PVC with an MLPPP bundle as either of the endpoints.





# Configuring Permanent Virtual Circuits (PVCs)

This chapter describes how to access and configure point-to-point, redirect, and multicast DLCI Frame Relay permanent virtual circuits (PVCs).

A permanent virtual circuit defines an end-to-end connection between two logical ports within the Lucent network. You can configure PVCs after you configure the switches, physical ports, logical ports, and trunks.

This section contains:

- [“About Permanent Virtual Circuits \(PVCs\)” on page 7-2](#)
- [“Working with PVCs” on page 7-9](#)
- [“Working with Redirect PVC Connections” on page 7-30](#)
- [“Working with Multicast DLCIs” on page 7-39](#)
- [“Managing Circuits” on page 7-43](#)

Refer to the following related information:

- See [Chapter 11, “Configuring Management Paths,”](#) for information about management PVCs (MPVCs), redirect MPVCs, and management DLCIs.
- See [Appendix C, “Priority Routing,”](#) for important information about defining PVC routing priorities.
- For information about configuring Frame Relay-to-ATM Service Interworking (FRF.8) and Frame Relay-to-ATM Network Interworking (FRF.5) circuits, refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- For information about configuring Ethernet LPorts, refer to the *IP Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*. Also see [“Configuring Ethernet Virtual Circuits \(EVCs\)” on page 9-1](#) for defining an Ethernet Virtual Circuit between Frame Relay and Gigabit Ethernet modules for use on the CBX 3500 switch input and output modules (IOMs).

- For information about card attributes and defining the physical ports *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.
- If you have the NavisAX product, you can provision end-to-end circuits between PSAX 4500 devices and CBX 500 switches, as described in the *NavisAX Administrator's Guide*. For information on viewing end-to-end circuit configuration, status, and summary statistics using Navis EMS-CBGX, refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

## About Permanent Virtual Circuits (PVCs)

This section provides PVC configuration guidelines and background information.

This section contains:

- [“Reliable Scalable Circuit” on page 7-2](#)
- [“PVC Endpoint Rules” on page 7-3](#)
- [“PVC Establishment Rate Control” on page 7-4](#)
- [“VC Overload Control” on page 7-5](#)
- [“Rate Enforcement” on page 7-6](#)
- [“About DLCI Numbers” on page 7-8](#)

## Reliable Scalable Circuit

The 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 endpoint 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, which allows you to cancel the PVC or redirect PVC configuration and prevent a card out-of-sync 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
  - Both switches are unmanaged.
  - Both switches are managed. Both cards (endpoints) have a status of *up*.
  - Both switches are managed. Both cards have a status of *up*.
- Redirect PVC
  - All three switches are unmanaged.

- All three switches are managed. All three 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 about Reliable Scalable Circuit reported error types, see [Appendix A](#).

To disable this feature, edit the `cascadeview.cfg` file and remove the pound signs (#) from the following lines:

```
#CV_CARD_STATS=DISABLE
#EXPORT CV_CARD_STATS
```

## PVC Endpoint Rules

[Table 7-1](#) 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 7-1. PVC Endpoint Rules**

PVC Type	Switch	NMS	Task
Both circuit endpoints are fixed <sup>a</sup> (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 <code>show ospf names</code> command to find the interface number.
First endpoint is fixed <sup>a</sup> while second endpoint is variable <sup>b</sup> and primary <sup>c</sup>	Fixed endpoint is always the caller.	Fixed endpoint is always designated endpoint 2 in NMS.	See the Add PVC dialog box ( <a href="#">Figure 7-3 on page 7-11</a> ) in the NMS.
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 Add PVC dialog box ( <a href="#">Figure 7-3 on page 7-11</a> ) in the NMS.
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 <code>Cvlistcontained</code> command in Provisioning Server to find the SNB ID.
First endpoint is variable and primary while second endpoint is backed up <sup>d</sup>	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 <code>Cvlistcontained</code> command in Provisioning Server to find the SNB ID.  For the NMS, see the Add PVC dialog box ( <a href="#">Figure 7-3 on page 7-11</a> ).

## Configuring Permanent Virtual Circuits (PVCs)

### About Permanent Virtual Circuits (PVCs)

---

**Table 7-1. PVC Endpoint Rules (Continued)**

PVC Type	Switch	NMS	Task
First endpoint is backed up while second endpoint is variable and primary	Sets whatever configuration is given from the NMS.	Backed up endpoint is always designated endpoint 1 in NMS.	See the Add PVC dialog box ( <a href="#">Figure 7-3 on page 7-11</a> ).

- <sup>a</sup> Fixed refers to endpoints that do not have an SNB configured.  
<sup>b</sup> Variable refers to an endpoint with a SNB on the primary interface.  
<sup>c</sup> Primary refers to an endpoint that is the primary lport for a SNB.  
<sup>d</sup> Backed up refers to endpoints where a backup lport is active for a SNB.



**Note** – For more information on using the `show ospf names` and `cvlistcontained` commands, refer to the *B-STDX, CBX, and GX Switch Troubleshooting User's 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. This feature is supported on CBX 500 switch.

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.



**Note** – You can trace events related to the PVC Establishment Rate Control feature using the Event Log. Refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on the Event Log feature.

---

For more information on the VC Overload Control feature, see [“VC Overload Control” on page 7-5](#).

## 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 on CBX 500 switch for PVC, SVC, and Offnet circuit (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, refer to the *Navis EMS-CBGX Getting Started Guide*.

## About Overload Severity Levels

The overload severity level for a module is displayed on the View Card Attributes dialog box (refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on this dialog box). Overload severity levels are different on the CBX 500 switch 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 Severity Level, refer to the *Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

## 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  $T_c$  ( $T_c = B_c / CIR$ ), it classifies the frame as follows:

- Under the committed burst rate ( $B_c$ )
- Over the committed burst rate but under the excess burst rate ( $B_e$ )
- Over the excess burst rate

Color designators (green, amber, and red) identify packets travelling through the network. Congested nodes use the designators to determine which frames to discard first in various congested states or congestion conditions. [Table 7-2](#) describes the designators (traffic colors) and discard policy.

**Table 7-2. 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 that the network delivers. The red-frame percent (pr) is determined as follows.

$$Pr = \frac{\text{Allowed red frame bits}}{Bc + Be + \text{allowed red frame bits}}$$

## Rate Enforcement Schemes

You can configure the rate enforcement scheme. This option provides additional flexibility, increased rate enforcement accuracy, and improved switch performance. You set the rate enforcement scheme in the Add PVC dialog box under the Traffic Type attributes (“[Traffic Type Attributes for PVCs and Redirect PVCs](#)” on [page 7-18](#)).

[Table 7-3](#) 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 7-3. Rate Enforcement Schemes**

Scheme	Rate Enforcement Accuracy	Switch Performance
Jump	1	2
Simple	2	1

## About DLCI Numbers

A data link connection identifier (DLCI) number is a 10-bit address that identifies PVCs. The DLCIs identify the logical endpoints of a virtual circuit and only have local significance.

Depending on your link management type, use the guidelines in [Table 7-4](#) to define DLCI numbers.

**Table 7-4. DLCI Number Guidelines**

DLCI Number Range	Description
0-15	Reserved
16-991	Available for all link management types
992-1007	Available for LMI Rev1 only
1008-1023	Reserved



## Working with PVCs

This section contains:

- “Accessing PVCs Using Navis EMS-CBGX” on page 7-9
- “Defining a Point-to-Point Circuit Connection” on page 7-11
- “Manually-Defining the Circuit Path” on page 7-28

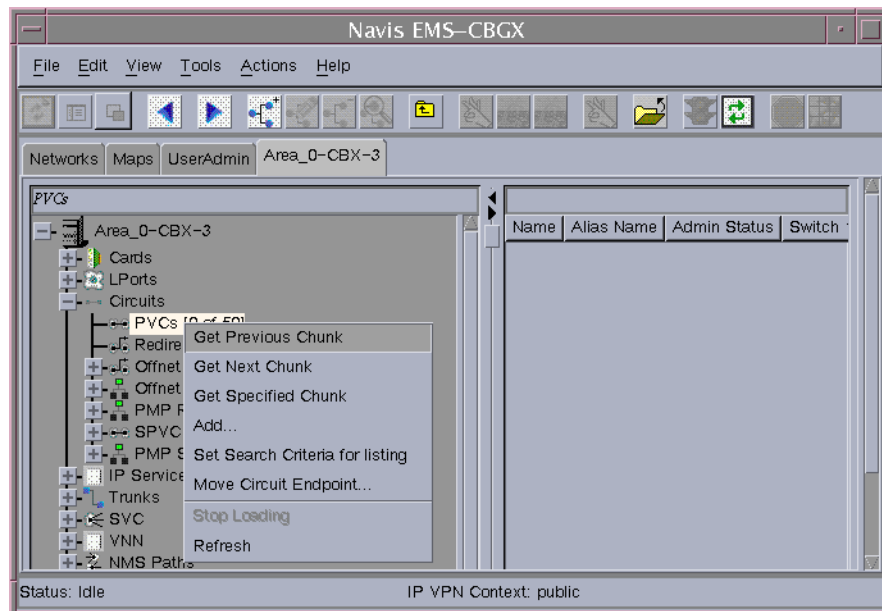


**Note** – Refer to the *Navis EMS-CBGX Installation and Administration Guide* for information on group-wise resource partitioning.

## Accessing PVCs Using Navis EMS-CBGX

To access PVCs using Navis EMS-CBGX, perform the following tasks:

1. In the `Switch` tab, expand the `Circuits` node.
2. Right-click the `PVCs` node to access the popup menu (Figure 7-1).

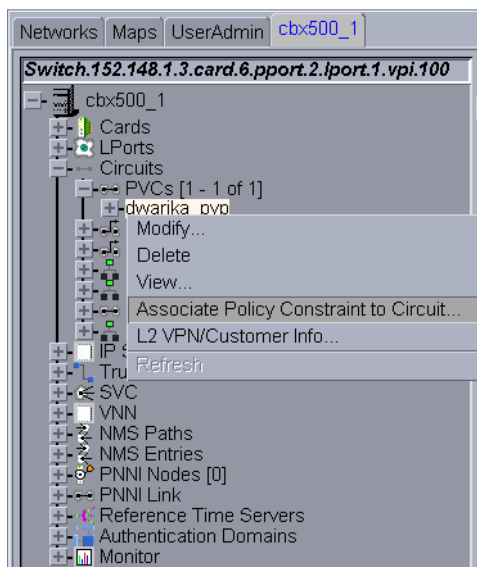


**Figure 7-1. Navigation Panel: PVCs Node**

The following commands are available:

- **Add** — Creates a new PVC. See “Defining a Point-to-Point Circuit Connection” on page 7-11.
- **Set Search Criteria For Listing** — Enables you to enter a search string that determines how circuits are listed. You may then use the Disable Search Criteria For Listing command to cancel listing based on your search string.

- **Move Circuit Endpoint** — Enables you to move circuit endpoints between logical ports. See [“Moving Circuits”](#) on page 7-43.
  - **Add PVC Using This Template** — Enables you to define a new PVC based on an existing template. See [“Using Templates to Define Circuits”](#) on page 7-48.
3. Expand the PVCs node to display a list of defined circuits. Right-click a specific circuit to access the popup menu as shown in [Figure 7-2](#).



**Figure 7-2. Navigation Panel: Circuits Node**

The following commands are available:

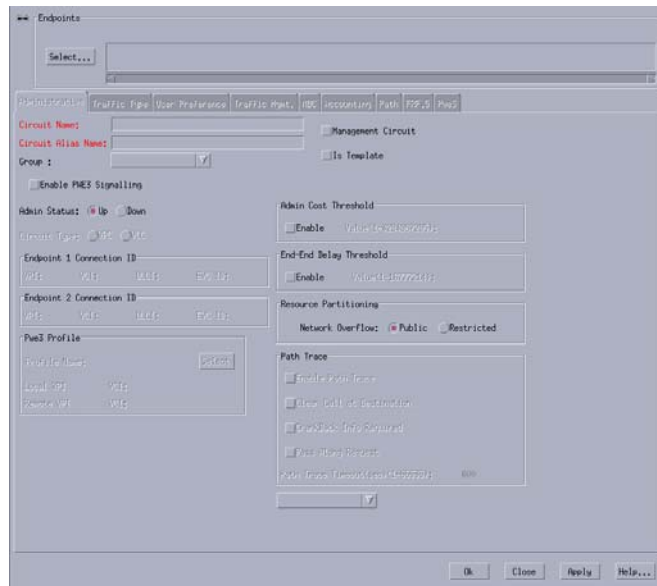
- **Modify** — Enables you to configure an existing PVC using the Modify PVC dialog box.
- **Delete** — Deletes an existing PVC.
- **View** — Enables you to view the PVC configuration in read-only mode.
- **Oper Info** — Displays status information about the PVC in the PVC Operational Information dialog box.
- **OAM** — Enables you to perform OAM loopback testing using the PVC OAM Loopback dialog box.
- **Associate Policy Constraint to Circuit** - Enable you to set a policy constraint for normal call setup and rerouted call setup.
- **L2 VPN/Customer Info** — Enables you to assign the PVC to a Layer 2 VPN or customer name. See [Chapter 10, “Configuring Layer2 Virtual Private Networks \(VPNs\),”](#) for more information.

## Defining a Point-to-Point Circuit Connection

To add a point-to-point circuit, perform the following tasks:

1. In the Switch tab, expand the `Circuits` node.
2. Right-click the `PVCs` node and then click `Add` on the popup menu as shown in [Figure 7-1 on page 7-9](#).

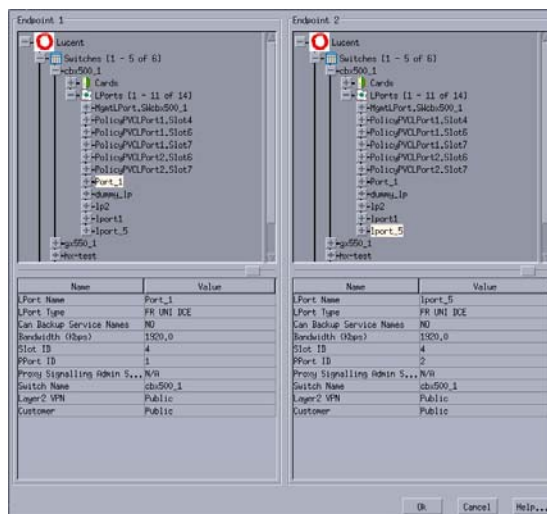
The Add PVC dialog box is displayed ([Figure 7-3](#)).



**Figure 7-3.** Add PVC Dialog Box

- Click **Select** to define the circuit endpoints.

The Select Endpoints dialog box is displayed (Figure 7-4).



**Figure 7-4. Select Endpoints Dialog Box**

- Define the circuit endpoints using the following instructions, depending on whether you are defining a standard circuit, or fault-tolerant or resilient LMI PVC connection.

For a standard circuit configuration:

- Expand the **Switches** node, select a switch, and use the **Cards** or **LPorts** node to select Endpoint 1. **Table 7-5** lists the standard logical port configurations.

**Table 7-5. Logical Port Endpoints for Circuits**

Endpoint 1	Endpoint 2
FR UNI DCE/DTE, FR NNI	FR UNI DCE/DTE, FR NNI
FR UNI DCE/DTE, FR NNI	Encapsulated FRAD, PPP
Encapsulated FRAD	Encapsulated FRAD

Note that if you enable the Layer2 VPN/VNN Customer View function (see **“Using the Layer2 VPN/Customer View Feature”** on page 10-8), only logical ports that belong to the Layer2 VPN or customer you select appear in the list.

- Continue with **step 5**.

For a fault-tolerant or resilient LMI PVC connection:

- a. Expand the `Service Names` node, and select a service name from the list.

You can configure a fault-tolerant PVC connection only for the following Frame Relay logical port types:

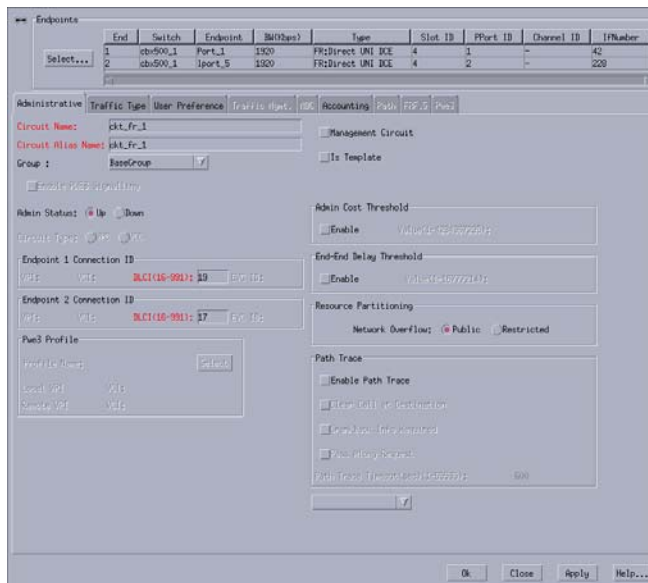
- UNI DCE
- UNI DTE
- UNI NNI

For more information about fault tolerant PVCs, see [Chapter 12, “Configuring Fault-tolerant PVCs.”](#) For more information about resilient LMI (RLMI), see [Chapter 13, “Configuring Resilient LMI.”](#)

- b. Continue with [step 5](#).
5. Verify the information in the `Select Endpoints` dialog box to ensure the correct endpoints have been selected.
  6. Choose `OK` to return to the `Add PVC` dialog box. Configure the following tabs using the instructions in this chapter:
    - **Administrative** — Defines administrative information, such as circuit name, administrative status, and circuit type. See [“Administrative Attributes for PVCs” on page 7-14.](#)
    - **Traffic Type** — Defines the traffic descriptor settings for forward and reverse traffic. See [“Traffic Type Attributes for PVCs and Redirect PVCs” on page 7-18.](#)
    - **User Preference** — Defines PVC features that deal with port congestion and traffic policing. See [“User Preference Attributes for PVCs and Redirect PVCs” on page 7-21.](#)
    - **Accounting** — Use the optional `Accounting` tab to configure `NavisXtend Accounting Server` parameters for this circuit. For more information, refer to the *NavisXtend Accounting Server Administrator’s Guide*.
    - **Path** — The `Path` tab enables you to manually define a circuit path and the OSPF algorithm’s circuit routing decisions. For more information, see [“Manually-Defining the Circuit Path” on page 7-28.](#)
    - **FRF.5** — Enables you to configure FRF.5 parameters for Frame Relay-to-ATM interworking circuits. For information on configuring Frame Relay-to-ATM Service Interworking (FRF.8) and Frame Relay-to-ATM Network Interworking (FRF.5) circuits, refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.*

## Administrative Attributes for PVCs

The Add PVC dialog box Administrative tab is shown in [Figure 7-5](#).



**Figure 7-5. Add PVC Dialog Box: Administrative Tab**

The Administrative tab contains the fields described in [Table 7-6](#).

**Table 7-6. Add PVC Dialog Box: Administrative Tab**

Element	Description
Circuit Name	Enter a unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map. <b>Note:</b> <i>In the Modify PVC and View PVC dialog boxes, Circuit Name is read-only.</i>
Circuit Alias Name	<i>(Optional)</i> Enter a unique, alphanumeric name to identify the redirect circuit. Do not use parentheses or asterisks. This name must be unique to the entire map. The default name is the circuit name.  The service providers use the circuit name alias to identify the redirect circuit in a way that is meaningful to their customers.
Group	Select a group to which you want to associate the circuit. The circuit can belong to any group or to the BaseGroup.  Refer to the <i>Navis EMS-CBGX Installation and Administration Guide</i> for a detailed information on group-wise resource partitioning.

**Table 7-6. Add PVC Dialog Box: Administrative Tab (Continued)**

Element	Description
Enable PWE3 Signalling	<p>Check this box to enable PWE3 signalling on this circuit. The Pwe3 tab will be available only if this box is checked.</p> <p><i>Note: PWE3 signaling applies to CBX 3500 ATM circuit endpoints. For more information on PWE3, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>
Is Template	<p><i>(Optional)</i> Enable this option to save these settings as a template to use again to configure another PVC with similar options. See <b>“Using Templates to Define Circuits”</b> on page 7-48 for more information.</p>
Management Circuit	<p>Select Management Circuit to include this PVC configuration in the Network Management Station (NMS) initialization script file. This file contains all the Simple Network Management Protocol (SNMP) set requests necessary to replicate the entire switch configuration. After you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity. See <b>Chapter 11</b> for information on DLCI configurations.</p> <p><i>Note: This option is useful in a few management DLCI configurations.</i></p>
Admin Status	<p>Select <i>Up</i> (default) to activate the circuit at switch startup, or select <i>Down</i> to take the circuit offline to run diagnostics such as PVC loopback.</p>
DLCI (Primary and Secondary Endpoints)	<p>For primary and secondary endpoints, enter a Data Link Connection Identifier (DLCI) in the range 16 to 991. When the link management protocol on the LPort is set to Local Management Interface (LMI) Rev1, use the range 16 to 1007.</p> <p>A DLCI is a 10-bit address that identified PVCs. The DLCIs identify the logical end points of a virtual circuit and only have local significance.</p>
EVC ID (Pivot Endpoint) <i>(Only for Gigabit Ethernet endpoint)</i>	<p>For pivot endpoint, enter an Ethernet Virtual Circuit (EVC) ID in the range 1 to 32000.</p> <p>An EVC ID identifies a circuit that is attached to a VLAN or multiple VLANs.</p>

**Table 7-6. Add PVC Dialog Box: Administrative Tab (Continued)**

Element	Description
Admin Cost Threshold	<p>When 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 then enter a value of 1000, the redirect PVC will not be routed over a path whose total administrative cost exceeds 1000.</p> <p>The total administrative cost for a path is calculated by adding the sums of the administrative cost for each trunk in the path. The valid range of values for this field is from 1 to 4294967295.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>Do not enable this option if you use End-End Delay routing.</i></p>
End-End Delay Threshold	<p>When 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 then enter a value of 500 microseconds, the redirect PVC will not be routed over a path whose total end-to-end delay exceeds 500 microseconds.</p> <p>The total end-to-end delay for a path is calculated by adding the sums of the end-to-end delay for each trunk in the path. The valid range for this field is from 0 to 16777214 microseconds.</p> <p>If the End-to-End Delay Threshold is disabled to the circuit, then the operational status window displays Unavailable in the delay field.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>The value you enter should reflect your network topology. If a PVC will typically traverse high-speed trunks, then set the delay rate lower; increase the delay if the PVC must use low-speed trunks.</i></p>
Resource Partitioning	<p>Select one of the following Network Overflow options:</p> <ul style="list-style-type: none"> <li>• <i>Public</i> (default) - Redirect PVCs are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the traffic of the customer is allowed to run over common trunks (shared by a variety of different customers).</li> <li>• <i>Restricted</i> – Redirect 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.</li> </ul> <p>Resource Partitioning determines how the redirect PVC traffic is managed during trunk overflow or failure conditions. This feature is used with Virtual Private Networks (VPNs).</p>



**Table 7-6. Add PVC Dialog Box: Administrative Tab (Continued)**

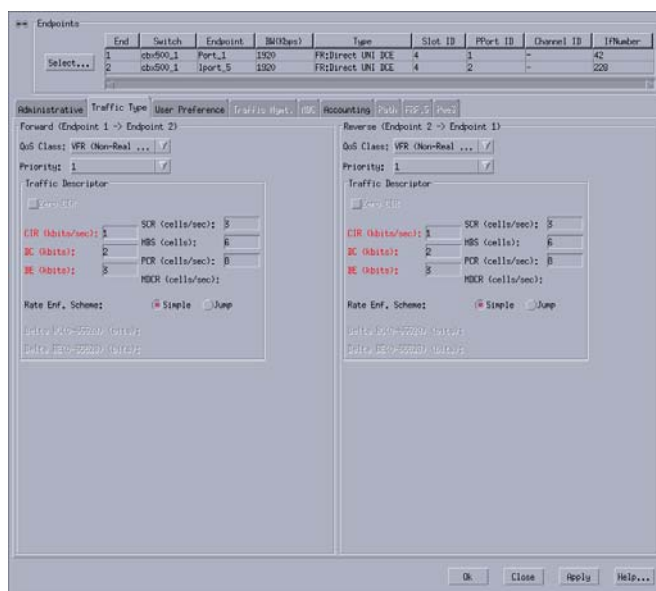
Element	Description
Path Trace	<p>Path Trace enables you to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network.</p> <ul style="list-style-type: none"> <li>• <b>Enable Path Trace</b> – Select Enabled to enable path trace at the switch initializing the circuit or Disabled (default) if you do not want to have path trace enabled.</li> <li>• <b>Clear Call at Destination</b> – Enable or disable the removal of this circuit after the path trace is complete. Select Enabled for the circuit to be deleted from the switch after the specified path trace timeout period. Path trace information for this circuit will also be made available for the timeout period. If you wish for the circuit to remain, select Disabled (default). If this field is enabled, the circuit will not be created in the PRAM. Navis EMS-CBGX will create a temporary circuit. After the creation of this circuit, no modifications can be made to it.</li> <li>• <b>Crankback Info Required</b> – Enable or disable collection of crankback information. Select Enabled to instruct the switch to collect and maintain the crankback information on the traced path. If this field is disabled (default), crankback information is not collected.</li> <li>• <b>Pass Along Request</b> – Enable or disable pass along request for this path trace. Select Enabled (default) to have the path trace continue through nodes that do not support the path trace feature, causing the trace results to contain some gaps. Disable this field to cause the path trace to terminate at any switch that does not support the path trace feature. A partial path trace will be returned.</li> <li>• <b>Path Trace Timeout (sec)</b> – Enter a number of seconds (0-65535) for which you want the trace results to be maintained in the switch. The default is ten minutes (600 seconds).</li> </ul> <p>For information about configuring path tracing at the logical port level, see <a href="#">“Administrative Attributes for Frame Relay LPorts” on page 3-15</a>. For more information about how path tracing works, refer to the <i>Switch Diagnostics User’s Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i>.</p>

## Traffic Type Attributes for PVCs and Redirect PVCs

The Add PVC dialog box Traffic Type tab is shown in [Figure 7-6](#). Specify traffic descriptor settings for forward and reverse traffic.



**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 7-6.** Add PVC Dialog Box: Traffic Type Tab

The Traffic Type tab contains the fields described in [Table 7-7](#).

**Table 7-7. Add PVC Dialog Box: Traffic Type Tab**

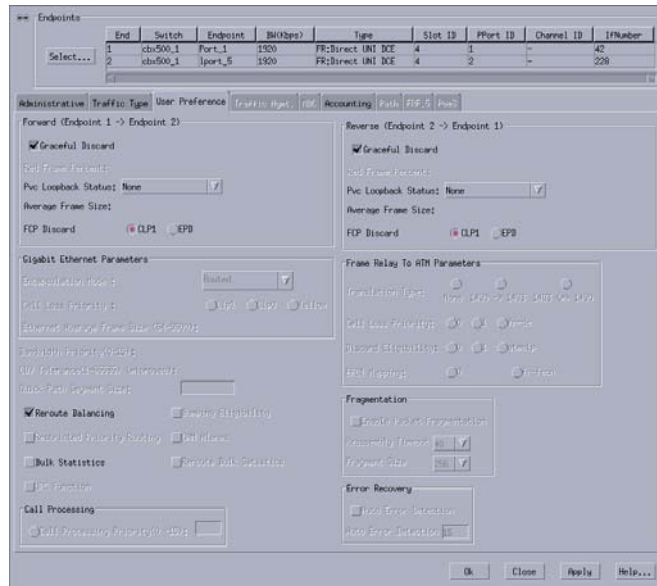
Element	Description
QoS Class	<p>Select one of the following Frame Relay QoS classes:</p> <ul style="list-style-type: none"> <li>• <i>VFR (Real Time)</i> – Variable frame rate (VFR). Used for special delay-sensitive applications that require low delay variation between endpoints.</li> <li>• <i>VFR (Non-Real Time)</i> – Handles transfer of long, bursty data streams over a pre-established connection. This service provides low data loss but no delay guarantee. 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.</li> <li>• <i>UFR</i> – Unspecified frame rate (UFR). Used for LAN traffic, primarily. The CPE should compensate for any delay or frame loss.</li> </ul>
Priority	<p>Select 1, 2, or 3 to configure the priority of data being transmitted on this circuit. Circuit priority determines the data's forward priority. The highest priority is 1 (do not discard data); the lowest priority is 3 (discard data). The default priority for Frame Relay is 1.</p> <p><i>Note: To configure the priority of transmitted data for a standard or redirect management PVC (MPVC) select 1, 2, or 3. The default priority is 1. (See <a href="#">Chapter 11, "Configuring Management Paths,"</a> for more information about standard and redirect MPVCs.)</i></p>
Zero CIR	<p>Set the CIR parameter to <i>On</i> or <i>Off</i>.</p> <ul style="list-style-type: none"> <li>• <i>On</i> – Indicates that the PVC has an assigned CIR value of zero and is a best-effort delivery service. Customer data that is subscribed to zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on zero CIR PVCs have DE set to one (1).</li> <li>• <i>Off</i> – (default) Disables zero CIR.</li> </ul> <p><i>Note: If you set Zero CIR Enabled to On, you cannot set the CIR, Bc, and Be values.</i></p>
CIR (Kbps)	<p>Enter the committed information rate (CIR) in Kbps at which the network transfers data under normal conditions. Normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc). The value on each PVC is asymmetric (you can set a different CIR in each direction), which provides more efficient use of bandwidth.</p>
BC (Kbits) (Committed Burst Size)	<p>Enter the maximum amount of data, in Kbits, that the network attempts to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as Bc/CIR. This value must be greater than zero and is typically set to the same value as CIR.</p>

**Table 7-7. Add PVC Dialog Box: Traffic Type Tab (Continued)**

Element	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 as Bc/CIR. The network treats this data as Discard Eligible (DE) data.
Rate Enf Scheme	<p>Select <i>Simple</i> (default) or <i>Jump</i>. The configurable rate enforcement scheme provides additional flexibility, increased rate enforcement accuracy, and improved switch performance. See “Rate Enforcement” on page 7-6 for more information.</p> <p><i>Note: Simple indicates time (Tc) as measured in periodic intervals. If you select the Simple scheme, the “bad” PVC detection feature is disabled.</i></p>
Delta BC (bits)	<p>Set the number of Delta Bc bits for this circuit between 0 - 65528. (The default value is 65528.)</p> <p>This value is the maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval, provided there is positive committed bit (Bc) credits before receiving the frame, but negative Bc credits after accepting the frame.</p>
Delta BE (bits)	<p>Set the number of Delta Be bits for this circuit between 0 - 65528. (The default value is 65528.)</p> <p>This value is the maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval, provided there is positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame.</p>

## User Preference Attributes for PVCs and Redirect PVCs

The Add PVC dialog box User Preference tab is shown in [Figure 7-7](#).



**Figure 7-7. Add PVC Dialog Box: User Preference Tab**

The User Preference tab contains the fields described in [Table 7-8](#).

**Table 7-8. Add PVC Dialog Box: User Preference Tab**

Element	Description
<b>Forward and Reverse (Endpoint 1 &lt;-&gt; Endpoint 2)</b>	
Graceful Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Selected</i> (default) - Forwards a few red packets if there is no congestion.</li> <li><i>Non-Selected</i> - Immediately discards the red packets.</li> <li>Graceful Discard defines how the circuit handles “red” packets. The 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 <i>Selected</i>.</li> </ul>

**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
Red Frame Percent	Set this value only if Graceful Discard is set to On. (If set to On, the default value is 100 percent.) The Red Frame Percent value limits the number of red frames the network is responsible for delivering.
PVC Loopback Status	<p>Select one of the following to display the current loopback status: <i>None</i>, <i>Local</i>, <i>Remote</i>, or <i>Both</i>.</p> <p><b>Note:</b> <i>You can modify this circuit only if None is displayed. If none is not displayed, do not attempt to modify or delete the selected circuit.</i></p> <p>Refer to the <i>Switch Diagnostics User's Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000</i> for more information about loopback testing and the Enhanced PVC Loopback feature.</p>
Average Frame Size	Displays the average frame size (in bytes) of the frames on the circuit.
FCP Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>CLP1</i> (default) - Selective CLP1 discard is provisioned for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate (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, then the cell is discarded. <b>Note:</b> <i>Early Packet Discard (EPD) is not performed in this case.</i></li> <li>• <i>EPD</i> - ATM Flow-control Processor (FCP) can perform EPD for UBR, ABR, and VBR-BRT PVCs. If this option is selected, then 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 the cells in the next packet are discarded for that PVC.</li> <li>• FCP Discard is displayed when you select a QoS class that supports FCP Discard.</li> </ul>
<b>Gigabit Ethernet Parameters</b>	
Encapsulation Mode	<p>Select <i>Routed</i> (default) or <i>Bridged</i> to determine the encapsulated format in which the Ethernet Virtual Circuit (EVC) passes data.</p> <p><b>Note:</b> <i>This is applicable for Ethernet endpoint only.</i></p>

**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
Cell Loss Priority	<p>Select one of the following options: <i>Clp0</i>, <i>Clp1</i>, or <i>Yellow</i> (default) to set the Cell Loss Priority (CLP). When the Ethernet frames are segmented into ATM cells on Gigabit Ethernet Universal Line Card (ULC), the CLP bit in each cell is set based on this configuration of the EVC.</p> <p><b>Note:</b> <i>This is applicable for Ethernet endpoint only.</i></p>
Ethernet Average Frame Size (64-8192)	<p>Enter a value in the range 64 to 8192 bytes.</p> <p>Ethernet Average Frame Size is used to calculate the Interworking Overhead (IOH) factor for the Traffic parameters conversion.</p> <p><b>Note:</b> <i>This is applicable for Ethernet endpoint only.</i></p>

**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
<b>Other Parameters</b>	
Bandwidth Priority (0...15)	<p>Specify a value from 0 through 15, where 0 is the default and indicates the highest priority.</p> <p>See <a href="#">Appendix C, "Priority Routing,"</a> for more information.</p>
CDV Tolerance	<p>Enter a value between 1 - 65535 microseconds 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 microseconds.</p>
Reroute Balancing	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enabled</i> – Allows this circuit to use reroute tuning. This feature enables the switch to redistribute PVCs across trunks, based on OSPF updates and cost metrics. You must first configure the reroute tuning parameters for the selected switch. For more information, refer to the <i>Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000</i>.</li> <li>• <i>Disabled</i> – This circuit does not use the reroute tuning parameters.</li> </ul>
Bumping Eligibility	<p>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.</p> <p>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).</p> <p>See <a href="#">Appendix C, "Priority Routing,"</a> for more information.</p>
Restricted Priority Routing	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enabled</i> – (default) Use this option to provision new circuits at the lowest bandwidth priority, regardless of configured higher bandwidth priority and bumping eligibility settings.</li> <li>• <i>Disabled</i> – Use this option if you want to use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits.</li> </ul> <p>See <a href="#">Appendix C, "Priority Routing,"</a> for more information.</p>



**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
OAM Alarms	Select to enable OAM alarms on this circuit. When enabled, the switch sends OAM F5 or F4 AIS (alarm indicator signal) cells out of each UNI logical port endpoint to indicate that the circuit is down.
UPC Function	<p>Enables 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. The default is enabled.</p> <p>When you do not enable UPC, the circuit allows all traffic, including non-conforming traffic, into the port. As a result, 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, <i>Lucent recommends that you enable the UPC function on all circuits.</i></p> <p><i>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 (without the ABR option) for both logical ports and circuits.</i></p>
Bulk Statistics	<p>Enable to configure statistics collection from the logical port using the NavisXtend Statistics Server. Choices are Enable or Disable. The default setting is Disable.</p> <p>Refer to the <i>NavisXtend Statistics Server User's Guide</i> for more information.</p>
<b>Frame Relay To ATM Parameters</b>	
Translation Type	<p>Select one of the following ATM Translation Type protocols:</p> <ul style="list-style-type: none"> <li>• <i>None</i> – Each end of the circuit uses the 1490 protocol.</li> <li>• <i>1490 -&gt; 1483</i> - The default if you have a Frame Relay logical port on endpoint 1 and an ATM logical port on endpoint 2.</li> <li>• <i>1483 &lt;==&gt; 1490</i> – The default for interworking circuits.</li> </ul>
Cell Loss Priority	<p>Select the cell loss priority (CLP) setting. The CLP bit is in each cell's cell header. Options include:</p> <ul style="list-style-type: none"> <li>• <i>0</i> – Sets the CLP bit to 0.</li> <li>• <i>1</i> – Sets the CLP bit to 1.</li> <li>• <i>fr-de</i> – 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.</li> </ul>

**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
Discard Eligibility	Select one of the following Discard Eligibility (DE) settings: <ul style="list-style-type: none"> <li>• 0 – Sets the DE to 0.</li> <li>• 1 – Sets the DE to 1.</li> <li>• <i>atm-clp</i> (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.</li> </ul>
EFCI Mapping	Select one of the following explicit forward congestion indication (EFCI) settings: <ul style="list-style-type: none"> <li>• 0 – Ignores EFCI to FECN (forward explicit congestion notification) bit mapping.</li> <li>• <i>fr-fecn</i> – (default) Maps the EFCI bit on the ATM endpoint to the Frame Relay FECN bit.</li> </ul>
<p><b>Fragmentation</b></p> <p>Applies to a circuit that has an MLFR UNI/NNI Bundle logical port endpoint on a 6-Port Channelized DS3/1/0 Frame Relay I/O Module</p>	
Enable Packet Fragmentation	Enable this option for packet fragmentation. Specify the fragment size in the Fragment Size field. Packet fragmentation partitions frames for this circuit into equal lengths before sending data over the MLFR bundle so that member links can be evenly loaded with data.
Reassembly Timeout	Select the length of time that frame fragments in a packet for this circuit will wait at the destination for the missing fragments before the packet is dropped. The values are available from 0 to 140 milliseconds, in increments of 10.
Fragment Size	Select a value for the length of the fragments into which frames are partitioned. The values are available choices are 128, 256, and 512 bytes. <p><b>Note:</b> <i>This field is displayed when Packet Fragmentation is enabled.</i></p>
<p><b>Error Recovery</b></p> <p>Applies to a circuit that has an MLFR UNI/NNI Bundle logical port endpoint on a 6-Port Channelized DS3/1/0 Frame Relay I/O Module</p>	

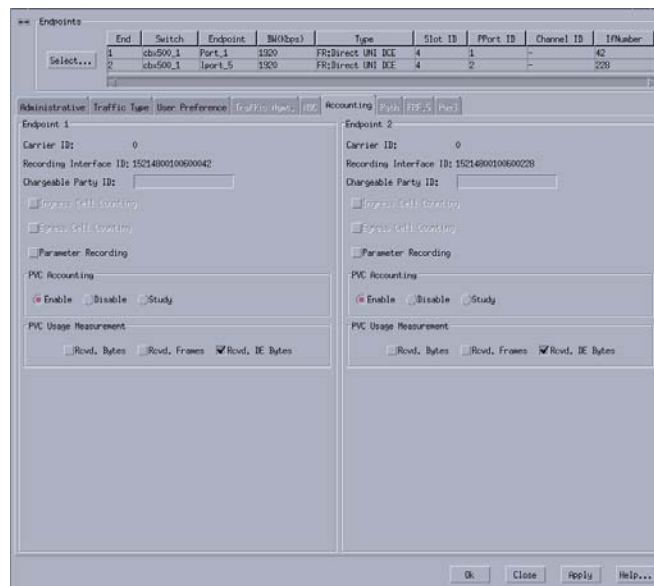
**Table 7-8. Add PVC Dialog Box: User Preference Tab (Continued)**

Element	Description
Auto Error Detection	<p>Enable this option to specify the number of retries that should be attempted before the circuit connection is shut down. Enter a value in the range 0 to 255. The default value is 15. Auto error detection identifies errors coming into the MLFR bundle logical port on the circuit, such as lost events, and shuts down the connection for the circuit.</p> <p><b>Note:</b> <i>The Auto Error Detection value overrides the Auto Error Detection setting made at the LPort level. It also overrides the Error Retry Count setting made at the LPort level.</i></p>

### Accounting Attributes for PVCs

Use the optional Accounting tab to configure NavisXtend Accounting Server parameters for this circuit. For more information, refer to the *NavisXtend Accounting Server Administrator's Guide*.

The Add PVC dialog box Accounting tab is shown in **Figure 7-8**.



**Figure 7-8. Add PVC Dialog Box: Accounting Tab**

## Path Attributes for PVCs

The Path tab 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 Add PVC dialog box Path tab is shown in [Figure 7-9](#).

