

# Network Administrator's Guide

## SA 100 / SA 600 / SA 1200

*Ascend Communications, Inc.*

Product Code: 80084  
Revision 00  
September 1998

---

Copyright © 1998 Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.

---

## ASCEND COMMUNICATIONS, INC. END-USER LICENSE AGREEMENT

ASCEND COMMUNICATIONS, INC. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE AND ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE “PROGRAM”) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE SOFTWARE, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. OPENING THE PACKAGE(S) OR USING THE ASCEND SWITCH(ES) CONTAINING THE PROGRAM WILL INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, ASCEND IS UNWILLING TO LICENSE THE PROGRAM TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE PROGRAM WITHIN TEN (10) DAYS FROM SHIPMENT TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR LICENSE FEE WILL BE REFUNDED. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND ASCEND, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

**1. License Grant.** Ascend hereby grants to you, and you accept, a non-exclusive, non-transferable license to use the computer software, including all patches, error corrections, updates and revisions thereto in machine-readable, object code form only (the “Software”), and the accompanying User Documentation, only as authorized in this License Agreement. The Software may be used only on a single computer owned, leased, or otherwise controlled by you; or in the event of inoperability of that computer, on a backup computer selected by you. You agree that you will not pledge, lease, rent, or share your rights under this License Agreement, and that you will not, without Ascend’s prior written consent, assign or transfer your rights hereunder. You agree that you may not modify, reverse assemble, reverse compile, or otherwise translate the Software or permit a third party to do so. You may make one copy of the Software and User Documentation for backup purposes. Any such copies of the Software or the User Documentation shall include Ascend’s copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by you or any person under your authority or control.

**2. Ascend’s Rights.** You agree that the Software and the User Documentation are proprietary, confidential products of Ascend or Ascend's licensor protected under US copyright law and you will use your best efforts to maintain their confidentiality. You further acknowledge and agree that all right, title and interest in and to the Program, including associated intellectual property rights, are and shall remain with Ascend or Ascend's licensor. This License Agreement does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License Agreement.

---

**3. License Fees.** The license fees paid by you are paid in consideration of the license granted under this License Agreement.

**4. Term.** This License Agreement is effective upon your opening of the package(s) or use of the switch(es) containing Software and shall continue until terminated. You may terminate this License Agreement at any time by returning the Program and all copies or portions thereof to Ascend. Ascend may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Ascend, you agree to return to Ascend the Program and all copies or portions thereof. Termination of this License Agreement shall not prejudice Ascend's rights to damages or any other available remedy.

**5. Limited Warranty.** Ascend warrants, for your benefit alone, for a period of 90 days from the date of shipment of the Program by Ascend (the "Warranty Period") that the program diskettes in which the Software is contained are free from defects in material and workmanship. Ascend further warrants, for your benefit alone, that during the Warranty Period the Program shall operate substantially in accordance with the User Documentation. If during the Warranty Period, a defect in the Program appears, you may return the Program to the party from which the Program was acquired for either replacement or, if so elected by such party, refund of amounts paid by you under this License Agreement. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Ascend of any warranties made under this Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM IS LICENSED "AS IS", AND ASCEND DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES OF NONINFRINGEMENT.

**6. Limitation of Liability.** Ascend's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the greater of: (i) ten thousand US dollars (\$10,000) or (ii) the total license fee paid to Ascend for the use of the Program. In no event shall Ascend be liable for any indirect, incidental, consequential, special, punitive or exemplary damages or lost profits, even if Ascend has been advised of the possibility of such damages.

---

**7. Proprietary Rights Indemnification.** Ascend shall at its expense defend you against and, subject to the limitations set forth elsewhere herein, pay all costs and damages made in settlement or awarded against you resulting from a claim that the Program as supplied by Ascend infringes a United States copyright or a United States patent, or misappropriates a United States trade secret, provided that you: (a) provide prompt written notice of any such claim, (b) allow Ascend to direct the defense and settlement of the claim, and (c) provide Ascend with the authority, information, and assistance that Ascend deems reasonably necessary for the defense and settlement of the claim. You shall not consent to any judgment or decree or do any other act in compromise of any such claim without first obtaining Ascend's written consent. In any action based on such a claim, Ascend may, at its sole option, either: (1) obtain for you the right to continue using the Program, (2) replace or modify the Program to avoid the claim, or (3) if neither (1) nor (2) can reasonably be effected by Ascend, terminate the license granted hereunder and give you a prorata refund of the license fee paid for such Program, calculated on the basis of straight-line depreciation over a five-year useful life. Notwithstanding the preceding sentence, Ascend will have no liability for any infringement or misappropriation claim of any kind if such claim is based on: (i) the use of other than the current unaltered release of the Program and Ascend has provided or offers to provide such release to you for its then current license fee, or (ii) use or combination of the Program with programs or data not supplied or approved by Ascend to the extent such use or combination caused the claim.

**8. Export Control.** You agree not to export or disclose to anyone except a United States national any portion of the Program supplied by Ascend without first obtaining the required permits or licenses to do so from the US Office of Export Administration, and any other appropriate government agency.

**9. Governing Law.** This License Agreement shall be construed and governed in accordance with the laws and under the jurisdiction of the Commonwealth of Massachusetts, USA. Any dispute arising out of this Agreement shall be referred to an arbitration proceeding in Boston, Massachusetts, USA by the American Arbitration Association.

**10. Miscellaneous.** If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorneys' fees and expenses of arbitration. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

# Contents

## About This Guide

What You Need to Know.....	xxv
Reading Path .....	xxvi
How to Use This Guide.....	xxvii
Related Documents .....	xxviii
Ascend.....	xxviii
Third Party.....	xxviii
Customer Comments.....	xxviii
Customer Support .....	xxviii
Conventions .....	xxix

## Chapter 1

### Overview

About the SA Units.....	1-2
SA 100 Broadband Service Unit .....	1-3
SA 600 Broadband Service Concentrator .....	1-4
SA 1200 Broadband Service Concentrator .....	1-5
Interface Control Module .....	1-6
Protocol Option Devices .....	1-6
Management and Configuration of SA Units .....	1-7
WebXtend Management Software .....	1-7
Cost-effective Platform Independence.....	1-8
Secure Access .....	1-9
Theory of Operation.....	1-10
Connections .....	1-11
ATM Traffic .....	1-16
Non-ATM Service Types.....	1-20
Advanced Topics .....	1-24
Connection Admission Control .....	1-24
About VPI and VCI Ranges .....	1-25
Enabling PVPs by Setting a Port's VPI Range .....	1-26
How the SA units manage bandwidth.....	1-27
Cell Buffering in the SA Units .....	1-33
Congestion Thresholds and Congestion Actions .....	1-36
Traffic Policing Details.....	1-37

## Chapter 2

### Getting Started

Powering Up the SA 100 .....	2-2
Powering Up the SA 600 .....	2-3
Powering Up the SA 1200 .....	2-4
Changing the IP address.....	2-6
Accessing WebXtend.....	2-8
WebXtend Conventions .....	2-11
Navigating Buttons and Fields .....	2-11
Clicking vs. Double-Clicking.....	2-12
OK, Cancel, and Apply Buttons.....	2-12
Events/Alarms Field and Button .....	2-12
Window Buttons.....	2-12
Command Buttons.....	2-12
Help Field .....	2-13
WebXtend Screen Hierarchy .....	2-14
Understanding the Program Flow.....	2-14
Understanding the Screens .....	2-15
Common Screen Fields .....	2-16
Logging Off WebXtend .....	2-18
Shutting Down an SA Unit .....	2-18
What's Next? .....	2-19

## Chapter 3

### Configuring the System

Accessing System Administration Functions .....	3-2
Setting System Security.....	3-5
Setting System Timing .....	3-8
Specifying IP Routes .....	3-11
Modifying, Deleting, or Connecting IP Routes .....	3-13
Specifying ILMI Node Prefixes .....	3-14
About ILMI Node Prefixes .....	3-15
Modifying or Deleting ILMI Node Prefixes.....	3-18
Specifying ASPVC Addresses .....	3-19
Configuring Power Supplies on SA 600 and SA 1200 Units.....	3-21
Configuring Connection Admission Control Parameters.....	3-22
Configuring Switch Fabric CAC .....	3-22
Configuring Priority Queues.....	3-26
Configuring Cell Highway VPI/VCI Ranges .....	3-28
What's Next? .....	3-30

## Chapter 4

### Configuring Ports

Accessing Interface Management Functions.....	4-2
Selecting an ICM.....	4-3
Selecting a Port.....	4-7
Configuring an Ethernet Port.....	4-9
Configuring a DS1 or E1 Port.....	4-11
Setting Short-Haul/Long-Haul Equalization .....	4-19
Configuring a DS3/E3 Port.....	4-21

Trail Trace (E3 only) .....	4-27
Far End Alarm and Control (D3 with C-bit framing only) .....	4-28
Configuring an OC-3c/STM-1 Port .....	4-30
Configuring OC-3c/STM-1 Port Advanced Options .....	4-36
Configuring a Path for an OC-3c/STM-1 Port .....	4-38
Configuring a Path for an OC-3c/STM-1 Port - Advanced Options .....	4-41
Configuring Port-level CAC .....	4-43
Configuring the ATM Interface .....	4-46
About Signaling Protocols, User/Network Side, and ILMI .....	4-50
Setting ILMI Port Prefixes .....	4-52
About ILMI Prefixes .....	4-52
Modifying or Deleting ILMI Port Prefixes .....	4-54
Configuring a Universal Serial Port .....	4-55
What's Next? .....	4-60

## Chapter 5

### Configuring Network Services and Connections

Selecting a Network Service and Managing Connections .....	5-2
Setting up Connections .....	5-7
Alternate Methods of Selecting a Network Service .....	5-9
About Connections and Dial Types .....	5-10
Switched Connections and Trunks .....	5-10
PVP Dial Type .....	5-12
PVC Orig Dial Type .....	5-12
A-SPVC Dial Type .....	5-13
SPVC Dial Type .....	5-14
Dial-Type Addressing Formats Summary .....	5-16
Connection Setup Examples .....	5-17
Example 1: PVP .....	5-17
Example 2: PVC (CES to ATM) .....	5-20
Example 3: PVC (ATM to ATM) .....	5-22
Example 4: A-SPVC .....	5-24
Example 5: SPVC .....	5-31
Configuring ATM UNI Services and Connections .....	5-33
Configuring ATM UNI Connections .....	5-37
Adding a Connection .....	5-38
Modifying a Connection .....	5-44
Enabling and Disabling a Connection .....	5-44
Deleting a Connection .....	5-45
Configuring Inverse Multiplex (IMA) Services .....	5-46
Configuring IMA Links .....	5-53
Modifying an IMA Group .....	5-54
Viewing IMA Group Statistics .....	5-55
Viewing IMA Link Statistics .....	5-60
Configuring Native LAN Services .....	5-64
Adding an NLS Group .....	5-65
Modifying an NLS Group .....	5-68
Deleting an NLS Group .....	5-68
Creating Tunnels for an NLS Group .....	5-69



Modifying an NLS Tunnel .....	5-76
Enabling and Disabling an NLS Tunnel.....	5-76
Deleting an NLS Tunnel.....	5-77
Viewing MAC Address Cache Information.....	5-78
Defining Static MAC Addresses.....	5-80
Deleting Static MAC Addresses.....	5-82
Configuring Circuit Emulation Services.....	5-83
Configuring CES Interworking Functions.....	5-88
Adding a CES-IWF Connection.....	5-89
Configuring Dynamic Bandwidth Allocation.....	5-96
Modifying a CES-IWF Connection.....	5-99
Enabling and Disabling a Connection.....	5-100
Deleting a CES-IWF Connection.....	5-101
Configuring Universal Serial Frame Service.....	5-102
Configuring USF Interworking Functions.....	5-106
Adding a USF-IWF Connection.....	5-107
Modifying a USF-IWF Connection.....	5-114
Enabling and Disabling a Connection.....	5-115
Deleting a USF-IWF Connection.....	5-116
Configuring Voice Compression Service .....	5-117
Configuring VCS Interworking Functions.....	5-121
Adding a VCS-IWF Connection .....	5-122
Modifying a VCS-IWF Connection .....	5-127
Enabling and Disabling a Connection.....	5-128
Deleting a VCS-IWF Connection.....	5-128
Setting VCS Compression Options .....	5-129
Configuring VCS Timeslots .....	5-131
What's Next? .....	5-134

## Chapter 6      **Monitoring an SA Unit**

Accessing Monitoring Functions .....	6-2
ICM Front Panel Indicators .....	6-4
SUM Front Panel Indicators (SA 600 and SA 1200 only) .....	6-5
Monitoring System-Level Status .....	6-6
Viewing Power Supply Status Information (SA 600 and SA 1200 only) .....	6-9
Viewing System Utility Module (SUM) Status Information (SA 600 and SA 1200 only) .....	6-11
Viewing System Inventory Information.....	6-11
Viewing System MIB Statistics .....	6-12
Monitoring a Slot .....	6-13
Viewing Microprocessor Utilization.....	6-17
Viewing Slot Inventory Information .....	6-19
Viewing Slot Cell Highway Statistics.....	6-22
Viewing CAC Bandwidth Statistics .....	6-25
Viewing Protocol Accelerator Statistics.....	6-26
Viewing ATM File Check Information.....	6-27
Monitoring PODs.....	6-29
POD Front Panel Indicators .....	6-29

Accessing POD Status Windows .....	6-36
Viewing POD Inventory Information.....	6-38
Viewing POD Cell Highway Statistics .....	6-39
Monitoring Ports .....	6-40
Monitoring Ethernet Ports .....	6-41
Monitoring DS1/E1 Ports.....	6-43
Viewing Performance Statistics for an Interval.....	6-47
Viewing Alarms and Defects on DS1/E1 Ports .....	6-50
Viewing the Status of Transmission Convergence on DS1/E1 Cell Ports.....	6-53
Viewing CES-IWF Statistics .....	6-54
Monitoring DS3/E3 Ports.....	6-55
Viewing Performance Statistics for an Interval on DS3/E3 Ports .....	6-62
Viewing Alarms and Defects on DS3/E3 Ports .....	6-62
Monitoring OC-3c/STM-1 Ports .....	6-66
Viewing Interval Performance Statistics on OC-3c/STM-1 Ports.....	6-70
Viewing Alarms and Defects on OC-3c/STM-1 Ports .....	6-70
Viewing Path Statistics on OC-3c/STM-1 Ports.....	6-73
Viewing Interval Performance Statistics on OC-3c/STM-1 Paths .....	6-77
Monitoring Universal Serial Ports.....	6-78
Monitoring the ATM Layer .....	6-80
Viewing ATM Status Information on DS1/E1 Cell Ports .....	6-81
Viewing ATM Layer Statistics on DS3/E3 Ports .....	6-81
Viewing ATM Status Information on OC-3c/STM-1 Paths.....	6-81
Monitoring Connections .....	6-84
Monitoring ATM-UNI Connections .....	6-87
Viewing CAC Statistics.....	6-90
Viewing Statistics on Individual ATM-UNI Connections .....	6-93
Monitoring IMA Connections: Group and Link Statistics.....	6-97
Monitoring NLS Connections .....	6-98
Monitoring CES-IWF Connections.....	6-101
Monitoring Universal Serial Frame Connections.....	6-103
Monitoring Voice Compression Service Connections .....	6-105
Viewing VCS Port Statistics .....	6-107
Viewing Connection Statistics.....	6-108
Viewing ATM Connection Statistics .....	6-110
Viewing Interworking Function Statistics.....	6-115
Viewing NLS Group Status Information.....	6-116
Viewing CES-IWF Statistics .....	6-118
Viewing USF-IWF statistics .....	6-121
Viewing VCS-IWF statistics .....	6-124
What's Next? .....	6-127

**Chapter 7      Managing Events**

Displaying the Events/Alarms Log.....	7-2
Viewing Details of Individual Events/Alarms .....	7-4
Managing Events and Traps.....	7-5
Generating Event Files (not supported).....	7-7
Filtering Events and Alarms.....	7-8
Filtering Traps.....	7-10
What's Next? .....	7-13

**Chapter 8      Testing an SA Unit**

Accessing Diagnostics Functions .....	8-2
Testing Cell Highways .....	8-3
Testing with Port Loopbacks.....	8-7
Testing DS1/E1 Ports.....	8-8
Testing DS3/E3 Ports.....	8-10
Testing OC-3c/STM-1 Ports .....	8-12
Testing Universal Serial Ports .....	8-14
Inserting Intentional Errors .....	8-15
Inserting Errors to Test a Port .....	8-15
Inserting Errors to Test an OC-3c/STM-1 Path.....	8-15
What's Next? .....	8-16

**Chapter 9      Using Utilities**

Accessing SA Utilities .....	9-2
Saving Configurations.....	9-4
Initializing the System.....	9-5
Shutting Down the System .....	9-5
Exiting to the Shell .....	9-5
Transferring Files with Zmodem.....	9-5
What's Next? .....	9-6

**Chapter 10     Resolving Problems**

Technical Support Checklist.....	10-2
Contacting the Technical Assistance Center.....	10-2
Phone .....	10-2
E-mail and Fax .....	10-2

**Appendix A    Using the Craft Interface**

Setting up the VT100 Terminal .....	A-2
About the SA Unit's Boot Sequence .....	A-3
About the Craft Interface .....	A-4
Accessing the Craft Interface.....	A-6
Craft Interface Conventions.....	A-7
Navigating Buttons and Fields .....	A-7
Activating Pull-down Menus.....	A-7
OK vs. Cancel vs. Apply Buttons.....	A-8
Events/Alarms Button/Field .....	A-8

Help Field .....	A-8
Using the Craft-Only Functions .....	A-9
Transferring Files with Zmodem .....	A-9
Accessing Zmodem from the Utilities Window .....	A-10
Accessing the SA Unit's Operating System Shell .....	A-11
Accessing OASOS .....	A-11

## Appendix B      Operating System (OASOS) Command Set

OASOS Commands .....	B-2
CAT .....	B-3
CD .....	B-4
CLEAR .....	B-5
CMP .....	B-6
CP .....	B-7
DATE .....	B-9
ECHO .....	B-10
HEAD .....	B-11
HELP .....	B-12
KILL .....	B-13
LS .....	B-14
MKDIR .....	B-16
MV .....	B-17
PING .....	B-18
PWD .....	B-19
REBOOT .....	B-20
RMDIR .....	B-21
RZ .....	B-22
SA_CFG .....	B-23
SA_CORIP .....	B-24
SA_EXEC .....	B-26
SA_FLASH .....	B-27
SA_FLOG .....	B-28
SA_IPLOG .....	B-29
SA_LNBS .....	B-30
SA_RLOG .....	B-31
SA_ROUTE .....	B-32
SA_WANIP .....	B-33
SYNC .....	B-35
SZ .....	B-36
TELNET .....	B-37
TOUCH .....	B-38
UPGRADE .....	B-39

## Appendix C      Using FTP to Transfer Files

Using FTP to Transfer Files .....	C-2
Using FTP to Back Up Configuration Data .....	C-2
Using FTP to Restore Configuration Data .....	C-2

<b>Appendix D</b>	<b>Upgrading the SA Unit's Software</b>	
	About the Release Notes .....	D-2
	Backing Up and Restoring Configuration Data .....	D-2
<b>Appendix E</b>	<b>Downloading the Enterprise MIB</b>	
	Accessing the Ascend FTP Site .....	E-2
<b>Appendix F</b>	<b>NavisCore Integration</b>	
	Downloading the Java Runtime Environment .....	F-2
	Downloading the Sahara.tar File.....	F-3
	Sahara.tar Contents.....	F-3
	Unpacking the Sahara.tar File.....	F-4
	Installing the Navis WebXtend Files .....	F-5
	Verifying the Navis WebXtend Installation .....	F-5
	Uninstalling the Navis WebXtend Files .....	F-6
<b>Appendix G</b>	<b>Managing SA Units Remotely</b>	
	Setting up a Connection to a Remote SA Unit .....	G-2
	Preparing an SA unit for remote management .....	G-3
	Creating the connection from local to remote .....	G-4
<b>Appendix H</b>	<b>Acronyms</b>	
	<b>Glossary</b>	
	<b>Index</b>	

# List of Figures

Figure 1-1.	SA Products Consolidating Traffic onto a WAN .....	1-2
Figure 1-2.	SA 100 Broadband Service Unit.....	1-3
Figure 1-3.	SA 600 Broadband Service Concentrator.....	1-4
Figure 1-4.	SA 1200 Broadband Service Concentrator.....	1-5
Figure 1-5.	WebXtend Web-based Management .....	1-8
Figure 1-6.	SA-family high-level theory of operation.....	1-10
Figure 1-7.	Traffic flow through an ICM .....	1-11
Figure 1-8.	Cell Highways .....	1-12
Figure 1-9.	PVP/PVC-based connection between two SA units.....	1-13
Figure 1-10.	AS-PVC-based connection between two SA units.....	1-14
Figure 1-11.	S-PVC-based connection.....	1-14
Figure 1-12.	ATM traffic through an ICM from IPOD to XPOD.....	1-17
Figure 1-13.	Priority Queuing .....	1-18
Figure 1-14.	Non-ATM traffic through an SA unit.....	1-20
Figure 1-15.	CES traffic through an SA unit.....	1-22
Figure 1-16.	Voice Compression Service traffic through an SA unit .....	1-23
Figure 1-17.	Bandwidth Accounting - Example 1.....	1-27
Figure 1-18.	Bandwidth Accounting - Example 2.....	1-28
Figure 1-19.	Priority queue cell buffers and oversubscription.....	1-35
Figure 2-1.	SA 100 Rear Panel (AC power shown).....	2-2
Figure 2-2.	SA 100 Status Indicators .....	2-2
Figure 2-3.	SA 600 Power Switch(es).....	2-3
Figure 2-4.	SA 600 Status Indicators .....	2-3
Figure 2-5.	SA 1200 Power Switch(es).....	2-4
Figure 2-6.	SA 1200 Status Indicators .....	2-5
Figure 2-7.	Log On Window .....	2-8
Figure 2-8.	Main Menu.....	2-9
Figure 2-9.	WebXtend Screen Hierarchy Example.....	2-14
Figure 2-10.	Typical WebXtend Window .....	2-15
Figure 2-11.	Logoff Window .....	2-18
Figure 3-1.	System Administration Window.....	3-2
Figure 3-2.	System Security Window .....	3-5
Figure 3-3.	Add Operator Window .....	3-6
Figure 3-4.	System Security Options Window.....	3-6
Figure 3-5.	System Timing Window .....	3-8
Figure 3-6.	IP Routes Window .....	3-11
Figure 3-7.	Add IP Route Window.....	3-12
Figure 3-8.	IP Route Options Window.....	3-13
Figure 3-9.	Connection Management Window .....	3-13
Figure 3-10.	ILMI Process – DTE mode.....	3-15
Figure 3-11.	ILMI Node Prefix Table Window .....	3-16
Figure 3-12.	Add Node Prefix Window .....	3-16
Figure 3-13.	Node Prefix Options Window .....	3-18
Figure 3-14.	ASPVC Address Configuration Window .....	3-19

Figure 3-15.	Configure Power Supply Units Window .....	3-21
Figure 3-16.	Switch Fabric CAC Configuration Window.....	3-22
Figure 3-17.	VC Buffer Configuration Window .....	3-24
Figure 3-18.	Priority Queue Configuration Window .....	3-26
Figure 3-19.	Cell Highway Configuration Window.....	3-28
Figure 4-1.	Interface Management Window (SA 600 shown) .....	4-2
Figure 4-2.	Configure System Window.....	4-3
Figure 4-3.	Configure ICM Window .....	4-5
Figure 4-4.	Configure POD Window .....	4-7
Figure 4-5.	Configure Ethernet Port Window .....	4-9
Figure 4-6.	Configure DS1/E1 Port Window (DS1 shown).....	4-11
Figure 4-7.	DS1/E1 POD Port Loopbacks .....	4-16
Figure 4-8.	Equalization Short Haul and Long Haul Windows .....	4-19
Figure 4-9.	Configure DS3 Port Window.....	4-21
Figure 4-10.	Configure E3 Port Window .....	4-22
Figure 4-11.	DS3/E3 POD Loopbacks .....	4-25
Figure 4-12.	Trail Trace Window.....	4-27
Figure 4-13.	Far End Alarm and Control Window.....	4-28
Figure 4-14.	Configure OC-3/STM-1 Port Window .....	4-30
Figure 4-15.	OC-3c/STM-1 POD Loopbacks .....	4-34
Figure 4-16.	Configure OC-3/STM-1 Port (Advanced) Window .....	4-36
Figure 4-17.	Configure OC-3/STM-1 Path Window.....	4-38
Figure 4-18.	Configure OC-3/STM-1 Path (Advanced) Window.....	4-41
Figure 4-19.	Port CAC Configure Window .....	4-44
Figure 4-20.	Configure ATM Interface Window .....	4-46
Figure 4-21.	ILMI Port Prefix Table Window .....	4-53
Figure 4-22.	Add Port Prefix Window .....	4-53
Figure 4-23.	Port Prefix Options window .....	4-54
Figure 4-24.	Configure Universal Serial Port Window.....	4-55
Figure 4-25.	Universal Serial POD Port Loopbacks .....	4-59
Figure 5-1.	Select Service Window.....	5-2
Figure 5-2.	Select Port Window (ATM UNI shown).....	5-2
Figure 5-3.	Connections Window (ATM UNI shown) .....	5-3
Figure 5-4.	Connection Options Window Example (ATM UNI shown) .....	5-4
Figure 5-5.	Connection Setup and Mirroring Example .....	5-7
Figure 5-6.	Connection Options Example .....	5-8
Figure 5-7.	Traditional PVP/PVC vs Switched Connections .....	5-11
Figure 5-8.	ASPVC Address Configuration – Default Primary Trunk .....	5-11
Figure 5-9.	PVP Dial Type.....	5-12
Figure 5-10.	Traditional PVC Dial Type.....	5-12
Figure 5-11.	A-SPVC Dial Type.....	5-13
Figure 5-12.	SPVC Dial Type .....	5-14
Figure 5-13.	PVP Connection Required.....	5-17
Figure 5-14.	PVP Connection Setup Procedure .....	5-18
Figure 5-15.	PVP Connection Setup Results.....	5-19
Figure 5-16.	IWF/PVC Connection Required.....	5-20
Figure 5-17.	PVC Connection Setup Procedure.....	5-21
Figure 5-18.	PVC Connection Setup Results .....	5-21