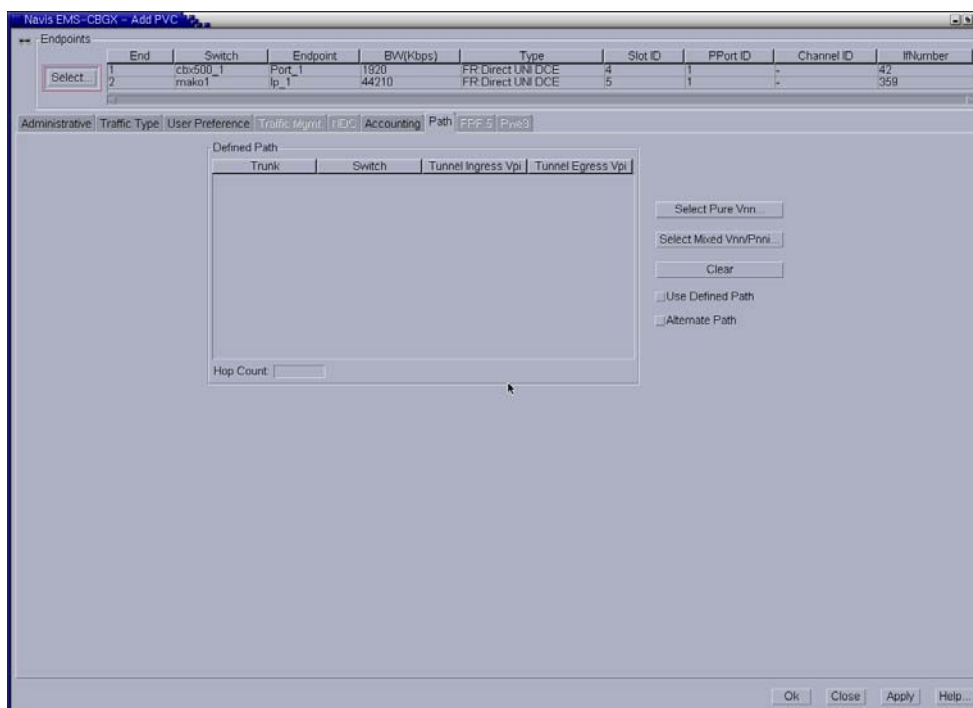


Figure 7-9. Add PVC Dialog Box: Path Tab

## 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 Private Network-to-Network Interface (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.



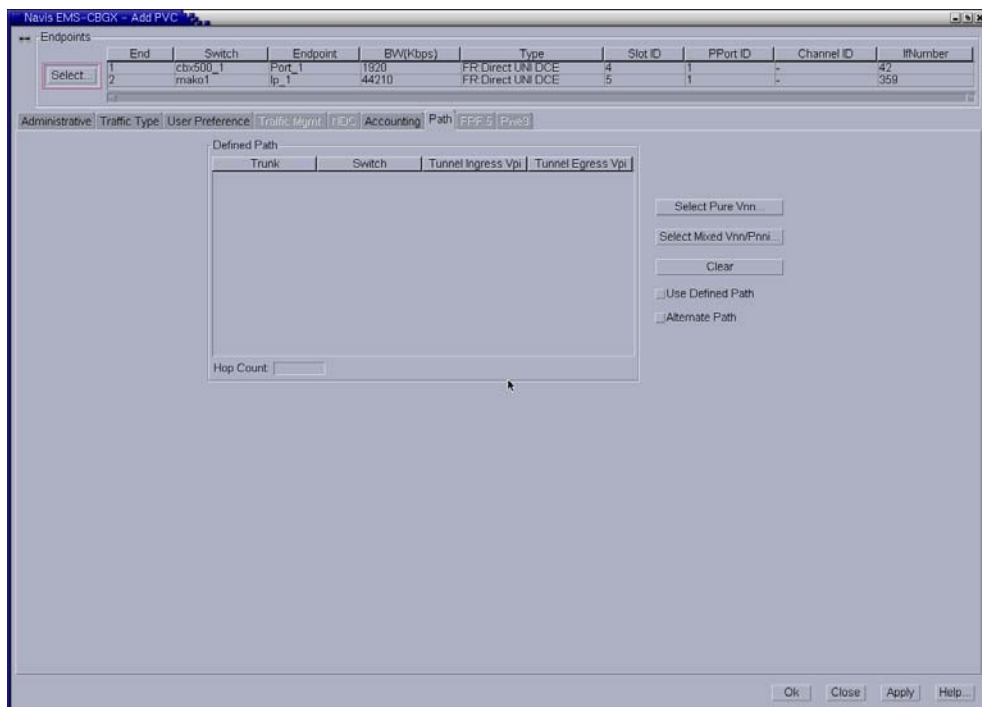
**Note** – PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*.

To manually define the circuit path, perform the following tasks:

1. Add a new PVC, or modify an existing PVC, using the instructions in **“Reliable Scalable Circuit”** on page 7-2.

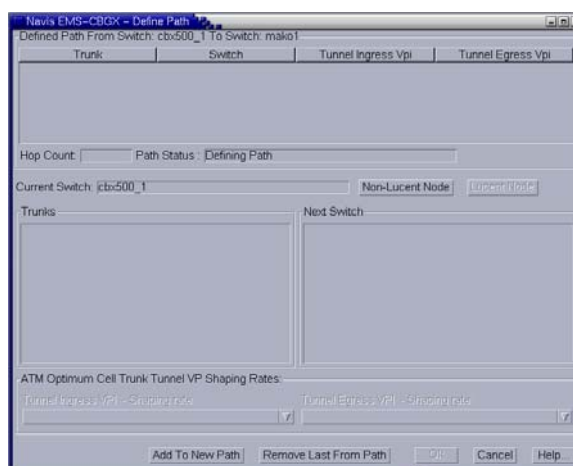
The Add or Modify PVC dialog box is displayed.

2. Click the Path tab as shown in **Figure 7-10**.



**Figure 7-10. Add/Modify PVC Dialog Box: Path Tab**

3. In the Path tab, click **Select Pure VNN** or **Select Mixed VNN/PNNI** to display the Define Path dialog box as shown in **Figure 7-11**.



**Figure 7-11. Define Path Dialog Box**

The Defined Path section displays a listing of hops (trunk-switch pairs) in the defined path.

4. Define the path using the `Trunks` and `Next Switch` lists, selecting trunk-switch pairs from the list of available hops to include the hop in the circuit path, and click `Add to Path`. When there are multiple trunks between two switches, select `[Any Trunk]` to route the circuit based on OSPF.

Click `Non-Lucent Node` to enter the 22-byte PNNI node ID and optional interface ID identifying other vendor equipment. After defining non-Lucent nodes, click `Lucent Node` to define the next hop to a Lucent switch, entering the internal IP Address of the next Lucent switch node and optional logical port interface ID.

Navis EMS-CBGX adds the path to the Defined Path section when the path is complete.

5. Choose `OK` when you have defined the path.
6. Click `Clear` to clear the defined path.
7. In the `Path` tab, enable or disable the `Use Defined Path` check box to specify whether to use the defined path or to enable the network routing to specify the circuit path.
  - *Enabled* – Routes the circuit based on the manually defined route.
  - *Disabled* – Routes the circuit based on the network's OSPF algorithm.
8. Enable or disable the `Alternate Path` check box to specify whether OSPF should route the circuit path if the manual route fails.
  - *Yes* – Enables OSPF to route the circuit based on the best available path if the manually defined path fails.
  - *No* – Prevents the circuit from being rerouted; the circuit remains down until the defined path is available.
9. In the `Add or Modify PVC` dialog box, click `OK` to add or modify the PVC when your configuration is complete.

## Working with Redirect PVC Connections

This section describes how to configure redirect permanent virtual circuits (PVCs) for Frame Relay UNI and NNI logical ports. Redirecting PVCs provides PVC backup recovery in the event of data terminal equipment (DTE) state changes.



**Note** – Redirect PVCs are not supported on a Point-to-Point Protocol (PPP) logical port.

---

Redirecting PVCs enables you to configure a PVC with the following three endpoints:

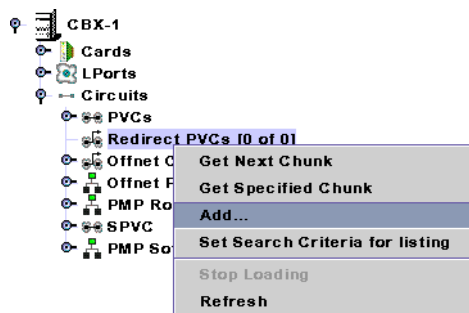
- Pivot
- Primary
- Secondary

Each endpoint has its own port and data link connection identifier (DLCI) combination. Typically, traffic follows the path between the pivot and primary endpoints. When the primary endpoint 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 endpoints. Redirecting PVCs takes place only if the called endpoint is down. Redirecting PVCs does not take place if the PVC segment within the network becomes inactive (for example, if there is no route to the primary endpoint, or the trunk is down).

## Accessing Redirect PVCs Using Navis EMS-CBGX

To work with redirect PVCs using Navis EMS-CBGX, perform the following tasks:

1. In the Switch tab, expand the `Circuits` node.
2. Right-click the `Redirect PVCs` node to access the popup menu as shown in [Figure 7-12](#).

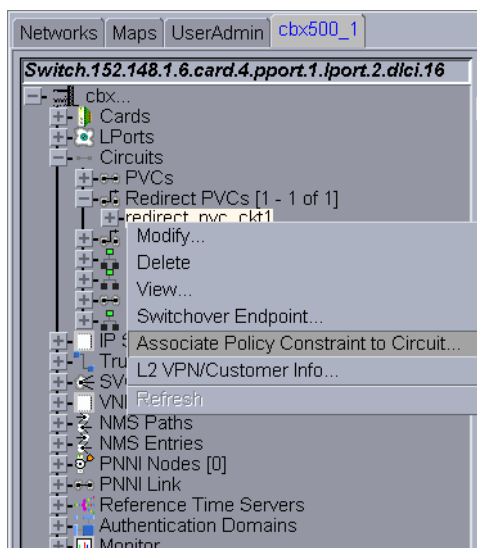


**Figure 7-12. Right-Clicking on the Redirect PVCs Node**

The following commands are available:

- **Add** — Creates a new redirect PVC. See [“Defining a Redirect PVC Connection”](#) on page 7-33.
- **Set Search Criteria For Listing** — Enables you to enter a search string that determines how circuits are listed. You may then use the Disable Search Criteria For Listing command to cancel listing based on your search string.

- Expand the Redirect PVCs node to display a list of defined circuits. Right-click a specific circuit to access the popup menu as shown in [Figure 7-13](#).



**Figure 7-13. Navigation Panel: Redirect PVCs**

The following commands are available:

- **Modify** — Enables you to configure an existing redirect PVC using the Modify Redirect PVC dialog box.
- **Delete** — Deletes an existing redirect PVC.
- **View** — Enables you to view the redirect PVC configuration in read-only mode.
- **Oper Info** — Displays status information about the redirect PVC in the Redirect PVC Operational Information dialog box.
- **Switchover Endpoint** — Enables you to switch between the primary and secondary endpoints.
- **OAM** — Enables you to perform OAM loopback testing using the Redirect PVC OAM Loopback dialog box.
- **Associate Policy Constraint to Circuit** - Enable you to set a policy constraint for normal call setup and rerouted call setup.
- **L2 VPN/Customer Info** — Enables you to assign the redirect PVC to a Layer 2 VPN or customer name. See [Chapter 10, “Configuring Layer2 Virtual Private Networks \(VPNs\),”](#) for more information.



## Defining a Redirect PVC Connection

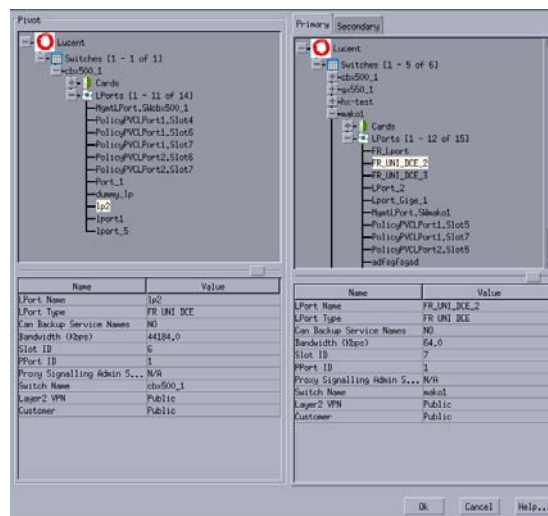
To add a redirect PVC, perform the following tasks:

1. In the Switch tab, expand the `Circuits` node.
2. Right-click the `Redirect PVCs` node and click `Add` on the popup menu, as shown in [Figure 7-12 on page 7-31](#).

The `Add Redirect PVC` dialog box is displayed ([Figure 7-3](#)).

3. Click `Select` to define the circuit endpoints.

The `Select Endpoints` dialog box is displayed ([Figure 7-14](#)).



**Figure 7-14. Select Endpoints Dialog Box**

4. Select the appropriate switch and LPort names for the pivot, primary, and secondary endpoints.
5. Choose `OK` to return to the `Add Redirect PVC` dialog box. Configure the following tabs using the instructions in this chapter:
  - **Administrative** — Defines administrative information, such as circuit name, administrative status, and circuit type. See [“Administrative Attributes for Redirect PVCs” on page 7-34](#).
  - **Traffic Type** — Defines the traffic descriptor settings for forward and reverse traffic. These options are the same as those for a regular PVC. See [“Traffic Type Attributes for PVCs and Redirect PVCs” on page 7-18](#).



**Note** – You *must* configure Traffic Type attributes before choosing OK in the Add Redirect PVC dialog box to save the redirect PVC configuration. Otherwise, the default values for committed information rate (CIR), committed burst size (Bc), and excess burst size (Be) will generate an error message. See “Traffic Type Attributes for PVCs and Redirect PVCs” on page 7-18.

- **User Preference** — Defines features that deal with port congestion and traffic policing. These options are the same as those for a regular PVC. See “User Preference Attributes for PVCs and Redirect PVCs” on page 7-21.
- **Accounting** — Use the optional Accounting tab to configure NavisXtend Accounting Server parameters for this circuit. For more information, refer to the *NavisXtend Accounting Server Administrator’s Guide*.

## Administrative Attributes for Redirect PVCs

The Add Redirect PVC dialog box Administrative tab is shown in Figure 7-15.

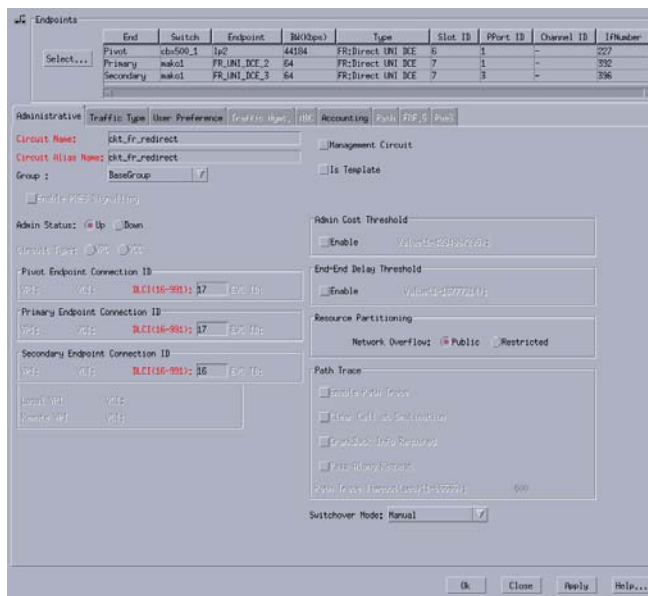


Figure 7-15. Add Redirect PVC Dialog Box: Administrative Tab

The Administrative tab contains the fields described in [Table 7-9](#).

**Table 7-9. Add Redirect PVC Dialog Box: Administrative Tab**

Element	Description
Circuit Name	Enter a unique, 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	<i>(Optional)</i> Enter a unique, alphanumeric name to identify the redirect circuit. Do not use parentheses or asterisks. This name must be unique to the entire map. The default name is the circuit name.  The service providers use the circuit name alias to identify the redirect circuit in a way that is meaningful to their customers.
Group	Select a group to which you want to associate the redirect PVC. The redirect PVC can belong to any group or to the BaseGroup.  Refer to the <i>Navis EMS-CBGX Installation and Administration Guide</i> for a detailed information on group-wise resource partitioning.
Enable PWE3 Signalling	Check this box to enable PWE3 signalling on this circuit. The Pwe3 tab will be available only if this box is checked.  <b>Note:</b> PWE3 signaling applies to CBX 3500 ATM circuit endpoints. For more information on PWE3, refer to the <i>ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i> .
Management Circuit	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. After 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 DLCI configurations. The default value is No. (For more information about management DLCIs, see <a href="#">Chapter 11, “Configuring Management Paths.”</a> )
Template	<i>(Optional)</i> Save these settings as a template to use again to configure another PVC with similar options. To create a template, choose Yes in the Template field. The default is No. See <a href="#">“Using Templates to Define Circuits” on page 7-48</a> for more information.
Admin Status	Select <i>Up</i> (default) to activate the circuit at switch startup, or select <i>Down</i> to take the circuit offline to run diagnostics such as PVC loopback.
Pivot / Primary / Secondary Endpoint Connection ID	Enter a unique DLCI number (16 through 991) for the pivot, primary, and secondary endpoint logical ports. See <a href="#">“About DLCI Numbers” on page 7-8</a> for more information about DLCI numbers.

**Table 7-9. Add Redirect PVC Dialog Box: Administrative Tab (Continued)**

Element	Description
Admin Cost Threshold	<p>When 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 then enter a value of 1000, the redirect PVC will not be routed over a path whose total administrative cost exceeds 1000.</p> <p>The total administrative cost for a path is calculated by adding the sums of the administrative cost for each trunk in the path. The valid range of values for this field is from 1 to 4294967295.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>Do not enable this option if you use End-End Delay routing.</i></p>
End-End Delay Threshold	<p>When 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 then enter a value of 500 microseconds, the redirect PVC will not be routed over a path whose total end-to-end delay exceeds 500 microseconds.</p> <p>The total end-to-end delay for a path is calculated by adding the sums of the end-to-end delay for each trunk in the path. The valid range for this field is from 0 to 16777214 microseconds.</p> <p>If the End-to-End Delay Threshold is disabled to the circuit, then the operational status window displays Unavailable in the delay field.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>The value you enter should reflect your network topology. If a redirect PVC will typically traverse high-speed trunks, then set the delay rate lower; increase the delay if the redirect PVC must use low-speed trunks.</i></p>
Resource Partitioning	<p>Select one of the following Network Overflow options:</p> <ul style="list-style-type: none"> <li>• <i>Public</i> (default) - Redirect PVCs are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the traffic of the customer is allowed to run over common trunks (shared by a variety of different customers).</li> <li>• <i>Restricted</i> – Redirect 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.</li> </ul> <p>Resource Partitioning determines how the redirect PVC traffic is managed during trunk overflow or failure conditions. This feature is used with Virtual Private Networks (VPNs).</p>

**Table 7-9. Add Redirect PVC Dialog Box: Administrative Tab (Continued)**

Element	Description
Path Trace	<p>Path Trace enables you to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network. Path trace can track even failed connections and report all paths attempted.</p> <ul style="list-style-type: none"> <li>• Path Trace Admin Status – Enable or disable the path trace feature for this circuit. Select Enabled to enable path trace or Disabled (default) if you do not want to have path trace enabled.</li> <li>• Crankback Info Required – Enable or disable collection of crankback information. Select Yes to instruct the switch to collect and maintain the crankback information, that is, information about dynamic rerouting of call setups around failed nodes or links (or links with insufficient resources) on the traced path. If No (default) is selected, crankback information will not be collected.</li> <li>• Pass Along Request – Enable or disable pass along request for this path trace. Select Yes (default) to have the path trace continue through nodes that do not support the path trace feature. This may cause the trace results to contain some gaps between successive entries of logical nodes and logical ports traversed by this connection or party. Select No to cause the path trace to terminate at any switch that does not support the path trace feature. A partial path trace will be returned.</li> <li>• Path Trace Timeout (sec) – Enter a number of seconds (0-65535) for which you want the trace results to be maintained in the switch. The default is ten minutes (600 seconds).</li> </ul> <p>For information about configuring path tracing at the logical port level, see <a href="#">“Administrative Attributes for Frame Relay LPorts” on page 3-15</a>. For more information about how path tracing works, refer to the <i>Switch Diagnostics User’s Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000</i>.</p>

**Table 7-9. Add Redirect PVC Dialog Box: Administrative Tab (Continued)**

Element	Description
Switchover Mode	<p>Select one of the following configurations:</p> <ul style="list-style-type: none"><li data-bbox="669 415 1409 478">• <i>Manual</i> – Enables you to switch the circuit connection between the pivot endpoint and the primary or secondary endpoint.</li><li data-bbox="669 508 1409 730">• <i>Non-Revertive</i> – Triggers an automatic forward switchover to establish the connection between the pivot and secondary endpoints in case of primary endpoint failure. If the secondary endpoint goes down and the primary endpoint recovers, then no automatic switchover is triggered. The administrator must manually switch the circuit connection from the working secondary endpoint backward to the primary endpoint.</li><li data-bbox="669 760 1409 907">• <i>Revertive</i> – Triggers an automatic forward switchover to establish the connection between the pivot and secondary endpoints in case of primary endpoint failure. If the primary endpoint recovers, then the backward switchover is triggered automatically to re-establish the connection between the pivot and primary endpoints.</li></ul>

## Setting the Redirect PVC Delay Timer

The Redirect PVC Delay Timer field is an option in the Add Logical Port dialog box for Frame Relay 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 Timer only for the primary endpoint. 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 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.



**Note** – Modifying the value of this attribute does not admin down the logical port.

---

## Working with Multicast DLCIs

The Set Multicast DLCIs function enables you to add, modify, and delete multicast DLCI configurations for a Frame Relay network. A multicast DLCI is a circuit configured as multiple groups of circuits on the same logical port. You can define up to 32 multicast groups per switch. You must first configure Frame Relay circuits to define the DLCIs. You then allocate these circuits as member DLCIs in the multicast configuration.

Lucent currently supports one-way multicast. A multicast DLCI enables the network to:

- Accept a frame on a single DLCI.
- Replicate the frame.
- Distribute the frame to multiple circuit destinations.

This configuration requires you to enter a DLCI for a multicast group made up of several circuits. The DLCI represents the circuit endpoints. You must first configure the DLCIs before you can allocate them as member DLCIs in the multicast group. See [Table 7-6 on page 7-14](#) and for information about defining a unique DLCI for a logical port.

## Multicast DLCI Member Limits

The following sections describe how to determine the maximum number of multicast DLCI members on B-STDx and CBx modules that support multicast DLCI circuits.

### Multicast DLCI Member Limits for B-STDx Modules

The number of multicast members supported on B-STDx modules is a function of the number of bytes available on the module and the frame size being transmitted, as follows:

$$\text{member limit} = \text{bytes available} / \text{frame size}$$

This formula determines the maximum number of multicast members supported at the egress module where the multicast DLCI actually resides. In general, the number of multicast members supported decreases as the frame size increases.

The number of bytes available depends on the B-STDx module type:

- All IOPA modules (UIO, DSX, T1, E1, etc.) have a maximum of 32000 bytes available.
- All IOPB modules (HSSI, ATM, 12-port E1) have a maximum of 9500000 bytes.



**Note** – The ATM CS and ATM IWU I/O modules do not support multicast DLCI.

**Table 7-10** lists common frame sizes and the maximum number of multicast members supported on each B-STDx module type.

**Table 7-10. Multicast DLCI Member Limits (B-STDx Modules)**

Frame Size (in bytes)	IOPA Module Maximum Multicast Members	IOPB Module Maximum Multicast Members
64	514	14936
128	257	7468
256	128	3734
512	64	1867
1024	32	933
2048	16	466
4096	8	233
8160	4	117

### Multicast DLCI Member Limits for CBX Modules

CBX IOM2 modules that support multicast DLCI determine frame size on a per-forwarding engine (FE) basis. Each module may support one or two FEs, depending upon the module type. On modules that support two FEs, each FE supports a range of DS3 frame ports, as shown in **Table 7-11**.

**Table 7-11. Forwarding Engine Support on CBX IOM2 Modules**

Module	No. of FEs	Supporting Physical Port Nos.
8-Port Subrate DS3 FR/IP IOM	2	1-4 (FE 1) 5-8 (FE 2)
6-Port DS3 FR/IP IOM	2	1-3 (FE 1) 4-6 (FE 2)
32-Port Channelized T1/E1 FR/IP IOM	1	1-32



**Table 7-11. Forwarding Engine Support on CBX IOM2 Modules**

Module	No. of FEs	Supporting Physical Port Nos.
4-Port Channelized DS3 FR/IP IOM (DS3/1 version)	1	1-4
4-Port Channelized DS3 FR/IP IOM (DS3/1/0 version)	1	1-4

**Table 7-12** specifies the maximum multicast DLCI members supported on CBX modules for each multicast DLCI circuit, depending on the frame size.

The values listed in **Table 7-12** are supported on *each* FE for the CBX modules shown in **Table 7-11 on page 7-40**. For example, the 8-Port Subrate DS3 FR/IP IOM consists of two FEs, and each FE supports four DS3 frame ports (that is, one FE supports ports 1 through 4 and another FE supports ports 5 through 8). This means that for a frame size of 64 bytes, ports 1 through 4 can support 128 multicast members and ports 5 through 8 can also support 128 multicast members.

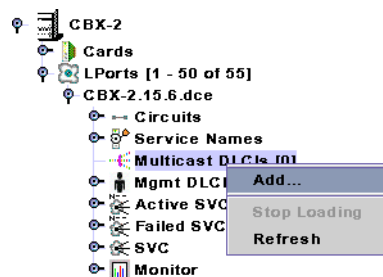
**Table 7-12. Multicast DLCI Member Limits (CBX Modules)**

Frame Size (bytes)	Maximum Multicast Members (per Forwarding Engine)
64	128
128	128
256	64
512	64
1024	32
2048	32
4096	16
8160	10

## Adding a New Multicast DLCI

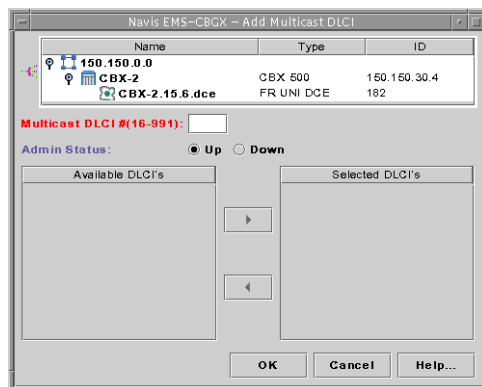
To configure multicast DLCIs, perform the following tasks:

1. In the `Switch` tab, expand the `LPorts` node.
1. Expand the node for the `LPort` you want to manage.
2. Right-click the `Multicast DLCIs` node and then click `Add` as shown in [Figure 7-16](#).



**Figure 7-16.** Adding a Multicast DLCI

The `Add Multicast DLCI` dialog box is displayed ([Figure 7-17](#)).



**Figure 7-17.** Add Multicast DLCI Dialog Box

3. In the `Multicast DLCI` field, enter a DLCI number to identify the multicast group. For more information, see [“About DLCI Numbers”](#) on page 7-8.
4. In the `Available DLCIs` list, select the DLCIs (circuit endpoints) you want to allocate as members of the multicast group, and click on the right arrow button. The selected DLCI now appears in the `Assigned DLCIs` list.

The `Assigned DLCIs` list displays the DLCIs you already selected for this multicast group. A multicast group must have at least one member. If you delete a circuit that is a member of a multicast group, the system automatically deletes it from the multicast group.

5. Using the `Admin Status` control, select `Down` or `Up` to indicate whether to activate the multicast DLCI when the switch or port comes online.
6. Choose `OK` to complete the configuration.

## Managing Circuits

This section contains information about the following administrative tasks:

- [“Moving Circuits” on page 7-43](#)
- [“Using Templates to Define Circuits” on page 7-48](#)
- [“Deleting Circuits” on page 7-50](#)

## Moving Circuits

The Move Circuit function enables you to move circuit endpoints defined for one logical port (the source) to another logical port (the destination). If you are upgrading a switch and do not want to lose PVC connections, you can use this function to move circuits to another switch.

This function has the following restrictions:

- You cannot move circuits you previously defined as part of a fault-tolerant PVC configuration (defined with a service name or designated as a backup).
- You cannot move a circuit that is currently in use.
- You cannot move a circuit if you receive an error that indicates there is a problem acquiring a lock for the circuit and all associated logical ports.
- You cannot move a circuit that has a manually defined circuit path.
- You cannot define more than one circuit for a Frame Relay Assembler/Disassembler (FRAD) logical port.
- The DLCI must be unique to the destination logical port.
- You cannot move a circuit if the source logical port type is not a valid type for the destination port. For example, you cannot move a Frame Relay or SMDS logical port type to an ATM DS3 module, since it does not support these services. Similarly, you cannot move a Switched Multimegabit Data Service (SMDS) logical port type to a 32-Port Channelized T1/E1 FR/IP IOM because the 32-Port Channelized T1/E1 FR/IP IOM does *not* support SMDS.
- The Move Circuit function will fail if moving a circuit exceeds the maximum number of circuits allowed for the destination logical port.
- You cannot move a circuit that is a member of a multicast DLCI configuration.

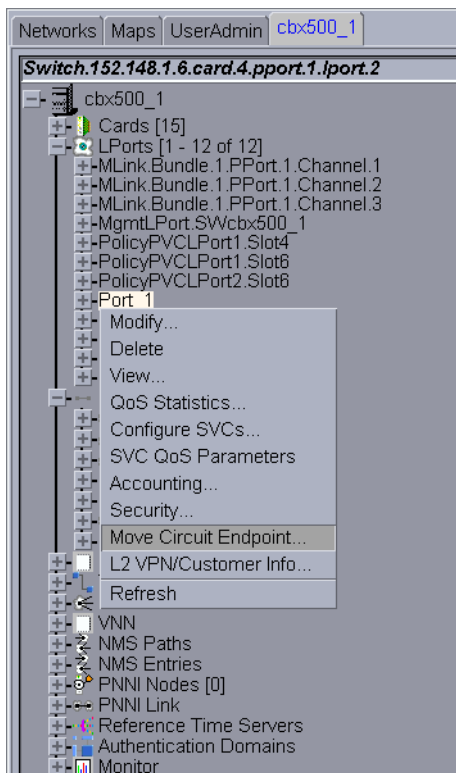
For more information on moving circuit endpoints, see the following topics:

- [“Moving Circuit Endpoint from an LPort instance” on page 7-44](#)
- [“Moving Circuit Endpoint from a Circuit instance” on page 7-46](#)

## Moving Circuit Endpoint from an LPort instance

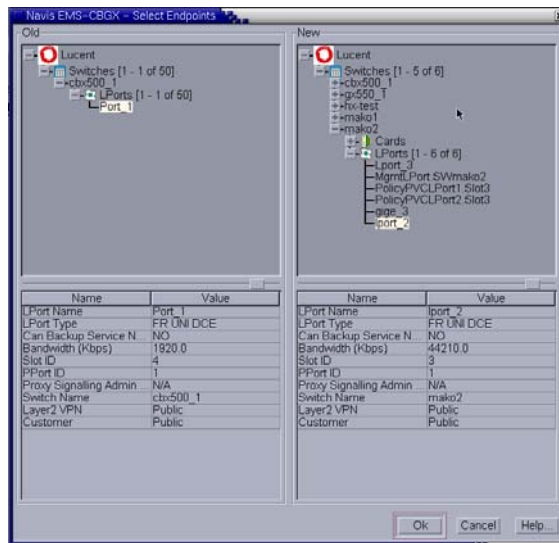
To move a circuit endpoint from an LPort instance, perform the following tasks:

1. In the `Switch` tab, expand the `LPorts` node.
2. Right-click an LPort instance and then select `Move Circuit Endpoint` from the popup menu as shown in [Figure 7-18](#).



**Figure 7-18. Moving a Circuit Endpoint from an LPort instance**

3. In the Move Circuit Endpoint dialog box, click **Select** to select the endpoints.  
The Select Endpoints dialog box is displayed (Figure 7-19).



**Figure 7-19. Select Endpoints Dialog Box**

4. Select the logical ports between which you want to move circuit endpoints. The left-hand side of the dialog box reflects the old (source) logical port, and the right-hand side of the dialog box reflects the new (destination) logical port.
5. Select the new endpoint by repeating this procedure or select an endpoint from a physical port.
6. Choose **OK** when you have selected the logical ports.

7. To complete the circuit endpoint move, select the circuits to be moved in the Move Circuit Endpoint dialog box, and click Start to begin the move process (Figure 7-20).

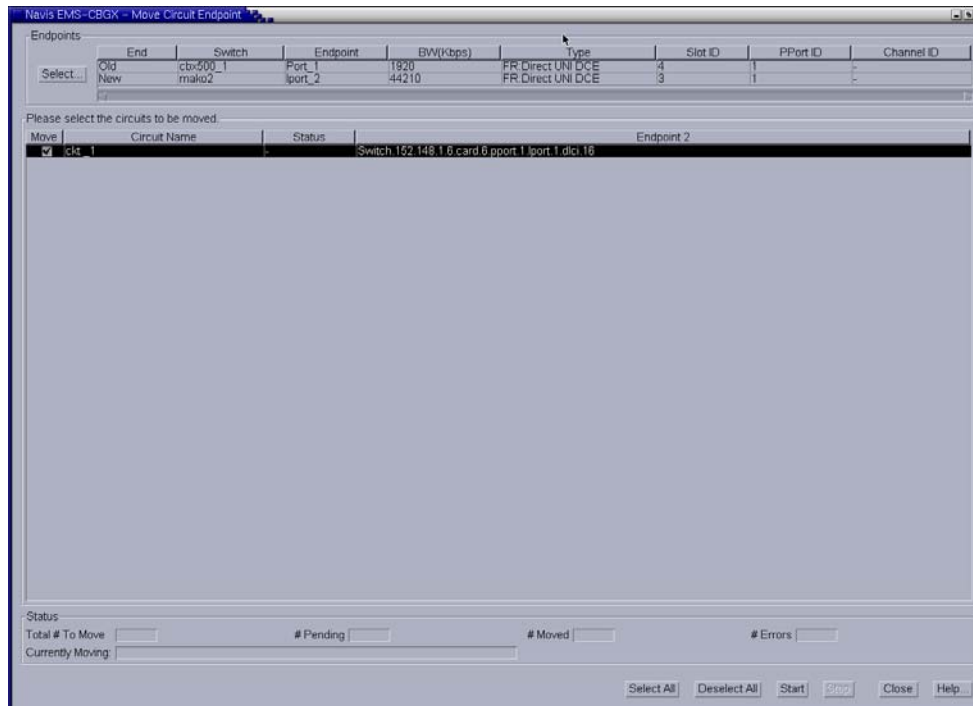


Figure 7-20. Move Circuit Endpoint Dialog Box

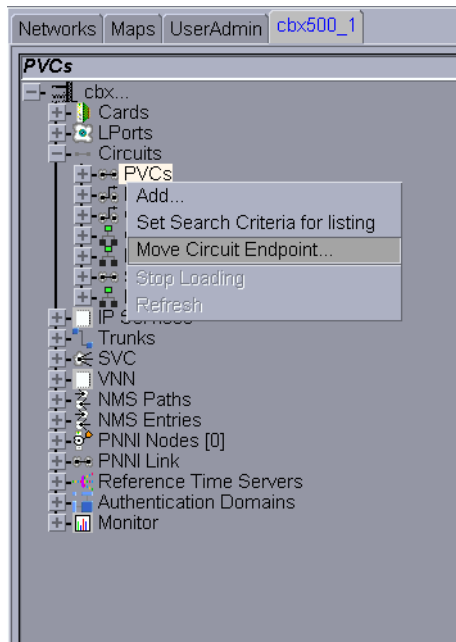
8. Click Close to close the Move Circuit Endpoint dialog box.

### Moving Circuit Endpoint from a Circuit instance

To move a circuit endpoint from a Circuit instance, perform the following tasks:

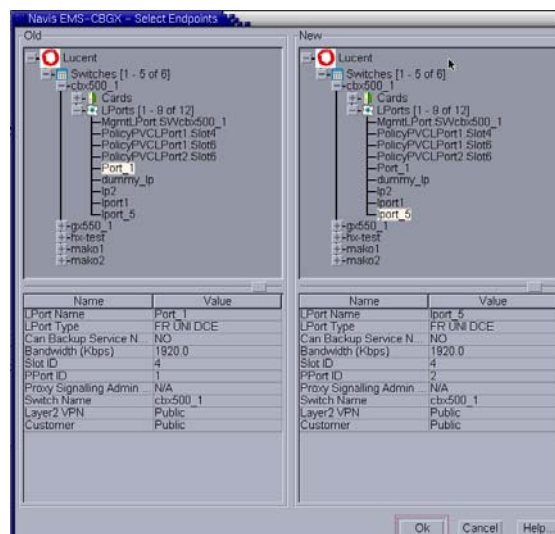
1. In the Switch tab, expand the Circuits node.
2. Select the PVCs node.

3. Right-click the PVCs node and then select `Move Circuit Endpoint` from the popup menu as shown in **Figure 7-21**.



**Figure 7-21. Moving a Circuit Endpoint**

4. In the `Move Circuit Endpoint` dialog box, click `Select` to select the endpoints. The `Select Endpoints` dialog box is displayed (**Figure 7-22**).



**Figure 7-22. Select Endpoints Dialog Box**

5. Select the logical ports between which you want to move circuit endpoints. The left-hand side of the dialog box reflects the old (source) logical port, and the right-hand side of the dialog box reflects the new (destination) logical port.

6. Select the new endpoint by repeating this procedure or select an endpoint from a physical port.
7. Choose OK when you have selected the logical ports.
8. To complete the circuit endpoint move, select the circuits to be moved in the Move Circuit Endpoint dialog box, and click Start to begin the move process (Figure 7-23).

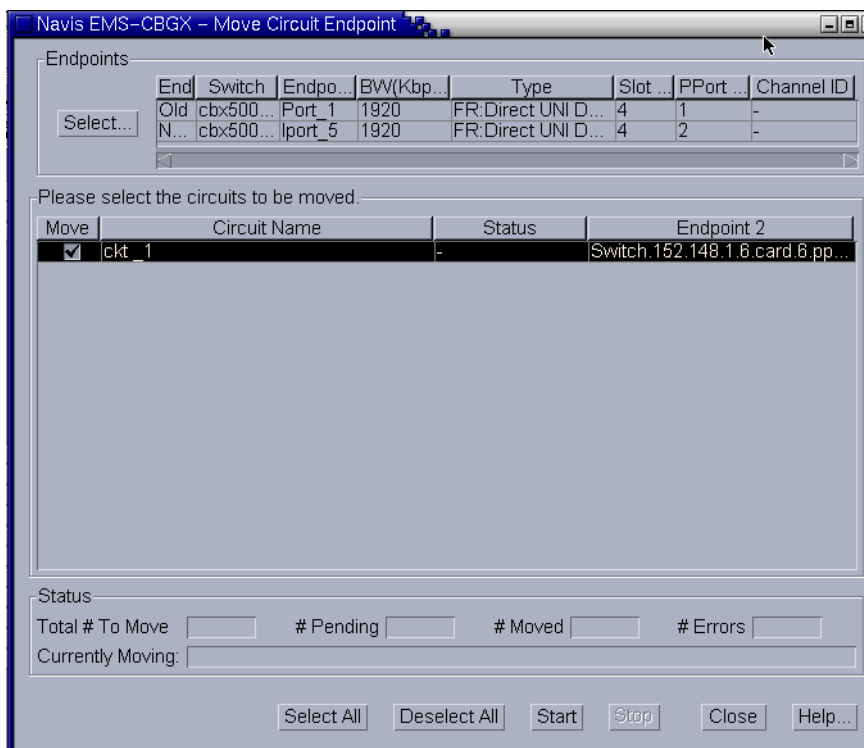


Figure 7-23. Move Circuit Endpoint Dialog Box

9. Choose Close to close the Move Circuit Endpoint dialog box.

## Using Templates to Define Circuits

If you have previously defined a PVC configuration and saved it as a template (using the *Is Template* field), you can create a new PVC using the same parameters.

To create a new PVC from a template, perform the following tasks:

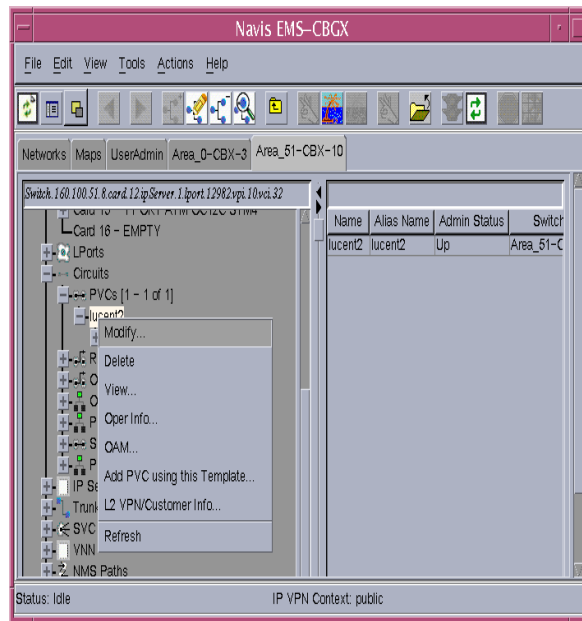
1. In the Switch tab, expand the Circuits node.
2. Expand the PVCs node.



- Right-click on a template-enabled PVC instance, and select **Add PVC** using this Template from the popup menu as shown in [Figure 7-24](#).

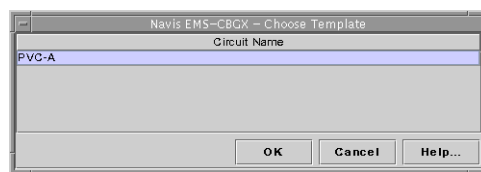


**Note** – The template-enabled PVC instance is available only if you have defined a PVC and then saved it as a template using the *Is Template* option.