Figure 5-19.	ATM-UNI PVC Connection Required .....	5-22
Figure 5-20.	ATM-UNI PVC Connection Setup Procedure .....	5-23
Figure 5-21.	ATM-UNI PVC Connection Setup Results .....	5-23
Figure 5-22.	A-SPVC Remote-side Connection Setup – ASPVC Address Configuration .....	5-24
Figure 5-23.	A-SPVC Remote-side Connection Setup – SAP Configuration....	5-25
Figure 5-24.	A-SPVC Remote-side Connection Setup – Selecting the CES Port.....	5-26
Figure 5-25.	A-SPVC Remote-side Connection Setup – Interworking function .....	5-27
Figure 5-26.	A-SPVC Originating-side Connection Setup – ASPVC Address Configuration .....	5-28
Figure 5-27.	A-SPVC Originating-side Connection Setup – SAP Configuration.....	5-29
Figure 5-28.	A-SPVC Originating-side Connection Setup – Interworking function .....	5-30
Figure 5-29.	SPVC Remote-side Connection Setup.....	5-32
Figure 5-30.	Select ATM UNI Port Window .....	5-33
Figure 5-31.	ATM UNI Connections Window.....	5-34
Figure 5-32.	Add/Modify ATM UNI Connection Window .....	5-38
Figure 5-33.	Connection Options - ATM-UNI.....	5-44
Figure 5-34.	Connection Management Window .....	5-45
Figure 5-35.	Delete Connection Window.....	5-45
Figure 5-36.	IMA Operation Example .....	5-46
Figure 5-37.	IMA Frame Synchronization Process .....	5-47
Figure 5-38.	Select IMA POD Window .....	5-47
Figure 5-39.	Configure POD Window .....	5-48
Figure 5-40.	IMA Groups Window .....	5-48
Figure 5-41.	Add/Modify IMA Group Window.....	5-49
Figure 5-42.	Configure IMA Link Window .....	5-53
Figure 5-43.	IMA Group Options Window .....	5-54
Figure 5-44.	IMA Group Statistics Window .....	5-55
Figure 5-45.	Select IMA Link Window .....	5-60
Figure 5-46.	IMA Link Statistics Window.....	5-60
Figure 5-47.	Native LAN Service (NLS) Groups Window.....	5-64
Figure 5-48.	Add NLS Groups Window .....	5-65
Figure 5-49.	NLS Group Options Window .....	5-68
Figure 5-50.	NLS Tunnels Window .....	5-69
Figure 5-51.	Add/Modify NLS Tunnel Window.....	5-70
Figure 5-52.	Connection Options Window (NLS Tunnel).....	5-76
Figure 5-53.	Connection Management Window .....	5-77
Figure 5-54.	MAC Address Cache Window .....	5-78
Figure 5-55.	Static MAC Adresses Window.....	5-80
Figure 5-56.	Add Static MAC Address Window .....	5-81
Figure 5-57.	Static MAC Address Options Window.....	5-82
Figure 5-58.	Select CES Port Window.....	5-83
Figure 5-59.	Configure CES Connection Window.....	5-84
Figure 5-60.	Add/Modify Unstructured CES-IWF Window (DS1 shown) .....	5-89



Figure 5-61.	Add/Modify Structured DS1 CES-IWF Window.....	5-90
Figure 5-62.	Conditioning Window .....	5-94
Figure 5-63.	Dynamic Bandwidth Window. ....	5-97
Figure 5-64.	Connection Options Window (CES-IWF).....	5-99
Figure 5-65.	Connection Management Window .....	5-100
Figure 5-66.	Select USF Port Window.....	5-102
Figure 5-67.	Configure USF Connection Window.....	5-103
Figure 5-68.	Add/Modify USF IWF Window.....	5-107
Figure 5-69.	Connection Options Window (USF-IWF).....	5-114
Figure 5-70.	Connection Management Window .....	5-115
Figure 5-71.	Select VCS Port Window .....	5-117
Figure 5-72.	Configure VCS Connection Window .....	5-118
Figure 5-73.	Add/Modify VCS-IWF Window .....	5-122
Figure 5-74.	Connection Options Window (VCS-IWF) .....	5-127
Figure 5-75.	Connection Management Window .....	5-128
Figure 5-76.	VCS Compression Window.....	5-129
Figure 5-77.	Add/Modify DS1 Timeslot Window .....	5-132
Figure 6-1.	Monitor Status Window – SA 100.....	6-2
Figure 6-2.	Monitor Status Window – SA 600.....	6-2
Figure 6-3.	Monitor Status Window – SA 1200.....	6-3
Figure 6-4.	Display System Status Window.....	6-6
Figure 6-5.	Power Supply Status Window (SA 600 shown).....	6-9
Figure 6-6.	System Inventory Statistics (SA 600 shown) .....	6-11
Figure 6-7.	MIB II Statistics Window .....	6-12
Figure 6-8.	Display ICM Status Window.....	6-14
Figure 6-9.	Processor Utilization Window .....	6-17
Figure 6-10.	Board Inventory Statistics Window.....	6-19
Figure 6-11.	Select Cell Highway(s) Window .....	6-22
Figure 6-12.	Cell Highway/Priority Queue Stats Window.....	6-23
Figure 6-13.	CAC Bandwidth Stats Window .....	6-25
Figure 6-14.	Protocol Accelerator Statistics Window .....	6-26
Figure 6-15.	ATM File Check Window .....	6-27
Figure 6-16.	Display POD Status Window .....	6-36
Figure 6-17.	POD Inventory Statistics Window.....	6-38
Figure 6-18.	Display Ethernet Port Status Window .....	6-41
Figure 6-19.	Display DS1/E1 Port Status Window (DS1 shown).....	6-43
Figure 6-20.	Select Interval Window .....	6-47
Figure 6-21.	Display Current Interval Window .....	6-47
Figure 6-22.	Display Intervals Window .....	6-48
Figure 6-23.	DS1 Faults Window.....	6-50
Figure 6-24.	E1 Faults Window .....	6-50
Figure 6-25.	Display Transmission Convergence Status Window.....	6-53
Figure 6-26.	Display DS3 Port Status Window.....	6-55
Figure 6-27.	Display E3 Port Status Window .....	6-56
Figure 6-28.	DS3/E3 Faults Window (DS3 shown).....	6-62
Figure 6-29.	Display PLCP Status Window.....	6-63
Figure 6-30.	Display Transmission Convergence Status Window.....	6-64
Figure 6-31.	Display OC-3/STM-1 Port Status Window .....	6-66

Figure 6-32.	OC-3/STM-1 Line Faults Window .....	6-70
Figure 6-33.	OC-3/STM-1 Path Faults Window .....	6-70
Figure 6-34.	Display OC-3/STM-1 Path Status Window .....	6-73
Figure 6-35.	Display Universal Serial Port Status Window .....	6-78
Figure 6-36.	Display ATM Status Window (DS3 ATM port shown) .....	6-80
Figure 6-37.	Connection Monitoring Example .....	6-85
Figure 6-38.	ATM UNI Connections Window .....	6-87
Figure 6-39.	CAC Port Statistics Window .....	6-90
Figure 6-40.	CAC Configuration Stats Window .....	6-92
Figure 6-41.	Connection Options Window (UNI) .....	6-93
Figure 6-42.	Connections Summary Window .....	6-95
Figure 6-43.	Connections Statistics Window .....	6-96
Figure 6-44.	Native LAN Service (NLS) Groups Window .....	6-98
Figure 6-45.	NLS Group Options Window .....	6-99
Figure 6-46.	Native LAN Service (NLS) Tunnels Window .....	6-99
Figure 6-47.	NLS Tunnel Options Window .....	6-100
Figure 6-48.	Configure CES Connection Window .....	6-101
Figure 6-49.	Options Window (CES-IWF) .....	6-102
Figure 6-50.	Configure USF Connection Window .....	6-103
Figure 6-51.	Connection Options Window .....	6-104
Figure 6-52.	Configure VCS Connection Window .....	6-105
Figure 6-53.	Connection Options Window (VCS-IWF) .....	6-106
Figure 6-54.	VCS Port Statistics Window .....	6-107
Figure 6-55.	Connection Options Window Example .....	6-108
Figure 6-56.	Connection Statistics Window .....	6-111
Figure 6-57.	NLS Group Statistics Window .....	6-116
Figure 6-58.	CES-IWF Statistics Window .....	6-118
Figure 6-59.	USF-IWF Statistics Window .....	6-121
Figure 6-60.	VCS-IWF Statistics Window .....	6-124
Figure 7-1.	Events/Alarms Log Window .....	7-2
Figure 7-2.	Event/Alarm Detail Window .....	7-4
Figure 7-3.	Event Management Window .....	7-5
Figure 7-4.	Setup Event Log Filters Window .....	7-8
Figure 7-5.	Setup Trap Filters Window .....	7-10
Figure 7-6.	Trap Destinations Window .....	7-12
Figure 7-7.	Add Trap Destination Window .....	7-12
Figure 8-1.	Diagnostics Window .....	8-2
Figure 8-2.	Select Slot (ICM) Window .....	8-3
Figure 8-3.	Select Cell Highways Self Test Window .....	8-4
Figure 8-4.	Cell Highways Self Test Window .....	8-5
Figure 8-5.	DS1/E1 POD Port Loopbacks .....	8-8
Figure 8-6.	DS3/E3 POD Loopbacks .....	8-10
Figure 8-7.	OC-3c/STM-1 POD Loopbacks .....	8-12
Figure 8-8.	Universal Serial Frame POD Loopbacks .....	8-14
Figure 9-1.	Utilities Window .....	9-2
Figure A-1.	System Administration Window — Craft Interface Version .....	A-5
Figure A-2.	System Administration Window — WebXtend Version .....	A-5
Figure A-3.	Craft Interface Utilities Window .....	A-10

## Contents

---

Figure B-1.	OASOS Commands .....	B-2
Figure G-1.	Remote Management of SA Units without Ethernet Ports .....	G-2

# List of Tables

Table 1-1.	VPI/VCI Bits per POD Type .....	1-25
Table 1-2.	Traffic Parameters monitored on each GCRA/Service Class .....	1-37
Table 1-3.	Traffic Policing Actions .....	1-38
Table 2-1.	Main-Menu Buttons and Functions .....	2-10
Table 2-2.	Common Fields/Buttons .....	2-16
Table 3-1.	System Administration Fields and Buttons .....	3-3
Table 3-2.	Adding an Operator .....	3-7
Table 3-3.	System Timing Fields and Buttons .....	3-9
Table 3-4.	Adding an IP Route .....	3-12
Table 3-5.	Add Node Prefix Fields and Buttons .....	3-17
Table 3-6.	ASPVC Address Configuration Fields and Buttons .....	3-20
Table 3-7.	SF CAC Configuration Fields and Buttons .....	3-23
Table 3-8.	VC Buffer Configuration Fields and Buttons .....	3-25
Table 3-9.	Priority Queue Configuration Fields and Buttons .....	3-27
Table 3-10.	Cell Highway Configuration Fields and Buttons .....	3-29
Table 4-1.	Configure System Fields and Buttons .....	4-4
Table 4-2.	Configure ICM Fields and Buttons .....	4-5
Table 4-3.	Configure POD Fields and Buttons .....	4-8
Table 4-4.	Configure Ethernet Port Fields and Buttons .....	4-10
Table 4-5.	Configure DS1/E1 Port Buttons and Fields .....	4-13
Table 4-6.	Equalization Buttons and Fields .....	4-20
Table 4-7.	Configure DS3/E3 Port Fields and Buttons .....	4-23
Table 4-8.	Trail Trace Fields .....	4-27
Table 4-9.	Far End Alarm and Control Fields .....	4-29
Table 4-10.	High-Bandwidth Recommended Per-VC Buffering Settings .....	4-31
Table 4-11.	Configure OC-3/STM-1 Port Fields and Buttons .....	4-32
Table 4-12.	Configure OC-3/STM-1 Port (Advanced) Fields and Buttons .....	4-37
Table 4-13.	Configure OC-3/STM-1 Path Fields and Buttons .....	4-39
Table 4-14.	Configure OC-3/STM-1 Path (Advanced) Fields and Buttons .....	4-42
Table 4-15.	Port CAC Configuration Fields and Buttons .....	4-45
Table 4-16.	Configure ATM Interface Fields and Buttons .....	4-47
Table 4-17.	Signaling Protocols and ILMI .....	4-50
Table 4-18.	Add Port Prefix Fields and Buttons .....	4-54
Table 4-19.	Configure Universal Serial Port Fields and Buttons .....	4-56
Table 5-1.	Connection Options Fields and Buttons .....	5-5
Table 5-2.	Dial-Type Addressing Formats .....	5-16
Table 5-3.	ATM UNI Connections Fields and Buttons .....	5-35
Table 5-4.	Add/Modify ATM UNI Connection Fields .....	5-39
Table 5-5.	Add/Modify IMA Group Buttons and Fields .....	5-49
Table 5-6.	Configure IMA Link Buttons and Fields .....	5-53
Table 5-7.	IMA Group Statistics Fields and Buttons .....	5-56
Table 5-8.	IMA Link Statistics Fields and Buttons .....	5-61
Table 5-9.	Add NLS Group Fields .....	5-66
Table 5-10.	Add/Modify NLS Tunnel Fields .....	5-71

Table 5-11.	MAC Address Cache Fields and Buttons .....	5-79
Table 5-12.	Add Static MAC Address Fields .....	5-81
Table 5-13.	Configure CES Connection Fields and Buttons .....	5-85
Table 5-14.	Add/Modify Unstructured/Structured CES-IWF Fields and Buttons.....	5-91
Table 5-15.	Transmitter Control Sources.....	5-96
Table 5-16.	Dynamic Bandwidth Fields and Buttons .....	5-98
Table 5-17.	Configure USF Connection Fields and Buttons .....	5-104
Table 5-18.	Add/Modify USF-IWF Fields and Buttons .....	5-108
Table 5-19.	Configure VCS Connection Fields and Buttons .....	5-119
Table 5-20.	Add/Modify VCS-IWF Fields and Buttons .....	5-123
Table 5-21.	VCS Compression Fields and Buttons .....	5-129
Table 5-22.	Add/Modify DS1 Timeslot Fields and Buttons .....	5-133
Table 6-1.	ICM Front Panel Indicators .....	6-4
Table 6-2.	SUM Status Indicators .....	6-5
Table 6-3.	Display System Status Fields and Buttons .....	6-7
Table 6-4.	Power Supply Status Fields .....	6-10
Table 6-5.	System Inventory Statistics.....	6-11
Table 6-6.	MIB II Statistics Buttons .....	6-12
Table 6-7.	Display Board Status Fields and Buttons .....	6-15
Table 6-8.	Processor Utilization Fields .....	6-18
Table 6-9.	Board Inventory Statistics Fields .....	6-20
Table 6-10.	Cell Highway/Priority Queue Stats Fields and Buttons .....	6-24
Table 6-11.	CAC Bandwidth Stats Fields .....	6-25
Table 6-12.	Protocol Accelerator Statistics Fields and Buttons .....	6-26
Table 6-13.	ATM File Check Fields .....	6-27
Table 6-14.	10/100 Ethernet POD Front Panel Indicators .....	6-29
Table 6-15.	DS1 POD Front Panel Indicators .....	6-30
Table 6-16.	E1 POD Front Panel Indicators .....	6-31
Table 6-17.	DS3 POD Front Panel Indicators .....	6-32
Table 6-18.	E3 POD Front Panel Indicators .....	6-33
Table 6-19.	OC-3c/STM-1 POD Front Panel Indicators .....	6-34
Table 6-20.	Universal Serial POD Front Panel Indicators .....	6-35
Table 6-21.	Display POD Status Fields and Buttons .....	6-37
Table 6-22.	POD Inventory Statistics Fields .....	6-38
Table 6-23.	Display Ethernet Port Status Fields and Buttons .....	6-42
Table 6-24.	Display DS1/E1 Port Status Fields and Buttons .....	6-44
Table 6-25.	DS1 Faults Fields and Buttons .....	6-51
Table 6-26.	E1 Faults Fields and Buttons .....	6-52
Table 6-27.	Display DS3 Port Status Fields and Buttons .....	6-57
Table 6-28.	Display E3 Port Status Fields and Buttons .....	6-60
Table 6-29.	DS3/E3 Faults Fields and Buttons .....	6-62
Table 6-30.	Display PLCP Status Fields and Buttons .....	6-64
Table 6-31.	Display OC-3/STM-1 Port Status Fields and Buttons .....	6-67
Table 6-32.	OC-3/STM-1 Line Faults Fields and Buttons .....	6-71
Table 6-33.	OC-3/STM-1 Path Faults Fields and Buttons .....	6-71
Table 6-34.	Display OC-3/STM-1 Path Status Fields and Buttons .....	6-74
Table 6-35.	Display Universal Serial Port Status Fields and Buttons .....	6-79

Table 6-36.	Display ATM Status Fields and Buttons .....	6-82
Table 6-37.	ATM UNI Connections Fields and Buttons .....	6-88
Table 6-38.	CAC Port Statistics Fields and Buttons .....	6-91
Table 6-39.	CAC Configuration Statistics Fields .....	6-92
Table 6-40.	Connections Summary Fields .....	6-95
Table 6-41.	Connections Statistics Fields .....	6-96
Table 6-42.	VCS Port Statistics Fields and Buttons .....	6-107
Table 6-43.	Connection Statistics/NLS Group Statistics Fields and Buttons .....	6-112
Table 6-44.	NLS Group Statistics Fields and Buttons .....	6-117
Table 6-45.	CES-IWF Statistics Fields and Buttons .....	6-118
Table 6-46.	USF-IWF Statistics Fields and Buttons .....	6-122
Table 6-47.	VCS-IWF Statistics Fields and Buttons .....	6-125
Table 7-1.	Events/Alarms Log Fields .....	7-3
Table 7-2.	Event/Alarm Detail Fields .....	7-4
Table 7-3.	Event Management Buttons and Fields .....	7-6
Table 7-4.	Setup Event Log Filters Fields and Buttons .....	7-9
Table 7-5.	Setup Trap Filters Fields and Buttons .....	7-11
Table 8-1.	Cell Highway Self Test Fields and Buttons .....	8-6
Table 9-1.	Utilities Fields and Buttons .....	9-3
Table A-1.	Boot Sequence .....	A-3

# About This Guide

The *SA 100 / SA 600 / SA 1200 Network Administrator's Guide* is a task-oriented manual that describes how to configure, test, and monitor the SA 100, SA 600, or SA 1200 devices through WebXtend™, its built-in Web browser interface. This guide is intended for the network administrator who is responsible for configuring and maintaining the network.

## What You Need to Know

As a reader of this guide, you need to know how to:

- Use the operating system (Windows, Mac OS, UNIX, etc.) that is running on the computer system connected to the SA device
- Use the Web-browser software that is running on the computer system connected to the SA device
- Surf Web pages on the Internet

This guide assumes that you have done the following:

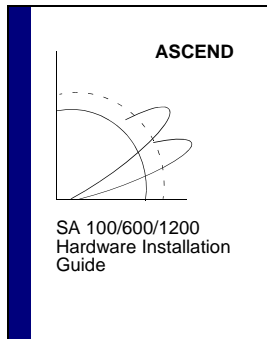
- Installed the SA unit hardware, as described in the *Hardware Installation Guide* (product code 80085)
- Installed Java-enabled Web-browser software, such as Netscape Communicator, on the computer system connected to the SA unit



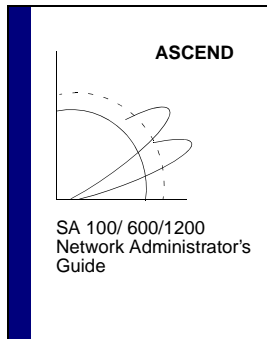
Read the Release Notes which accompanied your SA device for additional information about this product.

## Reading Path

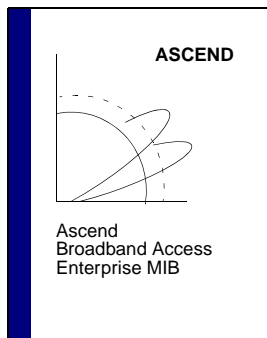
The SA 100 / SA 600 / SA 1200 documentation set includes the following manuals:



This guide describes how to set up, install, and test the SA 100, SA 600, and SA 1200 hardware. It also provides basic troubleshooting solutions for potential hardware-related problems.



These guides describe how to use WebXtend, the built-in Web-browser interface, to configure, test, and maintain the SA 100 Broadband Service Unit, SA 600 Broadband Service Concentrator, and SA 1200 Broadband Service Concentrator.



This guide describes the Ascend Broadband Access Enterprise Management Information Base (MIB), the database containing network configuration and performance information about the SA units.



## How to Use This Guide

This guide contains the following information:

Read	To Learn About...
Chapter 1	The general functions and features of the SA units and WebXtend, its Web browser interface.
Chapter 2	How to power up and shut down an SA unit, log on and off WebXtend and use the WebXtend conventions.
Chapter 3	Configuring the system-level parameters of the SA unit.
Chapter 4	Configuring the SA unit's ports including Ethernet, DS1/E1, DS3/E3, Universal Serial Frame, Universal Serial CES, DS1 Compressed Voice, and OC-3c/STM-1 ports.
Chapter 5	Configuring the SA unit's network services, including ATM User Network Interface (UNI), Native LAN Service (NLS), Universal Frame Service, Compressed Voice Service, IMA, and Circuit Emulation Service (CES).
Chapter 6	Monitoring the status of the SA unit.
Chapter 7	Customizing the SA unit's event and alarm functions.
Chapter 8	Testing the SA unit's operations.
Chapter 9	Using WebXtend to save and restore the configuration of an SA unit and to initialize and shut down the SA unit.
Chapter 10	How to troubleshoot the SA unit and, if necessary, contact the Ascend Technical Assistance Center.
Appendix A	The general functions and features of the SA unit's craft interface and how to perform functions that are only accessible through this interface.
Appendix B	The SA unit's built-in operating system command set.
Appendix C	Using FTP to transfer files, back up, and restore the SA unit's configuration data.
Appendix D	Upgrading the SA unit's on-board software.
Appendix E	Downloading the Ascend Broadband Access Enterprise MIB.
Appendix F	Integrating an SA unit into a NavisCore network management system.
Appendix G	Managing the SA unit remotely.
Appendix H	Acronyms and abbreviations used in this guide.
Glossary	Technical terms used in this guide.

## Related Documents

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

### Ascend

- *Hardware Installation Guide – SA 100 / SA 600 / SA 1200* (product code #80085)
- *Ascend Broadband Access Enterprise MIB* (product code #80055)

### Third Party

- The manual that accompanies your Web-browser software

## Customer Comments

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

- Fill out the Customer Comment Form located at the back of this guide and return it to us.
- E-mail your comments to [cspubs@ascend.com](mailto:cspubs@ascend.com).
- FAX your comments to 1-203-949-0703, attention Technical Publications.
- Open a case in CaseView for documentation.

## Customer Support

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

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

# Conventions

This guide uses the following conventions:

Convention	Indicates	Example
[ <i><b>bold italics</b></i> ]	Variable parameters to enter.	[ <i><b>your IP address</b></i> ]
Courier Regular	Screen or system output; command names in text.	Please wait...
<b>Bold</b>	User input in body text.	Type <b>cd install</b> and ...
<b>Courier Bold</b>	User input in a command line.	> <b>show ospf names</b>
Menu => Option	A selection from a menu.	NavisCore => Logon
<i>Italics</i>	Book titles, new terms, and emphasized text. Also directories, pathnames, and filenames.	<i>Network Management Station Installation Guide</i>
Boxes around text	Notes, warnings, cautions.	See examples below.



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



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



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

# Overview

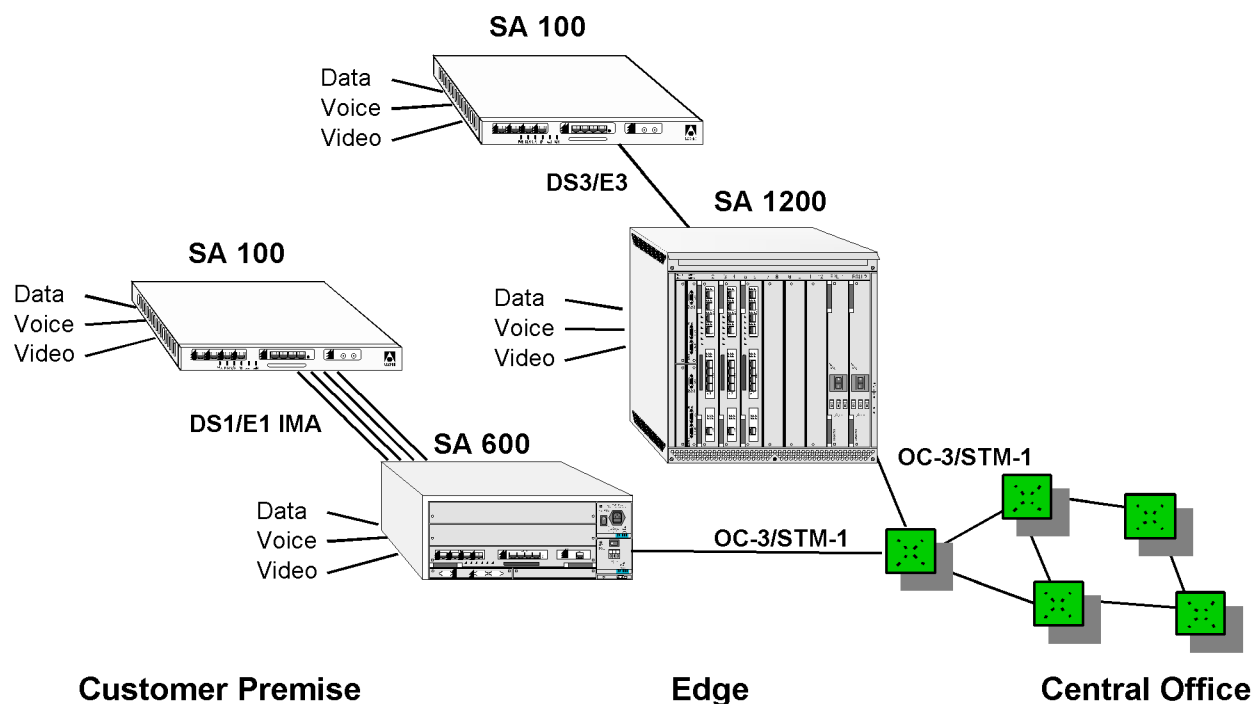
This chapter provides the following background and conceptual information:

- General functions and features of the SA unit
- General functions and features of WebXtend (the SA Web browser-interface)
- Theory of operation of the SA unit

## About the SA Units

The SA 100, SA 600, and SA 1200 provide a high mix of applications in a low-cost access system to broadband wide area networks (WANs) and campus backbones. Unique interface modularity provides economical integration of data, voice, video, and ATM cell traffic. High-performance, cross-flow switching supports a wide variety of voice, video, and data connections. Interchangeable modules called *Protocol Option Devices* (PODs) furnish a scalable upgrade path among Ascend's SA broadband access products.