**Figure 7-24. Adding a PVC Based on a Template**

The Choose Template dialog box is displayed ([Figure 7-25](#)).



**Figure 7-25. Choose Template Dialog Box**

- Select a PVC from the **Circuit Name** list and choose **OK**.

The **Add PVC** dialog box is displayed, with the same values as the selected template PVC, except for **Name**, **Alias**, and other values that are required to be unique.

- Select each of the tabs and modify the fields in each tab, if necessary. Choose **Help** for descriptions of the fields and buttons in each tab.
- Choose **OK** to provision the PVC and close the **Add PVC** dialog box.

## Deleting Circuits

To delete a circuit, perform the following tasks:

1. In the `Switch` tab, expand the `Circuits` node.
2. Expand the `PVCs` node and then select the circuit you want to delete.
3. Right-click the circuit node and then select `Delete` from the popup menu.
4. Click `Yes` to confirm the deletion.

## Configuring Offnet Circuits

A permanent virtual circuit (PVC) is established administratively (that is, by network management) rather than on demand (that is, using signaling across the UNI). An Offnet circuit (or soft PVC) is established by the network using signaling. After the Offnet circuit configuration is in place, the switch at one end of the Offnet initiates the signaling. This release supports up to 4096K Offnet circuits per card.

The NMS provisions one end of the Offnet circuit 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** – In this release, Soft PVC (SPVC) is referred to as Offnet Circuit.

---

This chapter contains:

- [“Supported Modules” on page 8-2](#)
- [“About Offnet Circuits \(SPVCs\)” on page 8-2](#)
- [“Defining a Point-to-Point Offnet Circuit Connection” on page 8-5](#)
- [“Restarting an OffNet Circuit” on page 8-30](#)

## Supported Modules

Table 8-1 lists the Frame Relay modules on which Offnet circuits are supported.

**Table 8-1. Offnet Circuit Frame Relay Module Support**

CBX 3500 and CBX 500	B-STDX 9000
6-Port DS3 FR/IP IOM (CBX 500 only)	4-Port Channelized T1 I/O Module
4-Port Channelized DS3 FR/IP IOM (CBX 500 only)	12-Port Unchannelized E1 I/O Module
8-Port Subrate DS3 FR/IP IOM	2-Port HSSI I/O Module
32-Port Channelized T1/E1 FR/IP IOM	10-Port DSX-1 I/O Module
6-Port Channelized DS3/1/0 FR IOM	1-Port Channelized DS3 I/O and DS3/1/0 Modules

## About Offnet Circuits (SPVCs)

When working with Offnet circuits, you configure a connection that is point-to-point.

When you create an Offnet circuit, 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 then assign a Data Link Connection Identifier (DLCI) value. You configure the other endpoint (known as the *terminating endpoints*) with addresses, as you would an SVC. The originating endpoint uses signaling to access the terminating endpoints.

If you configure the terminating endpoint with a port prefix, then 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 Offnet circuit to connect.

Offnet circuits are supported on CBX 3500, CBX 500, and B-STDX 9000 multiservice switches through mixed virtual network navigator (VNN) and PNNI domains.



**Note** – In order to use the Interworking feature within the PNNI routing domain, you must enable the PNNI routing protocol in the network. Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*, for information on enabling PNNI on Lucent switches.

In addition, you must enable the PNNI Name Translation parameter on the Set Switch Attributes dialog box so that the switch can use the PNNI routing protocol and interoperate with other PNNI switches in the network. Refer to the *Navis EMS-CBGX Getting Started Guide* for information on enabling this parameter when you set switch attributes.

---

## Frame Relay Offnet Circuit Scalability

Prior to this release, Offnet Circuits supported only Frame Relay (FR)-to-FR, FR-to-ATM, and ATM-to-FR types. In earlier releases of Navis EMS-CBGX, the design for Frame Relay-to-Frame Relay Offnet circuits on the CBX 500 was not scalable. Since the Offnet circuits use more resources than the PVCs, the number of Offnet circuits that could be configured on a card was far less than the number of PVCs that could be configured on the same card. If the Offnet circuits are managed in the same way as the PVCs, then there can be an increase in the number of Offnet circuits that can be configured on a card to match the same number of PVCs. The combined total of PVCs and Offnet circuits supported in this release equals the total number of PVCs supported in previous releases.

In this release, Offnet Circuits support the Frame Relay-to-Frame Relay type and the Gigabit Ethernet-to-Frame Relay type of Offnet circuits.

Frame Relay Offnet circuit scalability is supported on all CBX 3500 and CBX 500 Frame Relay cards such as IOM, IOP, 2-Port HSSI, DS3/1/0. It is also supported on the CBX 3500 2-Port ULC Gigabit Ethernet card.

## Using PVC/PVP Termination

Before you configure Offnet circuits, you must first configure the SVC address or the prefix you want to assign to the Offnet circuit terminating endpoint. This endpoint may not actually terminate the Offnet circuit. When you configure an SVC port address, you enable or disable PVC or permanent virtual path (PVP) termination. If you disable termination, then the egress logical port signals the Offnet circuit on as a regular SVC.

The PVC and PVP termination enable you to send calls through the network to a non-SVC endpoint, using an SVC. [Table 8-2 on page 8-4](#) lists the results of using PVC or PVP termination.

As you configure PVC or PVP termination, consider the following:

- If you enable PVC termination, you can optionally specify a VPI/VCI or allow the Offnet circuit 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 Offnet circuit originator or the network to choose a VPI, and the switch terminates the SPVPC on the associated logical port.
- If you enable both PVC and PVP termination, you must allow the Offnet circuit originator or the network to select the VPI/VCI or VPI.

Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information about configuring PVC/PVP Termination on the SVC.

## Specifying the Target Select Type

The originating endpoint may optionally specify the remote VPI or VPI/VCI for an Offnet circuit. 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 Offnet circuit traverses only Lucent Virtual Network Navigator (VNN) or PNNI links. A few LAN-based Frame Relay networks currently support the PNNI protocol.
- If the Offnet circuit must traverse UNI or Interim Inter-switch Signalling Protocol (IISP) links, and one end of the Offnet circuit is not Lucent equipment, you cannot use the Specified target select type.

**Table 8-2** summarizes the results of using Offnet circuit target select type in conjunction with PVC/PVP termination.

**Table 8-2. OffNet Circuit Target Select Type**

<b>Originating Endpoint Target Select Type</b>	<b>Terminating Endpoint Termination Type</b>	<b>Behavior at Terminating Endpoint</b>
Any	Any	Network allocates any available VPI or VPI/VCI.

**Table 8-2. OffNet Circuit Target Select Type (Continued)**

Originating Endpoint Target Select Type	Terminating Endpoint Termination Type	Behavior at Terminating Endpoint
Any	Specified VPI or VPI/VCI	Accept Offnet circuit on a specified VPI or VPI/VCI. The SVC port address is dedicated to terminating this single Offnet circuit.
Specified VPI or VPI/VCI	Any	Accept Offnet circuit on a specified VPI or VPI/VCI; the SVC port address may terminate additional Offnet circuits.
Specified VPI or VPI/VCI	Specified VPI or VPI/VCI	Accept Offnet circuit if VPI or VPI/VCI match; reject Offnet circuit if they do not match. The SVC port address is dedicated to terminating this single Offnet circuit.

Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for information on setting the VPI/VCI values for SPVCs.

## Defining a Point-to-Point Offnet Circuit Connection

When working with Offnet circuits, you can configure a connection that is point-to-point. This section covers point-to-point Frame Relay Offnet circuits, configured through the Navis EMS-CBGX Offnet Circuits option.

You can access the Circuits node from the switch, or from an LPort node.

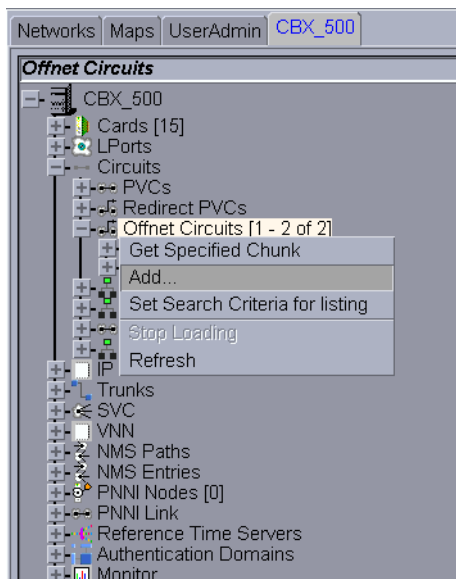


**Note** – When you create an Offnet Circuit from an LPort node, the selected LPort is automatically set as the Endpoint 1 of the new Offnet Circuit.

To open the Add Offnet Circuit dialog box, perform the following tasks:

1. In the Navigational Panel, expand the `Circuits` node.
2. Select the `Offnet Circuits` node.

3. Right-click the Offnet Circuits node and then select Add from the pop-up menu. The Add OffNet Circuit dialog box is displayed as in [Figure 8-3 on page 8-10](#).



**Figure 8-1. Navigation Panel: Offnet Circuits node**

4. Select the circuit endpoints. The Offnet Endpoint Selection dialog box is displayed.
5. Continue with [“Selecting an Endpoint From a Switch”](#) or [“Selecting an Endpoint From a Physical Port”](#) to select the endpoint.

### Selecting an Endpoint From a Switch

To select an endpoint from a switch, perform the following tasks:

1. In the Offnet EndPoint Selection dialog box, expand the node for the desired switch for Endpoint 1.  
If you are creating an Offnet Circuit from an LPort node, Endpoint 1 is already set for that LPort. Skip to step 4.
2. Expand the LPorts node under the switch.
3. Select the desired LPort.
4. Select the SVC Address tab or the Select Address tab to select or create a Terminating Endpoint.
5. Continue with [“Selecting the Terminating Endpoint Address.”](#)



## Selecting an Endpoint From a Physical Port

To select an endpoint from a physical port, perform the following tasks:

1. In the `Select Endpoints` dialog box, expand the node for the desired switch for Endpoint 1.  
  
If you are creating an Offnet Circuit from an LPort node, Endpoint 1 is already set for that LPort. Skip to step 8.
2. Expand the `Cards` node under the switch and expand the node for the desired card or module.
3. Expand the `PPorts` node and expand the node for the desired physical port.
4. Expand the `LPorts` node and select the desired LPort.
5. Select the `SVC Address` or the `Select Address` tab to select or create a Terminating Endpoint.
6. Continue with **“Selecting the Terminating Endpoint Address.”**

## Selecting the Terminating Endpoint Address

To complete this configuration, perform the following tasks:

1. If you know the SVC terminating endpoint address, select it from the SVC Address tab (Figure 8-2).

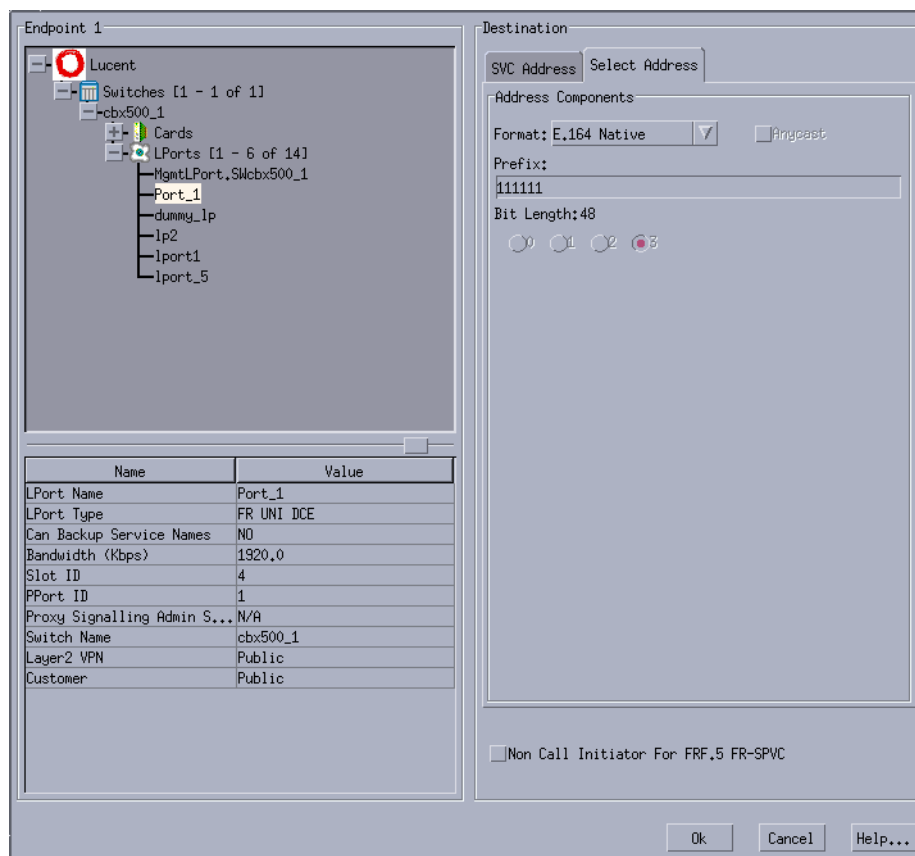


Figure 8-2. Offnet Endpoints Selection dialog box

2. If you do not know the address, select the Select Address tab and then use Table 8-3 to select the address format and configure the terminating endpoint address.

Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on ATM End System Address (AESA) formats.

**Table 8-3. Address Formats and Address Components**

Address Format	Address Components
E.164 Native	In the <code>Prefix</code> 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.
X.121	In the <code>X.121</code> field, enter the address in the range 0 to 9. X.121 addresses are an ITU-T standard used in X.25 networks. X.121 addresses are sometimes referred to as IDNs (International Data Numbers) and consist of 14 ASCII digits.
DCC and ICD AESA (or Anycast)	In the <code>DCC</code> 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 in those fields.
E.164 AESA (or Anycast)	In the <code>E.164</code> field, enter the full or partial E.164 AESA address. Since the initial domain identifier (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 <i>Fh</i> . For example, 5085551234 should be entered as 000005085551234F.  After entering in the IDI portion of the address, enter the appropriate HO-DSP, ESI, and SEL portions to complete the address.
Custom AESA	In the <code>AFI</code> field, enter the custom authority and format identifier (AFI) you want to use.  Then 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.

3. To configure a new port address, see the instructions [Chapter 14, “Configuring Switched Virtual Circuit \(SVC\) Parameters.”](#)
4. Select `Non-call Initiator For FRF.5 FR-SPVC` if this endpoint is not the call initiator in the circuit. The `Address Components` field in the `Select Address` tab is cleared since the address information is not needed.
5. Choose `OK`. The `Add Offnet Circuit` dialog box is displayed with the selected endpoints.
6. Continue with [“Configuring Offnet Circuit Parameters” on page 8-10.](#)



**Table 8-4. Add OffNet Circuits: Administrative Tab**

Field	Action/Description
Circuit Name	Enter a unique, alphanumeric name to identify the circuit. Do not use parentheses and asterisks. This name must be unique to the entire map.
Circuit Name Alias	<i>(Optional)</i> Enter a unique, alphanumeric name to identify the offnet circuit. Do not use parentheses or asterisks. This name must be unique to the entire map. The default name is the circuit name.  The service providers use the circuit name alias to identify the offnet circuit in a way that is meaningful to their customers.
Group	Select a group to which you want to associate SPVC. SPVC can belong to any group or to the BaseGroup.  Refer to the <i>Navis EMS-CBGX Installation and Administration Guide</i> for a detailed information on group-wise resource partitioning.
Management Circuit	Select Management Circuit to include this PVC configuration in the Network Management Station (NMS) initialization script file. This file contains all the Simple Network Management Protocol (SNMP) set requests necessary to replicate the entire switch configuration. After you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity.  <b>Note:</b> <i>This option is useful in a few management DLCI configurations.</i>
Is Template	<i>(Optional)</i> Enable this option to save these settings as a template to use again to configure another PVC with similar options.
Enable PWE3 Signaling	Enable this option to facilitate the Pseudo Wire Emulation Edge to Edge (PWE3) signaling on this circuit. The PWE3 tab will be available only if this box is enabled.
Admin Status	Select <i>Up</i> (default) to activate the circuit at switch startup, or select <i>Down</i> to take the circuit offline to run diagnostics such as PVC loopback.
<b>Endpoint 1 Connection ID</b>	
DLCI <i>(Frame Relay UNI endpoints only)</i>	For Endpoint 1, enter an Data Link Connection ID (DLCI) in the range 16 to 991.  A DLCI is a 10-bit address that identified PVCs. The DLCIs identify the logical end points of a virtual circuit and only have local significance.
<b>Endpoint 2 Connection ID</b>	
Destination Service Type	Select <i>ATM</i> or <i>Frame</i> , depending on the service on the destination endpoint.

**Table 8-4. Add OffNet Circuits: Administrative Tab**

Field	Action/Description
Target Select Type	<p>Select <i>Any</i> or <i>Required</i>. <i>Any</i> indicates that the terminating endpoint uses any available VPI or VCI value. If you need to specify a VPI or VCI for the terminating endpoint, you must complete the PVC or PVP Termination fields on the Add SVC Port Address dialog box.</p> <p><i>Required</i> indicates that the terminating endpoint uses the VPI or VCI address you specify. If this is an SPVPC, enter the VPI; for an SPVCC, enter the VPI and VCI.</p>
VPI	<p>If <i>Required</i> is selected for the Target Select Type, then enter a unique virtual path identifier (VPI) value ranging from 0 to 15.</p>
VCI	<p>If <i>Required</i> is selected for the Target Select Type, then enter a unique virtual channel identifier (VCI) value ranging from 32 to 255.</p>
DLCI ( <i>Frame Relay only</i> )	<p>If applicable, displays the DLCI, a 10-bit address that identifies PVCs. The DLCIs identify the logical end points of a VC and only have local significance.</p>
Admin Cost Threshold	<p>When you enable this option, the offnet 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 then enter a value of 1000, the offnet PVC will not be routed over a path whose total administrative cost exceeds 1000.</p> <p>The total administrative cost for a path is calculated by adding the sums of the administrative cost for each trunk in the path. The valid range of values for this field is from 1 to 4294967295.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>Do not enable this option if you use End-End Delay routing.</i></p>
End-to-End Delay Threshold	<p>When you enable this option, the offnet 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 then enter a value of 500 microseconds, the offnet PVC will not be routed over a path whose total end-to-end delay exceeds 500 microseconds.</p> <p>The total end-to-end delay for a path is calculated by adding the sums of the end-to-end delay for each trunk in the path. The valid range for this field is from 0 to 16777214 microseconds.</p> <p>If the End-to-End Delay Threshold is disabled to the circuit, then the operational status window displays Unavailable in the delay field.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>The value you enter should reflect your network topology. If a offnet PVC will typically traverse high-speed trunks, then set the delay rate lower; increase the delay if the offnet PVC must use low-speed trunks.</i></p>

**Table 8-4. Add OffNet Circuits: Administrative Tab**

Field	Action/Description
Resource Partitioning	<p>Select one of the following Network Overflow options:</p> <ul style="list-style-type: none"> <li>• <i>Public</i> (default) - Offnet PVCs are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the traffic of the customer is allowed to run over common trunks (shared by a variety of different customers).</li> <li>• <i>Restricted</i> – Offnet 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.</li> </ul> <p>Resource Partitioning determines how the offnet PVC traffic is managed during trunk overflow or failure conditions. This feature is used with Virtual Private Networks (VPNs).</p>
<b>Path Trace</b>	
Enable Path Trace	<p>Enable this option to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network. Path trace can track even failed connections and report all paths attempted.</p>
Clear Call at Destination	<p>Enable or disable the removal of this circuit after the path trace is complete.</p> <p>Enable this option for the circuit to be deleted from the switch after the specified path trace timeout period. Path trace information for this circuit will also be made available for the timeout period. Disable this option for the circuit to remain (default).</p> <p>If this field is enabled, the circuit will not be created in the PRAM. Navis EMS-CBGX will create a temporary circuit. After the creation of this circuit, no modifications can be made to it.</p>
CrankBack Info Required	<p>Enable this option to instruct the switch to collect and maintain the crankback information, that is, information about dynamic rerouting of call setups around failed nodes or links (or links with insufficient resources) on the traced path. Disable this option if you do not want to collect crankback information.</p>
Pass Along Request	<p>Enable this option to have the path trace continue through nodes that do not support the path trace feature. This may cause the trace results to contain some gaps between successive entries of logical nodes and logical ports traversed by this connection or party. Disable this option to cause the path trace to terminate at any switch that does not support the path trace feature. A partial path trace will be returned.</p>
Path Trace Timeout	<p>Displays the number of seconds in the range 0 to 65535 for which you want the trace results to be maintained in the switch. The default is ten minutes (600 seconds).</p>

## Traffic Type Attributes

The Traffic Type tab of the Add/Modify OffNet Circuit dialog box is explained.

1. Select the Traffic Type tab from the Add OffNet Circuit dialog box to specify traffic descriptor (TD) settings for forward and reverse traffic (Figure 8-4).



**Note** – If you do not enable the Non Call Initiator For FRF.5 FR-SPVC option on the OffNet EndPoint Selection dialog box, then the Traffic Type tab is unavailable; these attributes do not need to be set.

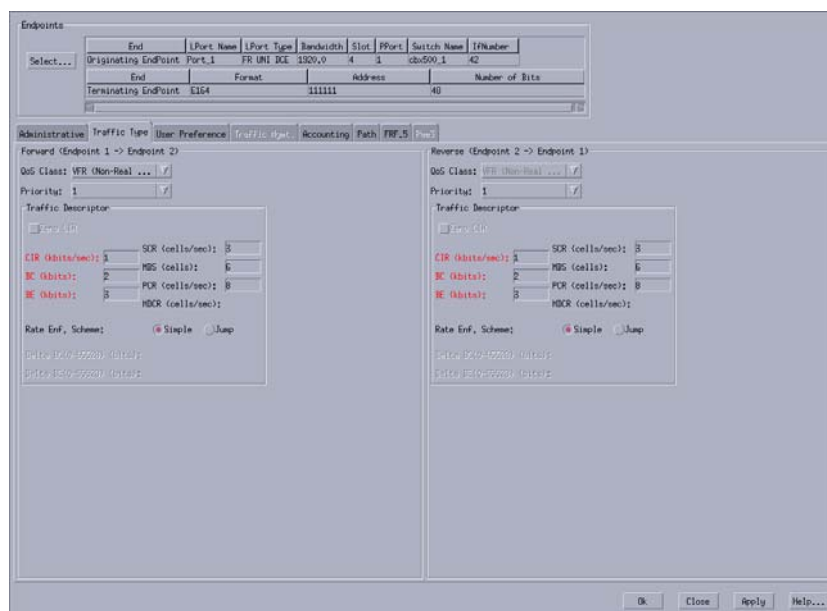


Figure 8-4. Add OffNet Circuit: Traffic Type Tab

On an FRF.5 circuit, you do not configure the Reverse QoS class but it is set by the NMS based on the service type of the destination endpoint and the QoS class of the originating endpoint. However, you can configure the TDs for the destination endpoint. If both endpoints are Frame Relay service, then the QoS class of the originating endpoint is used for the terminating endpoint.



**Table 8-5** lists the allowed QoS classes for the offnet circuit endpoints.

**Table 8-5. Allowable QoS Classes**

QoS Class	ATM Endpoint	Frame Relay Endpoint
VBR-RT	Applicable	Not Applicable
VBR-NRT	Applicable	Not Applicable
UBR	Applicable	Not Applicable
VFR-RT	Not Applicable	Applicable
VFR-NRT	Not Applicable	Applicable
UFR	Not Applicable	Applicable

2. Complete the `Traffic Type` tab fields as described in **Table 8-6**.



You *must* configure Traffic Type attributes before choosing OK in the Add Offnet Circuit 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.

---

**Table 8-6. Add OffNet Circuit: Traffic Type Tab**

Field	Action/Description
<b>Forward (Endpoint 1 → Endpoint 2)</b>	
QoS Class	<p>Select one of the following Gigabit Ethernet Quality of Service (QoS) classes:</p> <ul style="list-style-type: none"> <li>• <i>VFR (Real Time)</i> – Variable Frame Rate (VFR) (Real Time) is used for special delay-sensitive applications that require low delay variation between the endpoints.</li> <li>• <i>VFR (Non-Real Time)</i> – Variable Frame Rate Non-Real Time (NRT) handles transfer of long, bursty data streams over a pre-established connection. This service provides low data loss but no delay guarantee. It is also used for short, bursty data such as LAN traffic. The Customer Premise Equipment (CPE) protocols adjust for any delay or loss incurred through the use of VFR-NRT.</li> <li>• <i>UFR</i> – Primarily, Unspecified Frame Rate (UFR) is used for Local Area Network (LAN) traffic. The CPE should compensate for any delay or frame loss.</li> </ul> <p><b>Notes:</b> For a CBX 500 switch that uses the FCP, resource management (RM) cells are sent in the backward direction. As a result, they assume the QoS class of the other direction.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Priority	<p>Select 1, 2, or 3 to configure the priority of data being transmitted on this circuit. The circuit priority determines the forward priority of the data. The highest priority is 1 (do not discard data); the lowest priority is 3 (discard data). The default priority for Frame Relay is 1.</p> <p><b>Note:</b> To configure the priority of transmitted data for a standard or redirect management PVC (MPVC) select 1, 2, or 3. The default priority is 1.</p>

**Table 8-6. Add OffNet Circuit: Traffic Type Tab**

Field	Action/Description
<b>Traffic Descriptor</b>	
Zero CIR	<p>Enable this option to indicate that the PVC has an assigned CIR value of zero, and it is a best-effort delivery service. The customer data that is subscribed to zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on zero CIR PVCs have DE set to one (1).</p> <p><b>Note:</b> For ATM-to-Frame Relay and Frame Relay-to-Frame Relay Offnet circuits, when you enable Zero CIR, then:</p> <ul style="list-style-type: none"> <li>• At endpoint 1, you cannot set CIR, Bc, and Be values.</li> <li>• At endpoint 2, you cannot configure Zero CIR. QoS is displayed as UFR. CIR and Bc cannot be configured. They are displayed as 0 (zero). You can only configure the Be value.</li> </ul>
CIR	Enter the Committed Information Rate (CIR) in Kbps at which the network transfers data under normal conditions. The normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc). The value on each PVC is asymmetric (you can set a different CIR in each direction), which provides more efficient use of bandwidth.
BC	Enter the maximum amount of data (Committed Bit size), in Kbits, that the network attempts to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as Bc/CIR. This value must be greater than zero and is typically set to the same value as CIR.
BE	Enter the maximum amount of uncommitted data (Excess Bit), in Kbits, the network will attempt to deliver during a specified time interval, Tc. Tc is calculated as Bc/CIR. The network treats this data as Discard Eligible (DE) data.
SCR	<i>(Read-only)</i> Displays the sustainable cell rate (SCR) in cells per second for the Frame Relay endpoint.
MBS	<i>(Read-only)</i> Displays the maximum burst size (MBS) in cells for the Frame Relay endpoint.
PCR	<i>(Read-only)</i> Displays the peak cell rate (PCR) in cells per second for the Frame Relay endpoint.
Delta BC (0-65528) (bits)	Set the number of Delta BC (Committed Bit) bits for this circuit in the range 0 to 65528. The default value is 65528. This value is the maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval, provided there is positive Bc credits before receiving the frame, but negative Bc credits after accepting the frame.

**Table 8-6. Add OffNet Circuit: Traffic Type Tab**

Field	Action/Description
Delta BE (0-65528) (bits)	<p>Set the number of Delta BE (Excess Bit) bits for this circuit in the range 0 to 65528. The default value is 65528.</p> <p>This value is the maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval, provided there is positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame.</p>
Rate Enf. Scheme	<p>Select <i>Simple</i> (default) or <i>Jump</i>. The configurable rate enforcement scheme provides additional flexibility, increased rate enforcement accuracy, and improved switch performance.</p> <p><b>Note:</b> <i>Simple</i> indicates time (<math>T_c</math>) as measured in periodic intervals. If you select the <i>Simple</i> scheme, then the “bad” PVC detection feature is disabled. The <i>Jump</i> scheme is supported only on Ethernet Ingress point for Ethernet Virtual Circuit (EVC).</p>
Rate Enf. Scheme	<p>Select <i>Enabled</i> (default) to support the <i>Jump</i> scheme, or select <i>Disabled</i>. The configurable rate enforcement scheme provides additional flexibility, increased rate enforcement accuracy, and improved switch performance.</p>
<b>Reverse (Endpoint 2 → Endpoint 1)</b>	
QoS Class	Displays the Quality of Service (QoS) selected.
Priority	<p>Select 1, 2, or 3 to configure the priority of data being transmitted on this circuit. The circuit priority determines the forward priority of the data. The highest priority is 1 (do not discard data); the lowest priority is 3 (discard data). The default priority for Frame Relay is 1.</p> <p><b>Note:</b> <i>To configure the priority of transmitted data for a standard or redirect management PVC (MPVC) select 1, 2, or 3. The default priority is 1.</i></p>

**Table 8-6. Add OffNet Circuit: Traffic Type Tab**

Field	Action/Description
<b>Traffic Descriptor</b>	
Type	<p>Select one of the available traffic descriptions, say:</p> <ul style="list-style-type: none"> <li>• PCR CLP=0+1, SCR CLP=0, MBS CLP=0</li> <li>• PCR CLP=0+1, SCR CLP=0, MBS CLP=0, Tagging</li> <li>• PCR CLP=0+1, SCR CLP=0+1, MBS CLP=0+1</li> </ul> <p><i>PCR CLP=0 (cells/sec)</i> – Displays only if you selected a TD combination that includes PCR CLP=0. If so, specify the peak cell rate (PCR) in cells per second (CS) for high-priority traffic (that is, the CLP=0 cell stream).</p> <p><i>PCR CLP=0+1 (cells/sec)</i> – Specify the PCR in CPS for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream).</p> <p><i>SCR CLP=0 (cells/sec)</i> – Displays only if you selected a TD combination that includes SCR CLP=0. If so, specify the sustainable cell rate (SCR) in CPS for the combined high-priority traffic (that is, the CLP=0 cell stream).</p> <p><i>SCR CLP=0+1 (cells/sec)</i> – Displays only if you selected a TD combination that includes SCR CLP=0+1. If so, specify the SCR in CPS for the combined high- and low-priority traffic (that is, the CLP=0+1 aggregate cell stream).</p> <p><i>MBS CLP=0 (cells)</i> – Displays only if you selected a TD combination that includes MBS CLP=0. If so, specify the maximum burst size (MBS) in CPS for the combined high-priority traffic (that is, the CLP=0 cell stream).</p> <p><i>MBS CLP=0+1 (cells)</i> – Displays only if you selected a TD combination that includes MBS CLP=0+1. If so, specify the MBS in CPS for the combined high- and low-priority traffic (that is, the CLP=0+1 cell stream).</p> <p><i>MCR CLP=0 (cells/sec)</i> – Displays only if you selected a TD combination that includes MCR CLP=0. If so, specify the minimum cell rate (MCR) in CPS for the combined high-priority traffic (that is, the CLP=0 cell stream).</p> <p>Although the MCR TD is only applicable to a CBX 500 switch 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 switch with FCP, the PVC might traverse a CBX 500 switch FCP trunk. In this case, the provisioned attribute is used.</p> <p><b>Note:</b> <i>On ATM circuit emulation (CE) endpoint(s), the PCR, SCR, and MCR CPS values default to 118980 and cannot be changed.</i></p>
SCR	Enter the sustainable cell rate (SCR) in cells per second for the Frame Relay endpoint.

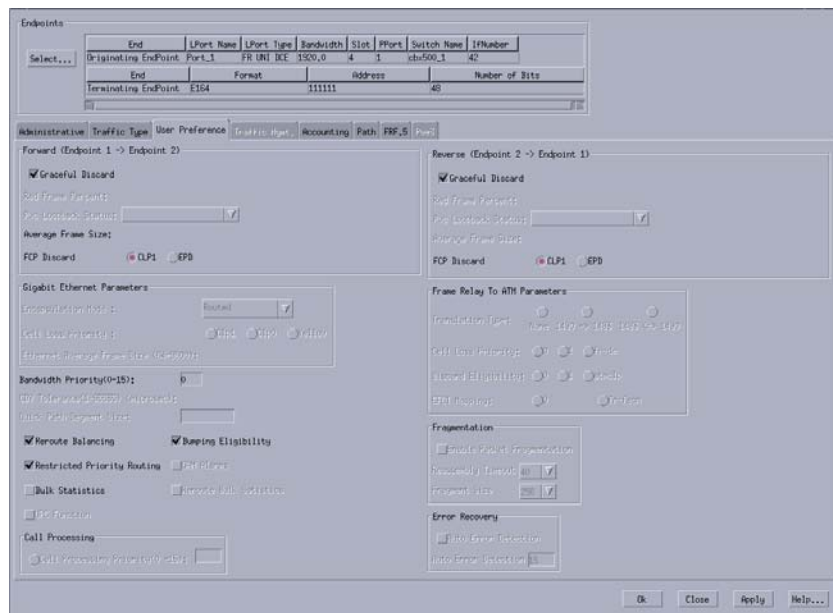
**Table 8-6. Add OffNet Circuit: Traffic Type Tab**

Field	Action/Description
MBS	Enter the maximum burst size (MBS) in cells for the Frame Relay endpoint.
PCR	Enter the peak cell rate (PCR) in cells per second for the Frame Relay endpoint.

### User Preference Attributes

The User Preference tab of the Add/Modify OffNet Circuit dialog box is explained.

1. Select the `User Preference` tab from the `Add OffNet Circuit` dialog box to select the TDs for this offnet circuit (Figure 8-5).



**Figure 8-5. Add OffNet Circuit: User Preference Tab**

2. Complete the `User Preference` tab fields as described in [Table 8-7](#).

**Table 8-7. Add OffNet Circuit: User Preference Tab**

Field	Action/Description
<b>Forward (Endpoint 1 → Endpoint 2)</b>	
Graceful Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Selected</i> (default) - Forwards a few red packets if there is no congestion.</li> <li><i>Non-Selected</i> - Immediately discards the red packets.</li> </ul> <p>Graceful Discard defines how the circuit handles “red” packets. The 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 <i>Selected</i>.</p>
FCP Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>CLPI</i> (default) - Selective CLP1 discard is provisioned for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate (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, then the cell is discarded. <b>Note:</b> <i>Early Packet Discard (EPD)</i> is not performed in this case.</li> <li><i>EPD</i> - ATM Flow-control Processor (FCP) can perform EPD for UBR, ABR, and VBR-BRT PVCs. If this option is selected, then 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 the cells in the next packet are discarded for that PVC.</li> </ul> <p>FCP Discard is displayed when you select a QoS class that supports FCP Discard.</p>
Bandwidth Priority (0-15)	Enter a value to indicate the bandwidth priority in the range 0 (zero) to 15. The default value is 0 (zero), and it indicates the highest priority.
CDV Tolerance	Enter a value in the range 1 to 65535 microseconds to define the Cell Delay Variation Tolerance (CDVT). The Usage Parameter Control (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 microseconds.
Reroute Balancing	Select <i>Selected</i> (default) to reroute the Call for an optimal path in case of Current PVCs or Offnet circuits, or select <i>Non-Selected</i> .

## Configuring Offnet Circuits

### Defining a Point-to-Point Offnet Circuit Connection

Field	Action/Description
Restricted Priority Routing	<p>Enable this option to provision a new PVC at the lowest bandwidth priority regardless of configured higher bandwidth priority and bumping eligibility settings.</p> <p>Disable this option if you use the configured bandwidth priority and bumping eligibility settings for newly provisioned circuits.</p>
Bulk Statistics	<p>Enable Bulk Statistics to configure statistics collection from a circuit using the NavisXtend Statistics Server. By default, this option is disabled.</p> <p><i>Note: If you enable Bulk Statistics at the circuit level, then the change does not take effect unless you first enable Bulk Statistics at the Switch, Card, and LPort levels.</i></p>
Bumping Eligibility	<p>Enable this option to enable non-real time circuits to become active, whether or not sufficient bandwidth exists.</p> <p>Disable this option to keep the non-real time circuit in retry mode until sufficient bandwidth is available.</p> <p>If Restricted Priority Routing is not enabled, then a non-real time circuit that has been bumped remains in retry mode until sufficient bandwidth is available, regardless of the bumping eligibility setting.</p>
UPC Function	<p>Enable this option to tag the circuits or drop the cells as they come into the port that do not conform to the configured traffic descriptors. The default is enabled.</p> <p>When you do not enable Usage Parameter Control (UPC), the circuit allows all traffic, including non-conforming traffic, into the port. As a result, 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, <i>Lucent recommends that you enable the UPC function on all circuits.</i></p> <p><b>Note:</b> <i>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.</i></p>
OAM Alarms	<p>When this option is enabled, the switch sends Operations, Administration, and Maintenance (OAM) F5 or F4 Alarm Indicator Signal (AIS) cells out of each UNI logical port endpoint to indicate that the circuit is down.</p>
Reroute Bulk Statistics	<p>Enable this option to turn on or off the collection and storage of reroute statistics for an applicable circuit on the switch. The switch level, card level, and LPort level bulk statistics should be enabled for this option to be successfully enabled.</p>



Field	Action/Description
<b>Reverse (Endpoint 2 → Endpoint 1)</b>	
FCP Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>CLP1</i> (default) - Selective CLP1 discard is provisioned for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate (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, then the cell is discarded. <b>Note:</b> <i>Early Packet Discard (EPD)</i> is not performed in this case.</li> <li>• <i>EPD</i> - ATM Flow-control Processor (FCP) can perform EPD for UBR, ABR, and VBR-BRT PVCs. If this option is selected, then 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 the cells in the next packet are discarded for that PVC.</li> </ul> <p>FCP Discard is displayed when you select a QoS class that supports FCP Discard.</p>
<b>Frame Relay to ATM Parameters</b>	
Translation Type	<p>Select one of the following Translation Type protocols:</p> <ul style="list-style-type: none"> <li>• <i>None</i> – Each end of the circuit uses the 1490 protocol.</li> <li>• <i>1490 → 1483</i> - The default value if you have a Frame Relay logical port on endpoint 1 and an ATM logical port on endpoint 2.</li> <li>• <i>1483 &lt;=&gt; 1490</i> – The default value for interworking circuits.</li> </ul>
Cell Loss Priority	<p>Select one of the following options: <i>0 (zero)</i>, <i>1</i>, or <i>fr-de</i> (default) to set the Cell Loss Priority (CLP) for Frame Relay to ATM.</p>
Discard Eligibility	<p>Select one of the following Discard Eligibility (DE) settings:</p> <ul style="list-style-type: none"> <li>• <i>0</i> – Sets DE to 0.</li> <li>• <i>1</i> – Sets DE to 1.</li> </ul> <p><i>atmclp</i> (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.</p>

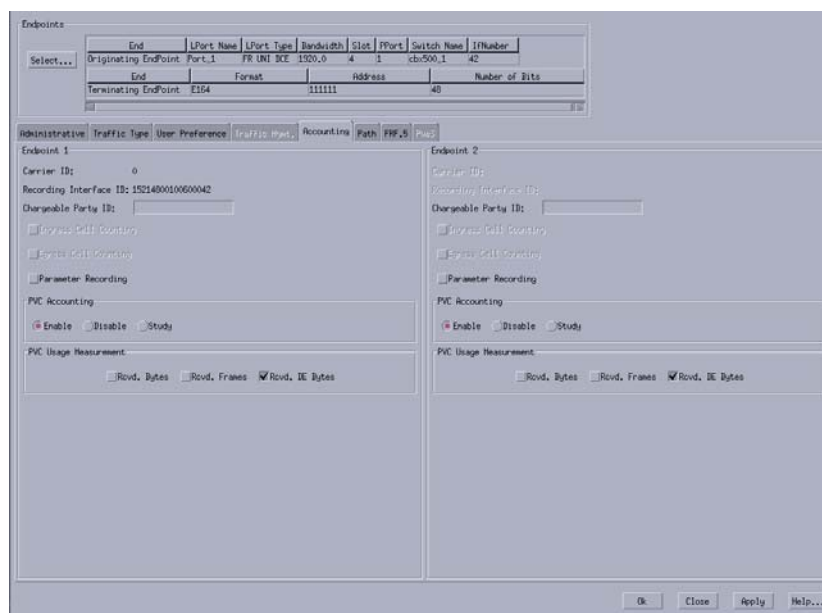
Field	Action/Description
EFCI Mapping	Select one of the following Explicit Forward Congestion Indication (EFCI) settings: <ul style="list-style-type: none"> <li>0 – Ignores EFCI to Forward Explicit Congestion Notification (FECN) bit mapping.</li> <li><i>fr-fecn</i> (default) – Maps the EFCI bit on the ATM endpoint to the Frame Relay FECN bit.</li> </ul>

Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information about configuring these attributes.

### Accounting Attributes

The Accounting tab of the Add/Modify OffNet Circuit dialog box is explained.

1. Select the Accounting tab from the Add OffNet Circuit dialog box to set the accounting parameters for this offnet circuit (Figure 8-6).



**Figure 8-6. Add OffNet Circuit: Accounting Tab**

2. Complete the Accounting tab fields as described in Table 8-8.

**Table 8-8. Add OffNet Circuit: Accounting Tab**

Field	Action/Description
<b>Endpoint 1</b>	

**Table 8-8. Add OffNet Circuit: Accounting Tab**

Field	Action/Description
Carrier ID	Displays a 5-digit Carrier Identifier (ID). This number uniquely identifies the carrier at each end of the network interface. If you have not yet configured accounting at the LPort level, then this field is set to 0 (zero).
Recording Interface ID	Displays a 16-digit circuit Recording Interface ID, made up of the 12-digit IP address and the LPort interface number (no dots, and padded with zeros to fill all 12 digits).
Chargeable Party ID	If applicable, then enter the chargeable party ID (in decimal format) for the circuit.
Parameter Recording	Enable this option to include the circuit parameter information (QoS, CIR, BC, and BE) in the billing record.
PVC Accounting	Select one of the following PVC Accounting options: <ul style="list-style-type: none"> <li>• Enable — PVC usage data is collected on the PVC, if PVC Accounting is set to <i>Enable</i> at the switch level. If PVC Accounting is set to <i>Disable</i> at the switch level, setting this field to <i>Enable</i> has no effect (accounting will still be inhibited on the PVC).</li> <li>• Disable — PVC usage data is not collected on the PVC, even if PVC Accounting is set to <i>Enable</i> at the switch level.</li> <li>• Study — Functions the same as the <i>Enable</i> setting, except that the resulting records are marked as “study” to differentiate them from normal accounting records. This feature enables you to collect information for research</li> </ul>
PVC Usage Measurement	Select the one of the following options to include the counts in the billing records: <ul style="list-style-type: none"> <li>• Rcvd. Bytes</li> <li>• Rcvd. Frames</li> <li>• Rcvd. DE Bytes</li> </ul>
<b>Endpoint 2</b>	
Carrier ID	Displays a 5-digit Carrier Identifier (ID).
Recording Interface ID	Displays a 16-digit circuit Recording Interface ID, made up of the 12-digit IP address and the LPort interface number (no dots, and padded with zeros to fill all 12 digits).
Chargeable Party ID	If applicable, then enter the chargeable party ID (in decimal format) for the circuit.

**Table 8-8. Add OffNet Circuit: Accounting Tab**

Field	Action/Description
Ingress Cell Counting, Egress Cell Counting	<p>Enable the Ingress Cell Counting and Egress Cell Counting options to include cell counts from this circuit in PVC usage data collection, when PVC Accounting is set to Enabled at the switch and port levels. If you select either or both cell counting options, then the resulting accounting records contain both time-based and usage-based measurements.</p> <p>If you do not select either Ingress or Egress Cell Counting options, then the cell counts from this circuit are not included in PVC usage data collection. If you do not select either cell counting field, then the resulting usage data records contain only time-based measurements.</p>
PVC Accounting	<p>Select one of the following PVC Accounting options:</p> <ul style="list-style-type: none"> <li>• Enable — PVC usage data is collected on the PVC, if PVC Accounting is set to <i>Enable</i> at the switch level. If PVC Accounting is set to <i>Disable</i> at the switch level, setting this field to <i>Enable</i> has no effect (accounting will still be inhibited on the PVC).</li> <li>• Disable — PVC usage data is not collected on the PVC, even if PVC Accounting is set to <i>Enable</i> at the switch level.</li> <li>• Study — Functions the same as the <i>Enable</i> setting, except that the resulting records are marked as “study” to differentiate them from normal accounting records. This feature enables you to collect information for research</li> </ul>

## Path Attributes

The Path tab of the Add/Modify OffNet Circuit dialog box is explained.

1. Select the Path tab from the Add OffNet Circuit dialog box to set the circuit path parameters for this offnet circuit (Figure 8-7).

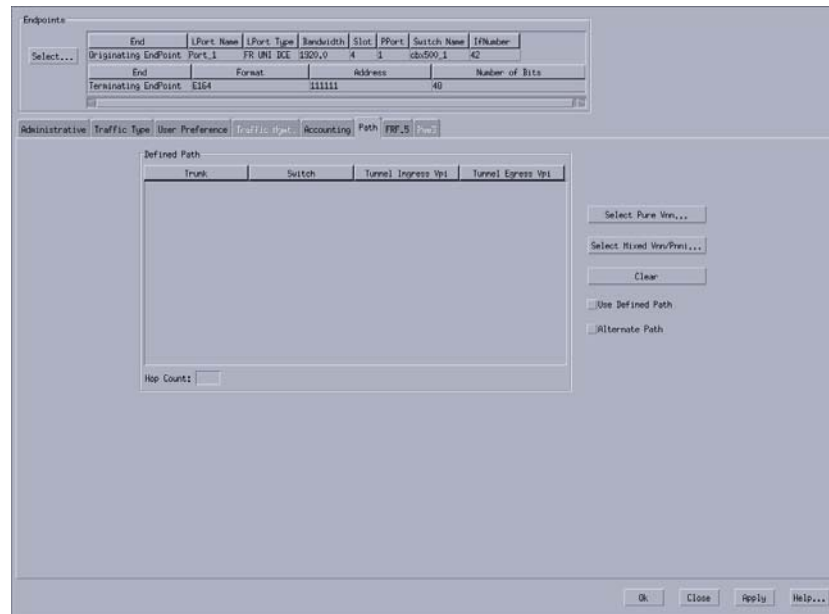


Figure 8-7. Add OffNet Circuit: Path Tab

2. In the Path tab, click the Select Pure VNN or Select Mixed VNN/PNNI button to display the Define Path dialog box.

The Defined Path section displays a listing of hops (trunk-switch pairs) in the defined path (Figure 8-8 on page 8-27).

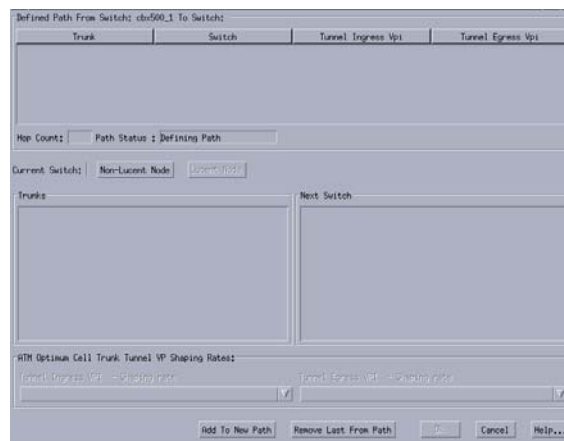


Figure 8-8. Define Path dialog box

## Configuring Offnet Circuits

### Defining a Point-to-Point Offnet Circuit Connection

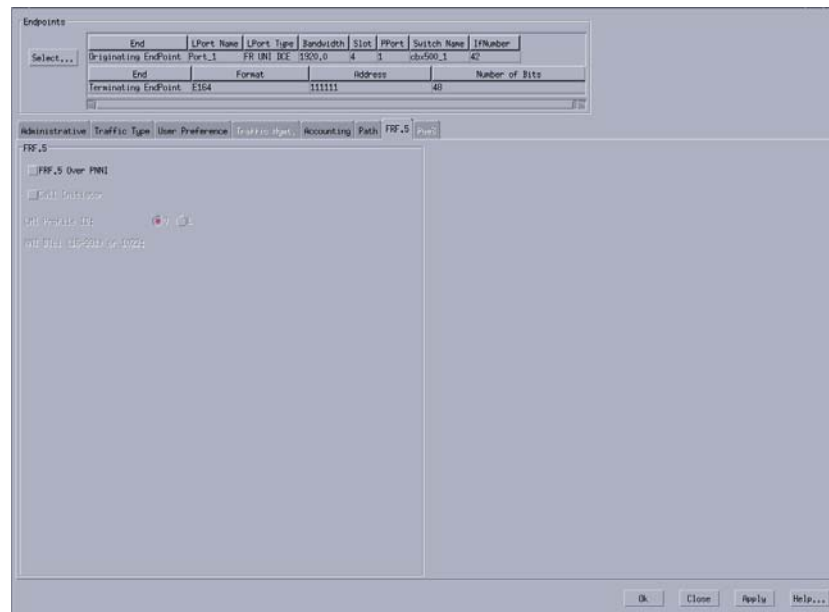
---

3. Define the path using the `Trunks` and `Next Switch` fields, selecting trunk-switch pairs from the list of available hops to include the hop in the circuit path, and then click the `Add to New Path` button. When there are multiple trunks between two switches, then select `[Any Trunk]` to route the circuit based on OSPF.
4. Click `Non-Lucent Node`. The `PNNI Node ATM Address` dialog box is displayed.
5. Enter a 22-byte `PNNI Node ID` in hexadecimal and `Interface ID` identifying other vendor equipment. The `Interface ID` is optional.
6. After defining non-Lucent nodes, click `Lucent Node` to define the next hop to a Lucent switch.
7. Enter the `Internal IP Address` of the next Lucent switch node and optional `Logical Port Interface ID`.  
  
Navis EMS-CBGX adds the path to the `Defined Path` section when the path is complete.
8. Choose `OK` when you have defined the path.
9. In the `Path` tab, enable or disable the `Use Defined Path` option to specify whether to use the defined path or to enable the network routing to specify the circuit path respectively.
  - `Enable` – Routes the circuit based on the manually defined route.
  - `Disabled` – Routes the circuit based on the OSPF algorithm of the network.
10. Enable or disable the `Alternate Path` option to specify whether OSPF should route the circuit path if the manual route fails.
  - `Enable` – Routes the circuit based on the best available path if the manually defined path fails.
  - `Disable` – Prevents the circuit from being rerouted; the circuit remains down until the defined path is available.
11. In the `Add OffNet Circuit` dialog box, choose `OK` to add or modify the circuit when your configuration is complete.

## FRF.5 Attributes

The FRF.5 tab of the Add/Modify OffNet Circuit dialog box is explained.

1. Select the `FRF.5` tab from the `Add OffNet Circuit` dialog box to set the FRF.5 parameters if this offnet circuit is an FRF.5 circuit (Figure 8-9). These fields are only applicable when the originating endpoint is on a Frame Relay logical port on either a CBX 500 or CBX 3500.



**Figure 8-9. Add OffNet Circuit: FRF.5 Tab**

2. Complete the FRF.5 tab fields in the `Add OffNet Circuit` dialog box as described in Table 8-9.

**Table 8-9. Add OffNet Circuit: FRF.5 Tab**

Field	Action/Description
FRF.5 Over PNNI	Select this option to enable the FRF.5 over PNNI capability.
Call Initiator	Select this option to enable this endpoint as the call initiator. Disable this option (default) to configure this endpoint as the call recipient.  If Call Initiator is enabled, Target Select Type must be Specified.
LMI Profile ID	If the FRF.5 Over PNNI option is enabled, select 1 or 0 (zero) for LMI Profile ID. The default is zero. Selecting 1 will signify this is an FRF.5 circuit.  <b>Note:</b> This LMI Profile ID must match the Terminating Endpoint LMI Profile ID.

**Table 8-9. Add OffNet Circuit: FRF.5 Tab**

Field	Action/Description
NNI DLCI	<p>If you enabled <code>LMI profile ID</code>, you <i>must</i> specify the <code>NNI DLCI</code> for the offnet circuit. The <code>NNI DLCI</code> can differ from the <code>DLCI</code> configured at the <code>UNI</code> port. The <code>LMI</code> that the <code>NNI</code> runs will use the <code>NNI DLCI</code> to identify the network interworking <code>PVC</code>.</p> <p>Enter an <code>NNI DLCI</code> value in the range 16 to 991 or 1022.</p> <p><b>Note:</b> <i>This NNI DLCI number must match the Terminating Endpoint NNI DLCI number.</i></p> <p><i>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.</i></p>



---

**Note** – If enabled, the Reliable Scalable Circuit feature verifies the card state of each Offnet `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.

---

## Restarting an OffNet Circuit

An offnet circuit can be restarted from the Navis EMS-CBGX switch navigation panel. Restarting an offnet circuit is useful when connecting with a new route and/or path. The circuit must be in a managed state for the Restart option to be available.

To restart an offnet circuit, perform the following tasks:

1. In the Navigational Panel, expand the `Circuits` node.
2. Expand the `OffNet Circuits` class node.
3. Right-click the `OffNet Circuit` you wish to restart and then select `Restart` from the pop-up menu.

The `Restart` option will only be available if the circuit is in a managed state.

4. Choose `Yes` to continue with the `Restart`.

The `Admin Down` and `Admin Up` commands are sent to the selected offnet circuit.



# Configuring Ethernet Virtual Circuits (EVCs)

This chapter explains how to define an Ethernet Virtual Circuit (EVC) between Frame Relay and Gigabit Ethernet modules for use on the CBX 3500 switch input and output modules (IOMs). The 2-Port ULC Gigabit Ethernet module supports service interworking connections through EVCs between the following endpoints over ATM or MPLS core:

- Ethernet to Ethernet
- Ethernet to ATM
- Ethernet to Frame

These endpoints may be accessed by right-clicking the PVCs class node and selecting Add from the pop-up menu, or by right-clicking the EVC instance node and selecting Modify or View from the pop-up menu.



---

**Note** – Refer to the *IP Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000* for details on configuring the 2-Port Gigabit Ethernet module, configuring Shapers and VLANs.

---

This chapter contains:

- [“Prerequisites” on page 9-2](#)
- [“Adding or Modifying EVCs” on page 9-2](#)

## Prerequisites

Before you begin, make sure that you have:

- Set the card attributes of the 2-Port Gigabit Ethernet module.
- Defined the physical ports on which the logical ports will reside.
- Read the following guides:
  - *The Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information about card attributes and defining the physical ports.
  - *The IP Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for details on configuring the 2-Port Gigabit Ethernet module, configuring Shapers and VLANs.

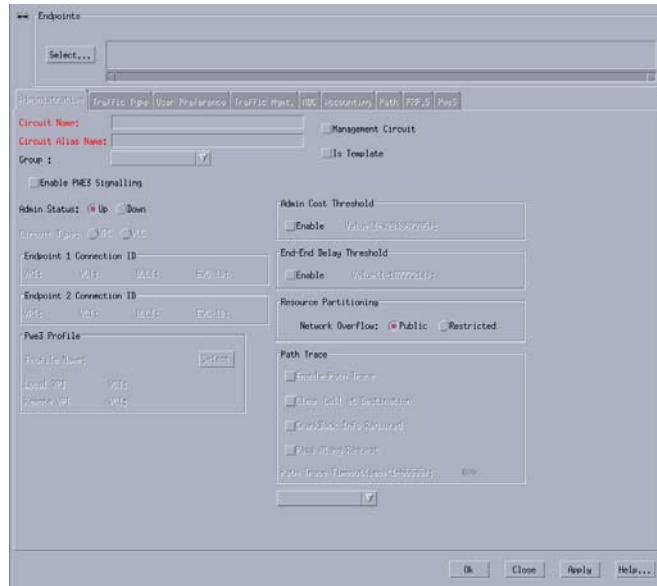
## Adding or Modifying EVCs

This section explains how to define or modify an EVC between Frame Relay and Gigabit Ethernet connection on the 2-Port ULC Gigabit Ethernet module.

To add or modify an EVC, perform the following tasks:

1. In the Navigation Panel, expand the instance node for the module.
2. Expand the `PPorts` node.
3. Expand the instance node for the PPort from which you want to select an LPort.
4. Expand the `LPorts` node.
5. Expand the instance node for the selected LPort. The following objects are displayed:
  - Circuits
  - Shapers
  - VLAN
  - Monitor
6. Expand the `Circuits` node. The following objects are displayed:
  - PVCs
  - Redirect PVCs
  - Offnet Circuits
7. Expand the `PVCs` node. The PVCs instance nodes are displayed.

8. Right-click the PVCs node and then select Add from the pop-up menu, or right-click the EVC instance node and then select Modify from the pop-up menu. The Add or Modify PVC dialog box is displayed (Figure 9-1).



**Figure 9-1. Add PVC Dialog Box**

For the 2-Port ULC Gigabit Ethernet module EVC, only the following tabs are active:

- Administrative
- Traffic Type
- User Preference
- Path

9. Select one endpoint as *Frame Relay* and the other endpoint as *Gigabit Ethernet* (Figure 9-2).

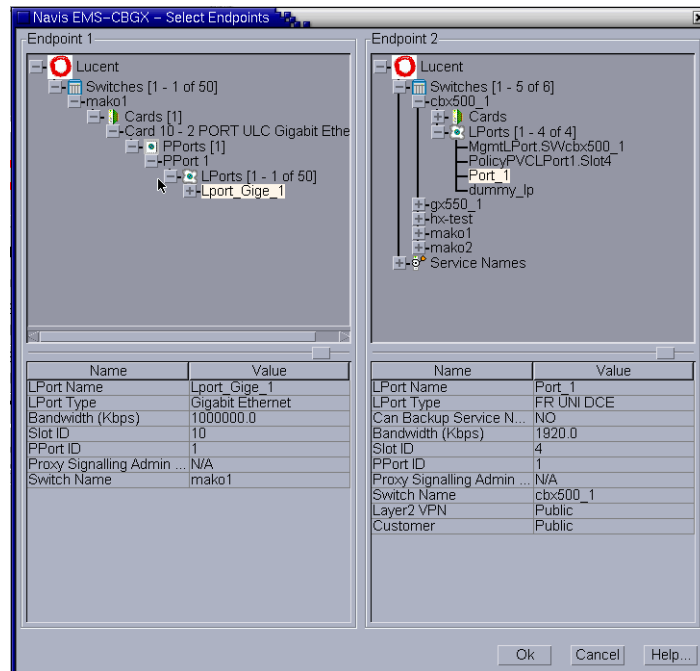


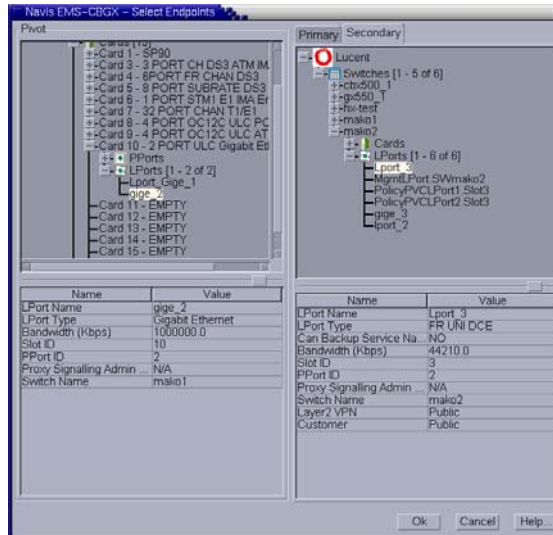
Figure 9-2. Select Endpoints Dialog Box



**Note** – Redirect PVCs and Offnet Circuits provisioning is similar to normal PVC (EVC) provisioning with the same attribute information described in “Adding or Modifying EVCs” on page 9-2. For selecting endpoints for Redirect PVCs and Offnet Circuits, see Figure 9-3 and Figure 9-4.

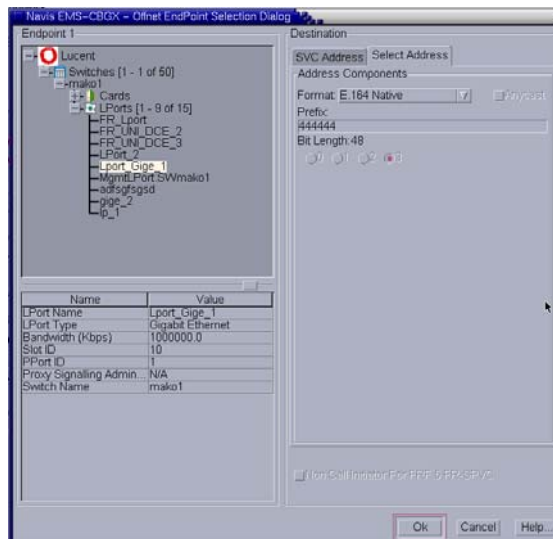
---

When defining Redirect PVC (with Pivot as Gigabit Ethernet, and Primary and Secondary as FR UNI DCE), the Select Endpoints dialog box is displayed as shown in **Figure 9-3**.



**Figure 9-3. Select Endpoints Dialog Box (for Redirect PVC)**

When defining an Offnet circuit between the originating endpoint as Gigabit Ethernet and the terminating endpoint (Destination Service Type as Frame), the Offnet Endpoint Selection Dialog box is displayed as shown in **Figure 9-4**.



**Figure 9-4. Offnet Endpoint Selection Dialog Box**

10. To configure PVC Circuit parameters, enter information in the following tabs, categorized by parameter type:
- “Administrative Attributes” on page 9-6
  - “Traffic Type Attributes” on page 9-11
  - “User Preference Attributes” on page 9-17
  - “Path Attributes” on page 9-20

## Administrative Attributes

The Administrative tab of the Add/Modify PVC dialog box is explained.

1. Select the Administrative tab (Figure 9-5).

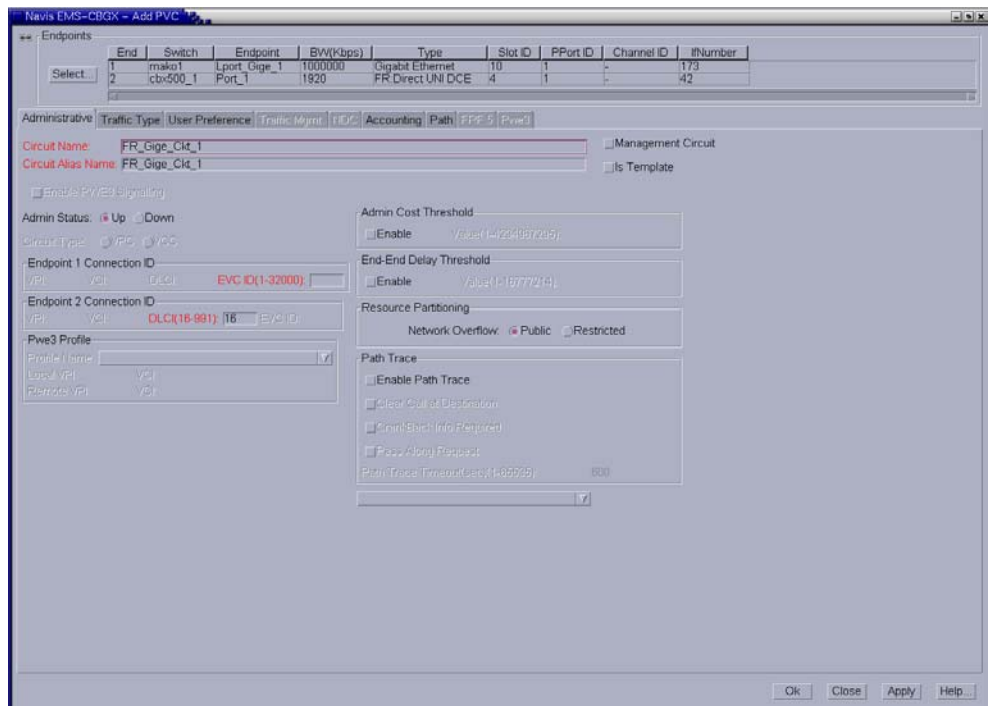


Figure 9-5. Add PVC: Administrative Tab

2. Complete the fields in the Administrative tab as described in [Table 9-1](#).



**Note** – Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for information on configuring a PWE3 circuit.

**Table 9-1. Add PVC: Administrative Tab**

Field	Action/Description
Circuit Name	Enter a 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	<p><i>(Optional)</i> Enter a unique, alphanumeric name to identify the redirect circuit. Do not use parentheses or asterisks. This name must be unique to the entire map. The default name is the circuit name.</p> <p>The service providers use the circuit name alias to identify the redirect circuit in a way that is meaningful to their customers.</p>
Group	<p>Select a group to which you want to associate EVC. EVC can belong to any group or to the BaseGroup.</p> <p>Refer to the <i>Navis EMS-CBGX Installation and Administration Guide</i> for a detailed information on group-wise resource partitioning.</p>
Admin Status	Select <i>Up</i> (default) to activate the circuit at switch startup, or select <i>Down</i> to take the circuit offline to run diagnostics such as PVC loopback.
Endpoint 1 and Endpoint 2 Connection IDs	<p>Endpoint 1 and endpoint 2 can either be Frame Relay and Gigabit Ethernet respectively, or Gigabit Ethernet and Frame Relay respectively.</p> <p>When one of the endpoints is <i>Frame Relay</i>, then enter a unique Data Link Connection Identifier (DLCI) in the range 16 to 991. When the link management protocol on the LPort is set to Local Management Interface (LMI) Rev1, use the range 16 to 1007. A DLCI is a 10-bit address that identified PVCs. The DLCIs identify the logical end points of a virtual circuit and only have local significance.</p> <p>When the other endpoint is <i>Gigabit Ethernet</i>, then enter an Ethernet Virtual Circuit (EVC) ID in the range 1 to 32000. An EVC ID identifies a circuit that is attached to a VLAN or multiple VLANs.</p>

**Table 9-1. Add PVC: Administrative Tab**

Field	Action/Description
Management Circuit	<p>Select Management Circuit to include this PVC configuration in the Network Management Station (NMS) initialization script file. This file contains all the Simple Network Management Protocol (SNMP) set requests necessary to replicate the entire switch configuration. After you download this file to the switch, this PVC can be used to establish NMS-to-switch connectivity.</p> <p><b>Note:</b> <i>This option is useful in a few management DLCI configurations.</i></p>
Is Template (Optional)	<p>(Optional) Enable this option to save these settings as a template to use again to configure another PVC with similar options.</p> <p><b>Note:</b> <i>You create templates for standard PVCs and redirect PVCs in the same way. However, the template lists for redirect and traditional PVCs are maintained separately.</i></p>
Admin Cost Threshold	<p>When 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 then enter a value of 1000, the PVC will not be routed over a path whose total administrative cost exceeds 1000.</p> <p>The total administrative cost for a path is calculated by adding the sums of the administrative cost for each trunk in the path. The valid range of values for this field is from 1 to 4294967295.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>Do not enable this option if you use End-End Delay routing.</i></p>
End-End Delay Threshold (cell transfer delay)	<p>When 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 then enter a value of 500 microseconds, the PVC will not be routed over a path whose total end-to-end delay exceeds 500 microseconds.</p> <p>The total end-to-end delay for a path is calculated by adding the sums of the end-to-end delay for each trunk in the path. The valid range for this field is from 0 to 16777214 microseconds.</p> <p>If the End-to-End Delay Threshold is disabled to the circuit, then the operational status window displays Unavailable in the delay field.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> <i>The value you enter should reflect your network topology. If a PVC will typically traverse high-speed trunks, then set the delay rate lower; increase the delay if the PVC must use low-speed trunks.</i></p>



**Table 9-1. Add PVC: Administrative Tab**

Field	Action/Description
<b>Resource Partitioning</b>	
Network Overflow	<p>Select one of the following Network Overflow options:</p> <ul style="list-style-type: none"> <li>• <i>Public</i> (default) - PVCs are routed over dedicated Layer2 VPN trunks. However, in the event of failure, the traffic of the customer is allowed to run over common trunks (shared by a variety of different customers).</li> <li>• <i>Restricted</i> – 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.</li> </ul> <p>Resource Partitioning determines how the PVC traffic is managed during trunk overflow or failure conditions. This feature is used with Virtual Private Networks (VPNs).</p>
Switchover Mode <i>(Redirect PVCs only)</i>	<p>Select one of the following configurations:</p> <ul style="list-style-type: none"> <li>• <i>Manual</i> – Enables you to switch the circuit connection between the pivot endpoint and the primary or secondary endpoint.</li> <li>• <i>Non-Revertive</i> – Triggers an automatic forward switchover to establish the connection between the pivot and secondary endpoints in case of primary endpoint failure. If the secondary endpoint goes down and the primary endpoint recovers, then no automatic switchover is triggered. The administrator must manually switch the circuit connection from the working secondary endpoint backward to the primary endpoint.</li> <li>• <i>Revertive</i> – Triggers an automatic forward switchover to establish the connection between the pivot and secondary endpoints in case of primary endpoint failure. If the primary endpoint recovers, then the backward switchover is triggered automatically to re-establish the connection between the pivot and primary endpoints.</li> </ul> <p>Enables you to configure redirect circuit traffic for endpoint 2 to primary or secondary when the DTE state of the primary or secondary endpoint fails.</p> <p><b>Note:</b> <i>To implement redirect PVC with Revertive mode, the entire network must be upgraded to the current network management and switch software release.</i></p>

**Table 9-1. Add PVC: Administrative Tab**

Field	Action/Description
<b>Path Trace</b>	
Enable Path Trace	Enable this option to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network. Path trace can track even failed connections and report all paths attempted.
CrankBack Info Required	Enable this option to instruct the switch to collect and maintain the crankback information, that is, information about dynamic rerouting of call setups around failed nodes or links (or links with insufficient resources) on the traced path. Disable this option if you do not want to collect crankback information.
Clear Call at Destination	<p>Enable or disable the removal of this circuit after the path trace is complete.</p> <p>Enable this option for the circuit to be deleted from the switch after the specified path trace timeout period. Path trace information for this circuit will also be made available for the timeout period. Disable this option for the circuit to remain (default).</p> <p>If this field is enabled, the circuit will not be created in the PRAM. Navis EMS-CBGX will create a temporary circuit. After the creation of this circuit, no modifications can be made to it.</p>
Pass Along Request	Enable this option to have the path trace continue through nodes that do not support the path trace feature. This may cause the trace results to contain some gaps between successive entries of logical nodes and logical ports traversed by this connection or party. Disable this option to cause the path trace to terminate at any switch that does not support the path trace feature. A partial path trace will be returned.
Path Trace Timeout	Enter the number of seconds in the range 1 to 65535 for which you want the trace results to be maintained in the switch. The default is ten minutes (600 seconds).
Enable Path Trace	Enable this option to view the paths for new and existing connections. You can use the path trace feature to track the logical ports and logical nodes that a hypothetical point-to-point circuit would traverse in a network. Path trace can track even failed connections and report all paths attempted.

## Traffic Type Attributes

The Traffic Type tab of the Add/Modify PVC dialog box is explained.

1. Select the Traffic Type tab (Figure 9-6).

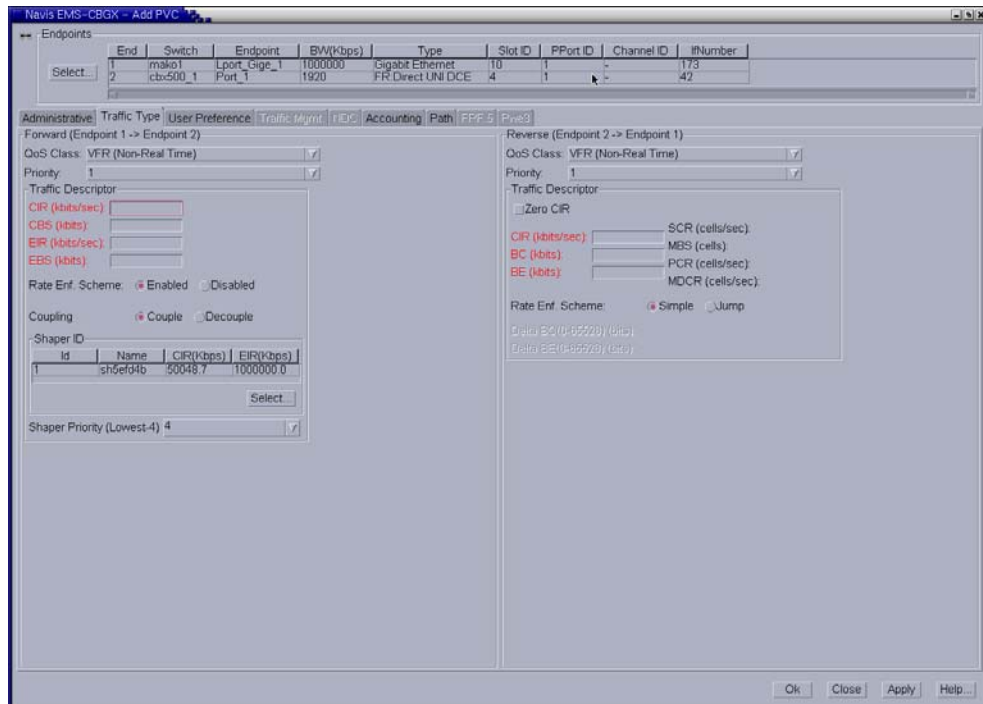


Figure 9-6. Add PVC: Traffic Type Tab

2. Forward traffic flows from Endpoint 1 to Endpoint 2, and reverse traffic flows from Endpoint 2 to Endpoint 1. Complete the Traffic Type fields as described in Table 9-2 to set traffic type attributes in each direction.

**Table 9-2. Add PVC: Traffic Type Tab**

Element	Description
<b>Forward (Endpoint 1 → Endpoint 2)</b>	
QoS Class	Select one of the following Gigabit Ethernet Quality of Service (QoS) classes: <ul style="list-style-type: none"> <li>• <i>VFR (Real Time)</i> – Variable Frame Rate (VFR) (Real Time) is used for special delay-sensitive applications that require low delay variation between the endpoints.</li> <li>• <i>VFR (Non-Real Time)</i> – Variable Frame Rate Non-Real Time (NRT) handles transfer of long, bursty data streams over a pre-established connection. This service provides low data loss but no delay guarantee. It is also used for short, bursty data such as LAN traffic. The Customer Premise Equipment (CPE) protocols adjust for any delay or loss incurred through the use of VFR-NRT.</li> <li>• <i>UFR</i> – Primarily, Unspecified Frame Rate (UFR) is used for Local Area Network (LAN) traffic. The CPE should compensate for any delay or frame loss.</li> </ul>
Priority	Select 1, 2, or 3 to configure the priority of data being transmitted on this circuit. The circuit priority determines the forward priority of the data. The highest priority is 1 (do not discard data); the lowest priority is 3 (discard data). The default priority for Frame Relay is 1.  <b>Note:</b> <i>To configure the priority of transmitted data for a standard or redirect management PVC (MPVC) select 1, 2, or 3. The default priority is 1.</i>
<b>Traffic Descriptor</b>	
CIR	Enter the Committed Information Rate (CIR) in Kbps at which the network transfers data under normal conditions. The normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc). The value on each PVC is asymmetric (you can set a different CIR in each direction), which provides more efficient use of bandwidth.

**Table 9-2. Add PVC: Traffic Type Tab**

Element	Description
CBS	Enter the maximum Committed Burst Size (CBS) in Kbits at which the network agrees to transfer, under normal conditions, during a time interval Tc.  <b>Note:</b> <i>If CIR is 0 (zero), then CBS is 0 (zero). If CIR is non-zero, then CBS is non-zero.</i>
EIR	Enter the Excess Information Rate (EIR) in Kbps.
EBS	Enter the maximum Excess Burst Size (EBS) in Kbits.  <b>Note:</b> <i>EIR is greater than or equal to CIR. If EIR is 0 (zero), then EBS is 0 (zero). If EIR is non-zero, then EBS is non-zero.</i>
Rate Enf. Scheme	Select <i>Enabled</i> (default) to support the <i>Jump</i> scheme, or select <i>Disabled</i> . The configurable rate enforcement scheme provides additional flexibility, increased rate enforcement accuracy, and improved switch performance.  <b>Note:</b> <i>The Jump scheme is supported only on Ethernet Ingress point for Ethernet Virtual Circuit (EVC). The Simple scheme is not supported.</i>
Coupling	Select <i>Couple</i> (default) to couple the CIR and EIR tokens for allowing frames that are non-conformant to individual Token Bucket Rate Enforcement Algorithm (TBRA) buckets, or select <i>Decouple</i> .
Shaper ID	Select shaper configured on the LPort. A default shaper is created automatically.
Shaper Priority (Lowest-4)	Select Egress shaper priority of the EVC.

**Table 9-2. Add PVC: Traffic Type Tab**

Element	Description
<b>Reverse (Endpoint 2 → Endpoint 1)</b>	
QoS Class	<p>Select one of the following Frame Relay Quality of Service (QoS) classes:</p> <ul style="list-style-type: none"> <li>• <i>VFR (Real Time)</i> – Variable Frame Rate (VFR) (Real Time) is used for special delay-sensitive applications that require low delay variation between the endpoints.</li> <li>• <i>VFR (Non-Real Time)</i> – Variable Frame Rate Non-Real Time (NRT) handles transfer of long, bursty data streams over a pre-established connection. This service provides low data loss but no delay guarantee. It is also used for short, bursty data such as LAN traffic. The Customer Premise Equipment (CPE) protocols adjust for any delay or loss incurred through the use of VFR-NRT.</li> <li>• <i>UFR</i> – Primarily, Unspecified Frame Rate (UFR) is used for Local Area Network (LAN) traffic. The CPE should compensate for any delay or frame loss.</li> </ul>
Priority	<p>Select 1, 2, or 3 to configure the priority of data being transmitted on this circuit. The circuit priority determines the forward priority of the data. The highest priority is 1 (do not discard data); the lowest priority is 3 (discard data). The default priority for Frame Relay is 1.</p> <p><b>Note:</b> <i>To configure the priority of transmitted data for a standard or redirect management PVC (MPVC) select 1, 2, or 3. The default priority is 1.</i></p>
<b>Traffic Descriptor</b>	
Zero CIR	<p>Enable this option to indicate that the PVC has an assigned CIR value of zero, and it is a best-effort delivery service. The customer data that is subscribed to zero CIR service can burst to the port speed if there is network bandwidth available to deliver frames. However, no frame-delivery guarantees are made. All frames entering the network on zero CIR PVCs have DE set to one (1).</p> <p><b>Note:</b> <i>If you set Zero CIR Enabled to On, then you cannot set the CIR, Bc, and Be values.</i></p>

**Table 9-2. Add PVC: Traffic Type Tab**

Element	Description
CIR	Enter the Committed Information Rate (CIR) in Kbps at which the network transfers data under normal conditions. The normal conditions refer to a properly designed network with ample bandwidth and switch capacity. The rate is averaged over a minimum increment of the Committed Rate Measurement interval (Tc). The value on each PVC is asymmetric (you can set a different CIR in each direction), which provides more efficient use of bandwidth.
BC	Enter the maximum amount of data (Committed Bit size), in Kbits, that the network attempts to transfer under normal conditions during a specified time interval, Tc. Tc is calculated as Bc/CIR. This value must be greater than zero and is typically set to the same value as CIR.
BE	Enter the maximum amount of uncommitted data (Excess Bit), in Kbits, the network will attempt to deliver during a specified time interval, Tc. Tc is calculated as Bc/CIR. The network treats this data as Discard Eligible (DE) data.
SCR	<i>(Read-only)</i> Displays the sustainable cell rate (SCR) in cells per second for the Frame Relay endpoint.
MBS	<i>(Read-only)</i> Displays the maximum burst size (MBS) in cells for the Frame Relay endpoint.
PCR	<i>(Read-only)</i> Displays the peak cell rate (PCR) in cells per second for the Frame Relay endpoint.
Delta BC (0-65528) (bits)	Set the number of Delta BC (Committed Bit) bits for this circuit in the range 0 to 65528. The default value is 65528. This value is the maximum number of bits the network agrees to transfer over the circuit (as committed bits) during the measurement interval, provided there is positive Bc credits before receiving the frame, but negative Bc credits after accepting the frame.

**Table 9-2. Add PVC: Traffic Type Tab**

Element	Description
Delta BE (0-65528) (bits)	<p>Set the number of Delta BE (Excess Bit) bits for this circuit in the range 0 to 65528. The default value is 65528.</p> <p>This value is the maximum number of bits the network agrees to transfer over the circuit (as excess bits) during the measurement interval, provided there is positive excess bit (Be) credits before receiving the frame, but negative Be credits after accepting the frame.</p>
Rate Enf. Scheme	<p>Select <i>Simple</i> (default) or <i>Jump</i>. The configurable rate enforcement scheme provides additional flexibility, increased rate enforcement accuracy, and improved switch performance.</p> <p><b>Note:</b> <i>Simple</i> indicates time (<math>T_c</math>) as measured in periodic intervals. If you select the <i>Simple</i> scheme, then the “bad” PVC detection feature is disabled.</p>



## User Preference Attributes

The User Preference tab of the Add/Modify PVC dialog box is explained.