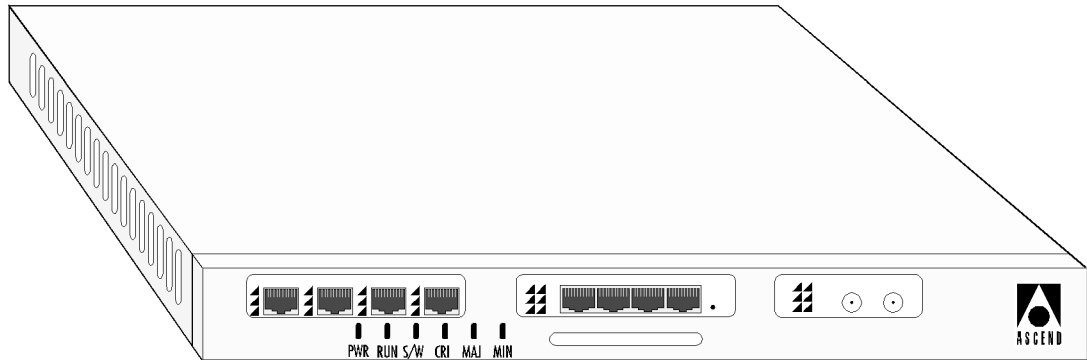
The SA units are ideal for high-mix, low-cost access to broadband WANs. **Figure 1-1** shows several SA units providing wide-area ATM access for a combination of video, voice, and LAN-based data traffic. The SA units provide wire-speed translation to and from ATM cells, and third-generation traffic management prevents bursty LAN traffic from degrading voice or video quality.



**Figure 1-1. SA Products Consolidating Traffic onto a WAN**

## SA 100 Broadband Service Unit

Figure 1-2 shows the SA 100 Broadband Service Unit.



**Figure 1-2. SA 100 Broadband Service Unit**

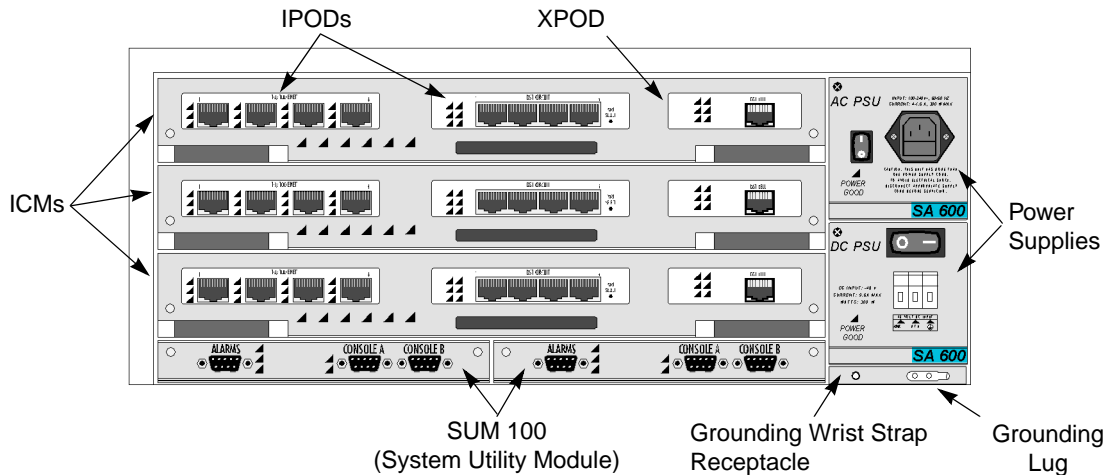
The SA 100 supports the following devices in a single chassis:

- One Interface Control Module (ICM)
- Up to two Interface Protocol Option Devices (IPODs)
- One Expansion Protocol Option Device (XPOD)
- One Cell Protocol Option Device (CPOD)  
(The CPOD is an internal component and is not visible from the exterior.)

The SA 100's compact chassis is suitable for rack-mount, wall-mount, or stand-alone configurations. Interchangeable PODs allow flexible configuration of voice, video and data interfaces.

## SA 600 Broadband Service Concentrator

Figure 1-3 shows the SA 600 Broadband Service Concentrator.



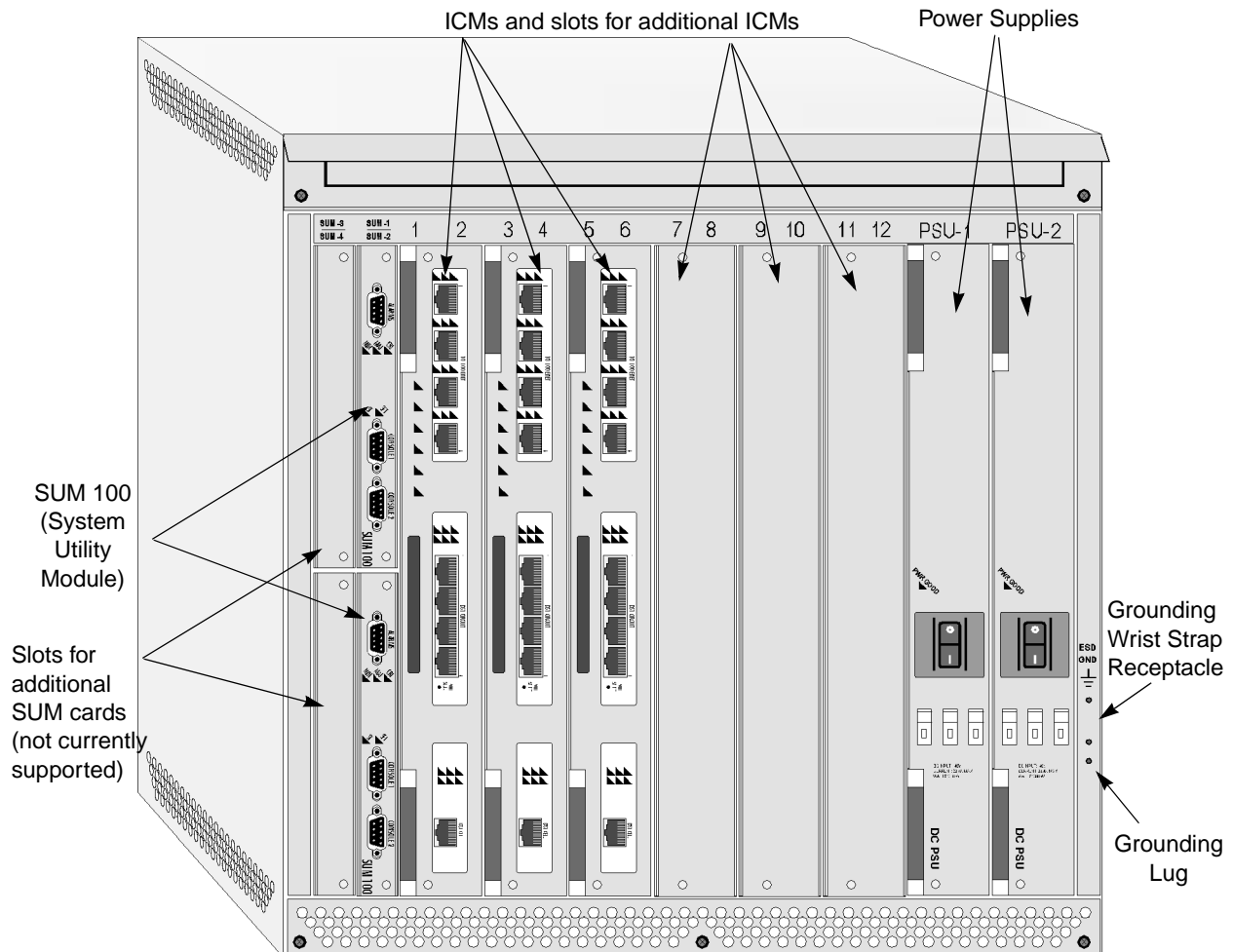
**Figure 1-3. SA 600 Broadband Service Concentrator**

The SA 600 supports the following devices in a single chassis:

- Up to three Interface Control Modules (ICMs)
- Up to two Interface Protocol Option Devices (IPODs) per ICM
- One Expansion Protocol Option Device (XPOD) per ICM
- One Cell Protocol Option Device (CPOD 200) per ICM  
(The CPOD is an internal component and is not visible from the exterior.)
- Two System Utility Module 100s (SUM 100) to provide craft interface ports and timing loopback functions
- Up to two redundant AC or DC power supplies

The SA 600 chassis is suitable for rack-mount or stand-alone configurations. Interchangeable PODs allow flexible configuration of packet, circuit, and cell interfaces.

## SA 1200 Broadband Service Concentrator



**Figure 1-4. SA 1200 Broadband Service Concentrator**

The SA 1200 supports the following devices in a single chassis suitable for rack-mount or stand-alone configurations:

- Up to six Interface Control Modules (ICMs)
- Up to two Interface Protocol Option Devices (IPODs) per ICM
- One Expansion Protocol Option Device (XPOD) per ICM
- One Cell Protocol Option Device (CPOD 200) per ICM  
(The CPOD is an internal component and is not visible from the exterior.)
- Two System Utility Module 100s (SUM 100) to provide craft interface ports and timing loopback functions
- Up to two redundant DC power supplies (AC to DC converter available)



## Interface Control Module

The Interface Control Module (ICM) is the basic building block of every Ascend broadband access system. Each ICM includes a cell subsystem and a packet subsystem that switch cells and packets simultaneously. Traffic flows can be routed between I/O ports on any installed ICM by way of parallel packet and cell interconnects.

The cell subsystem and associated I/O interfaces support ATM *cell switching* with an aggregate capacity of over one gigabit per second per ICM. A Protocol Accelerator on each ICM translates between flows at multiple levels—including ATM segmentation and reassembly, and protocol encapsulation—at speeds up to 200,000 packets per second. Because the Protocol Accelerator is based on a programmable microcode processor, it can “learn” new protocols through future software downloads.

An industry-standard RISC processor on the ICM supports system control and network management functions. A flash memory file system stores the operating system, all application software, and configuration data. To cost-effectively maintain remote Ascend broadband access systems, standard protocols can be used to download software over network connections.

## Protocol Option Devices

PODs are mezzanine boards that attach to the ICM. There are three types of PODs:

- IPODs support service interfaces including Ethernet, universal frame, circuit switching, and ATM UNI.
- XPODs provide additional interface capabilities including ATM wide-area connections, circuit switching, and other future enhancements.
- CPODs provide the cell switching function for each ICM. The SA 100 uses a CPOD 150, capable of switching cells between all interfaces on a single ICM. The SA 600 and SA 1200 require CPOD 200s, which are capable of switching cells between all interfaces on the ICM as well as switching cells across the backplane to other ICMs in the system.

You can easily configure the PODs on an ICM to meet your requirements. The flexible mix-and-match architecture of the ICM and PODs gives you complete control over both fan-out and interface mix.

## Management and Configuration of SA Units

You can manage SA units using a variety of management access methods. Each SA unit has a serial craft interface, enabling you to use a VT100 terminal or equivalent to fully configure and manage the device. In addition, you can configure each SA unit with an IP address, enabling you to manage the device using SNMP, FTP, Telnet, and the Java-based WebXtend utility over a direct Ethernet connection, or over an ATM management VPI/VCI.

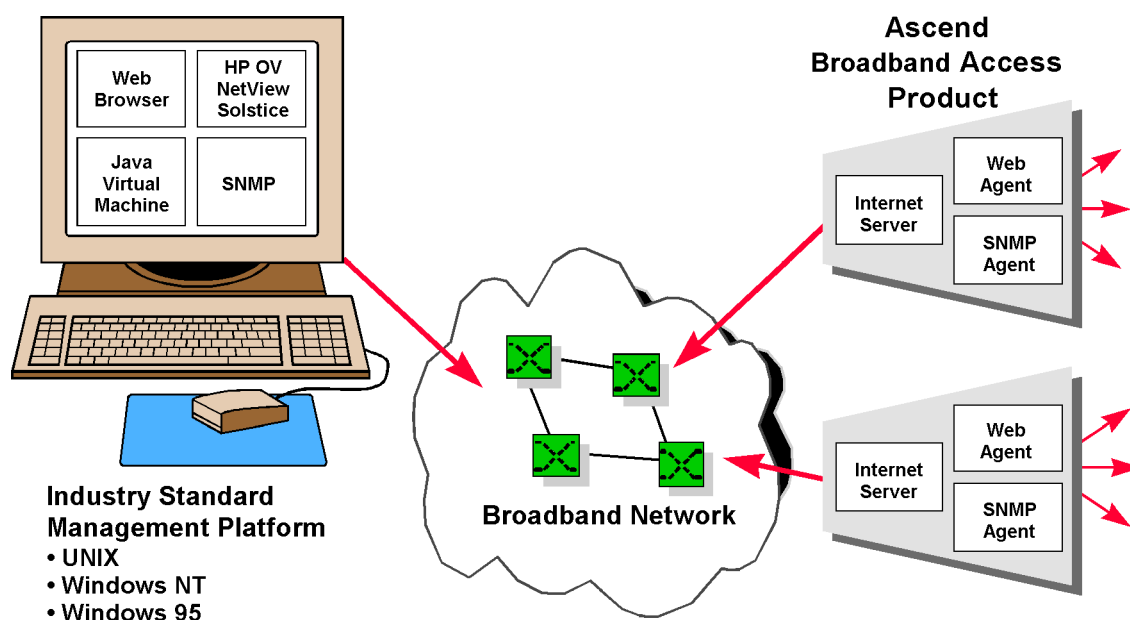
### WebXtend Management Software

WebXtend network management software combines Java and Web technology to deliver secure, user-friendly access to sophisticated management applications.