1. Select the User Preference tab (Figure 9-7).

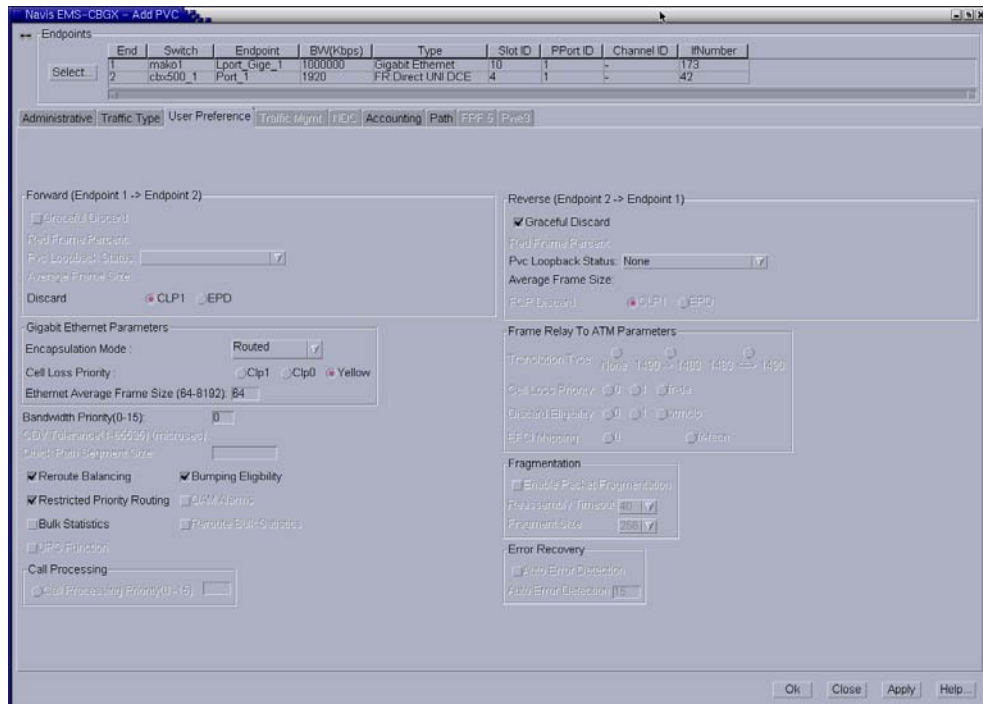


Figure 9-7. Add PVC: User Preference Tab

2. Complete the fields in the User Preference tab, as described in Table 9-3.

**Table 9-3. Add PVC: User Preference Tab**

Element	Description
<b>Forward (Endpoint 1 → Endpoint 2)</b>	
FCP Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>CLP1</i> (default) - Selective CLP1 discard is provisioned for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate (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, then the cell is discarded. <b>Note:</b> <i>Early Packet Discard (EPD)</i> is not performed in this case.</li> <li>• <i>EPD</i> - ATM Flow-control Processor (FCP) can perform EPD for UBR, ABR, and VBR-BRT PVCs. If this option is selected, then 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 the cells in the next packet are discarded for that PVC.</li> </ul> <p>FCP Discard is displayed when you select a QoS class that supports FCP Discard.</p>
<b>Gigabit Ethernet Parameters</b>	
Encapsulation Mode	Select <i>Routed</i> (default) or <i>Bridged</i> to determine the encapsulated format in which the Ethernet Virtual Circuit (EVC) passes data.
Cell Loss Priority	Select one of the following options: <i>Clp0</i> , <i>Clp1</i> , or <i>Yellow</i> (default) to set the Cell Loss Priority (CLP). When the Ethernet frames are segmented into ATM cells on Gigabit Ethernet Universal Line Card (ULC), the CLP bit in each cell is set based on this configuration of the EVC.
Ethernet Average Frame Size (64-8192)	<p>Enter a value in the range 64 to 8192 bytes for Ethernet average frame size. The default value is 64 bytes.</p> <p>Ethernet Average Frame Size is used to calculate the Interworking Overhead (IOH) factor for the Traffic parameters conversion.</p> <p><b>Note:</b> <i>This is applicable for Ethernet endpoint only.</i></p>

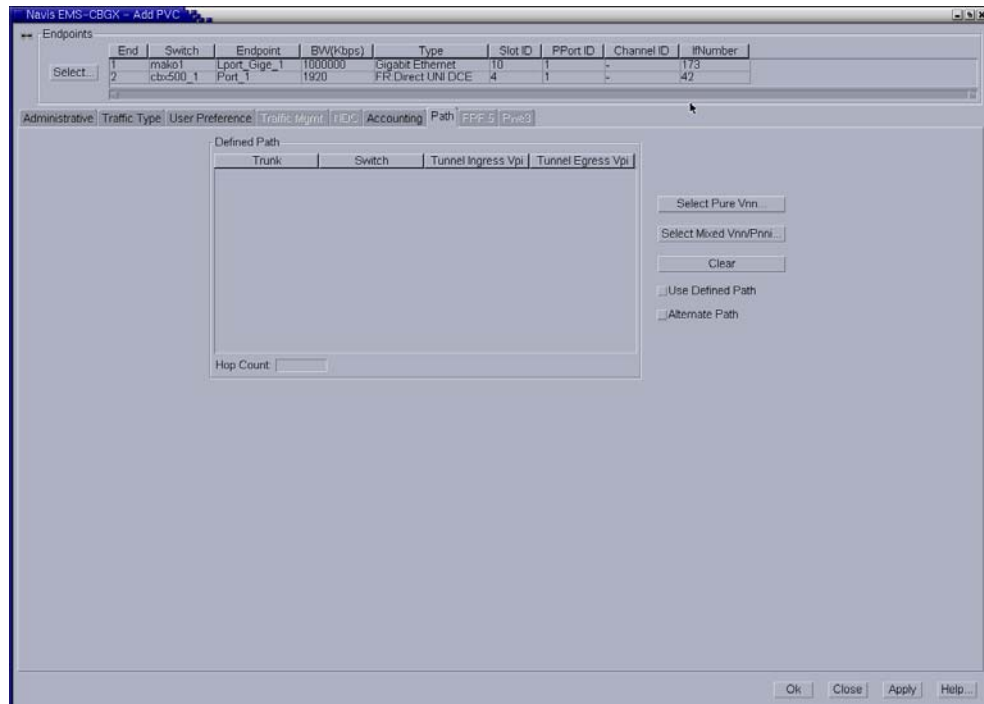
**Table 9-3. Add PVC: User Preference Tab**

Element	Description
Reroute Balancing	Select <i>Selected</i> (default) to reroute the Call for an optimal path in case of Current PVCs or SPVCs, or select <i>Non-Selected</i> .
Bulk Statistics	Enable this option to facilitate Bulk Statistics at the circuit level.
<b>Reverse (Endpoint 2 → Endpoint 1)</b>	
Graceful Discard	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Selected</i> (default) - Forwards a few red packets if there is no congestion.</li> <li>• <i>Non-Selected</i> - Immediately discards the red packets.</li> </ul> <p>Graceful Discard defines how the circuit handles “red” packets. The 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 <i>Selected</i>.</p>
PVC Loopback Status	<p>Select one of the following to display the current loopback status: <i>None</i>, <i>Local</i>, <i>Remote</i>, or <i>Both</i>.</p> <p><b>Note:</b> <i>You can modify this circuit only if None is displayed.</i></p>

## Path Attributes

The Path tab of the Add/Modify PVC dialog box is explained.

1. Select the Path tab (Figure 9-8).



**Figure 9-8. Add PVC: Path Tab**

The Path tab in the Add or Modify PVC dialog box enables you to manually define a circuit path and the OSPF algorithm's circuit routing decisions.

2. In the Add or Modify PVC dialog box, choose OK to save the PVC configuration



**Note** – For Redirect EVCs, the Path tab is *not* applicable.

---

# Configuring Layer2 Virtual Private Networks (VPNs)

This chapter describes how to configure a Layer2 Virtual Private Network (VPN) and how to configure a logical port and PVC for a Layer2 VPN. A Layer2 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 (ASR) or Customer Specific Routes (CSR).

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 stay with you as the network provider.



---

**Note** – Layer2 VPNs support the ATM Private Network-to-Network Interface (PNNI) routing protocol on CBX 500 and GX 550 switches. For information on configuring Layer2 VPNs for PNNI links, refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDx 9000*.

---

This chapter contains:

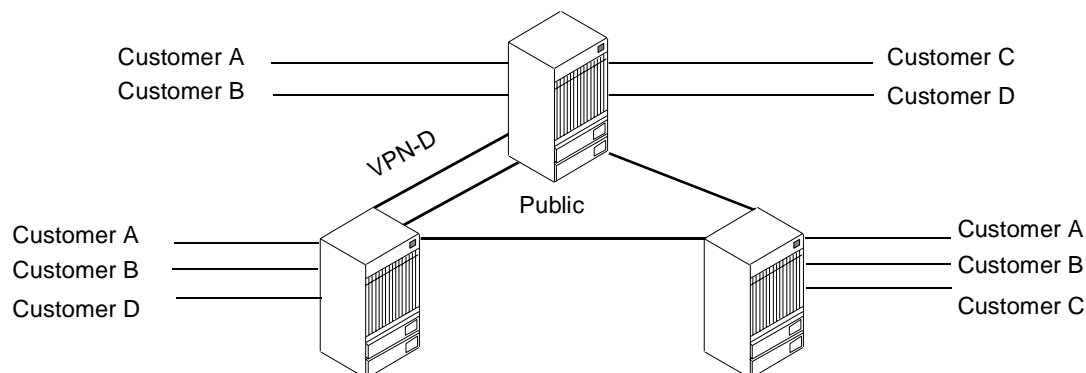
- “About Layer2 VPNs” on page 10-2
- “Configuring a Layer2 VPN” on page 10-3
- “Using the Layer2 VPN/Customer View Feature” on page 10-8
- “Configuring a PVC for Layer2 VPN” on page 10-9

## About Layer2 VPNs

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 specific VPN/customer associations. In addition, you need to dedicate selected public network trunks to specific VPNs.

You must configure all PVCs that you create on 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 10-1](#) provides a restrictive mode example.



- Action** Create VPN-D and associate Customer D.  
Configure PVC for VPN-D and Private Net Overflow to Restrict.
- Action** Under ALL conditions, PVC will use only trunk(s) assigned to VPN-D.  
During overflow or trunk failure, public trunks will not be used.  
In this example, if VPN-D fails, the PVC will fail until the trunk comes back up.

**Figure 10-1. 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 10-2](#)). 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.

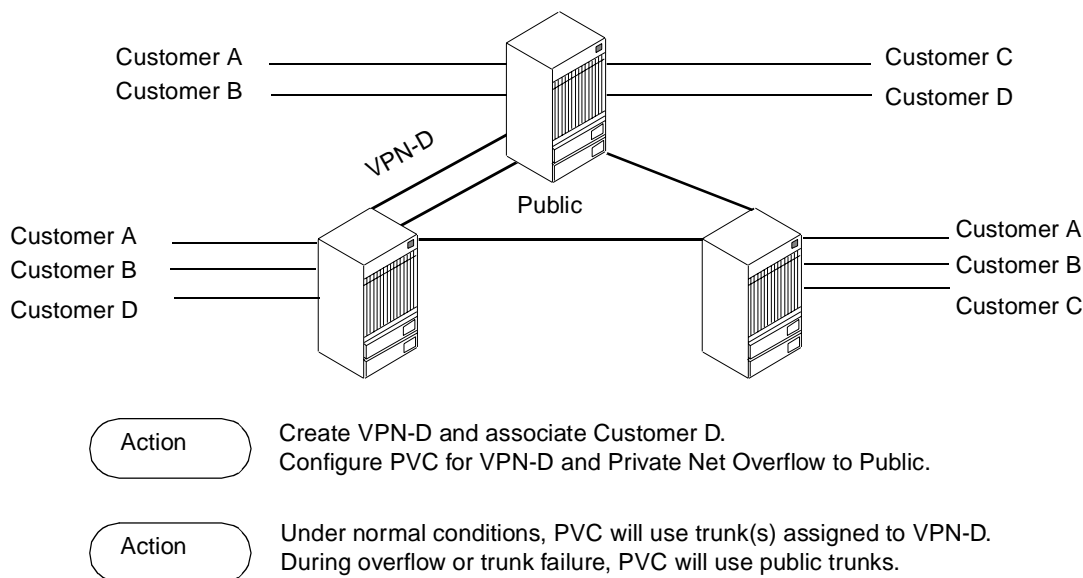


Figure 10-2. Layer2 VPN Inclusive Mode Example

## Configuring a Layer2 VPN

Use the following sequence to set up a Layer2 VPN:

1. Create the Layer2 VPN ([“Creating a Layer2 VPN”](#) on page 10-4).
2. Add customers to a specific Layer2 VPN ([“Adding Customers to a Layer2 VPN”](#) on page 10-5).
3. Dedicate a trunk to a specific Layer2 VPN (refer to [“Adding a Trunk”](#) on page 4-7).
4. For SVC traffic, when you configure the UNI or NNI logical port, specify the Network Overflow attribute (see [“General Attributes for SVCs”](#) on page 3-43). Then, dedicate this logical port to a specific VPN and customer (see [“Assigning Logical Ports to a Layer2 VPN”](#) on page 10-6).
5. Enable a network map view for a specific Layer2 VPN or customer to view logical ports (see [“Using the Layer2 VPN/Customer View Feature”](#) on page 10-8).

6. For PVC traffic, specify the Network Overflow attribute for the circuit (“Administrative Attributes for PVCs” on page 7-14). Then, dedicate the circuit to a specific VPN and customer (“Configuring a PVC for Layer2 VPN” on page 10-9).

## Creating a Layer2 VPN

To create a Layer2 VPN and add customers to this network:

1. In the Networks tab, expand the network you want to work with.
2. Expand the VPNs node.
3. Right-click on the VPNs node and click Add on the popup menu, as shown in Figure 10-3.

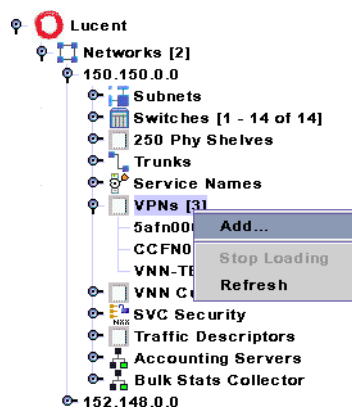


Figure 10-3. Adding a VPN



The Add VPN dialog box (Figure 10-4) is displayed.

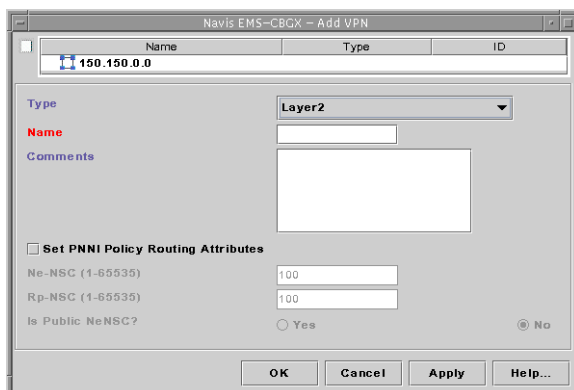


Figure 10-4. Add VPN Dialog Box

4. Set the Type to Layer2.
5. Enter a Name for this VPN and add any additional Comments.
6. Click OK.

## Adding Customers to a Layer2 VPN

To add customers to the Layer2 VPN:

1. In the Networks tab, expand the network you want to work with.
2. Expand the VNN Customers node.
3. Right-click on the VNN Customers node and click Add on the popup menu, as shown in Figure 10-3.

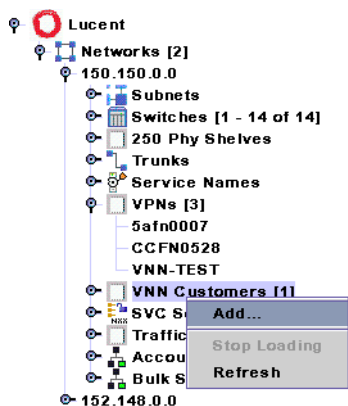
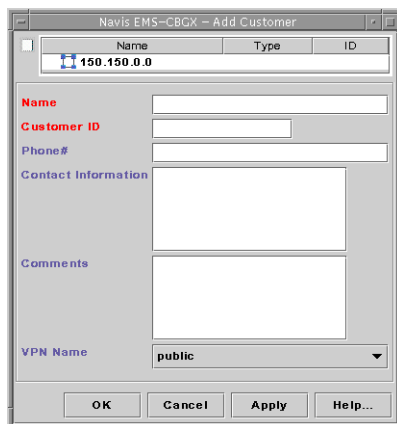


Figure 10-5. Adding a VNN Customer

The Add Customer dialog box (Figure 10-6) is displayed.



**Figure 10-6. Add Customer Dialog Box**

4. Enter a customer name.
5. Assign a value from 1 to 65535 for the Customer ID.
6. (Optional) Enter the phone number, contact name, and any additional comments.
7. Select the Name of the VPN to which this customer belongs.
8. Click OK.

## Assigning Logical Ports to a Layer2 VPN

To implement a Layer2 VPN for a network that contains SVCs, specify the Net Overflow attribute when you configure a UNI logical port (Table 3-4 on page 3-16). 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.

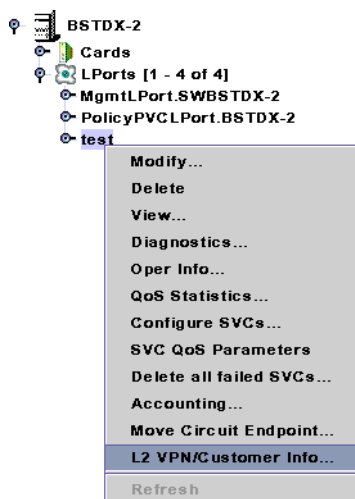


**Note** – Changing the Customer Name does not admin down the logical port.

---

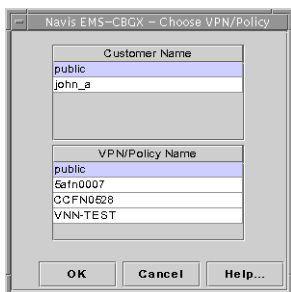
After configuring a logical port, dedicate it to a Layer2 VPN as follows:

1. In the Switch tab, expand the LPorts node and right-click on the logical port you want to assign.
2. Click L2 VPN / Customer Info on the popup menu, as shown in [Figure 10-7](#).



**Figure 10-7. Assigning a Logical Port to a Layer 2 VPN / Customer Name**

The Choose VPN / Policy dialog box ([Figure 10-8](#)) is displayed.



**Figure 10-8. Choose VPN / Policy Dialog Box**

3. From the list of customer names, select the name you want to assign to this LPort.
4. From the list of VPN/Policy names, select the name you want to assign to this LPort.
5. Click OK.

## 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 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 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 PVC for Layer2 VPN” on page 10-9](#) to assign the port to a VPN or customer.

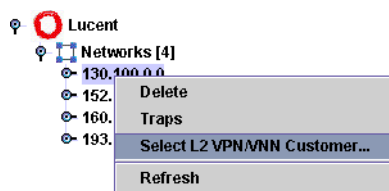


**Note** – To give a customer the ability to monitor network resources without the ability to provision, we recommend creating a new Navis EMS-CBGX user with View only privileges for all objects.

---

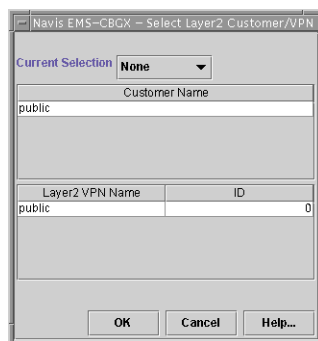
To use Layer2 VPN/Customer View:

1. In the Networks tab, right-click on the network, and click Select L2 VPN/VNN Customer, as shown in [Figure 10-9](#)



**Figure 10-9.** Selecting the L2 VPN/VNN Customer for a Network

The Select Layer2 Customer/VPN View dialog box ([Figure 10-10](#)) is displayed.



**Figure 10-10.** Select Layer2 Customer/VPN View Dialog Box

2. Use the Current Selection list box to select one of the following options:
  - Customer
  - Layer2 VPN
  - None – (default) Disables Layer2 VPN/Customer View. (With the Layer2 VPN/Customer 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 Customer name or Layer2 VPN name.
5. Choose OK.

## Configuring a PVC for Layer2 VPN

When you configure a PVC for VNN VPN, first specify the Private Net Overflow attribute (see “[Administrative Attributes for PVCs](#)” on page 7-14). This parameter determines whether this 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. In the Switch tab, expand the Circuits node.
2. Expand the PVCs node.
3. Right-click on the PVC you want to assign.
4. Click L2 VPN / Customer Info on the popup menu, as shown in [Figure 10-11](#).

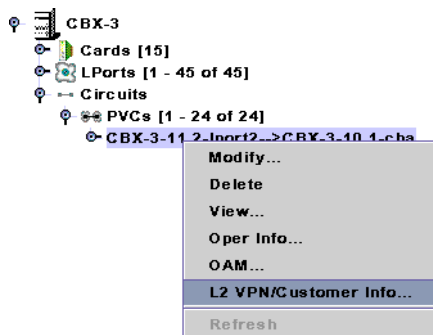
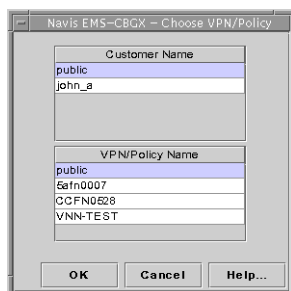


Figure 10-11. Assigning a Logical Port to a Layer 2 VPN / Customer Name

The Choose VPN / Policy dialog box (**Figure 10-12**) is displayed.



**Figure 10-12. Choose VPN / Policy Dialog Box**

5. From the list of customer names, select the name you want to assign to this PVC.
6. From the list of VPN/Policy names, select the name you want to assign to this PVC.
7. Click OK.

# Configuring Management Paths

This chapter describes how to configure a management path between the network management station (NMS) and IP host that you use to access the switch network, either for configuration or Telnet purposes. The management path 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 network management station. The management path configuration is node-specific and describes each management station that attaches via the switch. You can use the same procedure to establish communication between the switch and any IP host, such as the NavisXtend Accounting Server.

This chapter contains:

- [“Overview” on page 11-1](#)
- [“Using Management PVCs” on page 11-2](#)
- [“Using Management DLCIs” on page 11-7](#)
- [“Defining the Management Path” on page 11-9](#)

## Overview

The management path options described in this chapter are available when the NMS or IP host connects to the switch via a router or network interface card (NIC). You only need to define a management 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 MPVC is an actual PVC between the UNI or NNI logical port (to which the NMS or IP host connects) and the remote switch processor module, the switch that connects the NMS or IP host is not burdened by the traffic traversing the MPVC.

You can also use a *redirect* MPVC to create a management path for a connection that has *three* endpoints: pivot, primary, and secondary.

See [“Using Management PVCs” on page 11-2](#).

- **Management DLCI** — You can use this type of connection when the NMS or IP host connects to a LAN through a router that provides the Frame Relay connection to the switch. (The switch does not need an Ethernet module for this type of NMS connection.) Network traffic is sent through the attached Frame Relay UNI-DCE connector as a PVC. This type of connection also enables you to move the NMS from one LAN to another with few reconfiguration requirements.

See “Using Management DLCIs” on page 11-7.



**Note** – Management data link connection identifiers (DLCIs) are not supported on CBX 500 switches. You can use management PVCs instead.

---

## Using Management PVCs

A management PVC (MPVC) provides an access point to the switching network’s management plane (which is IP-based). Management PVCs offer an efficient, high-performance data path capable of transferring large amounts of management data, such as NavisXtend Accounting Server or Statistics Server files. This feature is available on B-STDx and CBX switch platforms.

Management PVCs provide better performance than management DLCIs for transferring large amounts of data. Unlike DLCIs, MPVCs do not require that management traffic be processed by the background IP application at each switch on the path to the endpoint. For more information about DLCIs, see “Using Management DLCIs” on page 11-7.

Management PVCs originate at the switch input/output (I/O) interface. On the B-STDx, this interface is referred to as the input/output processor (IOP), and on the CBX, this interface is referred to as the input/output module (IOM). They terminate at an internal logical port located on the switch processor module. This processor module is referred to as the control processor (CP) on the B-STDx and as the switch processor (SP) on the CBX. Management PVCs 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 MgmtLPort.SW<switchname> endpoint to any Frame or ATM logical port for interworking MPVC. You can configure MPVCs across different switch platforms (for example, B-STDx 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 control processor (CP).

---



Management PVCs enable you to configure a management path to an autonomous system external (ASE). After you define the management path, the IP process on the switch processor module can send and receive IP packets over the MPVC to and from the ASE. Note that IP packets are encapsulated within Frame Relay frames according to RFC 1490. 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. Refer to the *Getting Started User's Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for information about downloading the initialization script file.

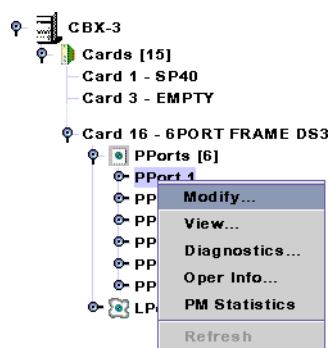
The following sections describe how to configure an Management Path using a standard or redirect MPVC. As part of this process, you need to first configure an unused physical port for which you can then define, in this example, a Frame Relay UNI logical port.

- “Defining Physical Port Attributes” on page 11-3
- “Defining a Frame Relay UNI Logical Port” on page 11-4
- “Defining a Standard or Redirect MPVC Connection” on page 11-5

## Defining Physical Port Attributes

To configure the physical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port you want to configure.
2. Expand the PPorts node.
3. Right-click on the physical port and select Modify from the popup menu, as shown in **Figure 11-1**.



**Figure 11-1. Modifying a Physical Port**

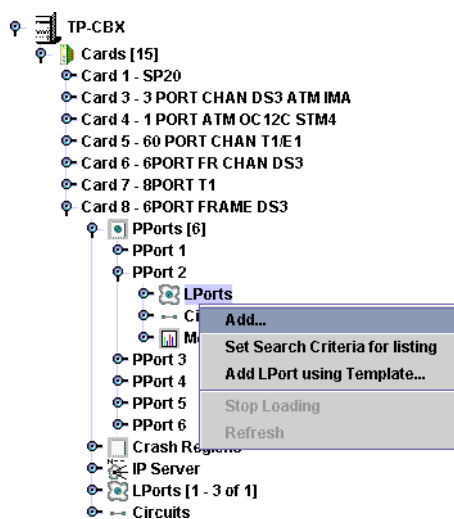
The Modify PPort dialog box is displayed.

4. Complete the dialog box fields. Refer to the *Switch Module Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* if you need information about changing default values.

## Defining a Frame Relay UNI Logical Port

To define a Frame Relay UNI logical port:

1. In the Switch tab, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which you want to configure a logical port.
2. Expand the PPorts node, and expand the node for the physical port.
3. Under the node for the physical port, right-click on the LPorts node and select Add from the popup menu, as shown in [Figure 11-2](#).



**Figure 11-2. Adding Logical Ports**

The Add Logical Port dialog box is displayed.

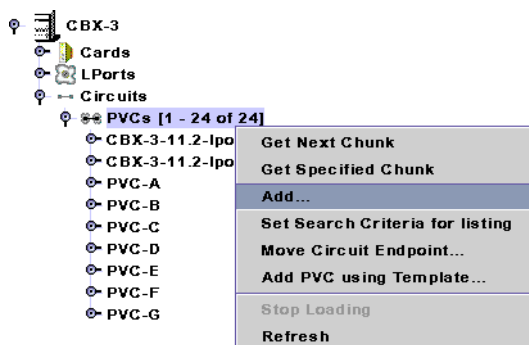
4. Use the instructions in [“Adding a Frame Relay LPort” on page 3-5](#) to set the Administrative Attributes, including the Redirect PVC Delay Timer attribute.
5. Click OK to configure the logical port.
6. To define a standard MPVC connection, use the instructions in the next section. To define a redirect MPVC, use the instructions in [“Defining a Standard or Redirect MPVC Connection” on page 11-5](#).

## Defining a Standard or Redirect MPVC Connection

To define a standard or redirect MPVC connection:

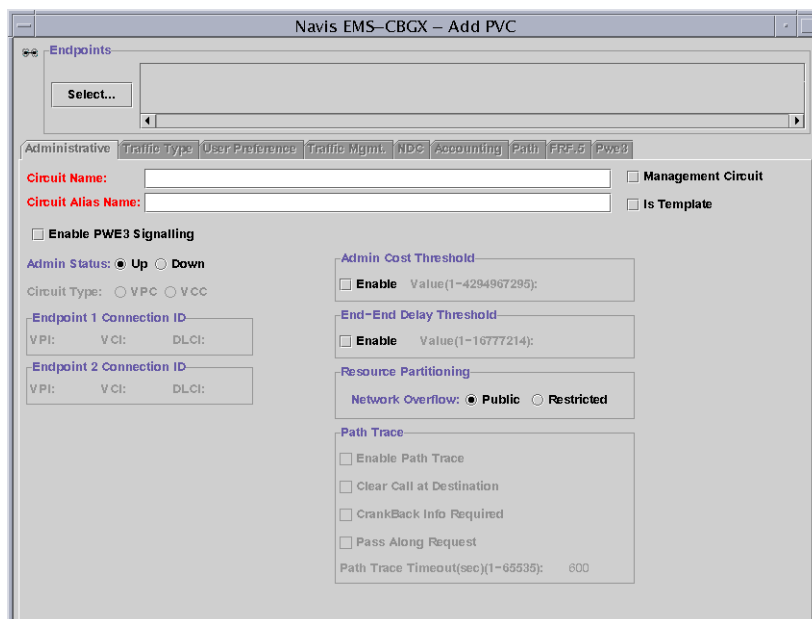
1. In the Switch tab, expand the Circuits node.
2. To define a standard MPVC connection, right-click on the PVCs node and click Add on the popup menu, as shown in [Figure 11-3](#).

If you want define a redirect MPVC connection, right-click on the Redirect PVCs node and click Add on the popup menu.



**Figure 11-3. Right-Clicking on the PVCs Node**

The Add PVC ([Figure 11-4](#)) or Add Redirect PVC dialog box is displayed.



**Figure 11-4. Add PVC Dialog Box**

3. Click on the Select button to define the circuit endpoints.

The Select Endpoints dialog box (Figure 11-5) is displayed.

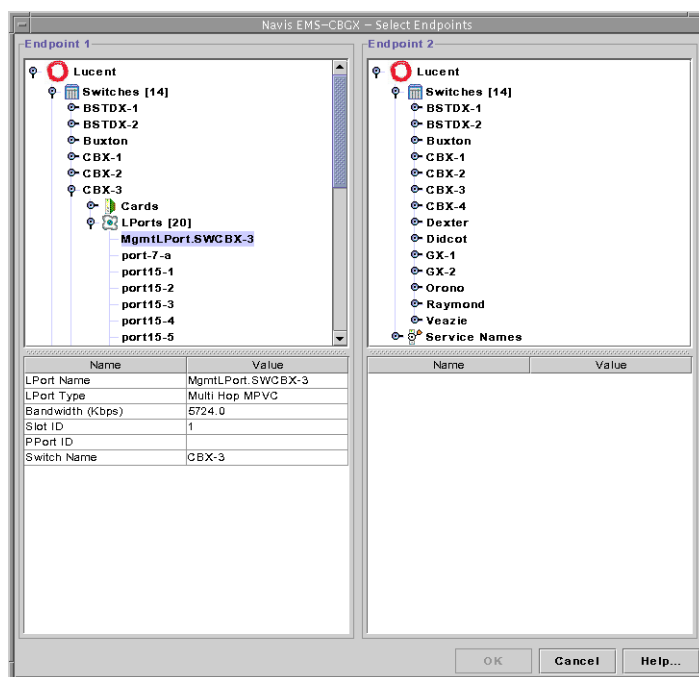


Figure 11-5. Select Endpoints Dialog Box

4. Select the name of the switch that you want to manage (where the management port [Endpoint 1] resides).
5. 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 Multi Hop MPVC.
6. Select the name of the switch and logical port where Endpoint 2 resides.  
If you are defining a redirect MPVC connection, you need to define both primary and secondary endpoints.
7. Choose OK.
8. In the Add PVC dialog box, enter a Circuit Name for the management PVC. You will select this name when you configure the management path.
9. Use the instructions in “Administrative Attributes for PVCs” on page 7-14 to set the Administrative attributes.
10. Use the instructions in “Traffic Type Attributes for PVCs and Redirect PVCs” on page 7-18 to set the Traffic Type attributes.
11. Use the instructions in “User Preference Attributes for PVCs and Redirect PVCs” on page 7-21 to set the User Preference attributes.

12. (Optional) To configure NavisXtend Accounting Server parameters for this circuit, configure the Accounting tab. For more information, refer to the *NavisXtend Accounting Server Administrator's Guide*.
13. Choose OK to define the circuit parameters and proceed to “**Defining the Management Path**” on page 11-9.

## Using Management DLCIs

You use a management DLCI when the NMS connects to the gateway switch through a router, which provides the Frame Relay connection to the switch.

The following sections describe how to configure a management DLCI. This access method enables you to monitor the network without the use of an Ethernet module in the switch. It also provides the flexibility to move the NMS from one LAN to another with few reconfiguration requirements.

To complete the management DLCI configuration, you must enter a static route in the router and the NMS workstation to access the internal IP network. Refer to the *B-STDX, CBX, and GX Switch Diagnostics User's Guide* for more information.

To configure a Management DLCI:

1. In the Switch tab for the switch that connects to the router that serves as the Frame Relay interface for the Network Management DLCI, expand the Cards node and expand the node for the module that contains the Frame Relay physical port on which the logical port resides.
2. Expand the PPorts node, and expand the node for the physical port containing the logical port.
3. Under the node for the physical port, right-click on the LPorts node and expand the node for the logical port configured to access the router that serves as the Frame Relay interface for the Network Management DLCI.

- Right-click on the Mgmt DLCIs node and click Add on the popup menu, as shown in Figure 11-6.

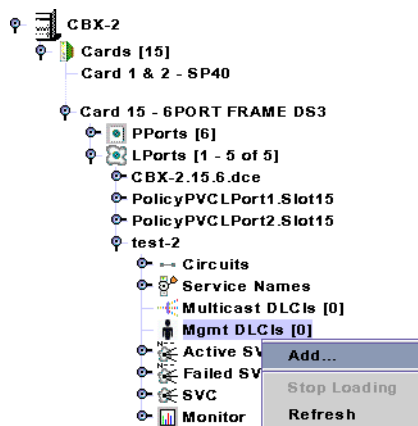


Figure 11-6. Adding a Management DLCI

The Add Management DLCI dialog box (Figure 11-7) is displayed.

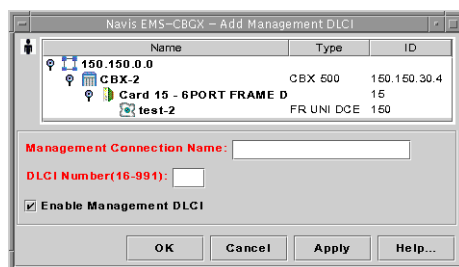


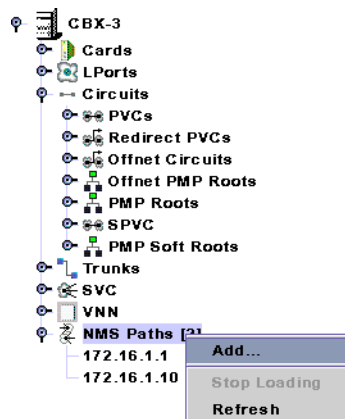
Figure 11-7. Add Management DLCI Dialog Box

- In the Management Connection Name field, enter a unique, continuous, alphanumeric name to identify the DLCI. Do not use hyphens, dashes, parentheses, or asterisks.
- In the DLCI Number field, enter the number that is used for the Management DLCI. For more information, see “About DLCI Numbers” on page 7-8.
- Click OK to complete the configuration and proceed to “Defining the Management Path” on page 11-9.

## Defining the Management Path

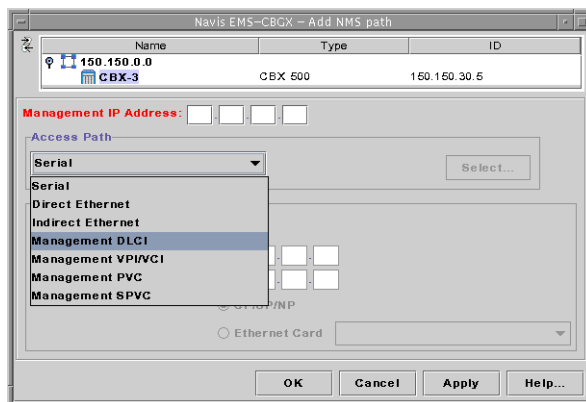
To define a management path:

1. In the Switch tab, expand the NMS Paths node.
2. Right-click on the NMS Paths node and click Add on the popup menu, as shown in [Figure 11-8](#).



**Figure 11-8.** Adding a Management Path

The Add NMS Path dialog box ([Figure 11-9](#)) is displayed.



**Figure 11-9.** Add NMS Path Dialog Box

3. Enter the NMS IP address in the Management IP Address field. This address is the IP address of the SPARCstation to which this switch connects.
4. Set the Access Path as follows:
  - To use a Management DLCI, select Management DLCI as the Access Path. Click the Select button, and choose the Management DLCI Name you defined in [“Using Management DLCIs”](#) on page 11-7.
  - To use a Management PVC, select Management PVC as the Access Path. Click the Select button, and choose the Management PVC Name you entered in [“Using Management PVCs”](#) on page 11-2.

5. Enable (default) or disable the ASE (Autonomous System External) Advertise option to advertise the new management path on the network. Disable this option if you do not want to advertise a switch's management path as a gateway to the NMS.

Using ASE Advertise to select switches that function as gateway switches to the NMS can provide better control of OSPF database size, network control traffic, and CPU usage.

6. Choose OK.



## Configuring Fault-tolerant PVCs

A fault-tolerant PVC configuration enables UNI DCE, UNI DTE, and FR NNI logical ports to serve as a backup for any number of active UNI or NNI ports. If a primary port fails or if you need to take a primary port offline, you manually activate the backup port. This function is sometimes referred to as *resilient UNI/NNI*.

This chapter contains:

- “[Configuration Procedure](#)” on page 12-1
- “[Creating a Primary Port](#)” on page 12-2
- “[Creating a Backup Port](#)” on page 12-4
- “[Activating a Backup Binding Port](#)” on page 12-4
- “[Returning the Primary Logical Port to Service](#)” on page 12-6

### Configuration Procedure

Use the following sequence to configure fault-tolerant PVCs:

1. Define a UNI DCE, UNI DTE, or FR NNI primary logical port as described in [Chapter 3, “Configuring Frame Relay LPorts.”](#) Make sure the Can Backup Service Names check box is disabled (see “[Administrative Attributes for Frame Relay LPorts](#)” on page 3-15).
2. Define and specify a Service Name that will be bound to the primary logical port.
3. Configure circuits to use the Service Name as the endpoint. Note that both endpoints can be different Service Names.
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, enabling the Can Backup Service Names check box (see “[Administrative Attributes for Frame Relay LPorts](#)” on page 3-15).
5. (*Optional*) Activate one of the backup logical ports, as needed (see “[Activating a Backup Binding Port](#)” on page 12-4).



---

**Note** – Observe the following limitations when configuring fault-tolerant PVCs:

- 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.
  - You cannot use redirect PVCs with Resilient UNI/NNI.
  - You cannot configure fault-tolerant PVCs on a logical port that is configured for Resilient Link Management Interface (RLMI).
- 

## Creating a Primary Port

To create a primary port, you assign a Service Name to a FR UNI or NNI logical port. (Do not choose a port that will be used for backup.) When you configure the circuit, choose this Service Name as the endpoint, instead of a switch and logical port combination. When you activate the backup port, the fault-tolerant PVC on the failed primary port is rerouted, preserving DLCIs 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.

The *Service Name* is a name you define to identify (bind to) the primary port. A circuit recognizes its service endpoint by this name, instead of the logical port name.



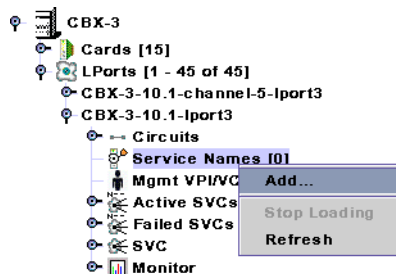
---

**Note** – Make sure that the Can Backup Service Names check box (see [“Administrative Attributes for Frame Relay LPorts” on page 3-15](#)) for the logical port is disabled. You cannot configure a Service Name for a logical port designated as a backup.

---

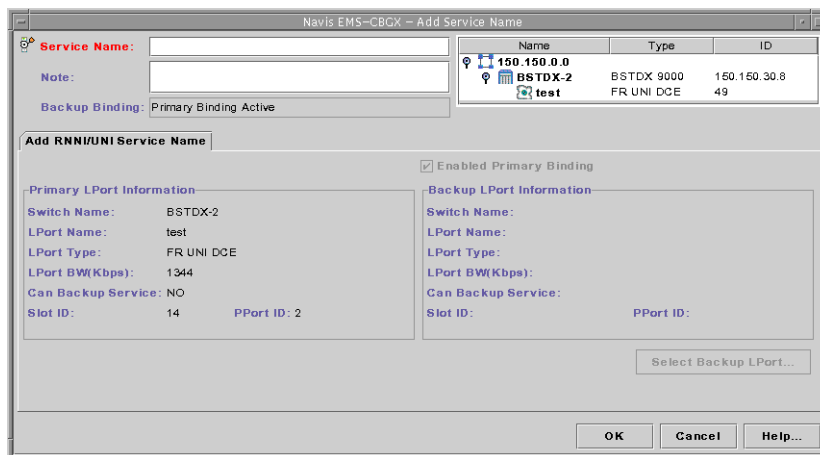
To create a service name:

1. In the Switch tab, expand the LPorts node.
2. Expand the node for the logical port for which you want to create a service name.
3. Right-click on the Service Names node and click Add on the popup menu, as shown in [Figure 12-1](#).



**Figure 12-1. Adding a Service Name**

The Add Service Name dialog box ([Figure 12-2](#)) is displayed with the Add RNNI/UNI Service Name tab available.