Modern networks typically comprise an assortment of devices from a number of different vendors. Each vendor offers its own management system, and each management system requires one or more workstations. Consequently, a large wide-area network can require dozens of workstations, each configured to manage a particular version of a particular vendor's product. Furthermore, each management system may present a unique user interface, which requires the network operator to invest considerable time and resources to learn a new system.

World Wide Web browsers are gaining favor as a widely-used and friendly interface to diverse systems. WebXtend is the first Web-based network management architecture to combine the power of Java-based computing with support for standard network management protocols. WebXtend provides a network management approach that emphasizes ease of use, cost-effective platform independence, unlimited access, and enhanced security.

WebXtend provides secure real-time monitoring and control for the entire broadband access system. The WebXtend architecture is based on a standard World Wide Web *client/server* model (see [Figure 1-5](#)). A Web server is embedded in every SA unit. The recommended Web-browser is Microsoft Internet Explorer version 4.01 with Service Pack 1. Another supported browser is Netscape Communicator, Version 4.0.6.



**Figure 1-5. WebXtend Web-based Management**

You manage SA broadband access systems using friendly point-and-click graphics. When you access a management function, the built-in Web server uploads the appropriate Java *applet* to the client. The Java applets support management functions such as configuration and fault management, and display of real-time data such as traffic statistics. For ease of use, WebXtend's management tools are organized into functional groups such as Administration, Utilities, and Interface Management. In addition, a full complement of utilities supports file management, real-time software upgrades, and other functions necessary for proper system maintenance.

### Cost-effective Platform Independence

Web browsers give WebXtend a familiar and easy-to-learn user interface to minimize training costs and maximize user productivity. WebXtend enables you to use a Java-enabled browser on any platform, eliminating the need to dedicate expensive workstations for managing broadband access products.

Every SA unit supports a *craft interface* for on-site configuration, provisioning, and testing. The VT100 interface provides simple, menu-driven commands to facilitate installation while delivering the same rich management functionality as the WebXtend software.

SA units also supports standard protocols for management access and control. Support for Telnet, FTP, IP addressing, and SNMP allows integration with generic MIB browsers and industry-standard management platforms like HP OpenView, NetView 6000, and SunNet Manager.

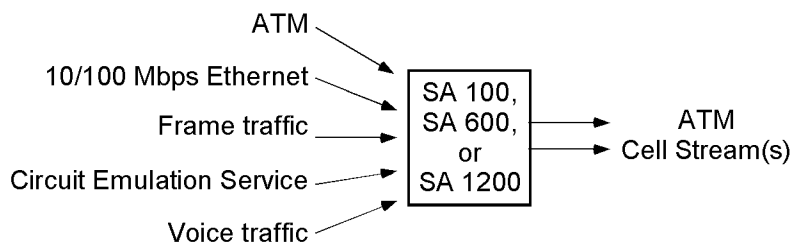
## **Secure Access**

Adherence to standard protocols permits WebXtend to operate over any type of connection, including LANs, WANs, dial modems, and the Internet. Flexible, robust security mechanisms furnish both service providers and their subscribers with access control and authorization. You can protect management traffic against unauthorized access by restricting it to secure IP connections.

## Theory of Operation

This section describes the Theory of Operation of the SA 100, SA 600, and SA 1200 family of service-access products, beginning at a very high level and working down to the details of the product. The background provided in this section will enable you to better understand and navigate WebXtend, ultimately making you a more efficient operator of the SA products.

The SA product family, viewed from the highest level, is designed to move various types of traffic inputs (ATM, Ethernet, CES, Frame, voice, etc.) from their native interfaces to one or more ATM cell stream output(s), as shown in **Figure 1-6**.



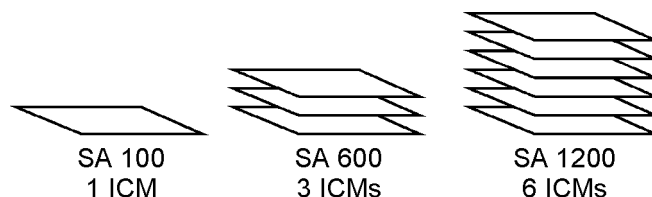
**Figure 1-6. SA-family high-level theory of operation**

Combining diverse traffic sources into ATM cell streams obviously requires adapting any non-ATM traffic into ATM cells. It is also critical that traffic be delivered to the correct end location. We'll discuss connections through the device next, and outline the differences between ATM and non-ATM traffic inputs.



As described earlier in this chapter, the basic building block of each SA family member is the ICM (Interface Control Module). The ICM (akin to a PC's motherboard) provides an underlying fabric on which reside various interface modules (PODs). IPODs and XPODs provide the physical interfaces; the CPOD ties the IPODs and XPODs together and routes cells between the interfaces.

The SA 100, SA 600, and SA 1200 chassis house one, three, or six ICMs, respectively. The figure below compares the three products.

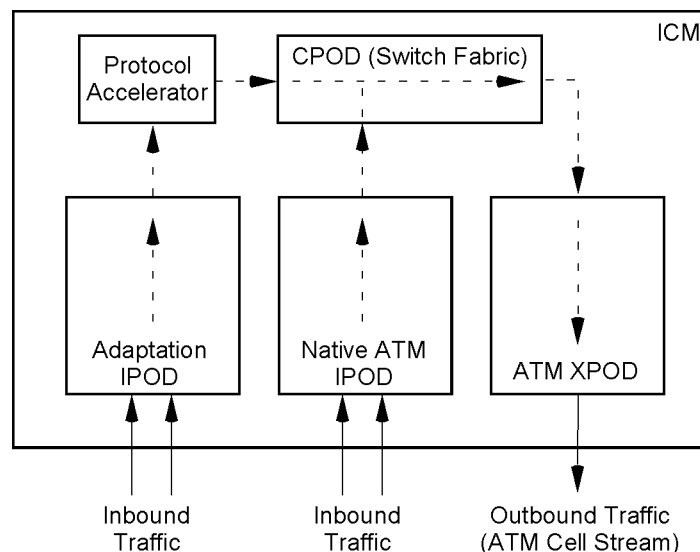


Each ICM can accommodate two IPODs and an XPOD, each of which provides from one to eight interface ports. The SA 600 and SA 1200 support multiple ICMs connected via backplane connections and the CPODs. Traffic may be routed from its source to any port on any POD on any ICM.

## Connections

Obviously, traffic sent into one port of an SA unit is expected to come back out on another port. *Connections* are the paths through the SA unit on which data flows. Every connection has two endpoints, called Endpoint A and Endpoint B. When you are configuring a connection, it may be helpful to consider Endpoint A as the ingress endpoint where the traffic enters the SA unit and Endpoint B as the egress endpoint where the traffic exits the SA unit. However, it is important to remember that connections are bi-directional and that once established, a connection makes no ingress/egress distinction between its endpoints and traffic flows between endpoints in both directions.

Figure 1-7 shows the general traffic flow on an ICM. Traffic is accepted from IPODs and is sent to the CPOD for routing, either directly or through the Protocol Accelerator first for conversion to ATM cells. From the CPOD, traffic is usually directed to an outbound POD, usually a trunk located on the XPOD.

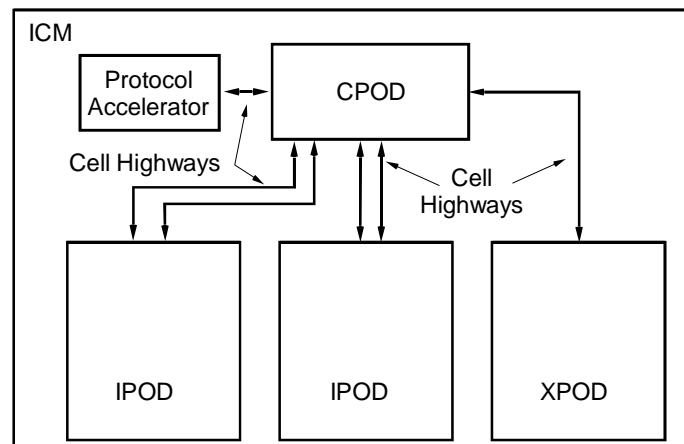


**Figure 1-7. Traffic flow through an ICM**

Routing a connection's traffic from its inbound interface to its outbound interface is the job of the CPOD. Each connection we set up into the SA unit must have a defined endpoint; the CPOD looks at the endpoint values and routes the traffic to the correct output interface on one of the PODs.

The internal routes that carry traffic between each IPOD and the switch fabric (CPOD), between the Protocol Accelerator and the CPOD, and between the CPOD and the XPOD are called *cell highways*. Each XPOD has one cell highway to the CPOD, and each IPOD has two cell highways to the CPOD (though some IPODs use only one of their cell highways).

Each cell highway supports up to 420,000 cells per second. This figure becomes important when the SA unit is deciding whether to accept any additional connections (this is discussed further below). **Figure 1-8** shows the cell highways on an ICM. In practice, not all cell highways are always in use, depending on the installed IPODs. When a packet-based IPOD (such as an Ethernet POD) is installed, its traffic must be converted to cells before passing to the CPOD. For example, assume an Ethernet IPOD is installed. The IPOD's cell highway would not be in use, but the Protocol Accelerator's cell highway would be in use. Alternatively, if all three installed PODs were native ATM PODs, the Protocol Accelerator would be idle and its cell highway unused.

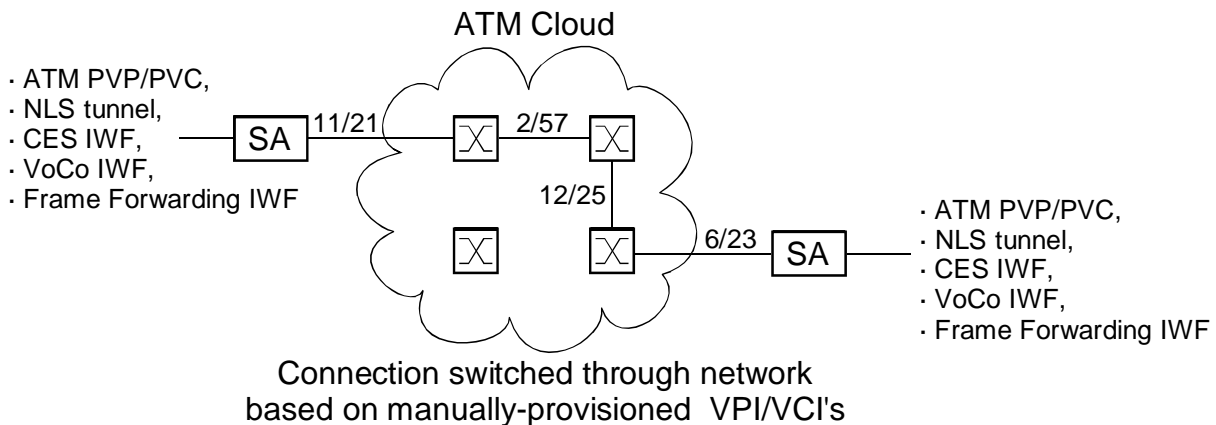


**Figure 1-8. Cell Highways**

### ***Setting up Connections***

Connections between ATM switches are either *Permanent Virtual Circuits* (PVCs) or *Switched Virtual Circuits* (SVCs), or a hybrid of these called a *Soft Permanent Virtual Circuit* (S-PVC). (Virtual paths, consisting of groups of virtual circuits are also supported by the SA units.)

PVC connections are provisioned (“nailed up”) manually; that is, their VP/VC endpoint values and the link-by-link route through the network must be set up by the operator. PVCs remain on the system’s “books” until deleted by the operator.



**Figure 1-9. PVP/PVC-based connection between two SA units**

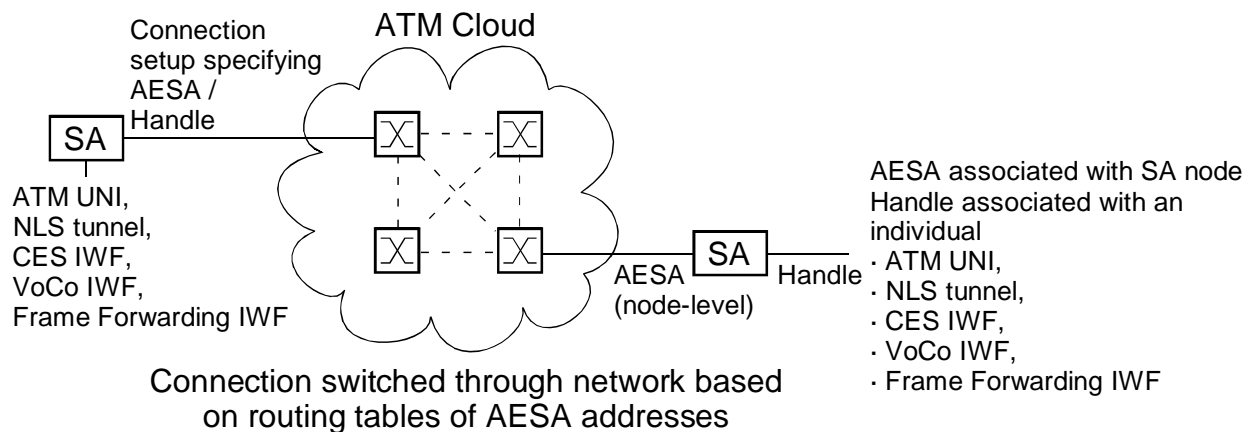
SVC connections are established on the fly using UNI signalling methods and AESA numbers (ATM End Station Address) assigned to every ATM device on the network. SVCs remain present only as long as needed, similar to a phone call which creates a connection from one point to another lasting until the parties hang up. The SA units will support true SVC connections in the future, but currently support two SVC-derivatives, S-PVCs and AS-PVCs, described below.