**Figure 12-2. Add RNNI/UNI Service Name Dialog Box**

4. Enter a Service Name (up to 32 characters). Optionally, you can enter a brief comment or description of the service in the Notes box.
5. Click OK to add the service name.

When you have configured the service name for the primary port:

- Continue with the instructions in [“Defining a Point-to-Point Circuit Connection” on page 7-11](#) to configure circuits as fault-tolerant PVCs.
- To reroute the Service Name endpoint of a fault-tolerant PVC, see [“Activating a Backup Binding Port.”](#)

## Creating a Backup Port

You can create a number of backup ports for later use with the same service name.

To create a backup port:

1. Define a FR UNI DCE, UNI DTE, or NNI logical port
2. Enable the Can Backup Service Names check box (see [“Administrative Attributes for Frame Relay LPorts”](#) on page 3-15).
3. To select a particular backup port during the backup binding procedure, see [“Activating a Backup Binding Port”](#) on page 12-4.

When a backup port is not in use, the port is idle and does not use network resources.

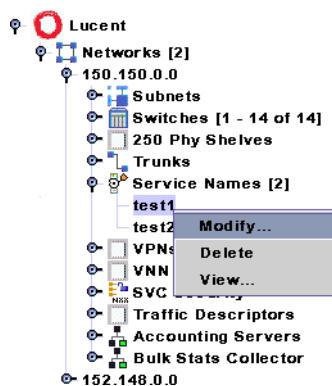
## Activating a Backup Binding Port

If a primary port fails (or needs administrative maintenance), you reassign the service name of the primary port to the backup port. Since fault-tolerant PVCs use the Service Name as an endpoint, all circuits configured for the primary port are rerouted to the backup port.

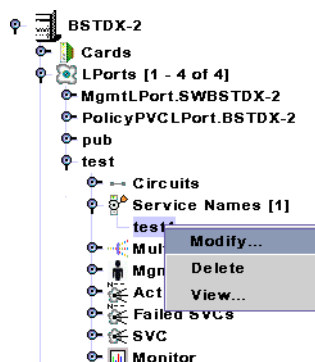
To enable the backup binding:

1. In either the Networks tab or the Switch tab, right-click on the node for the service name and click Modify, as shown in [Figure 12-3](#).

Networks tab:

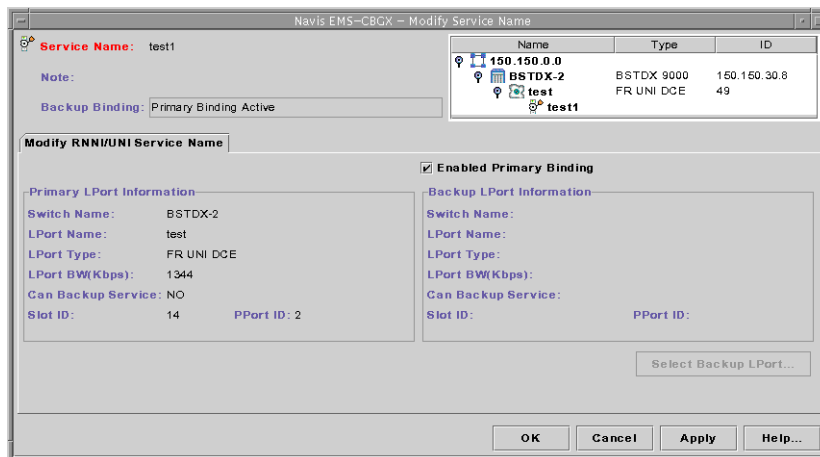


Switch tab:



**Figure 12-3. Modifying a Service Name**

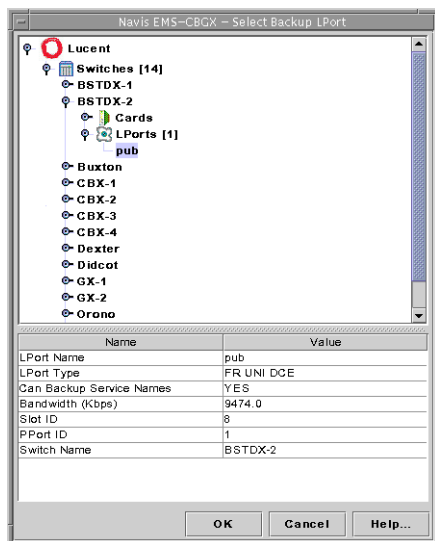
The Modify Service Name dialog box ([Figure 12-4](#)) is displayed. The Backup Binding status field displays the message Primary Binding Active.



**Figure 12-4. Modify Service Name Dialog Box**

2. Disable the Enabled Primary Binding check box, and click on the Select Backup LPort button.

The Select Backup LPort dialog box (Figure 12-4) is displayed.



**Figure 12-5. Select Backup LPort Dialog Box**

3. Select the backup logical port you want to use. Select an LPort Name that has the *same* logical port type as the port you need to back up. Only logical ports with the Can Backup Service Names check box enables are displayed.
4. Click OK to select the backup logical port.

The Modify Service Name dialog box displays information about the backup logical port. The Backup Binding status field displays the message Backup Binding Active.

5. Click OK to enable the backup service name binding.

## **Returning the Primary Logical Port to Service**

You can return to the primary logical port to service in future by enabling the Enabled Primary Binding check box in the Modify Service Name dialog box ([Figure 12-4](#)).

## Configuring Resilient LMI

This chapter describes how to configure a Resilient Local Management Interface (RLMI) which provides resiliency by monitoring LMI link status, and explains how to configure RLMI on Frame Relay UNI and NNI logical ports, and on ATM Network Interworking for and Frame Relay NNI logical ports on 1-port ATM IWU OC-3c/STM-1 and 1-port ATM CS DS3/E3 cards.

An RLMI preferred/backup pair can be a combination of any two FR UNI/NNI physical links. For example, a preferred UIO V.35 and a backup T1. In addition, the ATM Network Interworking for FR NNI logical port is supported 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.

This chapter contains:

- [“Configuration Overview” on page 13-1](#)
- [“Creating Service Names” on page 13-5](#)
- [“Configuring the RLMI Switchover Mode” on page 13-8](#)

### Configuration Overview

This section provides configuration guidelines and outlines the procedure for setting up an RLMI.

This section contains:

- [“About RLMIs” on page 13-2](#)
- [“Resilient LMI Terms” on page 13-2](#)
- [“Configuration Guidelines” on page 13-3](#)
- [“Resilient LMI Configuration Procedure” on page 13-4](#)

## About RLMIs

A Resilient Local Management Interface (RLMI) provides resiliency by monitoring LMI link status, enabling a pair of Frame Relay UNI or 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.

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; Bay Networks BNX routers can operate as Slave only.

RLMI supports FRF.4 SVC Signaling and 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 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 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 backup link.



**Table 13-1. Resilient LMI Terms (Continued)**

Term	Definition
Full Revertive	<p>If the Master RLMI switch's RLMI mode is configured as Full Revertive, the following occurs:</p> <ul style="list-style-type: none"> <li>• When the preferred link goes down, the backup link becomes the working link.</li> <li>• If or when the preferred link comes back up, the working link automatically switches back to the preferred link.</li> </ul>
Semi Revertive	<p>If the Master RLMI switch's RLMI mode is configured as Semi Revertive, the following occurs:</p> <ul style="list-style-type: none"> <li>• When the preferred link goes down, the backup link becomes the working link.</li> <li>• If or when the preferred link comes back up, the working link remains as the backup link (unless the backup link is down as well, then the preferred link becomes the working link again).</li> </ul>
Manual Switchover Only	<p>If the Master RLMI switch's RLMI mode is configured as Manual Switchover Only, the following occurs:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>

## Configuration Guidelines

This section lists the guidelines you should follow when you configure RLMI. Navis EMS-CBGX 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 PVC 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 UIO V.35 and a backup T1. In addition, the ATM Network Interworking for FR NNI logical port is supported 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 have the Can Backup Service Names field configured to No. The Backup port must have the Can Backup Service Names field configured to Yes.
- 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 Procedure

Use the following sequence to configure primary and backup RLMI logical ports:

1. Define either a Frame Relay UNI-DCE, UNI-DTE, or NNI logical port as described in [Chapter 3, “Configuring Frame Relay LPorts”](#), or an ATM Network Interworking for Frame Relay NNI logical port (refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000*).

Configure the following RLMI options:

- RLMI Master and Slave LPort Types (see [“Defining the Service Type and LPort Type” on page 3-10](#))
  - Can Backup Service Names (see [“Administrative Attributes for Frame Relay LPorts” on page 3-15](#)) to specify a backup or a primary port
  - RLMI Admin Status and RLMI Max Full Status Attempts (see [“Link Management Attributes for Logical Ports” on page 3-34](#))
2. Configure a service name for a preferred port and backup port pair (see [“Creating Service Names” on page 13-5](#)).
  3. Configure the RLMI switchover mode (see [“Configuring the RLMI Switchover Mode” on page 13-8](#)).

4. Add a circuit connection as described in [Chapter 7, “Configuring Permanent Virtual Circuits \(PVCs\)”](#), and configure the Resilient LMI service name as Endpoint 1 or Endpoint 2.



**Note** – To achieve resilient Frame Relay SVC operation, you must configure the same port prefix/address on both the preferred port and backup port.

## 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.

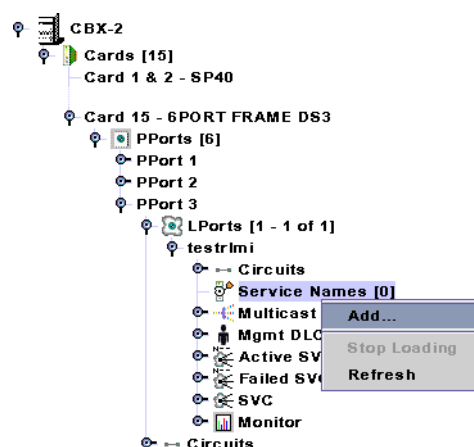


**Note** – You can create RLMI service names only on DTE or NNI logical ports configured with RLMI enabled and the Can Backup Service Names field set to No.

When selecting a backup logical port, the system displays only DCE or NNI logical ports configured with RLMI enabled and the Can Backup Service Names field set to Yes.

To create the service name bindings:

1. In the Switch tab, expand the LPorts node.
2. Expand the node for the logical port for which you want to create a service name. You can create RLMI service names only on DTE or NNI logical ports configured with RLMI enabled and the Can Backup Service Names field set to No.
3. Right-click on the Service Names node and click Add on the popup menu, as shown in [Figure 13-1](#).



**Figure 13-1.** Adding a Service Name

The Add Service Name dialog box (Figure 13-2) is displayed with the Add RLMI Service Name tab available.

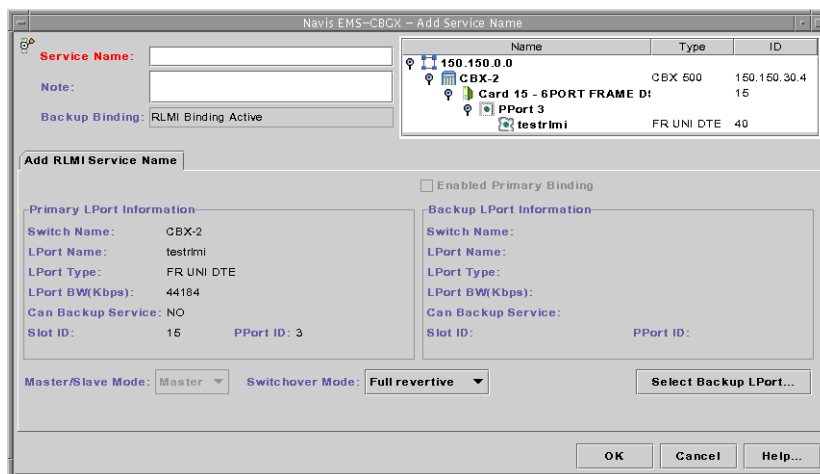


Figure 13-2. Add RLMI Service Name Dialog Box

4. Enter a Service Name (up to 32 characters). Optionally, you can enter a brief comment or description of the service in the Notes box.
5. Click OK to add the service name.
6. Configure the Master/Slave Mode parameter, selecting 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* – This mode determines which link to activate as the working link. Only Frame Relay UNI DTE or NNI logical ports can 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.

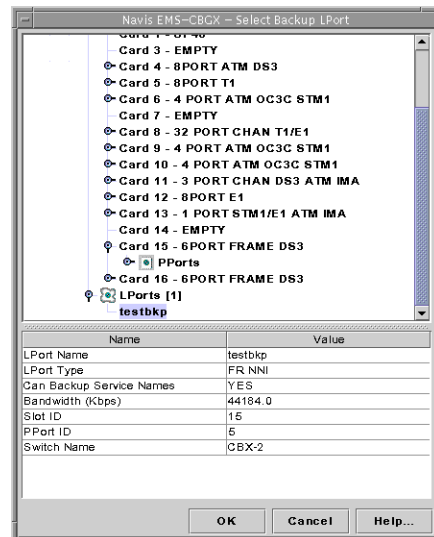
7. Configure the Switchover Mode parameter, selecting the mode of operation for automatic bindings when an interface changes up/down states.

You can configure the Switchover Mode only when the Master/Slave Mode parameter is configured as Master. By default, the Switchover Mode is set to Full Revertive. For more information about configuring the Switchover Mode, see “Configuring the RLMI Switchover Mode” on page 13-8.

- *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.

8. Click on the Select Backup LPort button.

The Select Backup LPort dialog box (Figure 13-3) is displayed.



**Figure 13-3. Select Backup LPort Dialog Box**

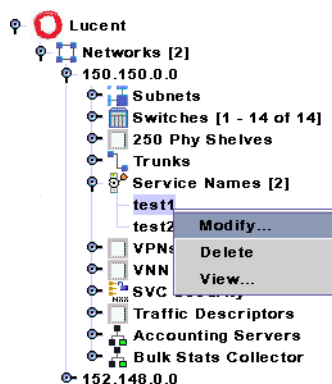
9. Select the backup logical port. When selecting a backup logical port, the system displays only DCE or NNI logical ports configured with RLMI enabled and the Can Backup Service Names field set to Yes.
10. In the Select Backup LPort dialog box, click OK.
11. In the Add Service Name dialog box, click OK.
12. Add a circuit connection and configure endpoints for an RLMI PVC connection (see “Defining a Point-to-Point Circuit Connection” on page 7-11).

## Configuring the RLMI Switchover Mode

To modify the RLMI parameters or force a preferred/backup switchover:

1. In either the Networks tab or the Switch tab, right-click on the node for the service name and click Modify, as shown in Figure 13-4.

Networks tab:



Switch tab:

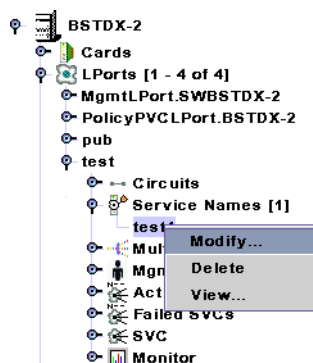


Figure 13-4. Modifying a Service Name

The Modify Service Name dialog box (Figure 13-5) appears. The Backup Binding status field displays the message RLMI Binding Active.

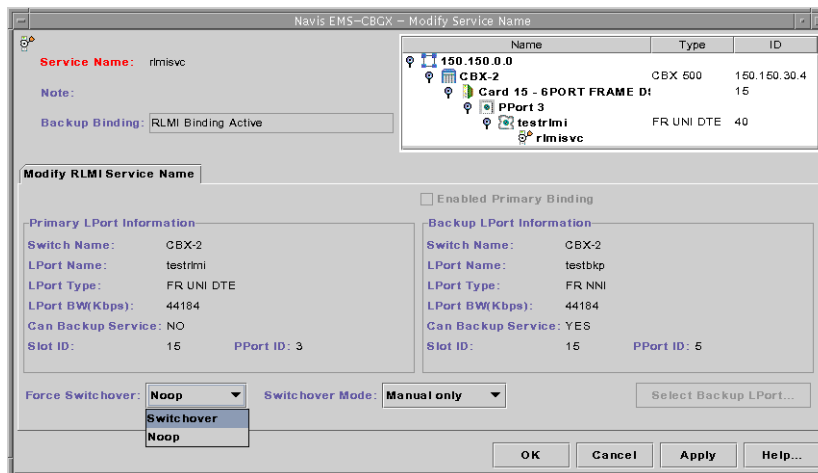


Figure 13-5. Modify Service Name Dialog Box

2. Select the Force 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).

The Force Switchover feature is disabled when the RLMI pair's Switchover Mode is set to Full Revertive.

3. If desired, select the Switchover Mode, which indicates the mode of operation for automatic bindings when an interface changes up/down states. You can configure the Switchover Mode only when the Master/Slave 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.
4. Choose OK.
  - To add a circuit connection and configure endpoints for an RLMI PVC connection, see [“Defining a Point-to-Point Circuit Connection”](#) on page 7-11.





## Configuring Switched Virtual Circuit (SVC) Parameters

This chapter describes how to use switched virtual circuits (SVCs). SVC connections are not predefined as they are for PVCs. Instead, end stations use a signaling protocol to indicate to the Frame Relay network the endpoint to which it should route the call (*called party*). To support SVC services, each user endpoint is assigned a unique address that identifies the endpoint and enables the network to route the call.

This chapter contains:

- “[Configuration Overview](#)” on page 14-2
- “[Administrative Tasks](#)” on page 14-6



**Note** – For information about using Open Shortest Path First (OSPF) name aggregation to minimize prefix and address memory consumption in Lucent network switches, see [Appendix B, “OSPF Name Aggregation.”](#)

---



**Note** – The B-STDX switch does not support the ATM Private Network-to-Network Interface (PNNI) routing protocol.

---

## Configuration Overview

This section provides an introduction to SVC address formats, route determination, network ID addressing, and the CBX and B-STDX modules that support Frame Relay SVC services.

This section contains:

- [“About Address Formats” on page 14-2](#)
- [“About Route Determination” on page 14-3](#)
- [“About Network ID Addressing” on page 14-5](#)
- [“I/O Modules for SVC Frame Relay Service” on page 14-6](#)

## About Address Formats

Before you can begin to configure your network for SVCs, you must decide which of the following address format types to use:

- **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 public Frame Relay or ATM networks (e.g., RBOCs) that already “own” E.164 address space.



**Note** – Both Frame Relay and ATM support native E.164 address formats. However, Frame Relay supports E.164 ATM End System Address (AESA) formats from release 09.00.00.00 onwards.

- **X.121 address format** — X.121 addresses are an ITU-T standard used in X.25 networks. X.121 addresses are sometimes referred to as IDNs (International Data Numbers) and consist of 14 ASCII digits. Only number values between 0-9 are valid.



**Note** – X.121 address formats are not configurable on ATM ports.

- **ATM End System Address address format** — The GX 550 and CBX 500 support four AESA formats:
  - **Data Country Code (DCC) AESA** — 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 International Standards Organization (ISO) reference 3166. DCC Anycast AESA provides a group address function for this address type.

- **International Code Designator (ICD) AESA** — For ICD AESAs, the IDI field contains the ICD 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.
- **E.164 AESA** — 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.
- **Custom AESA** — A Custom AESA address enables you to use a customized octet structure and a customized authority and format identifier (AFI).



---

**Note** – Refer to the *ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000* for more information on the AESA address formats.

---

You use address formats to develop a network numbering 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 formats you need to use.

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 Route Determination

The node prefixes, port prefixes, and port addresses that are configured on network nodes are used to determine the route for a given SVC. The route is determined by a “best match” hierarchy, 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 individual nodes. For example, if all addresses on a node contain the digits 15085551, you would define this as the node prefix. Using node prefixes to summarize or *aggregate* port prefixes and/or port addresses can result in more efficient routing determination. If more than one node has the same node prefix, this aggregation does not occur.

**Table 14-1** shows an example of three nodes configured with a combination of native E.164 node prefixes, port prefixes, and port addresses.

**Table 14-1. E.164 Node Prefix, Port Prefix, and Port Address Example**

	Node 1	Node 2	Node 3
<b>Node Prefixes</b>	508 6	None	508 603
<b>Port Prefixes</b>	508551 508552 508553	5085 508553 6035	508554 508555
<b>Port Addresses</b>	5085511111 5085511112 5085511113 5085555555 5085555556	None	None

Table 14-2 shows examples of the node to which a call is routed for certain called-party addresses, and why the call is routed to that node.

**Table 14-2. Routing by Called Party Address Example**

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 exactly matches 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 50855 on Node 2 and node prefix 508 on Node 1.
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.

**Table 14-2. Routing by Called Party Address Example (Continued)**

Called Party Address	Node	Reason
5085531111	1 or 2	Since the longest match occurs on both Nodes 1 and 2, the Admin Cost value assigned to port prefix 5085 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 5085.
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 (refer to <a href="#">“Defining Default Routes for Network-to-Network Connections”</a> on page 14-15).

## About Network ID Addressing

A network ID can be used to identify an inter-exchange carrier (IXC). You can configure network ID addressing on Frame Relay UNI and ATM UNI logical ports.

Depending on the administering authority, a network ID can be a 3-, 4-, or 8-digit Carrier Identification Code (CIC) or a 4-digit Data Network Identification Code (DNIC, X.121). Network ID addressing enables you to associate a network-to-network connection with a particular IXC using a route determination ID. It enables end users to presubscribe 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 presubscribed 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
- Configured 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 FRF.4, ATM UNI 3.x, 4.0, and IISP 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.

## I/O Modules for SVC Frame Relay Service

The following modules listed in [Table 14-3](#) support Frame Relay SVCs.

**Table 14-3. Frame Relay SVC Modules**

Low-Speed IOPA for B-STDX	High-Speed IOPB for B-STDX	High-Speed IOM2 for CBX	High-Speed IOM6 for CBX
8-Port UIO	2-Port HSSI	4-Port Channelized DS3/1 FR/IP	Not applicable
4-Port Unchannelized T1/E1	12-Port Unchannelized E1	4-Port Channelized DS3/1/0 FR/IP	Not applicable
4-Port Channelized T1/E1	1-Port Channelized DS3	6-Port DS3 FR/IP	6-Port Channelized DS3/1/0
10-Port DSX-1	1-Port Channelized DS3/1/0	8-Port Subrate DS3 FR/IP	Not applicable
Not applicable		32-Port Channelized T1/E1 FR/IP	

## Administrative Tasks

This section describes how to create and modify SVC node and port prefixes, default routes, port addresses, and network IDs.

This section contains:

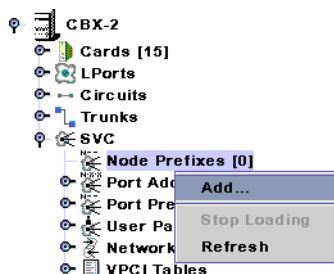
- [“Managing SVCs” on page 14-7](#)
- [“Configuring Node Prefixes” on page 14-7](#)
- [“Configuring Port Prefixes” on page 14-11](#)
- [“Defining Default Routes for Network-to-Network Connections” on page 14-15](#)
- [“Configuring Port Addresses” on page 14-16](#)
- [“Defining Network IDs” on page 14-20](#)



When a node acts as an Area Border Router (that is, when the node interfaces to trunks assigned to different OSPF areas), the node prefix OSPF Area ID is used to unambiguously assign addresses configured on that node to a particular OSPF area.

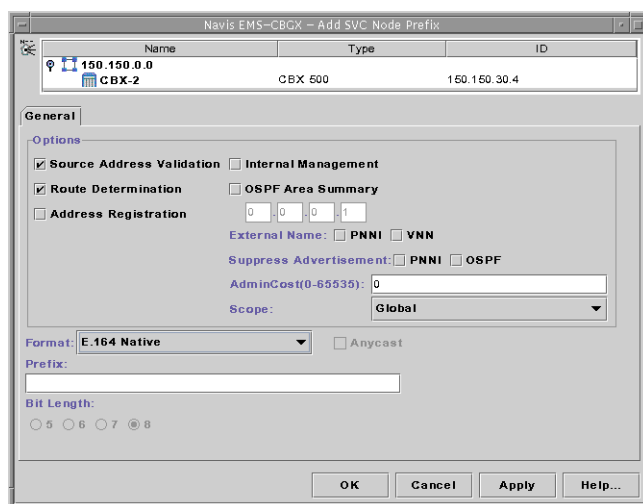
To define a node prefix:

1. In the Switch tab, expand the SVC node.
2. Right-click on the Node Prefixes node and click Add, as shown in [Figure 14-2](#).



**Figure 14-2. Adding a Node Prefix**

The Add SVC Node Prefix dialog box ([Figure 14-3](#)) is displayed.



**Figure 14-3. Add SVC Node Prefix Dialog Box**

3. Complete the Add SVC Node Prefix dialog box fields described in [Table 14-4](#).



**Table 14-4. Add SVC Node Prefix Dialog Box**

Element	Description
Source Address Validation	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – (default) Validates the calling party address against the node prefix associated with the UNI logical port that received the call setup message.</li> <li>• <i>Disable</i> – This node prefix is not used to validate calling party addresses.</li> </ul>
Route Determination	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – (default) The OSPF protocol uses this node prefix for routing aggregation.</li> <li>• <i>Disable</i> – The OSPF registration is not used.</li> </ul>
Address Registration	<p>An indicator of address registration.</p> <p><i>Note: This field is used only for Interim Local Management Interface (ILMI) address registration for ATM UNI-DCE “network-to-endsystem” logical ports. Address Registration is not supported for Frame Relay SVCs, and this field cannot be configured.</i></p>
Internal Management	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – Configures the prefix that corresponds to the switch itself as an addressable entity.</li> <li>• <i>Disable</i> – (default) Disregards this feature.</li> </ul>
OSPF Area Summary	<p>Select <i>Enable</i> if the node prefix summarizes an area border router. Then enter an OSPF Area ID. When a node acts as an area border router (that is, when the node interfaces to trunks assigned to different OSPF areas), the node prefix OSPF Area ID is used to unambiguously assign addresses configured on that node to a particular OSPF area.</p> <p>If you enable OSPF Area Summary, enter the OSPF Area ID. The OSPF Area ID is used to assign addresses configured on the node to a particular OSPF area.</p>
External Name: PNNI	<p>Advertises 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.</p> <p>If you remove the check from the box, this name is only reachable within the PNNI routing domain.</p>

**Table 14-4. Add SVC Node Prefix Dialog Box (Continued)**

Element	Description
External Name: OSPF	<p>Advertises 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.</p> <p>If you remove the check from the box, this name is only reachable within the VNN routing domain.</p>
Suppress Advertisement: PNNI	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group.</li> <li>• <i>Enable</i> – Prevents this address from being advertised across the PNNI domain.</li> </ul> <p><i>Note: This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>
Suppress Advertisement: OSPF	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the VNN OSPF routing domain.</li> <li>• <i>Enable</i> – Prevents this address from being advertised across the OSPF routing domain.</li> </ul>
Admin Cost	<p>Enter the administrative cost associated with this node prefix. If during the creation of an SVC, 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.</p>
Scope	<p>Organizational Scope defines how far into the hierarchical PNNI domain the switch should advertise this prefix or address.</p> <p><i>Note: This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>

**Table 14-4. Add SVC Node Prefix Dialog Box (Continued)**

Element	Description
Format	<p>Select the address format. Valid options include:</p> <ul style="list-style-type: none"> <li>• <i>E.164 (Native)</i> (default)</li> <li>• <i>X.121</i></li> <li>• <i>Default Route</i></li> <li>• <i>DCC AESA</i></li> <li>• <i>ICD AESA</i></li> <li>• <i>E.164 AESA</i></li> <li>• <i>Custom AESA</i></li> </ul> <p>For more information, see <a href="#">“Configuring Node Prefixes” on page 14-7</a>.</p> <p><i>Note:</i> See <a href="#">“About Address Formats” on page 14-2</a>.</p>
Prefix	<p>Enter the ASCII digits that represent the E.164 or X.121 address.</p> <p>For example, for E.164 addresses enter 5085552600 (a standard 10-digit U.S. phone number) or enter a partial number (such as 508). The value is converted to the ASCII hex values that represent each digit in the number. If you entered 5085552600, it converts to 35303835353532363030. This value is also displayed in the Prefix column on the Set All Node Prefixes dialog box (<a href="#">Figure 14-3 on page 14-8</a>).</p>
Bit Length	<p>As you type the address, the value in the Bit Length field changes to indicate the number of address bits that are checked during call screening and call routing.</p>
Anycast	<p>Indicates that the format type is an anycast version.</p>

4. Click OK to add the node prefix.

## Configuring 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. In the Switch tab, expand the Cards node, and expand the node for the card containing the port on which you want to configure a port prefix.
2. Expand the PPorts node, and expand the node for the specific physical port.
3. Expand the LPorts node, and select the node for the specific logical port.

- Expand the SVC node. Right-click on the Port Prefixes node and click Add, as shown in Figure 14-4.

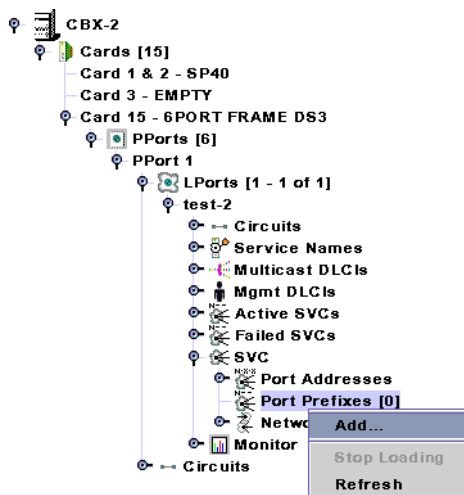


Figure 14-4. Adding a Port Prefix

The Add SVC Port Prefix dialog box (Figure 14-5) is displayed.

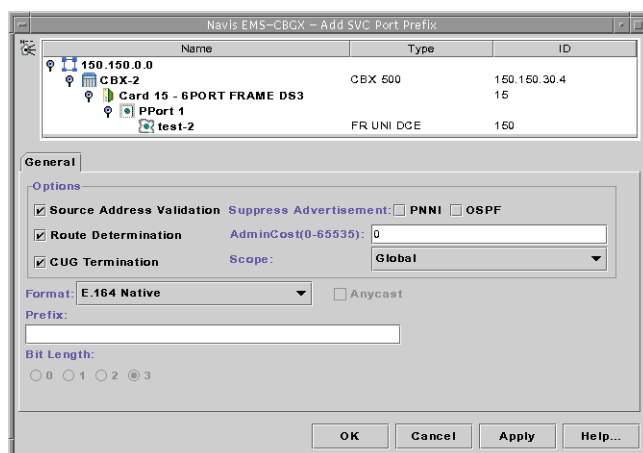


Figure 14-5. Add SVC Port Prefix Dialog Box

- Complete the Add SVC Port Prefix dialog box fields as described in Table 14-5.

Table 14-5. Add SVC Port Prefix Dialog Box

Element	Description
Source Address Validation	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Enable</i> – (default) Validates the calling party address against the port prefix associated with the UNI/NNI port that received the call setup message.</li> <li><i>Disable</i> – This port prefix is not used to validate calling party addresses.</li> </ul>

**Table 14-5. Add SVC Port Prefix Dialog Box (Continued)**

Element	Description
Route Determination	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Enable</i> – (default) The OSPF protocol uses this port prefix for route determination.</li> <li>• <i>Disable</i> – The OSPF registration is not used.</li> </ul>
CUG Termination	<p>Select Enable (default) 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 about CUGs, see <a href="#">Chapter 15, “Closed User Groups.”</a></p>
Suppress Advertisement: PNNI	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group.</li> <li>• <i>Enable</i> – Prevents this address from being advertised across the PNNI domain.</li> </ul> <p><i>Note:</i> This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</p>
Suppress Advertisement: OSPF	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the VNN OSPF routing domain.</li> <li>• <i>Enable</i> – Prevent this address from being advertised across the OSPF routing domain.</li> </ul>
Admin Cost	<p>Enter the administrative cost associated with the port prefix. If during the creation of an SVC, 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.</p>

**Table 14-5. Add SVC Port Prefix Dialog Box (Continued)**

Element	Description
Scope	<p>Organizational Scope defines how far into the hierarchical PNNI domain the switch should advertise this prefix or address.</p> <p><i>Note: This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>
Format	<p>Select the address format. Valid options include:</p> <ul style="list-style-type: none"> <li>• <i>E.164 (Native)</i> (default)</li> <li>• <i>X.121</i></li> <li>• <i>Default Route</i></li> <li>• <i>DCC AESA</i></li> <li>• <i>ICD AESA</i></li> <li>• <i>E.164 AESA</i></li> <li>• <i>Custom AESA</i></li> </ul> <p><i>Note: See “About Address Formats” on page 14-2.</i></p>
Prefix	<p>Enter all or part of the ASCII digits that represent the address. For example, enter 5085552600 (a standard 10-digit U.S. phone number) or enter a partial number (such as 508).</p> <p>The value that you enter in is converted to the ASCII hex values that represent each digit in the number. If you entered 508555260, it converts to 35303835353532363030. This value also appears in the Prefix column on the Set All Port Prefixes dialog box.</p>
Bit Length	<p>As you type the address, the value in the Bit Length field changes to indicate the number of address bits that are checked during call screening and call routing.</p>
Anycast	<p>Indicates that the format type is an anycast version.</p>

6. Click OK to add the SVC port prefix.

## Defining Default Routes for Network-to-Network Connections

For ports being used as 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 called-party address does not match any port prefixes or addresses, it reroutes the call to the port on which the default route is defined. If more than one port has a default route defined, the administrative cost value is used to determine the port to which the call is routed.



**Note** – When a default route is used, the switch provides partial protection from routing loops by preventing a call from being routed out the logical port on which it was received. It is important to note that, depending on the network topology, routing loops can still occur when multiple logical ports are provisioned with the default route.

You can define multiple default routes within a node or the network. The default route typically applies to network-to-network logical ports.

To define a default route:

1. In the Switch tab, expand the Cards node, and expand the node for the card containing the port on which you want to configure a port prefix.
2. Expand the PPorts node, and expand the node for the specific physical port.
3. Expand the LPorts node, and select the node for the specific logical port.
4. Expand the SVC node. Right-click on the Port Prefixes node and click Add, as shown in [Figure 14-6](#).

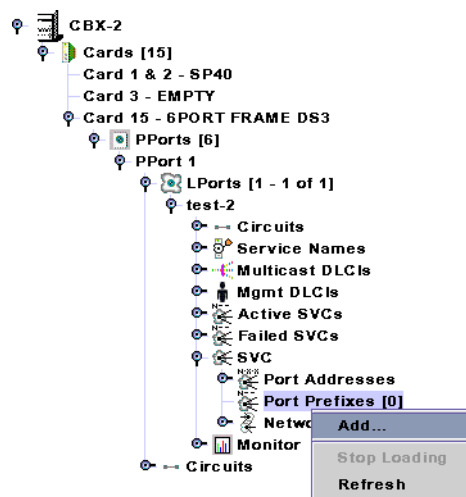
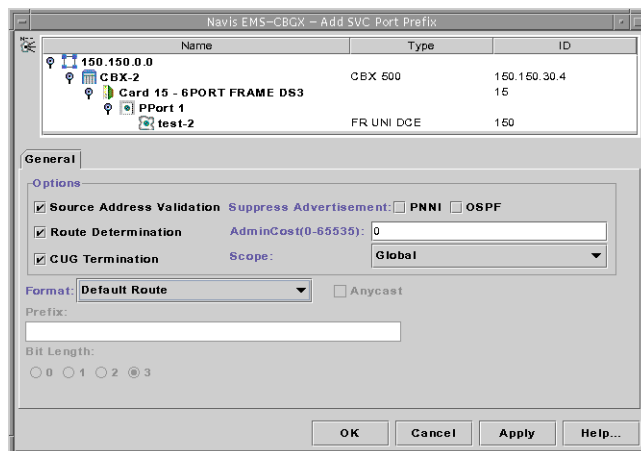


Figure 14-6. Adding a Port Prefix

The Add SVC Port Prefix dialog box (Figure 14-7) is displayed.



**Figure 14-7. Add SVC Port Prefix Dialog Box**

5. In the Format field, select Default Route.
6. Enter the Administrative Cost for the default route on this logical port.
7. Choose OK to add the default route.

## Configuring Port Addresses

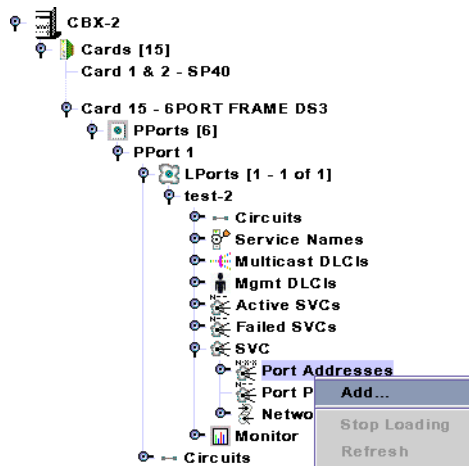
To fully specify an address to be used for calling party screening, you can define SVC addresses on all the logical ports on that physical port. For native E.164 addresses, you enter the 1-15 digit E.164 address; for X.121 addresses, you enter the 1-14 digit X.121 address.

To define an SVC port address:

1. In the Switch tab, expand the Cards node, and expand the node for the card containing the port on which you want to configure a port prefix.
2. Expand the PPorts node, and expand the node for the specific physical port.
3. Expand the LPorts node, and expand the specific logical port.

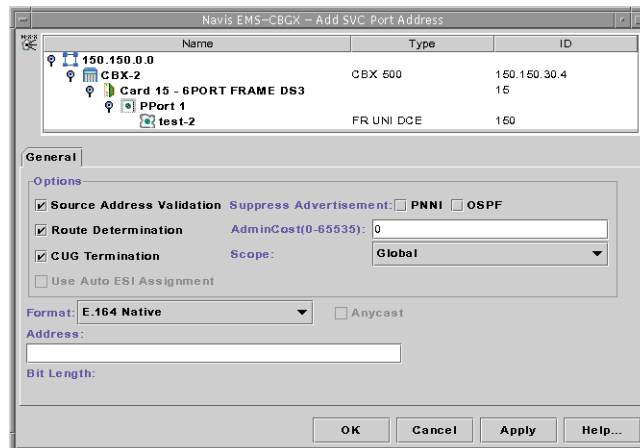


- Expand the SVC node. Right-click on the Port Addresses node and click Add, as shown in Figure 14-8.



**Figure 14-8. Adding a Port Address**

The Add SVC Port Address dialog box (Figure 14-9) is displayed.



**Figure 14-9. Add SVC Port Address Dialog Box**

- Complete the Add SVC Port Address fields described in Table 14-6.

**Table 14-6. Add SVC Port Address Dialog Box**

Element	Description
Source Address Validation	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Enable</i> – Validates the calling party address against the port address associated with the UNI port that received the call setup message.</li> <li><i>Disable</i> – This address is not used to validate calling party addresses.</li> </ul>

**Table 14-6. Add SVC Port Address Dialog Box (Continued)**

Element	Description
Route Determination	If enabled, the OSPF protocol uses this address for route determination.
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 <a href="#">Chapter 15, “Closed User Groups.”</a>
Using Auto ESI Assignment	<p>Choose this option to enable automatic assignment of end system identifier (ESI) bytes for the address.</p> <p><i>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.</i></p> <p><i>Refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000 for information on enabling the Auto ESI feature for other port address format types.</i></p>
Suppress Advertisement: PNNI	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the PNNI routing domain if the local switch is connected to a PNNI peer group.</li> <li>• <i>Enable</i> – Prevents this address from being advertised across the PNNI domain.</li> </ul> <p><i>Note: This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>
Suppress Advertisement: OSPF	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i> – (default) Allows this address to be advertised across the VNN OSPF routing domain.</li> <li>• <i>Enable</i> – Prevents this address from being advertised across the OSPF routing domain.</li> </ul>
Admin Cost	Enter the administrative cost associated with the port address. If during the creation of an SVC, 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.

**Table 14-6. Add SVC Port Address Dialog Box (Continued)**

Element	Description
Scope	<p>Organizational Scope defines how far into the hierarchical PNNI domain the switch should advertise this prefix or address.</p> <p><i>Note: This release supports Private Network-to-Network Interface (PNNI) on CBX 500 and GX 550 switches. PNNI is a standard designed by the ATM Forum. For more information about PNNI, refer to the ATM Forum PNNI specification. For information about Lucent ATM configuration and PNNI, refer to the ATM Services Configuration Guide for CBX 3500, CBX 500, GX 550, and B-STDX 9000.</i></p>
Format	<p>Select the address format. Valid options include:</p> <ul style="list-style-type: none"> <li>• <i>E.164 (Native)</i> (default)</li> <li>• <i>X.121</i></li> <li>• <i>Default Route</i></li> <li>• <i>DCC AESA</i></li> <li>• <i>ICD AESA</i></li> <li>• <i>E.164 AESA</i></li> <li>• <i>Custom AESA</i></li> </ul> <p>For more information, see <a href="#">“Configuring Port Addresses” on page 14-16</a>.</p> <p><i>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.</i></p> <p><i>Note: See <a href="#">“About Address Formats” on page 14-2</a>.</i></p>
Address	<p>Enter all or part of the ASCII digits that represent the address.</p> <p>For example, enter 5085552600 (a standard 10-digit U.S. phone number) or enter a partial number (such as 508).</p> <p>The value that you enter in the field is converted to the ASCII hex values that represent each digit in the number. If you entered 508555260, it converts to 353038353535323630. This value also appears in the Prefix column on the Set All Port Prefixes dialog box.</p>
Bit Length	<p>As you type the address, the value in the Bit Length field changes to indicate the number of address bits that are checked during call screening and call routing.</p>
Anycast	<p>Indicates that the format type is an anycast version.</p>

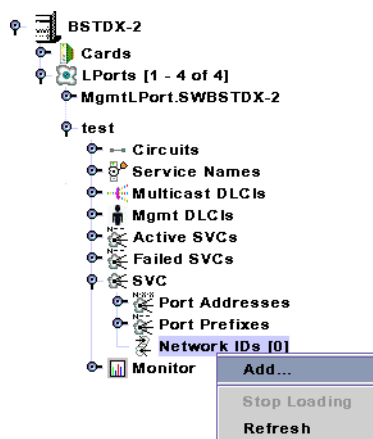
6. Click OK to add the SVC port address.

## Defining Network IDs

A network ID can be used to identify an inter-exchange carrier (IXC). You can configure network ID addressing on Frame Relay UNI and ATM UNI logical ports. For more information about Network IDs, see [“About Network ID Addressing” on page 14-5](#).

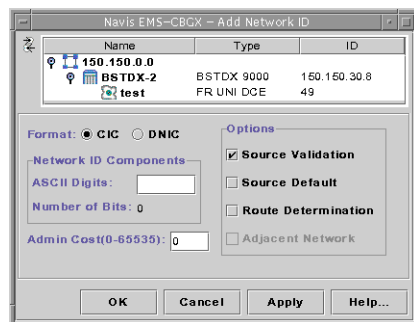
To define a network ID:

1. In the Switch tab, expand the Cards node, and expand the node for the card containing the port on which you want to configure a port prefix.
2. Expand the PPorts node, and expand the node for the specific physical port.
3. Expand the LPorts node, and select the node for the specific logical port.
4. Expand the SVC node. Right-click on the Network IDs node and click Add, as shown in [Figure 14-10](#).



**Figure 14-10. Adding a Network ID**

The Add Network ID dialog box ([Figure 14-11](#)) is displayed.



**Figure 14-11. Add Network ID Dialog Box**

5. Complete the Add Network ID dialog box fields described in [Table 14-7](#).

**Table 14-7. Add Network ID Dialog Box**

Element	Description
Format	Select an ID format. Options include: <ul style="list-style-type: none"> <li>• Carrier Identification Code (CIC)</li> <li>• Data Network ID Code (DNIC)</li> </ul>
ASCII Digits	Enter a number between 0-9 for CIC or DNIC formats. <ul style="list-style-type: none"> <li>• CIC IDs are 1-8 digit values.</li> <li>• DNIC IDs are 4 digit values.</li> </ul>
Number of Bits	Displays the number of bits in the network ID.
Admin Cost	Enter an administrative cost between 0 - 65535 for this network ID. The default is 0.
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 adjacent network parameter becomes inactive.
Source Default	Enable or Disable (default) source default for this network ID. Only one network ID on each port can have this attribute. When enabled, this network ID represents the preferred IXC for user calls originating on this logical port that do not signal a transit network selection.
Route Determination	Enable or Disable (default) route determination for this network ID. If you enable this field, source validation is disabled and the source default parameter becomes inactive. If enabled, the OSPF protocol uses this network ID for route determination.
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 can 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.

6. Choose OK to add the network ID.



# Closed User Groups

This chapter describes how to develop, configure and define closed user groups (CUG) in a network. A CUG is a division of all SVC network users into logically linked groups of users.

This chapter contains:

- [“Configuration Overview” on page 15-1](#)
- [“Administrative Tasks” on page 15-6](#)

## Configuration Overview

This section provides background information and examples of Closed User Groups (CUGs).

This section contains:

- [“About Closed User Groups \(CUGs\)” on page 15-1](#)
- [“About CUG Member Rules” on page 15-2](#)
- [“Developing Closed User Groups” on page 15-3](#)

## About Closed User Groups (CUGs)

A 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. Information about CUG membership and rules is available throughout the network.

A CUG is comprised of a set of rules called members. These rules represent SVC port addresses and prefixes for which you have enabled the CUG termination option (refer to [Table 14-6 on page 14-17](#)). You configure CUG member rules in either X.121 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 member 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 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, 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 X.121 digit is 4 bits and an E.164 digit is 8 bits.

The following examples show 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 (for example, 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 X.121), 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. A user mapping to a CUG member with incoming access enabled 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. A user mapping to a CUG member with outgoing access enabled can make 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.

For example, the following CUG member rule applies to E.164 addresses beginning with digits 1508.

Member Rule Name:	rule1
Member Value/Type:	1508* (E.164)
Incoming Access:	Y
Outgoing Access:	N

Users that 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

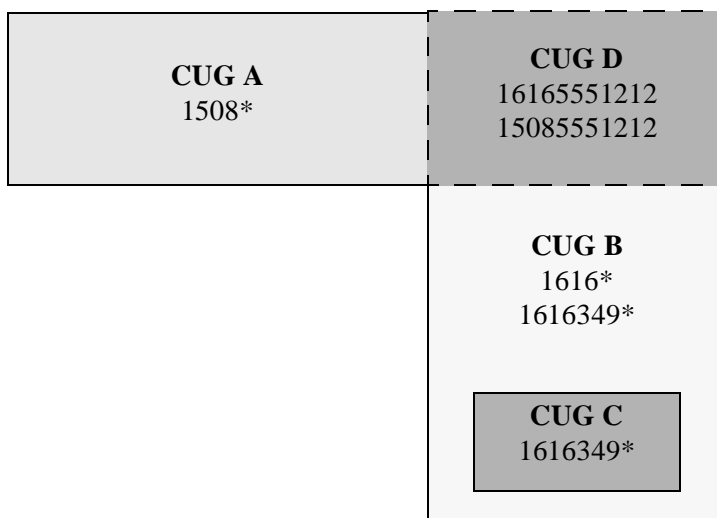
For each CUG you create, you can assign up to 128 different member rules; you can use an individual member rule in up to 16 different CUGs. In this way, a CUG is made up of all users that map to the addresses that these rules define. You can configure up to 1024 CUGs per switch.

When you create a CUG (“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 that map to Rule1 cannot receive calls from other CUG A members. Conversely, disable ICB to allow users that map to Rule1 to receive calls from other CUG A members.

If you enable the *outgoing calls barred* (OCB) attribute for Rule1, users that map to Rule1 cannot make calls to other CUG A members. Conversely, disable OCB to allow users that map to Rule1 to make calls to other CUG A members.

## Using CUGs in the Network

Figure 15-1 illustrates how you can implement CUGs in your network.



**Figure 15-1. 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, the following table 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 15-1. ICB/OCB Attributes and Member Rules**

	ICB	OCB	Member Rules	IA	OA
<b>CUG A</b>	No	No	1508*	No	No
<b>CUG B</b>	No Yes	No Yes	1616* 1616349*	No No	Yes No
<b>CUG C</b>	No	No	1616349*	No	No
<b>CUG D</b>	No No	No No	16165551212 15085551212	No Yes	Yes No

Some examples follow:

- 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 15-1 on page 15-4](#), [Table 15-2](#) illustrates how a single configured address can match multiple member rules, and can belong to more than one CUG.

**Table 15-2. 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 only can simplify call routing since the logical port only needs to check the address prefix digits to route the call. However, CUG membership must be recalculated at call time if the port to which this address is routed contains other CUGs with member rules that begin with the digits 1616.

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.

## Administrative Tasks

Use the following sequence to configure CUGs. Remember that each member rule should correspond to at least one SVC address.

1. Create SVC addresses and enable CUG termination (see [“Configuring Port Addresses” on page 14-16](#)).
2. Define the CUG member rules that represent the member addresses and call access. See [“Defining CUG Members” on page 15-6](#).
3. Define the CUG names (see [“Defining a CUG” on page 15-8](#)) and associate CUG members to specific CUGs. You can also modify call access attributes for a specific CUG.

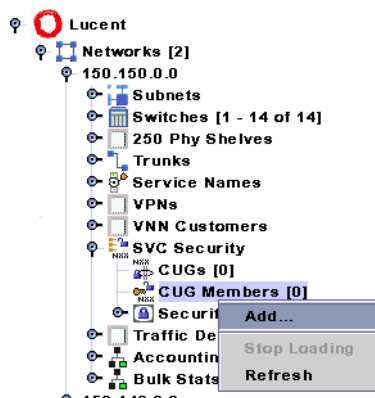
## Defining CUG Members

A CUG member is defined by a rule that matches one or more port addresses/prefixes and attributes that specify incoming and outgoing call access. After you define these members, you can associate them with specific CUGs.

In the Networks tab, the SVC Security node contains CUGs and CUG Members nodes.

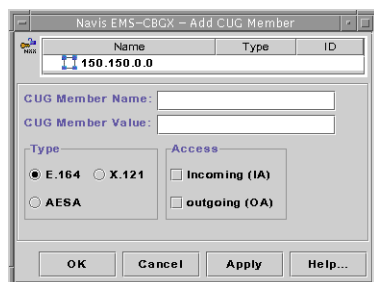
To define a CUG member:

1. In the Networks tab, expand the network you are managing.
2. Expand the SVC Security node.
3. Right-click on the CUG Members node and click Add on the popup menu, as shown in [Figure 15-2](#).



**Figure 15-2. Defining a CUG Member**

The Add CUG Member dialog box ([Figure 15-3](#)) is displayed.



**Figure 15-3. Add CUG Member Dialog Box**

4. Configure the member attributes described in [Table 15-3](#).

**Table 15-3. Add SVC CUG Member Dialog Box**

Element	Description
CUG Member Name	Enter a name (up to 32 characters).
CUG Member Value	Enter the CUG member rule using the guidelines in <a href="#">“About CUG Member Rules”</a> on page 15-2. Do not enter more than 15 characters for an E.164 address or more than 14 characters for an X.121 address.
Type	Select X.121 or E.164.

**Table 15-3. Add SVC CUG Member Dialog Box (Continued)**

Element	Description
Access: Incoming (IA)	This attribute specifies how incoming calls from non-CUG users or users of a different CUG are handled. <ul style="list-style-type: none"><li>• Enable to accept calls from users that do not belong to the same CUG.</li><li>• Disable (default) to reject calls from users that do not belong to the same CUG.</li></ul>
Access: Outgoing (OA)	This attribute specifies how outgoing calls to non-CUG users or users of a different CUG are handled. <ul style="list-style-type: none"><li>• Enable to allow calls to users not belonging to the same CUG.</li><li>• Disable (default) to block calls to users not belonging to the same CUG.</li></ul>

5. When you finish, click Apply to commit the configuration and configure additional CUG members, or click OK to add the CUG member and return to the Navis EMS-CBGX window.

## Defining a CUG

Next, set up the CUGs for your network. This is a simple process of supplying a name for each CUG.

Observe the following configuration limits:

- Up to 1024 CUGs per switch are supported.
- You can assign up to 128 members per CUG.
- You can assign each member to as many as 16 CUGs.

To create a CUG:

1. In the Networks tab, expand the network you are managing.
2. Expand the SVC Security node.
3. Right-click on the CUGs node and click Add on the popup menu, as shown in Figure 15-4.

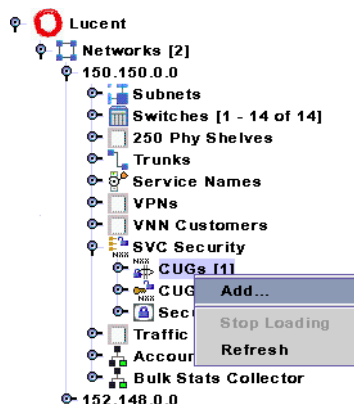


Figure 15-4. Defining a CUG

The Add CUG dialog box (Figure 15-5) is displayed.

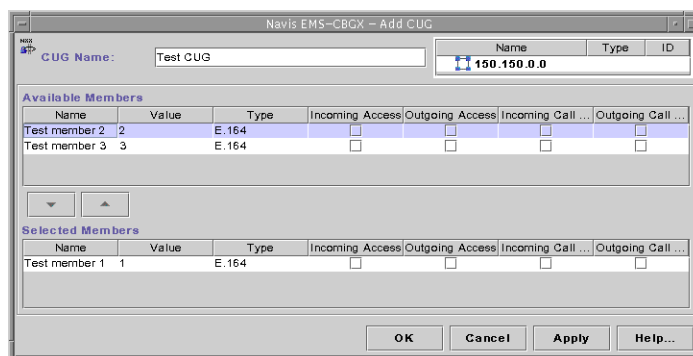


Figure 15-5. Add CUG Dialog Box

4. Enter a CUG name (up to 32 characters). The NMS assigns a CUG ID.
5. In the Available Members list, select the CUG members you want to add, and click on the down arrow button to add them to the Selected Members list.

6. Set the following member rules by clicking on the Incoming Call Barred and Outgoing Call Barred check boxes to enable or disable calls.
  - **Incoming Call Barred** — Specifies how incoming calls from the same CUG are handled. Enable to reject calls from users of the same CUG. Disable (default) to allow calls from users of the same CUG.
  - **Outgoing Call Barred** — Specifies how outgoing calls to the same CUG are handled. Enable to block calls to users of the same CUG. Disable (default) to allow calls to users of the same CUG.

You can configure the Incoming Access and Outgoing Access rules by modifying each of the CUG members individually.

7. When you finish, click Apply to commit the configuration and configure additional CUGs, or click OK to add the CUG and return to the Navis EMS-CBGX window.



# Port Security Screening

This chapter describes Port Security Screening, which ensures that your network cannot be compromised by unauthorized SVC access.

This chapter contains:

- [“Configuration Overview” on page 16-1](#)
- [“Administrative Tasks” on page 16-7](#)

## Configuration Overview

This section provides background information and configuration guidelines for managing Port Security Screening.

This section contains:

- [“About Port Security Screening” on page 16-2](#)
- [“Implementing Port Security Screening” on page 16-2](#)

## About 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 and X.121 formats for calling and called party addresses, and the Network Service Access Point (NSAP) AESA format for calling and called subaddresses.
- Matching information — Address criteria that either allows or disallows the SVC.

After you develop a set of screens, you can apply them to any 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 meets the matching 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, the decision as to whether an SVC is passed or blocked is made 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 use security screens on both ingress user ports, which represent SVC originating endpoints, or egress user ports, which in turn 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 16-1** describes the default ingress and egress security screen options. These defaults represent the port screen activation parameters.

**Table 16-1. Default Screens**

Default	Value	Description
Ingress Screen Mode	All Screens	All ingress screens you apply to this port are used to determine whether an incoming SVC is passed or blocked.
	Default Screen <i>(default)</i>	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 <i>(default)</i>	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 are used to determine whether an outgoing SVC is passed or blocked.
	Default Screen <i>(default)</i>	Disables the egress security screens applied to this port. Outgoing SVCs are screened according to the Default Egress Screen.
Default Egress Screen	Pass <i>(default)</i>	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. After 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 — Defines the SVCs to which this screen applies, either ingress (incoming) or egress (outgoing).
- Screen type — Determines whether or not 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 X.121-style address for calling or called addresses, or an NSAP AESA-style address for calling or called subaddresses. 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 [“Configuring Node Prefixes” on page 14-7](#) for more information about 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 (for example, 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 16-2 describes some examples using the port security screens.

**Table 16-2. Security Screens**

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

After you assign security screens to a logical port, if you set the ingress and egress screen modes to All Screens (Figure 16-4 on page 16-11), 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 for the matching criteria of this screen's default behavior. If it meets the matching 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, the decision on whether the port should block or pass an SVC is made 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 additional exception. You want to block all incoming SVCs that contain the 234 exchange number.

### **Logical Port Configuration Example**

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 you assign.

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

### Summary

As you begin to design port security screening features for your network, keep the following points in mind:

- 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.
- Configure and assign the security screen exceptions. The previous example passes all incoming 1800 SVCs.
- Configure and assign any exceptions to these screens. The previous example specifically blocks incoming SVCs from the 234 exchange; this includes incoming SVCs from 1800234\*.

## Administrative Tasks

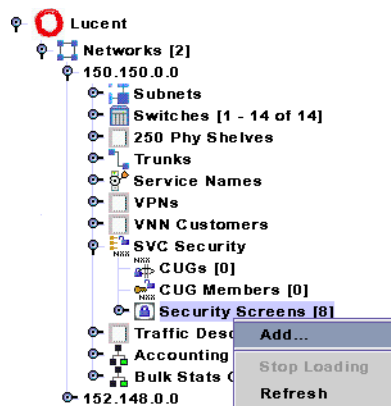
Use the following sequence to configure port security screening.

1. Configure logical ports (see [Chapter 3, “Configuring Frame Relay LPorts”](#)).
2. Configure SVCs (see [Chapter 14, “Configuring Switched Virtual Circuit \(SVC\) Parameters”](#)).
3. Create a set of security screens (see [“Creating Port Security Screen Definitions” on page 16-8](#)).
4. Define the logical port security screening defaults. If necessary, assign the security screens that provide exceptions to these defaults (see [“Assigning Security Screens to Logical Ports” on page 16-10](#)).

## Creating Port Security Screen Definitions

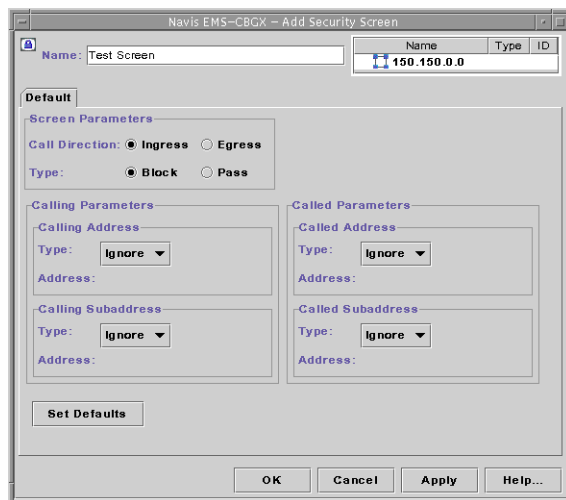
To create a security screen:

1. In the Networks tab, expand the network you are managing.
2. Expand the SVC Security node.
3. Right-click on the Security Screens node and click Add on the popup menu, as shown in [Figure 16-1](#).



**Figure 16-1.** Adding a Security Screen

The Add Security Screen dialog box ([Figure 16-2](#)) is displayed.



**Figure 16-2.** Add Security Screen Dialog Box



4. Configure the dialog box fields as described in [Table 16-3](#).

**Table 16-3. Add Security Screen Dialog Box**

Element	Description
Name	Enter a name (up to 32 characters) for this security screen.
Call Direction	The screen you configure is only applied to these SVCs. <ul style="list-style-type: none"> <li>• <i>Ingress</i> – (default) Screen incoming SVCs.</li> <li>• <i>Egress</i> – Screen outgoing SVCs.</li> </ul>
Type	Select the Type of screen. This determines the action this screen performs. <ul style="list-style-type: none"> <li>• <i>Block</i> – (default) Blocks all SVCs that match the criteria.</li> <li>• <i>Pass</i> – Passes all SVCs that match the criteria.</li> </ul>
Calling Address	Configure the Calling Address: <ul style="list-style-type: none"> <li>• <i>Type</i> – Select the address type, either E.164 or X.121. Select Ignore (default) if the screen does not use this parameter.</li> <li>• <i>Address</i> – Enter the address screen using the guidelines in <a href="#">“About Security Screen Addresses” on page 16-4</a>. Enter up to 15 characters for an E.164 address; enter up to 14 characters for an X.121 address.</li> </ul>
Calling Subaddress	Configure the Calling Subaddress. This parameter provides an optional level of screening. <ul style="list-style-type: none"> <li>• <i>Type</i> – Select AESA. Select Ignore (default) if the screen does not use this parameter.</li> <li>• <i>Address</i> – Enter the address screen (up to 40 characters) using the guidelines in <a href="#">“About Security Screen Addresses” on page 16-4</a>.</li> </ul>
Called Address	Configure the Called Address: <ul style="list-style-type: none"> <li>• <i>Type</i> – Select the address type, either X.121 or E.164. Select Ignore (default) if the screen does not use this parameter.</li> <li>• <i>Address</i> – Enter the address screen using the guidelines in <a href="#">“About Security Screen Addresses” on page 16-4</a>. Enter up to 15 characters for an E.164 address; enter up to 14 characters for an X.121 address.</li> </ul>
Called Subaddress	Configure the Called Subaddress. This parameter provides an optional level of screening. <ul style="list-style-type: none"> <li>• <i>Type</i> – Select AESA. Select Ignore (default) if the screen does not use this parameter.</li> <li>• <i>Address</i> – Enter the address screen (up to 40 characters) using the guidelines in <a href="#">“About Security Screen Addresses” on page 16-4</a>.</li> </ul>

5. Use the Apply button to create several screens in a single session, clicking Set Defaults to retrieve the default values if necessary. Otherwise, click OK to create the new screen and return to the Navis EMS-CBGX window.

## Assigning Security Screens to Logical Ports

After you create the security screens, you must modify existing logical ports to 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.

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.

To assign security screens to a port:

1. In the Switch tab, expand the LPorts node.
2. Right-click on the LPort you want to configure, and select Security from the popup menu, as shown in [Figure 16-3](#).

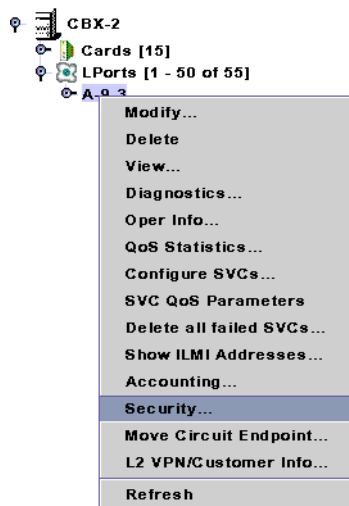
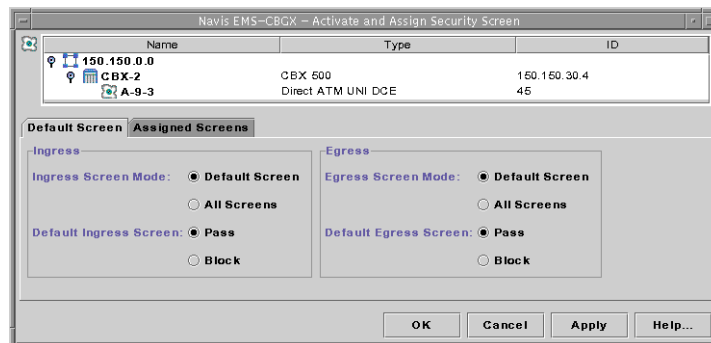


Figure 16-3. Assigning a Security Screen to a Logical Port

The Activate and Assign Security Screen dialog box (Figure 16-4) is displayed.



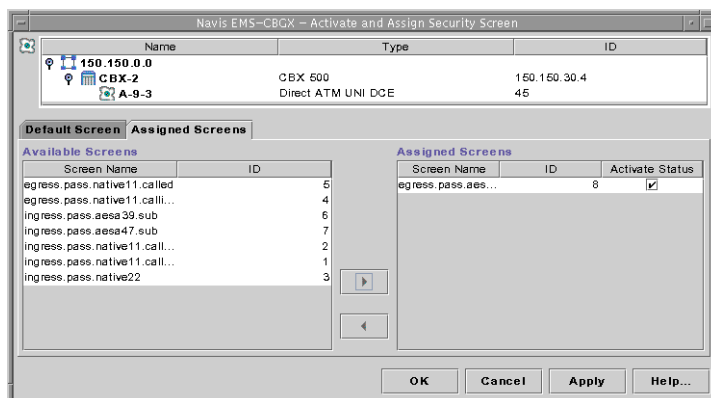
**Figure 16-4. Activate and Assign Security Screen: Default Screen Tab**

3. In the Default Screen tab, configure how incoming and outgoing SVCs are screened as described in Table 16-4.

**Table 16-4. Activate and Assign Security Screen Dialog Box**

Element	Description
Ingress Screen Mode	Configure how incoming SVCs are screened: <ul style="list-style-type: none"> <li>All Screens — Indicates that all ingress screens you apply to this port determine whether an incoming SVC is passed or blocked.</li> <li>Default Screen — Disables (default) the ingress security screens applied to this port. Incoming SVCs are screened according to how you set the Default Ingress Screen.</li> </ul>
Default Ingress Screen	Choose a button to specify what action the Default ingress security screen will take when the Ingress Screen mode is set to Default Screen: <ul style="list-style-type: none"> <li>Pass — All incoming SVCs to this port are passed (default).</li> <li>Block — All incoming SVCs to this port are blocked.</li> </ul>
Egress Screen Mode	Choose a button to specify what type of egress security screens will be used: <ul style="list-style-type: none"> <li>Default Screen — Disables (default) the egress security screens applied to this port. Outgoing SVCs are screened according to how you set the Default Egress Screen.</li> <li>All Screens — Indicates that all egress screens you apply to this port determine whether an outgoing SVC is passed or blocked.</li> </ul>
Default Egress Screen	Choose a button to specify what action the Default egress security screen will take when the Egress Screen mode is set to Default Screen: <ul style="list-style-type: none"> <li>Pass — All outgoing SVCs from this port are passed (default).</li> <li>Block — All outgoing SVCs from this port are blocked.</li> </ul>

4. In the Assigned Screens tab (Figure 16-5), use the arrow buttons to assign available screens to the logical port.



**Figure 16-5. Activate and Assign Security Screen: Assigned Screens Tab**

5. Enable the Activate Status check box for each assigned screen if you want to screen SVCs according to the rules of the screen.
6. When you finish activating and assigning screens, click OK to return to the Navis EMS-CBGX window.

## 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).

This appendix contains:

- “Circuit Add Errors” on page A-2
- “Circuit Modify Errors” on page A-4
- “Circuit Delete Errors” on page A-5

When you perform these operations, any errors (and the circuit endpoints that caused them) are reported. When an error occurs, the Abort, Retry, and Ignore options available to you are sensitive to the endpoint that caused the failure.

Error information is based on both the endpoint 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 endpoint cards). For each error combination (circuit operation, type of error, and endpoint failure), the error information indicates:

- The effect on the NMS database
- The state of both switches
- The out of sync status
- The effect of performing a PRAM sync
- Other special considerations

The tables in this appendix designate endpoint switches and cards for both standard and redirect PVC configurations:

- **Standard PVC Configuration**— Designates endpoint switches and cards as 1st and 2nd, indicating the send order for the SNMP set commands. An SNMP set is sent to the 1st endpoint, and (if successful) it is then sent to the 2nd endpoint. Note that for Circuit Add and Modify operations, the 1st endpoint is the lower-numbered node. For Circuit Delete, the 1st endpoint is the higher-numbered node.
- **Redirect PVC Configuration**— Designates endpoint 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 (if successful) Pivot. For Circuit Delete, the send order for the SNMP commands is Pivot, followed by (if successful) Primary, and (if successful) Secondary. The Pivot endpoint 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 endpoint cards being placed out of sync when the indicated failure occurs

---

## Circuit Add Errors

**Table A-1** 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 endpoint), *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 endpoints, *not* in the order of Pivot, Primary, and Secondary as is done with a Circuit Delete operation.

---

**Table A-1. Errors Encountered During Circuit Add Procedure**

Type of Failure	SNMP Set Failure Reason	Available Choices
<p><b>Standard PVC</b> – 1st switch unreachable (lower-numbered node)</p> <p><b>Redirect PVC</b> – Primary or Secondary switch unreachable</p>	<p>The SNMP request timed out (1st [or Primary or Secondary] endpoint identified).</p>	<p><i>Abort</i> – Discontinue attempt to add circuit (NMS database, switches, and out-of-sync status unmodified).</p> <p><i>Retry</i> – Attempt to add circuit again.</p>
<p><b>Standard PVC</b> – 2nd switch unreachable (higher-numbered node)</p> <p><b>Redirect PVC</b> – Pivot switch unreachable</p>	<p>The SNMP request timed out (2nd [or Pivot] endpoint identified).</p>	<p><i>Abort</i> – 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 endpoint cards will remove traces of circuit from switches.</p> <p><i>Ignore</i> – 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] endpoint card marked out-of-sync). PRAM sync of endpoint cards will put circuit into switches.</p> <p><i>Retry</i> – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the retry.</p>
<p><b>Standard PVC</b> – Circuit not present on 1st switch (lower-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on the Primary or Secondary switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (specific endpoint not identified).</p>	<p><i>Abort</i> – Discontinue attempt to add circuit (NMS database unmodified, nothing marked out-of-sync). PRAM sync of endpoint cards will remove traces of circuit from switches.</p> <p><i>Retry</i> – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the Retry.</p>
<p><b>Standard PVC</b> – Circuit not present on 2nd switch (higher-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on the Pivot switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (specific endpoint not identified).</p>	<p><i>Abort</i> – 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 endpoint cards will remove traces of circuit.</p> <p><i>Retry</i> – Attempt to add the circuit again. Dangling circuit on 1st (or Primary or Secondary) switch will not interfere with the Retry.</p>

## Circuit Modify Errors

**Table A-2** 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 endpoint), *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 endpoints, *not* in the order of Pivot, Primary, and Secondary as is done with a Circuit Delete operation.

**Table A-2. Errors Encountered During Circuit Modify Procedure**

Type of Failure	SNMP Set Failure Reason	Available Choices
<p><b>Standard PVC</b> – 1st switch unreachable (lower-numbered node)</p> <p><b>Redirect PVC</b> – Primary or Secondary switch unreachable</p>	The SNMP request timed out (1st [or Primary or Secondary] endpoint identified).	<p><i>Abort</i> – Discontinue attempt to modify circuit (NMS database, switches, and out-of-sync status unmodified).</p> <p><i>Retry</i> – Attempt to modify circuit again.</p>
<p><b>Standard PVC</b> – 2nd switch unreachable (higher-numbered node)</p> <p><b>Redirect PVC</b> – Pivot switch unreachable</p>	The SNMP request timed out (2nd [or Pivot] endpoint identified).	<p><i>Abort</i> – 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 endpoint cards will remove circuit modification.</p> <p><i>Ignore</i> – 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] endpoint card marked out-of-sync). PRAM sync of endpoint cards will modify circuit on both switches.</p> <p><i>Retry</i> – Attempt to modify the circuit again. Dangling circuit modification on 1st [or Primary or Secondary] switch will not interfere with the retry.</p>



**Table A-2. Errors Encountered During Circuit Modify Procedure (Continued)**

Type of Failure	SNMP Set Failure Reason	Available Choices
<p><b>Standard PVC</b> – Circuit not present on 1st switch (lower-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on the Primary or Secondary switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (specific endpoint not identified).</p>	<p><i>Abort</i> – Discontinue attempt to modify circuit (NMS database unmodified).</p> <p><i>Retry</i> – Attempt to modify the circuit again.</p>
<p><b>Standard PVC</b> – Circuit not present on 2nd switch (higher-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on the Pivot switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (specific endpoint not identified).</p>	<p><i>Abort</i> – 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 endpoint cards will remove circuit modification.</p> <p><i>Retry</i> – Attempt to modify the circuit again. Begin with 1st (or Primary or Secondary) switch, where dangling circuit modification will not interfere with the Retry.</p>

## Circuit Delete Errors

**Table A-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 endpoint), *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 endpoints, *not* in the order of Primary, Secondary, and Pivot as is done with a Circuit Add or Modify operation.

**Table A-3. Errors Encountered During Circuit Delete Procedure**

Type of Failure	SNMP Set Failure Reason	Available Choices
<p><b>Standard PVC</b> – 1st switch unreachable (higher-numbered node)</p> <p><b>Redirect PVC</b> – Pivot switch unreachable</p>	<p>The SNMP request timed out (1st [or Pivot] endpoint identified).</p>	<p><i>Abort</i> – Discontinue attempt to delete circuit (NMS database, switches, and out-of-sync status unmodified).</p> <p><i>Ignore</i> – Discontinue attempt to delete circuit, but delete the circuit from the NMS database (circuit not deleted on either switch, both endpoint cards marked out-of-sync). PRAM sync of endpoint cards will delete circuit on switches.</p> <p><i>Retry</i> – Attempt to delete the circuit again.</p>
<p><b>Standard PVC</b> – 2nd switch unreachable (lower-numbered node)</p> <p><b>Redirect PVC</b> – Primary or Secondary switch unreachable</p>	<p>The SNMP request timed out (2nd [or Primary or Secondary] endpoint identified).</p>	<p><i>Abort</i> – 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.</p> <p><i>Ignore</i> – 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 endpoint cards marked out-of-sync). PRAM sync of endpoint cards will delete circuit on switches.</p> <p><i>Retry</i> – Attempt to delete the circuit again, which now will not be able to succeed completely.</p> <p><i>Note:</i> <i>Retry process starts with 1st (or Pivot) switch, which has a deleted circuit that results in an error message. See the next table row for more information.</i></p>

**Table A-3. Errors Encountered During Circuit Delete Procedure (Continued)**

Type of Failure	SNMP Set Failure Reason	Available Choices
<p><b>Standard PVC</b> – Circuit not present on 1st switch (higher-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on Pivot switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (Specific endpoint not identified).</p>	<p><i>Abort</i> – Discontinue attempt to delete circuit (NMS database, switches, and out-of-sync status unmodified).</p> <p><i>Ignore</i> – Discontinue attempt to delete circuit, but delete the circuit from the NMS database (circuit not deleted on 1st [or Pivot] switch or 2nd [or Primary or Secondary] endpoint. (Error condition would also occur if circuit was never present.) Both circuit endpoint cards marked out-of-sync. PRAM sync cards delete circuits on switches.</p> <p><i>Retry</i> – Attempt to delete the circuit again.</p>
<p><b>Standard PVC</b> – Circuit not present on 2nd switch (higher-numbered node)</p> <p><b>Redirect PVC</b> – Circuit not present on Primary or Secondary switch</p>	<p>There is no such variable name in this MIB; possibly the card is down or not present (Specific endpoint not identified).</p>	<p><i>Abort</i> – 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.</p> <p><i>Ignore</i> – 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] endpoint card marked out-of-sync. PRAM sync of endpoint cards will delete circuits on switches.</p> <p><i>Retry</i> – Attempt to delete the circuit again, which will not be able to succeed completely.</p>



# 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 Frame Relay SVC or ATM SVC/Offnet circuit connections across Lucent network switches.

This appendix contains:

- [“About OSPF Name Aggregation” on page B-1](#)
- [“Using OSPF Name Aggregation” on page B-2](#)
- [“Network Hierarchical Addressing Plans” on page B-4](#)
- [“Monitoring Network OSPF Name Activity” on page B-6](#)

## 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, ICD). The OSPF also treats 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.

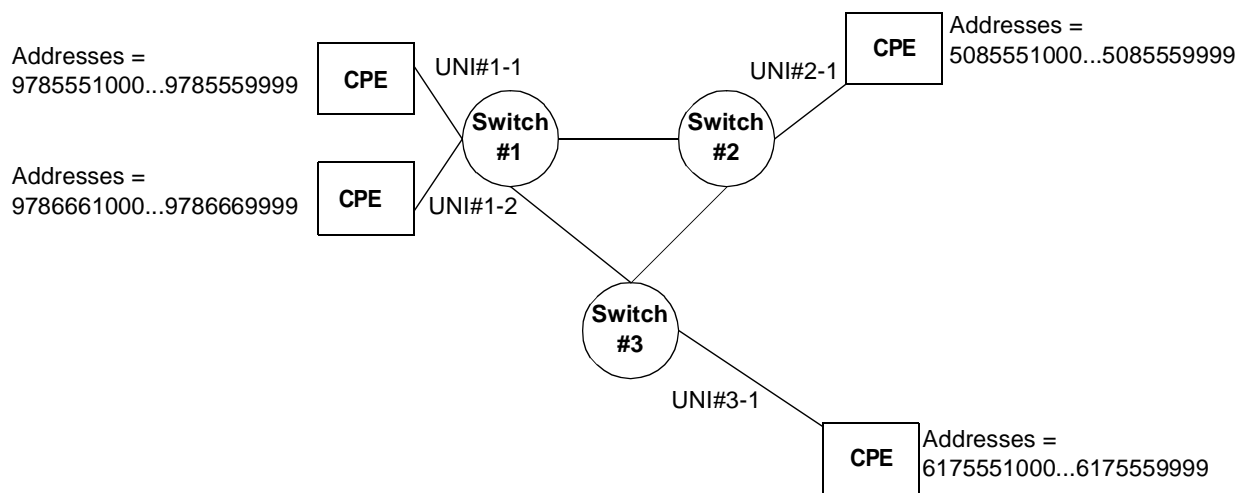
---

## 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 B-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 B-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 (e.g., switches or routers) that supports SVCs (or SPVCs). **Table B-2** shows the addresses that require routing in the sample network shown in **Figure B-1**.

**Table B-2. 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 (e.g., X.121, DCC, ICD).

In the sample network, assume that one thousand port addresses are possible on the CPE UNI#1-1, and all of these addresses start with 978555. Provisioning all one thousand 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 one thousand 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 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 B-1](#)), 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 B-1](#)), 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

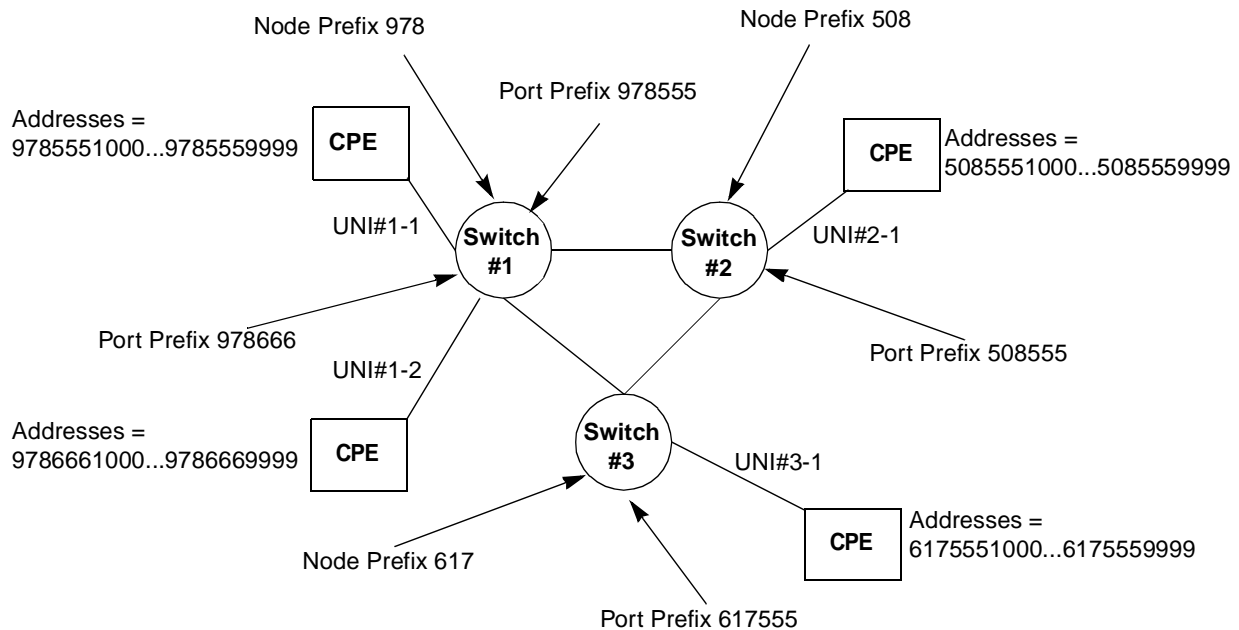
Using OSPF name aggregation in conjunction with a network *hierarchical addressing plan* can reduce memory consumption by minimizing the number of OSPF names required for provisioning addresses. This section summarizes some important hierarchical addressing concepts used in both voice and data networks 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 B-1](#), suppose that addresses for both CPE at UNI#1-1 and CPE at UNI#3 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 B-3 enhances the network scenario in Figure B-1 to show a hierarchical addressing plan that uses the E.164 public network addressing standard. (Any addressing standard would work the same way.)



**Figure B-3. Sample Network Showing Port and Network Prefixes**

Assume that 1,000 addresses are possible at each of the switches in Figure B-3. 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 name 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 B-3 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 B-3). 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 Navis EMS-CBGX to view this information, but the process is more difficult.) Refer to the *B-STDX, CBX, and GX Console Command User's Reference* for more information about console commands.

### 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 following 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, and 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 code 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
<b>2</b>	<b>0x00000000</b>	<b>0</b>	<b>N/A</b>	<b>978/24</b>	<b>250.1/0</b>
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 B-3](#), 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 the card in slot 3 of CBX 500 switch #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
<b>addr</b> s	<b>68868</b>	<b>98384</b>	<b>96</b>	<b>1024</b>	<b>113</b>

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.



# Priority Routing

This appendix provides guidelines for using Priority routing, which enables you to prioritize virtual circuits (PVCs and SVCs) in your network.

This appendix contains:

- [“About Priority Routing” on page C-1](#)
- [“Routing Priority Rules” on page C-4](#)
- [“Priority Routing and Path Cost” on page C-5](#)

## 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.

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 after the QoS class is established. Keep in mind that you must assign a higher priority to real time QoS classes.