The SA units have proprietary AS-PVC and S-PVC connection types, which combine facets of both PVCs and SVCs. AS-PVCs and S-PVCs have manually-provisioned endpoint values like PVCs, but the link-to-link network connections between the termination points of the connection are switched according to AESA number, similar to an SVC. Like a PVC, AS-PVCs and S-PVCs remain “on the books” until deleted, but unlike a PVC, these connection types do not use a static route to determine its path through the ATM network.

*Adaptation S-PVCs (AS-PVCs)* enable services to connect to their respective endpoints without specifying a particular destination VPI/VCI. Node-level AESA addresses are used in conjunction with a ‘handle’ indicating a specific service instance at the termination endpoint. For example, a particular NLS tunnel at an originating SA unit may be directed to a remote SA unit with a particular AESA. A corresponding NLS tunnel at the remote unit is set up as a termination, and assigned a handle. The AS-PVC terminator waits for an inbound connection setup request to arrive with the correct service handle. When a setup request arrives, the connection is assigned a VPI/VCI, the circuit is established, and data flows end to end through the network.

Figure 1-10 shows an example of an AS-PVC connecting two SA units.

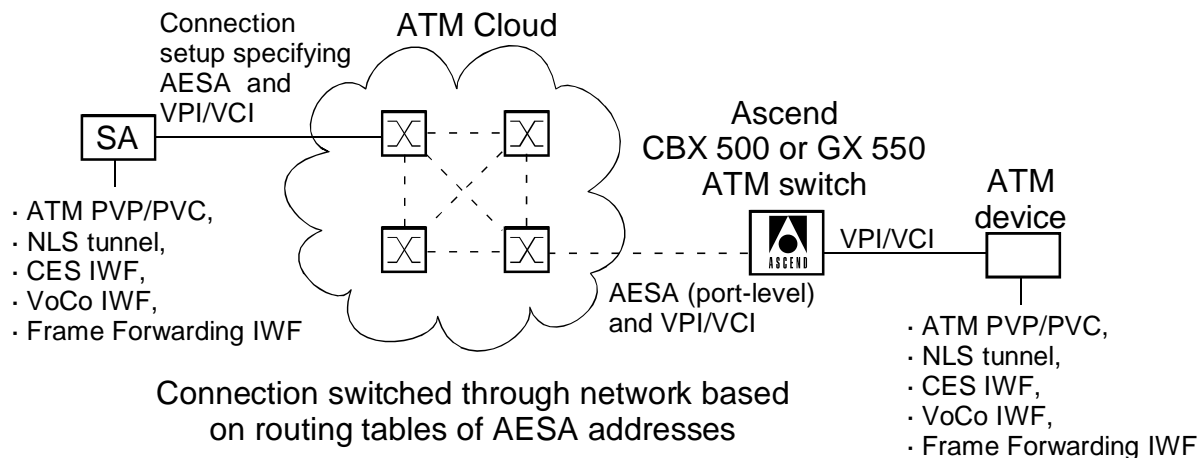




**Figure 1-10. AS-PVC-based connection between two SA units**

*S-PVCs* are used to connect an SA device to a port on an Ascend switch across an ATM network and then on to a particular VPI/VCI. The destination VPI/VCI may correspond to a non-Ascend ATM device, an Ascend device which does not support signalling, such as an older SA unit, or any other situation where signalled connections are not permitted.

**Figure 1-11** shows an S-PVC connecting an SA unit through an ATM network to a port on an Ascend switch and destination VPI/VCI.



**Figure 1-11. S-PVC-based connection**

Regardless of the connection type, when a request is made to establish a new connection, the system must evaluate its available resources to determine if sufficient resources exist to satisfy the request. This process is referred to as *Connection Admission Control* (CAC). Details of CAC are discussed further in **“Connection Admission Control” on page 1-24.**

Now that we've discussed how a connection is established and accepted to the system, we'll describe the types of traffic which can be passed over a connection. Depending on the PODs installed in the SA unit, various traffic types are supported. However, all traffic falls into one of two categories: native ATM traffic (cells) and non-ATM traffic (packet or circuit-based traffic).

## ATM Traffic

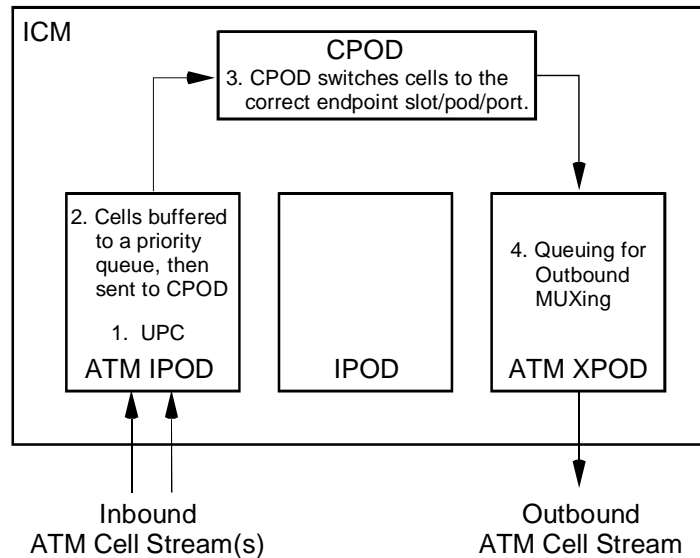
ATM cell traffic arriving at a POD goes through several stages on its way through the SA unit.

1. First, it may be policed for conformance to traffic contract parameters at the IPOD. This is called *Usage Parameter Control* (UPC). Not all PODs are equipped with the UPC feature, and when present, it may be disabled by the user.
2. Next, cells are queued for movement to the CPOD over the cell highway. Queuing and movement to the CPOD is according to priority, as determined by the traffic class (CBR, rt-VBR, nrt-VBR, UBR/ABR). CBR traffic has strict priority over all other traffic classes; if there are CBR cells to be sent to the CPOD, they are *always* sent before any other queues are serviced.

If there are no CBR cells to be sent, the remaining traffic classes take turns from each priority queue in a weighted round-robin schedule. Cells are drawn from high priority queues more often, but no queues are ignored.

3. The CPOD routes the traffic to the correct outgoing slot/POD/port and VPI/VCI and queues the cells for movement to the destination. The usual outbound endpoint is an ATM XPOD, where cells destined for many different VPI/VCIs are multiplexed into a single ATM cell stream.
4. Finally, at the outbound endpoint, cells are queued a final time for multiplexing into the outbound ATM cell stream. Again, the CBR cells have strict priority over all other traffic; if there are CBR cells queued, they are always sent before any other traffic is serviced.

This is illustrated in [Figure 1-12](#).



**Figure 1-12. ATM traffic through an ICM from IPOD to XPOD**

► Traffic flows in both directions through SA units; traffic received at the XPOD may be directed to an endpoint on an IPOD.

### ***Traffic Policing (UPC)***

The optional *Usage Parameter Control* (UPC) function evaluates each connection's (VP or VC) cell stream to determine whether it is complying with the traffic descriptors defined when the connection was established<sup>a</sup>. When UPC detects violations of the negotiated parameters, appropriate action may be taken: cells may be tagged (have their CLP bit set to 1) or discarded. You can configure the policing actions on a per-connection basis.

The traffic descriptors include peak cell rate (PCR), sustained cell rate (SCR), maximum burst size (MBS), and cell delay variation tolerance (CDVT). Service classes use different combinations of descriptors applied to either the CLP0 (cell-loss priority non-tagged cells only) cell stream or CLP0+1 cell stream (both tagged and untagged cells).

UPC provides two Generic Cell Rate Algorithms (GCRAs) to police connections. These GCRAs examine each cell flow according to a “dual leaky bucket” algorithm (refer to available ATM texts for details). The GCRAs can be programmed for policing mode (cells may be discarded or tagged if a connection's traffic descriptors are violated) or monitoring mode (violations are counted, but no action is taken against non-conforming cells).

<sup>a</sup>. UPC functions can be performed on a per-VP or per-VC basis.

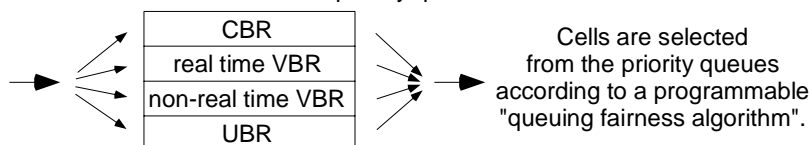
For details of traffic policing conformance definitions, see “Traffic Policing Details” on page 1-37.

### Priority Queuing

After UPC, cells are queued in an input buffer for transmission to the CPOD, where they are routed through the switch fabric towards the destination Slot/POD/Port, VPI/VCI.

Each ATM POD has a fixed number of cell buffers, which are distributed among the Priority Queues according to user-programmable percentages. There is a priority queue for each service class, and each virtual connection is assigned a number of cell buffers in the priority queue for its service class. Incoming cells are placed into the appropriate priority queue, depending on the service category of the VC.

Each service class has a priority queue of cell buffers.  
Every VC has access to a number  
of cell buffers in one of these priority queues.



The number of cell buffers a VC may use is called its depth.  
The number of cell buffers associated with each depth (shallow, medium, high)  
is customizable for each service class.

**Figure 1-13. Priority Queuing**

From the priority queues, cells are selected for processing through the switch fabric according to a *priority queuing fairness* algorithm, which assures that all queues get serviced, though higher priority queues are serviced more frequently. If there is any traffic in the CBR priority queue, it *always* takes precedence over lower priority traffic; the priority queuing fairness algorithm applies only to real-time VBR, non-real-time VBR, and UBR service classes. These three service classes take turns from each priority queue in a weighted round-robin schedule. Cells are drawn from high priority queues more often, but no queues are ignored.

### Switch Fabric (CPOD)

On arrival at the CPOD (the SA unit's switching fabric), cells are queued again for switching. When selected, they are sent on to their endpoint (Slot/POD/Port VPI/VCI).

The SA 100 uses a CPOD 150, which switches cells between any interface on a single ICM. The SA 600 and SA 1200 use CPOD 200 units, which can mesh to create a very large switch fabric. Any CPOD 200 can switch cells to any interface on any ICM installed in the SA 600 or SA 1200.

### ***Cell Muxing***

The final step in the path of ATM cells through an SA unit is usually an ATM XPOD where many outbound ATM cell streams are multiplexed into a single high-speed ATM cell stream.

The cell multiplexor's output queue structure differs from the input buffer structure. CBR traffic is placed in its own output buffer, and all other traffic shares an output buffer. The outgoing ATM cell stream is formed from these two queues, which are emptied based on the rate of the UNI devices and the queue priority. The CBR priority queue must be emptied before any cells are picked from the lower-priority queue.

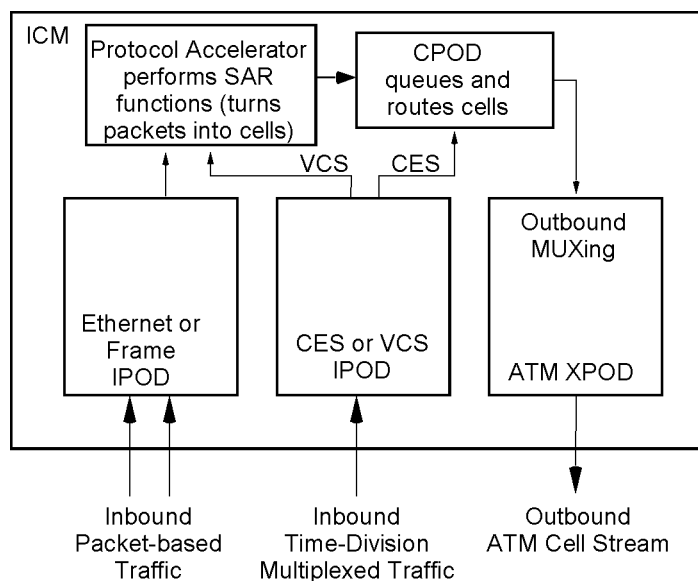
## Non-ATM Service Types

Non-ATM service types must be adapted into ATM cells before entering the CPOD for routing to their destination. This process is called *Segmentation and Reassembly*, and is performed by devices called SARs. The SAR function is performed either on the POD or by a SAR on the ICM called the Protocol Accelerator.