## 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 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; 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 indicates the highest priority. For PVCs, the default value is 0; 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 [“User Preference Attributes for PVCs and Redirect PVCs” on page 7-21](#) for more information about configuring these options.

## Using Restricted Priority Routing

Restricted priority routing works in the following additional 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 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 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 C-4](#) for details about path selection.

## Interoperability with Previous Releases

To use circuit-routing priority in your network, the following interoperability restrictions apply:

- All switch software must be at least Release 04.01.00.00 or higher for B-STDX switches.
- On a trunk, if either end resides on a 04.01.00.00 B-STDX switch, the trunk treats all PVCs equally (assumes all have a 0,0 priority).

On a circuit, if either end belongs to a 04.01.00.00 B-STDX switch, the circuit is automatically assigned a 0,0 priority. The NMS does not support any routing priority other than 0,0 on switches running Release 04.01.00.00 or lower.

## Priority Routing and Path Cost

By assigning specific bandwidth priority and bumping eligibility to Frame Relay 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 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. 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, bumping eligibility enabled) circuits. As a result, some 2, Enabled priority 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 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 will reestablish 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.

## Customer Names

This appendix provides guidelines for using Customer Names, an optional software feature that enables network providers to assign Frame Relay logical ports to a specific customer so that they can then use the customer name as a filter when viewing logical ports.

This appendix contains:

- [“Adding Customer Names” on page D-1](#)
- [“Associating a Logical Port with a Customer Name” on page D-3](#)

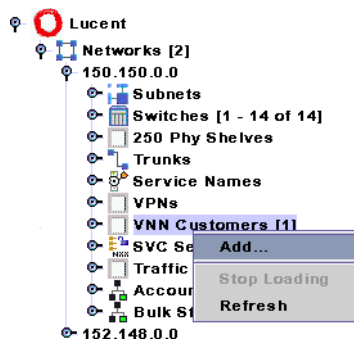
You can configure the Customer Names feature with or without the use of a virtual private network (VPN). For more information on using Customer Names with VPNs, see [Chapter 10, “Configuring Layer2 Virtual Private Networks \(VPNs\).”](#)

## Adding Customer Names

To add customer names:

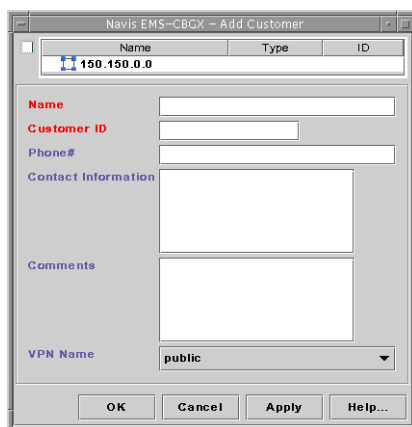
1. In the Networks tab, expand the network you are managing.
2. Expand the VNN Customers node.

3. Right-click on the VNN Customers node and click Add, as shown in [Figure D-1](#).



**Figure D-1. Adding a VNN Customer**

The Add Customer dialog box ([Figure D-2](#)) is displayed.



**Figure D-2. Add Customer Dialog Box**

4. Enter a customer Name.
5. Assign a value from 1 to 65535 for the Customer ID.
6. (*Optional*) Enter the phone number, contact name, and any additional comments.
7. Make sure the VPN Name defaults to Public.
8. Click OK.

## Associating a Logical Port with a Customer Name

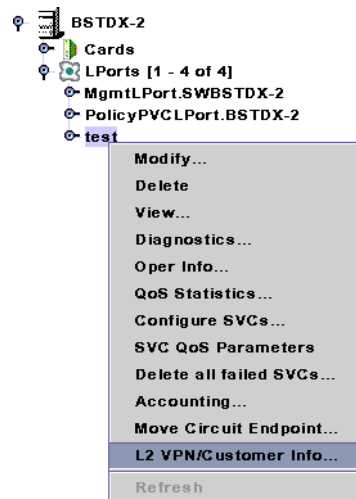
For specific information about configuring logical ports, see [Chapter 3, “Configuring Frame Relay LPorts.”](#)

After you configure a logical port, use the following steps to associate it with a customer name:



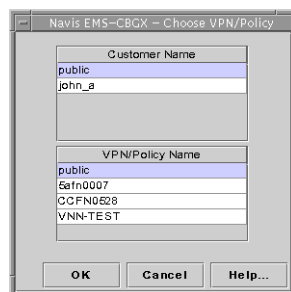
**Note** – Changing the Customer Name does not admin down the logical port.

1. In the Switch tab, expand the LPorts node and right-click on the logical port you want to assign.
2. Click L2 VPN / Customer Info on the popup menu, as shown in [Figure 4-3](#).



**Figure 4-3.** Assigning a Logical Port to a Layer 2 VPN / Customer Name

The Choose VPN / Policy dialog box ([Figure 4-4](#)) is displayed.



**Figure 4-4.** Choose VPN / Policy Dialog Box

3. From the list of customer names, select the name you want to assign to this LPort.

## Customer Names

### Using the Layer2 Customer/VPN View Feature

---

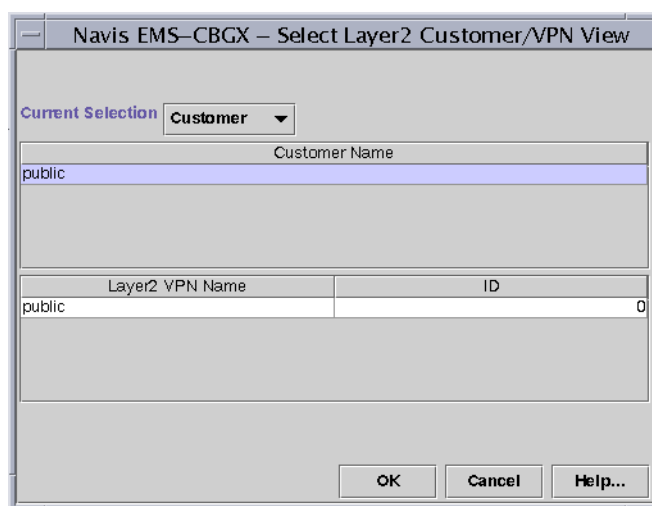
4. From the list of VPN/Policy names, select the name you want to assign to this LPort.
5. Click OK.

## Using the Layer2 Customer/VPN View Feature

The Layer2 Customer/VPN View feature enables a network 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 Customer/VPN View:

1. Right-click on the instance node of the network to which you want to assign a Layer2 VPN and customer name.
2. Select L2 VPN/Customer Info from the popup menu. The Select Layer2 Customer VPN View dialog box ([Figure D-5](#)) is displayed.



**Figure D-5. Select Layer2 Customer VPN View Dialog Box**

3. Use the Current Selection button to select Customer.
4. Select the customer name.
5. Choose OK.



# Abbreviations and Acronyms

This section lists abbreviations for units of measure (in specifications) and for terms and acronyms used in Lucent documentation. Refer also to the *Master Glossary*, which provides definitions for many of these terms.

This appendix contains:

- “Abbreviations” on page -1
- “Acronyms” on page -3

## Abbreviations

The following table lists some of the abbreviations used in documentation and product specifications.

Abbreviation	Meaning
Bc	Committed Burst Size
Be	Excess Burst Size
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)

## Acronyms

---

Abbreviation	Meaning
in.	inch(es)
k	kilo (1,000)
KB	kilobyte(s)
Kbps	kilobits per second
kg	kilogram
kHz	kilohertz
MB	megabyte(s)
Mbps	million bits per second
MHz	megahertz
min.	minute(s)
modem	modulator/demodulator
msec	millisecond
Pm	percent reduction for mild
Ps	percent reduction for severe
usec	microsecond (abbreviate with lowercase "u" for micro)
sec	second
Tc	time interval
vs.	versus
#	number; pound
x	by (multiplication)
>	greater than
<	less than
=	equal to

## Acronyms

The following table lists some of the acronyms used in this guide.

Acronym	Description
AESA	ATM End System Address
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Exchange
ASE	Autonomous System External
ASR	Application Specific Route
ATM	Asynchronous Transfer Mode
ATM UNI	ATM User Network Interface
BACP	Bandwidth Allocation Control Protocol
BECN	Backward Explicit Congestion Notification
BW	Bandwidth
CAC	Connection Admission Control
CCITT	Consultative Committee for International Telegraph and Telephone
CHAP	Challenge Handshake Authentication Control
CFR	Constant Frame Rate
CIC	Carrier Identification Code
CIR	Committed Information Rate
CLLM	Consolidated Link Layer Management
CP	Control Processor
CPE	Customer Premise Equipment
CRC	Cyclic Redundancy Check
CSR	Customer Specific Route
CSU	Channel Service Unit
CUG	Closed User Group
DCC	Data Country Code
DCE	Data Communications Equipment

## Acronyms

---

Acronym	Description
DE	Discard Eligibility
DLCI	Data Link Connection Identifier
DNIC	Data Network Identification Code
DS0	Digital Signal Level 0 (64 kbps)
DS1	Digital Signal Level 1 (1.544 Mbps)
DS3	Digital Signal Level 3 (44.7326 Mbps)
DTE	Data Terminal Equipment
EBW	Equivalent Bandwidth
EPD	Early Packet Discard
ESI	End System Identifier
EVC	Ethernet Virtual Circuit
FCP	Flow Control Processor
FECN	Forward Explicit Congestion Notification
FIFO	First In First Out
FR	Frame Relay
FRAD	Frame Relay Assembler/Disassembler
FTP	File Transfer Protocol
HDLC	High-level Data Link Control
HSSI	High Speed Serial Interface
IA	Incoming Access
ICB	Incoming Calls Barred
ICD	International Code Designator
IDN	International Data Numbers
ILMI	Interim Local Management Interface
IOM	Input/Output Module
IOP	Input/Output Processor
IP	Internet Protocol

Acronym	Description
ISO	International Standards Organization
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	ITU Telecommunication Standardization Sector (formerly CCITT)
IXC	Inter-exchange Carrier
KA	Keep Alive
LAN	Local Area Network
LCP	Link Control Protocol
LMI	Local Management Interface
LSP	Label Switched Path
LSU	Link State Update
LTP	Link Trunk Protocol
MBS	Maximum Burst Size
MFRU	Multilink Frame Relay Unit
MIB	Management Information Base
MLFR	Multilink Frame Relay
ML Member	Multilink Member
MLPPP	Multilink Point-to-Point Protocol
MPVC	Management Permanent Virtual Circuit
MRRU	Maximum Receive Reconstructed Unit
NAK	Negative Acknowledgment
NCP	Network Control Protocol
NIC	Network Interface Card
NMS	Network Management Station
NNI	Network-to-Network Interface
NPC	Network Parameter Control
NSAP	Network Service Access Point

## Acronyms

---

Acronym	Description
OA	Outgoing Access
OC	Optical Carrier
OCB	Outgoing Calls Barred
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PDN	Public Data Network
PDU	Protocol Data Unit
PNNI	Private Network-to-Network Interface
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
RBOC	Regional Bell Operating Company
RFC	Request for Comments
RIL	Remote Ignore Local
RLMI	Resilient Local Management Interface
SDLC	Synchronous Data Link Control
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
SP	Switch Processor
SPVC	Soft Permanent Virtual Circuit
SVC	Switched Virtual Circuit
TAC	Technical Assistance Center
TCP	Transmission Control Protocol
TD	Traffic Descriptor
TNS	Transit Network Selection
TS0	Telecom Signal Level

Acronym	Description
UFR	Unspecified Frame Rate
UIO	Universal Input/Output
UNI	User-to-Network Interface
VC	Virtual Circuit
VCI	Virtual Channel Identifier
VFR-RT/NRT	Variable Frame Rate-Real Time/Non-Real Time
VLAN	Virtual LAN
VNN	Virtual Network Navigator
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network





# Index

## A

Accounting Attributes, 8-24

Add, 4-13

Add Offnet Circuit

Accounting Tab Fields, 8-24

Administrative Tab Fields, 8-10

FRF.5 Tab Fields, 8-29

Path Tab Fields, 8-27

Traffic Type Tab Fields, 8-14, 8-16

User Preference Tab Fields, 8-20

Adding

fault-tolerant PVC circuit connections, 7-13

VPN customers, 10-5

Address

Custom AESA, 14-3

Data Country Code AESA, 14-2

E.164, 14-2, 15-2, 16-2

E.164 AESA, 14-3

International Code Designator AESA, 14-3

node prefix, 14-7

port prefix, 14-11

SVC port address format, 3-53

X.121, 14-2, 15-2, 16-2

Admin status

for logical ports, 3-13

for PVCs, 7-15, 7-35

Administrative

cost

circuits, 9-8

described, 4-1, 4-3

for SVC add network IDs, 14-21

for SVC port addresses, 14-18

for SVCs node prefixes, 14-10

routing metric, 2-25

threshold, 7-16, 7-36

tasks

deleting circuits, 2-28, 7-50

deleting logical ports, 2-28

deleting management or multicast DLCIs, 2-30

deleting trunks, 2-29

moving circuits, 7-43

using templates, 2-25

Amber frames, 2-5 to 2-7, 7-7

ANSI T1.617 Annex D

for frame relay, 3-34

ASE. *See* Autonomous system external

Assigning

DS0 channels, 3-18

DS0s to T1 logical ports, 3-18

port security screens, 16-10

TS0 channels, 3-18

Associate Policy Constraint to Circuit PVC, 7-10

Associate Policy Constraint to Circuit Redirect  
PVC, 7-32

Attributes

for authenticating PPP ports, 3-62

for logical ports, 3-5 to 3-7, 3-7 to 3-9, 3-11 to  
3-41

for PVCs, 7-13 to 7-28

Authentication attributes

for PPP ports, 3-62

PAP/CHAP option, 3-63

RADIUS server, [3-63](#)  
Auto detect, [3-34](#)  
Automatic trunk backup, [4-16](#)  
Autonomous system external, [11-10](#)

## B

Backup ports  
  activating fault-tolerant PVCs, [12-4](#)  
  creating, [12-4](#)  
Backup trunks, [4-5](#), [4-16](#)  
Backward explicit congestion notification (BECN), [2-5](#), [2-22](#), [2-23](#), [3-25](#)  
Bad PVC factor, [2-6](#), [2-7](#), [3-26](#)  
Bandwidth (BW)  
  allocating for QoS service classes, [3-32](#)  
  allocation control for PPP, [3-65](#)  
  defined BW for non-MLFR trunks, [4-11](#)  
  defining the trunk oversubscription factor, [4-2](#)  
  determining the available virtual bandwidth, [4-2](#)  
Bc. *See* Committed burst size (Bc)  
Be. *See* Excess burst size (Be)  
BECN. *See* Backward explicit congestion notification  
Binding ML Member logical ports, [5-14](#)  
Bulk Statistics. *See* Selectable Statistics attributes

## C

Call screening  
  for SVCs, [3-54](#)  
Calling Party  
  Screen Mode, [3-54](#)  
card attributes, [7-2](#), [9-2](#)  
CBX  
  modules  
    Channelized T1/E1 FR/IP, [2-13](#), [2-15](#), [3-19](#)  
    DS3 Frame, [2-9](#), [2-10](#), [3-16](#)  
    DS3/1, [2-8](#), [2-10](#), [7-41](#)  
    DS3/1/0, [2-8](#), [2-10](#), [2-26](#), [7-41](#)  
    forwarding engine support, [7-40](#)  
    multicast DLCI member limits, [7-40](#)  
    Subrate DS3 Frame, [2-9](#), [2-10](#), [7-40](#)

CCITT Q.933 Annex A  
  for frame relay logical ports, [3-34](#)  
Cell Loss Priority, [9-18](#)  
Channelized T1/E1 FR/IP modules  
  for CBX, [2-13](#)  
Channelized T1/E1 FR/IP modules (CBX)  
  congestion thresholds  
    about, [2-13](#)  
    default mono-class, [2-15](#)  
    default multi-class, [2-15](#)  
    maximum mono-class, [2-15](#)  
    maximum multi-class, [2-15](#)  
E1 mode  
  assigning channels to logical ports, [3-19](#)  
  logical ports  
    assigning channels, [3-19](#)  
  support  
    for SVCs, [14-6](#)  
T1 mode  
  assigning channels to logical ports, [3-19](#)  
Channels  
  assigning to logical ports  
    on CBX Channelized T1/E1 FR/IP modules, [3-19](#)  
Check interval, [3-26](#)  
CIR. *See* Committed information rate  
Circuit  
  priority, [7-19](#)  
Circuit path  
  manually defining, [8-27](#) to [8-28](#), [9-20](#)  
Circuits  
  configuring  
    fault-tolerant PVCs, [12-1](#)  
    priority routing, [7-24](#)  
    PVC endpoints, [7-11](#)  
    redirect PVCs, [7-30](#)  
    traffic type attributes, [7-18](#)  
  defining circuit connections, [7-9](#)  
  deleting, [7-50](#)  
  endpoint rules for, [7-3](#)  
  manually defining the path, [7-28](#) to [7-30](#)  
  moving, [7-43](#)  
  templates, [7-48](#)  
  with Multilink Frame Relay endpoint, [5-26](#)  
Clear delay, [3-26](#)

- 
- CLLM. *See* Consolidated Link Layer Management
  - Closed user groups (CUGs)
    - configuring, 15-6
    - defined, 15-1
    - defining
      - for a switch, 15-8 to 15-10
      - members, 15-6 to 15-8
    - member address, 15-2
    - SVCs
      - port addresses, 14-18
      - port prefixes, 14-13
  - Closed-loop congestion control
    - overview, 2-5
  - Committed burst size (Bc), 3-26, 7-6, 7-7, 7-19
  - Committed information rate (CIR)
    - available bandwidth, 4-2, 4-3
    - rate enforcement, 7-6
    - SVC maximum traffic descriptors, 3-48
    - traffic type attributes, 7-19, 7-20
    - trunk oversubscription factor, 4-2, 4-10
    - Zero CIR Enabled (Fwd/Rev), 7-19
  - configure a new port address, 8-9
  - configure Offnet Circuit parameters, 8-10
  - configure PVC or PVP termination, 8-3
  - Configuring
    - Authentication attributes, 3-62
    - bandwidth, 3-16
    - closed user groups, 15-6
    - fault-tolerant PVCs, 12-1
    - logical ports for SVCs, 3-42
    - management
      - DLCIs, 11-7
      - PVCs, 11-2
    - multicast DLCIs, 7-39
    - Multilink Frame Relay UNI/NNI, 5-1
    - Multilink MLPPP, 6-1
    - network management traffic, 4-11
    - node prefixes, 14-7
    - OPTimum trunking, 3-58
    - port addresses, 14-16
    - PVCs, 7-1
    - rate enforcement scheme, 7-20
    - redirect PVCs, 7-30
    - Reliable Scalable Circuit, 7-2
    - RLMI, 13-2
    - SVCs, 14-1
    - trunks, 4-1
    - Virtual Private Networks, 10-3
  - configuring Shapers, 9-1
  - configuring the 2-Port Gigabit Ethernet module, 9-1
  - Congestion
    - explicit, 2-22
    - implicit, 2-22
    - states, 2-5
    - thresholds
      - CLLM threshold states, 2-23
      - for logical ports, 2-7
  - Congestion control
    - closed-loop, 2-5
    - congestion states, 2-5
    - default threshold parameters
      - for ATM modules, 2-10
      - for Chan DS3 modules, 2-10
      - for Chan T1/E1 FR/IP modules (CBX), 2-15
      - for DSX modules, 2-10
      - for HSSI modules, 2-10
      - for UIO modules, 2-10
      - for Unchan T1/E1 modules, 2-10
    - link state updates (LSUs), 2-6
    - monitoring, 3-26
    - overview, 2-5
    - setting attributes, 3-24
    - TAQL, 2-17
    - threshold parameters, 2-7
    - WRED, 2-18
  - Consolidated Link Layer Management (CLLM)
    - Admin State, 3-25
    - congestion notification, 2-22
    - defined, 2-22
    - DLCI address (1007), 2-22
    - Interval, 3-25
    - messages, 2-23
    - threshold states, 2-23
    - Thrhld Mild percent, 3-25
    - Thrhld None percent, 3-25
  - Creating
    - backup ports, 12-4
    - trunk names, 4-10
  - CUGs. *See* Closed user groups
-

- Custom AESA, [14-3](#)
- Customer Names
  - customer view feature, [D-4](#)
- Customer names, [D-1](#)
  - adding to a VPN, [10-5](#)
  - associating with logical port, [D-3](#)
  - for VPN, [10-2](#)
  - viewing, [10-1](#), [10-8](#)
- Cyclic redundancy check (CRC), [2-3](#), [3-16](#)
  
- D**
- Data communications equipment (DCE)
  - logical port
    - error threshold, [3-35](#), [3-37](#)
    - event count, [3-35](#), [3-37](#)
    - poll verify timer, [3-35](#)
- Data Link Connection Identifier, [8-2](#), [9-7](#)
- Data link connection identifier (DLCI)
  - defined, [7-8](#)
  - for OPTimum trunk ports, [3-58](#), [3-59](#), [7-8](#)
  - SVC start and stop limits, [3-56](#)
- DCC, [14-2](#)
- DCE. *See* Data communications equipment
- Default route
  - for port prefixes, [14-15](#)
- Define Path dialog box, [8-27](#)
- Defining
  - Authentication attributes, [3-62](#)
  - circuit connections, [7-9](#)
  - CUG members, [15-6](#)
  - CUGs, [15-8](#) to [15-10](#)
  - default routes for network-to-network connections, [14-15](#)
  - E1 trunk logical ports not supported, [3-58](#)
  - Encapsulation FRAD, Direct Line Trunk, and PPP logical ports, [3-60](#)
  - graceful discard, [7-21](#)
  - multicast DLCIs, [7-39](#) to [7-42](#)
  - Multilink Frame Relay (MLFR) trunks, [3-65](#)
  - node prefixes, [14-7](#)
  - OSPF trunk administrative cost, [4-3](#)
  - service name bindings, [12-2](#)
  - SVCs
    - for Frame Relay, [14-1](#)
    - trunk oversubscription factor, [4-2](#)
    - UNI DCE/DTE or NNI logical ports, [3-10](#)
- defining the physical ports, [7-2](#), [9-2](#)
- Deleting
  - logical ports, [2-28](#)
- Differential delay, [5-6](#)
- Direct line trunk, [2-3](#)
- DLCI, [8-2](#), [9-7](#)
- DLCI. *See* Data link connection identifier
- DS0 channels
  - assigning to frame relay logical ports, [3-18](#)
- DS3 modules
  - CRC checking, [3-16](#)
  - default threshold values, [2-10](#)
  - for CBX, [2-9](#), [2-10](#)
    - Subrate, [2-9](#)
  - mono-class service thresholds, [2-8](#)
  - moving circuits, [7-43](#)
  - support
    - for MLFR, [3-66](#)
    - for PPP, [3-60](#)
    - for SVCs, [14-6](#)
- DS3/1 modules, [2-8](#), [2-10](#)
  - for CBX, [7-41](#)
- DS3/1/0 modules
  - default threshold values, [2-10](#)
  - for CBX, [2-8](#), [7-41](#)
  - logical port templates, [2-26](#)
  - mono-class service thresholds, [2-8](#)
  - Release 4.4 switch software requirement, [2-9](#)
  - support for PPP, [3-60](#)
- Dynamic Delay
  - for operational trunks, [4-13](#)
- Dynamic delay, [4-4](#)
  
- E**
- E.164 address format, [14-2](#), [15-2](#), [16-2](#)
- E.164 AESA, [14-3](#)
- E1 logical ports
  - assigning TS0 channels, [3-18](#)
  - congestion control threshold, [3-25](#)
  - defining trunk logical ports not supported, [3-58](#)

- 
- QoS
    - class of service, [2-24](#)
    - configuration guidelines, [2-24](#)
    - support
      - for MLFR, [3-66](#)
  - E1 modules (B-STDx)
    - default
      - mono- and multi-class thresholds, [2-12](#)
    - support
      - for SVCs, [14-6](#)
  - Encapsulation FRAD, [2-3](#)
    - defining logical ports, [3-60](#)
    - logical port endpoints for circuits, [7-12](#)
    - one circuit supported per logical port, [7-43](#)
  - Encapsulation Mode, [9-18](#)
  - End-to-End Delay
    - for PVC routing, [9-8](#)
  - End-to-end delay
    - QoS routing metric, [3-32](#)
    - threshold for PVC routing, [7-16](#), [7-36](#)
    - trunk administrative cost, [4-3](#)
    - used with static delay, [4-12](#)
  - Ethernet Average Frame Size, [9-18](#)
  - Ethernet logical ports
    - configuration prerequisites, [9-2](#)
  - Ethernet Virtual Circuit, [9-7](#)
  - EVC, [9-7](#)
  - Excess burst size (Be), [2-5](#), [2-6](#), [3-26](#), [7-6](#), [7-7](#), [7-20](#)
- F**
- Failure trap threshold
    - for SVCs, [3-44](#)
  - Fault-tolerant PVCs
    - activating a backup port, [12-4](#)
    - configuration sequence, [12-1](#)
    - configuring
      - logical ports for, [12-1](#)
    - defining the service name bindings, [12-2](#)
    - for UNI-DCE logical ports, [3-14](#)
    - overview, [2-4](#)
  - Features
    - new in this release, [1-x](#)
  - FECN. *See* Forward explicit congestion notification
  - FIFO blocks. *See* First In First Out (FIFO) Blocks
  - First In First Out (FIFO) Blocks, [3-71](#) to [3-75](#)
  - Forward explicit congestion notification (FECN), [2-5](#), [2-22](#)
  - Forwarding engine support
    - on CBX modules, [7-40](#)
  - Frame Relay
    - address formats, [14-2](#)
    - Implementation Agreements
      - FRF.10 (NNI SVCs), [13-3](#)
      - FRF.4 (SVCs), [13-2](#)
    - NNI, [2-3](#)
    - node prefixes, [14-7](#)
    - OPTimum PVC trunk, [2-3](#), [3-58](#)
    - OSPF Area ID, [14-9](#)
    - QoS for SVCs, [3-42](#)
  - Frame Relay and Gigabit Ethernet, [9-7](#)
  - Frame Relay Forum (FRF)
    - FRF.16, [5-2](#)
  - FRF.10 Implementation Agreement, [13-3](#)
  - FRF.4 Implementation Agreement, [13-2](#), [14-5](#)
  - FRF.5 Attributes, [8-29](#)
- G**
- Gigabit Ethernet and Frame Relay, [9-7](#)
  - Gigabit Ethernet Parameters, [9-18](#)
  - Graceful discard, [7-7](#)
    - defining for Frame Relay circuits, [7-21](#)
  - Green frames
    - congested and ingress switch behavior, [2-6](#)
    - rate enforcement and discard policy, [7-7](#)
- H**
- how to define an Ethernet Virtual Circuit, [7-1](#), [9-1](#)
- I**
- ICD, [14-3](#)
-

identifies a circuit, [9-7](#)  
identify the logical end points of a virtual circuit,  
[9-7](#)

Internet Protocol (IP)  
  host, [11-1](#)  
  IP-based management plane, [11-2](#)

## K

KA. *See* Keep-alive (KA)  
Keep-alive (KA)  
  control frames, [4-3](#)  
  measuring trunk delay, [4-4](#)  
  threshold, [4-4](#), [4-11](#)

## L

Least OSPF delay, [9-8](#)  
Link Management Interface (LMI)  
  DLCI number range for LMI Rev1, [7-8](#)  
  for RLMI, [13-2](#)  
  LMI Rev1 for Frame Relay logical ports, [3-34](#),  
    [3-58](#), [13-2](#)  
  NNI and UNI-DCE logical ports, [2-3](#)  
  poll errors, [3-35](#), [3-37](#)  
  Update Delay, [3-36](#)  
Link management protocol  
  DLCI number guidelines, [3-58](#)  
  for frame relay logical ports, [3-34](#)  
  setting attributes, [3-34](#)  
Link state update (LSU)  
  for congestion control, [2-6](#)  
Link trunk protocol, [4-3](#)  
LMI, [9-7](#)  
LMI. *See* Link Management Interface  
Load balancing  
  for SVCs, [3-44](#)  
Logical ports  
  accessing functions, [3-2](#)  
  configuring fault-tolerant PVCs, [12-1](#)  
  configuring RLMI, [13-1](#), [13-2](#)  
  deleting, [2-28](#)  
  direct line trunk, [2-3](#)

  encapsulation FRAD, [2-3](#)  
  ML Member, [2-4](#), [3-65](#), [3-66](#), [3-69](#)  
  Multilink Frame Relay UNI/NNI bundles, [5-8](#)  
  NNI, [2-3](#)  
  non-disruptive attributes, [2-27](#)  
  OPTimum PVC trunk, [2-3](#), [3-58](#)  
  overview, [2-2](#) to [2-4](#)  
  PPP according to RFC 1490, [2-4](#)  
  selecting a logical port type, [3-5](#), [3-6](#)  
  setting  
    QoS parameters, [2-24](#), [3-31](#) to [3-33](#)  
  types of, [2-2](#), [2-4](#), [3-6](#)  
  UNI-DCE, [2-2](#), [3-5](#) to [3-7](#), [3-7](#) to [3-9](#), [3-10](#) to  
    [3-59](#)  
  UNI-DTE, [2-2](#)  
Loopback status  
  for PVCs, [7-22](#)  
LSU. *See* Link state update

## M

Management DLCIs  
  defined, [11-2](#)  
  defining, [11-7](#) to [11-8](#)  
  loopback, [7-35](#)  
Management PVC  
  circuit priority, [7-19](#)  
  defined, [11-1](#)  
  redirect PVCs, [11-1](#)  
  using, [11-2](#)  
Management traffic  
  using trunks, [4-11](#)  
Maximum burst size (MBS)  
  PVCs, [8-19](#)  
MBS, *see* maximum burst size  
Member limits  
  for multicast DLCIs, [7-39](#)  
Minimum Cell Rate (MCR)  
  traffic descriptor type, [8-19](#)  
Minimum-hop paths, [4-3](#)  
ML Member logical ports, [2-4](#), [3-65](#), [3-66](#), [3-69](#)  
  binding and unbinding, [5-14](#)  
Moving  
  circuits, [7-43](#)

circuits for DS3 modules, 7-43

Multicast DLCIs

- defining, 7-39 to 7-42
- member limits for, 7-39
- overview, 7-39 to 7-40

Multilink Frame Relay

- circuits, 5-26
- configuring logical port for Layer2 VPN and customer, 5-25

MLFR trunks

- defining, 3-65
- ML Member logical ports, 3-66
- modifying logical port members, 5-23

UNI/NNI bundle logical ports

- about, 5-2
- accessing attributes and functions, 5-18

UNI/NNI ML Member logical ports

- binding and unbinding, 5-14

## N

Net overflow, 3-14

- configuring
- for circuits, 9-9

Network management communications

- configuring specific trunks, 4-11

Node prefixes

- configuring, 14-7

Non-disruptive attributes

- trunks, 4-5, 4-15

Non-Disruptive Logical Port and Trunk Attributes, 2-27

## O

Offnet circuit, 8-1

Open Shortest Path First (OSPF)

- area ID, 14-9
- bypassing on PVCs, 7-28 to 7-30, 8-27 to 8-28, 9-20
- defining trunk administrative cost, 4-3
- link state update, 2-6
- monitoring name activity, B-6

- name aggregation, B-1
- network hierarchical addressing plans, B-4
- routing circuits, 7-30, 8-28
- routing SVCs, 14-9, 14-13, 14-21

OPTimum trunking

- configuring for Frame Relay, 3-58
- for Frame Relay, 2-5

originating endpoint, 8-2

Overload Severity, 7-6

Oversubscription factor

- described, 4-2
- displaying, 4-10
- percentage, 3-33

Oversubscription of QoS, 3-33

## P

Path Attributes, 8-27

PCR, *see* peak cell rate

Peak cell rate (PCR)

- PVCs, 8-19

Permanent virtual circuit (PVC)

- administrative cost, 9-8
- bypassing OSPF, 7-28 to 7-30, 8-27 to 8-28, 9-20
- manually defining circuit path, 7-28 to 7-30, 8-27 to 8-28, 9-20
- MBS, 8-19
- MCR, 8-19
- PCR, 8-19
- routing with end-to-end delay, 9-8
- SCR, 8-19

Permanent Virtual Circuits (PVCs). *See* Circuits

PNNI routing protocol

- enabling, 8-3

PNNI. *See* Private Network-to-Network Interface

point-to-point Frame Relay SPVCs, 8-5

Point-to-Point Protocol (PPP)

- according to RFC 1490, 2-4, 3-60, 11-3
- defining Authentication attributes, 3-62

Port prefixes

- defining a default route, 14-15

Port security screening

- assigning screens, 16-10 to 16-12



- defined, [16-2](#)
  - egress screen mode, [16-3](#)
  - sample configuration, [16-5](#)
  - screen addresses, [16-4](#)
  - PPP. *See* Point-to-Point Protocol
  - Priority Frame
    - multi-class service thresholds, [2-7](#)
    - QoS, [2-7](#), [2-24](#)
    - setting
      - attributes, [3-29](#), [3-34](#)
      - SVC QoS parameters, [3-46](#)
      - Traffic Type attributes, [7-19](#)
  - Priority routing, [C-1](#) to [C-6](#)
    - configuring PVCs, [7-24](#)
    - configuring SVCs, [3-45](#)
    - interoperability with previous releases, [C-5](#)
  - Private Network-to-Network Interface (PNNI), [7-28](#), [14-10](#), [14-13](#), [14-14](#), [14-18](#), [14-19](#)
  - Private network-to-network interface (PNNI)
    - suppress PNNI advertisement, [14-10](#)
  - PVC, [7-1](#)
  - PVC Establishment Rate Control, [7-4](#)
    - with VC Overload Control disabled, [7-5](#)
    - with VC Overload Control enabled, [7-5](#)
- ## Q
- QoS
    - setting
      - attributes, [3-31](#)
  - QoS. *See* Quality of Service
  - Quality of Service (QoS)
    - Priority Frame, [2-7](#), [2-24](#)
    - service descriptions, [2-24](#)
    - setting
      - logical port QoS parameters, [3-31](#)
      - SVC QoS parameters, [3-46](#)
      - Traffic Type attributes, [7-19](#)
- ## R
- Rate enforcement, [7-6](#)
  - Rate enforcement scheme
    - configuring, [7-20](#)
  - Red frames
    - congested and ingress switch behavior, [2-6](#)
    - discard congestion thresholds, [2-5](#)
    - Graceful Discard, [7-7](#)
      - percent for Graceful Discard, [7-22](#)
      - rate enforcement and discard policy, [7-7](#)
  - Redirect PVC
    - configuring, [7-30](#)
    - Delay Timer, [7-38](#)
    - management PVC, [11-1](#)
    - Reliable Scalable Circuit, [7-2](#)
  - Reliable Scalable Circuit
    - configuring standard and redirect PVCs, [7-2](#)
    - disabling, [7-3](#)
    - error messages, [A-1](#)
  - Reroute balance
    - enabling, [7-24](#)
  - Resilient Link Management Interface (RLMI)
    - configuration sequence, [13-4](#)
    - configuring logical ports for, [13-1](#), [13-2](#)
    - fields
      - Can Backup Service Names, [3-14](#)
      - LPort Type, [3-10](#), [13-5](#)
      - RLMI Admin Status, [3-36](#)
      - RLMI Max Full Status Attempts, [3-36](#)
    - FRF.4 support, [13-2](#)
    - Link Mgmt Protocol, [3-34](#)
  - Resilient LMI PVCs
    - overview, [2-4](#)
  - restarting an offnet circuit, [8-30](#)
  - RFC 1490, [2-4](#), [3-60](#), [11-3](#)
  - RLMI. *See* Resilient Link Management Interface
  - Routing
    - metrics
      - administrative cost, [3-32](#)
      - end-to-end delay, [3-32](#)
- ## S
- Scope
    - PNNI domain, [14-10](#), [14-14](#), [14-19](#)
    - select an endpoint from a physical port, [8-7](#)
    - select an endpoint from a switch, [8-6](#)



- 
- Service name bindings
    - activating a backup binding port, 12-4
    - defining, 12-2
  - set the card attributes of Ethernet, 9-2
  - Setting
    - Congestion Control attributes, 3-24
    - Link Management attributes, 3-34
    - logical port net overflow, 3-14
    - logical port QoS parameters, 3-31
    - Priority Frame attributes, 3-29, 3-34
    - QoS attributes, 3-31
    - QoS Parameters, 2-24
    - Traffic Type attributes, 7-19
    - Trap Control attributes, 3-40
  - shaper, 9-13
  - Shaper ID, 9-13
  - Shaper Priority, 9-13
  - Signaling parameters, 3-43
  - Simple Network Management Protocol (SNMP)
    - designating trunks for, 4-11
    - Reliable Scalable Circuit, 7-2
    - using trunks for management traffic, 4-11
  - SNMP. *See* Simple Network Management Protocol
  - SPVC Frame Relay Module Support, 8-2
  - Static ARP entry
    - defining, 7-33
  - Static Delay, 4-4
    - used with end-to-end delay, 4-12
  - Subrate DS3 Frame modules
    - for CBX, 2-10, 7-40
  - Sustainable cell rate (SCR)
    - PVCs, 8-19
  - SVC terminating endpoint address, 8-8
  - SVCs. *See* Switched Virtual Circuits
  - Switched virtual circuits (SVC)
    - configuring
      - priority routing, 3-45
  - Switched virtual circuits (SVCs)
    - address formats, 14-2
    - attributes
      - priorities, 3-45
    - configuring, 14-1 to 14-21
      - logical ports for SVCs, 3-42 to 3-56
      - node prefixes, 14-7
    - CUG port addresses, 14-18
    - CUG port prefixes, 14-13
    - default network-to-network connections, 14-15
    - defining call screening, 3-54
    - DLCI start and stop limits, 3-56
    - failure trap threshold, 3-44
    - load balancing, 3-44
    - node prefixes, 14-7
    - OSPF Area ID, 14-9
    - overview, 14-1
    - QoS, 3-42
    - QoS parameters, 3-46
    - routing determination, 14-3
- ## T
- T1 logical ports
    - assigning DS0s, 3-18
    - congestion control threshold, 3-25
    - defining trunk logical ports not supported, 3-58
    - QoS
      - class of service, 2-24
      - configuration guidelines, 2-24
    - support
      - for MLFR, 3-66
  - T1 modules (B-STDx)
    - default
      - mono-class thresholds, 2-11
      - multi-class thresholds, 2-11
    - maximum
      - mono-service class thresholds, 2-8
    - support
      - for SVCs, 14-6
  - TAQL, 2-17
  - target select type, 8-4
  - Technical, xv
  - Templates
    - for circuits, 7-15, 7-35, 7-48
    - for Frame Relay logical ports, 2-25
  - terminating endpoints, 8-2
  - Thresholds
    - congestion, 2-7
  - Traffic Type Attributes, 8-14
  - Traffic type attributes
    - for PVCs, 7-18
-

Trap Control  
  setting  
    attributes, 3-40

Trap Control attributes  
  for logical ports, 3-40

Trunks  
  administrative cost, 4-3  
  automatic backup, 4-16  
  backup, 4-5, 4-16  
  configuring, 4-6 to 4-16  
  direct line trunk services, 3-60  
  direct trunks, 2-3  
  displaying  
    oversubscription factor, 4-10  
  excluding SMDS traffic, 4-11  
  for network management communications, 4-11  
  LMI Update Delay, 3-36  
  logical ports for Frame Relay, 2-5  
  managing traffic, 4-3  
  monitoring trunk congestion on the port, 3-26  
  Multilink Frame Relay, 3-65, 5-8  
  Net Overflow for managing SVC traffic, 3-14  
  non-disruptive attributes, 2-27, 4-5, 4-15  
  OPTimum PVC trunk logical ports, 2-2, 3-58  
  oversubscription factor, 4-2  
  overview, 4-1 to 4-3  
  Static and Dynamic Delay, 4-4  
  types of, 4-10

TSO channels  
  for frame relay logical ports, 3-18

Tuning  
  enabling circuits to use, 7-24

## U

Unbinding ML Member logical ports, 5-14

UNI-DCE  
  for Frame Relay, 2-2, 3-5 to 3-7, 3-7 to 3-9, 3-10 to 3-59

UNI-DTE  
  for Frame Relay, 2-2

Unspecified frame rate (UFR), 2-24, 2-25, 3-30, 3-44, 7-19

User Preference Attributes, 8-20

User Preference attributes  
  for PVCs, 7-21

## V

Variable frame rate non-real time (VFR-NRT), 2-8, 2-12, 2-24, 3-24, 3-30, 3-44, 3-47, 7-19

Variable frame rate real-time (VFR-RT), 2-24, 3-44, 3-47, 7-19

VC Overload Control, 7-5 to 7-6  
  PVC Establishment Rate Control, 7-4

Virtual Private Networks (VPNs)  
  adding customers, 10-6  
  configuring, 10-1, 10-3  
  overview, 10-1

VLANs, 9-1

VPN. *See* Virtual Private Networks (VPNs)

## W

WRED, 2-18

## X

X.121 address format, 14-2, 15-2, 16-2

# Frame Relay Services Configuration Guide for CBX 3500, CBX 500, and B-STDX 9000


## 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!


**EMAIL:** cspubs@lucent.com


**MAILING ADDRESS:**

Lucent Technologies  
Data Networking Group  
1 Robbins Road  
Westford, MA 01886


 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. \_\_\_\_\_

Cut Here 