Non-ATM traffic is either packet-based (Ethernet, frame) or circuit-based (time-division multiplexed traffic such as CES and Compressed Voice). In either case, an SAR adapts the traffic to ATM cells and puts the cells on a cell highway to the CPOD, as described below and illustrated in [Figure 1-14](#). Packet-based traffic is converted to ATM cells using AAL5 segmentation and reassembly, while circuit-based traffic uses AAL1 segmentation and reassembly (Compressed Voice traffic is an exception; see [“Compressed Voice” on page 1-23](#)).

Incoming packet-based traffic (and Compressed Voice traffic) is passed from the POD to the Protocol Accelerator. Traffic is segmented into ATM cells bound for a particular Slot/POD/Port VPI/VCI. The cells are then sent from the Protocol Accelerator to the CPOD. They are placed in an appropriate priority queue, then sent to their destination Slot/POD/Port VPI/VCI, usually an ATM POD where the cells are multiplexed into an outbound ATM cell stream.

Incoming Circuit Emulation Service traffic is processed by a SAR on the IPOD using AAL1 and sent directly to the CPOD. From that point on, it is treated as described above.



**Figure 1-14. Non-ATM traffic through an SA unit**

The SA product family currently supports several major classes of non-ATM traffic: Ethernet traffic, frame traffic, circuit emulation traffic and voice compression traffic. Each traffic type is discussed below.

## **Ethernet**

Each Ethernet POD offers the functions of a learning, transparent bridge. When an Ethernet packet arrives from a port on an Ethernet POD, the source and destination MAC addresses are checked against the MAC address forwarding table. If the source MAC address is not recognized, a new entry is logged in the address forwarding table with the source port information. If the destination MAC address already has a port or tunnel<sup>a</sup> in the forwarding table, it is immediately sent on its way.

If there is no entry for the destination MAC address in the table, the packet is broadcast to all ports and tunnels associated with the group the original message came from. The destination MAC replies, enabling the routing table to create an entry associating the MAC address with an ATM virtual connection (an endpoint consisting of Slot/POD/Port and VPI/VCI).

Once the destination Slot/POD/Port and VPI/VCI are known, the Protocol Accelerator uses the AAL5 adaptation protocol to convert and segment the packet into ATM cells, based on the parameters specified for the tunnel. These parameters include service type (CBR, VBR, UBR, etc.), service rate, congestion control, traffic descriptors, and other characteristics necessary to define the ATM connection.

The resulting cells are queued for transportation to the CPOD, where ATM traffic management functions are applied and cells are routed to the appropriate destination.

## **Frame**

Serial frame traffic is treated in a similar but simpler fashion. The current SA hardware supports a single frame service interworking function (connection) per port, so any traffic received on a frame port is mapped to an ATM tunnel, and is sent to the Protocol Accelerator for encapsulation into ATM cells. Frame packets are mapped to ATM cells according to a frame forwarding function. HDLC frames undergo AAL5 SAR. The resulting cells are queued for transportation to the CPOD, where ATM traffic management functions are applied and cells are routed to the appropriate destination.

Examples of frame traffic are connections from a router or Frame Relay Access Device (FRAD).

---

a. A *tunnel* is a virtual link from an Ethernet POD through the SA unit to another Ethernet device; the MAC address forwarding table treats it like any other Ethernet port.

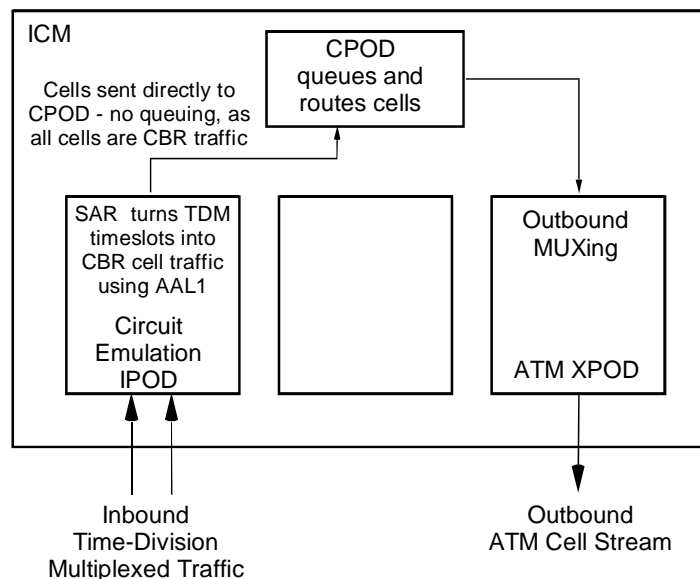


## Circuit Emulation

The SA units support Circuit Emulation Service (CES), which provides for encapsulation of time-division multiplexed (TDM) circuits into ATM cells, using AAL1 adaptation.

CES traffic is handled differently than the packet-based traffic (Ethernet and frame) discussed previously. Instead of using the ICM's Protocol Accelerator, CES PODs are each equipped with an onboard Segmentation and Reassembly (SAR) processor. The SAR encapsulates the incoming TDM stream into ATM cells, then puts the cells on the cell highway directly to the CPOD for routing. Because AAL1 adaptation is used, CES cell traffic is always CBR service class.

Figure 1-15 illustrates the path of CES traffic through an ICM.



**Figure 1-15. CES traffic through an SA unit**

The mechanism for converting constant bit rate traffic from a DS1/E1 source to ATM cells traffic is called an *interworking function* (IWF). Two types of circuit emulation interworking functions are supported: *structured* and *unstructured*. An unstructured CES interworking function maps a single TDM stream (usually a T1 connection, 1.544 mbps) to an ATM cellstream delivered to a single endpoint. A structured CES interworking function enables you to control the individual channels of the TDM stream (for example, each DS0 in a T1). Each DS0 may be sent to its own endpoint if desired. Structured IWFs require framing, and may be configured to transport signaling information as well as data.

CES interworking functions also support *dynamic bandwidth allocation* (DBA), a means for automatically taking advantage of idle connection time to send VBR or UBR traffic. (This is discussed further in [“Configuring Dynamic Bandwidth Allocation” on page 5-96.](#))

## Compressed Voice

While CES can accommodate voice traffic (for instance, a PBX), a specialized Voice Compression service (VCS) is available. This service combines toll-quality voice compression, Group III fax relay functions, and other voice-band processing via the DS1/E1 Voice Compression IPODs.

VCS combines some of the concepts of both time-division multiplexing and packet-based service. On the front end, VCS is similar to CES, with the input being a time-division multiplexed datastream. However, instead of being adapted and encapsulated, each timeslot's data is sent to a specialized Digital Signal Processor (DSP) which handles voice-specific processing such as background noise level tracking and matching, echo-cancellation, silence compression, and modem- and fax-bypass. The DSP creates data packets which are then sent to the Protocol Accelerator for AAL5 adaptation and encapsulation into ATM cells, which are subsequently sent to the CPOD and treated as any other cells.

Figure 1-16 illustrates VCS traffic through an ICM.

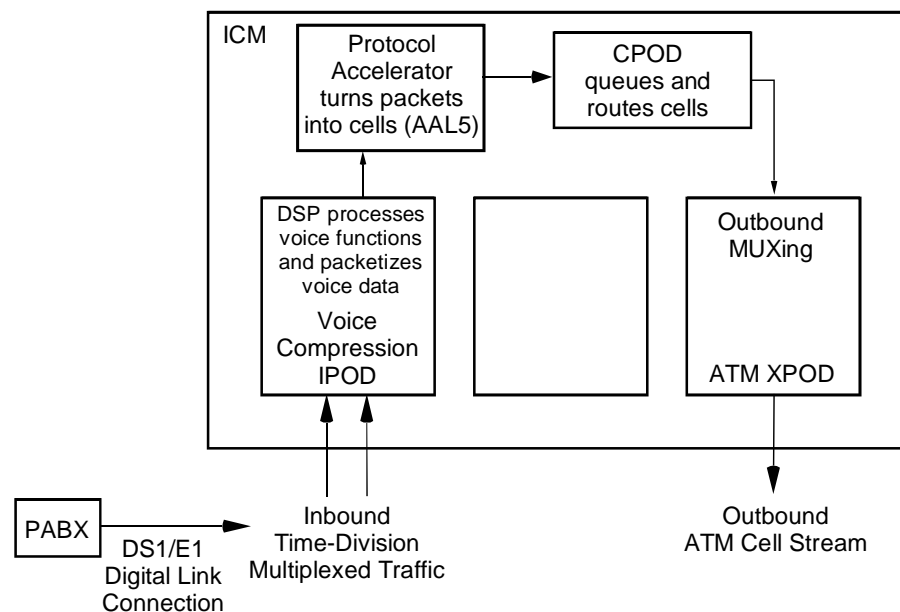


Figure 1-16. Voice Compression Service traffic through an SA unit

## Advanced Topics

This section provides additional detail and background on several more advanced concepts essential to a complete understanding of the SA units' operation. These are topics have been mentioned earlier but were considered too detailed to include until this point.

### Connection Admission Control

Connection Admission Control (CAC) is used by the system to ensure the Quality of Service (QoS) requested by a connection can be accommodated without affecting any other current connections.

CAC evaluates a connection request on several levels to determine whether the request can be accommodated, based on system resources and the demands of previously established connections. Specifically, CAC checks the following parameters. If the connection request fails any of these criteria, the connection request is denied.

- If a specific VPI and/or VCI have been requested, CAC checks to see if the VPI/VCI values are valid (within the designated ranges) and available (i.e., not currently in use).
- If the connection request is for a PVP, the range of reserved PVPs is checked; the PVP requested must be within the valid range. (Reservation of PVPs occurs at a physical port level; each port has a unique Slot/POD/Port identifier, allowing the same VPI/VCI identifiers to exist on multiple ports. For example, a quad DS1 IPOD can have four separate PVP ranges configured.)
- If the connection request is for a PVC, CAC ensures that the VP number is *outside* the reserved PVP range. PVCs may not have VP numbers within a reserved PVP range.
- The traffic descriptors specified for the connection are evaluated against available system resources.
- CAC checks the available cell highway bandwidth and the available bandwidth on source and destination ATM ports - if there is not enough bandwidth available to accommodate the connection request, the request is put into a holding state until sufficient bandwidth becomes available. (This feature is optional and may be disabled by the user. See [“How the SA units manage bandwidth” on page 1-27](#) for further discussion.)
- Cell buffer pools at source and destination are checked - if there are not enough buffers available to accommodate the connection request, the request is put into a holding state until sufficient buffers become available. See [“Cell Buffering in the SA Units” on page 1-33](#) for further discussion.

## About VPI and VCI Ranges

Part of CAC's function is to ensure that the source and destination VPI and VCI are within a range of valid values based on the endpoint hardware.

Each ATM cell has a fixed number of bits to carry the VPI/VCI values. The number of bits is determined by the type of POD hardware in use, and applies to all ports on a given cell highway. (Note: the OC-3c/STM-1 IPOD is currently the only POD which supports two cell highways; all other PODs use only one cell highway.)

**Table 1-1** shows the total bits available for VPI/VCIs on each type of ATM cell POD. Note that enabling PVP connections reduces the number of bits available (see [“Enabling PVPs by Setting a Port's VPI Range” on page 1-26](#)).

**Table 1-1. VPI/VCI Bits per POD Type**

POD Type	Total Bits (SA unit default – PVPs disabled)	Total Bits (PVPs enabled)
Basic XPODs	12	12
Enhanced XPODs	15	12
Dual DS-3 IPOD	15	12
Dual OC-3c/STM-1 IPOD	12	12
Single OC-3c/STM-1 IPOD	15	12
Quad DS1/E1 IPOD	15	12

The number of bits used for VPI/VCI addressing determines the range of valid VPI/VCI addresses. The maximum VPI or VCI value is determined by raising 2 to the the power of bits and subtracting one. The minimum VPI value is always 0, and the minimum VCI value is always 1.

For example, if the VPI bits = 6 and the VCI bits = 9, the VPI range for the cell highway is 0 to  $(2^6-1)$ , or 0 to 63. The valid VCI range for this cell highway is 1 to  $(2^9-1)$ , or 1 to 511.

For instructions on configuring VPI/VCI bits and ranges, see [“Configuring Cell Highway VPI/VCI Ranges” on page 3-28](#).

## Enabling PVPs by Setting a Port's VPI Range

Most applications of the SA units use Permanent Virtual Circuits (traditional PVC, ASPVC, or SPVC) rather than Permanent Virtual Paths. This is due to two factors. First, the overhead of PVPs makes them unattractive for most applications. PVPs use VPI values for addressing and any VPI value used by a PVP becomes unavailable for use by any PVCs, thus limiting the number of PVCs which can be set up on an SA unit. Second, PVPs can be used only to tie one ATM UNI connection to another ATM UNI connection. PVCs can be used for UNI-UNI connections as well adapting a non-ATM interworking function to an ATM connection.

For these reasons, the SA units' default condition is to have PVPs disabled. You cannot set up a PVP unless you deliberately enable the PVP feature and reserve a range of VPI values for use by the PVPs. PVPs may use only those VPI values in the specified range, and PVCs may use only those VPI values outside the specified range.

Unlike setting the VPI/VCI range, which is performed on a Cell Highway level, reserving a PVP range is done on a per-port basis. For example, a Quad DS-1 IPOD could have four separate PVP ranges configured.

Enabling PVPs on an SA unit involves three steps. First, VPI Ranges must be enabled at the cell highway level. Second, the VPI range for PVPs must be defined at a port level. Finally, the SA unit must be rebooted for the changes to take effect.

For instructions on enabling PVPs on an SA unit, see [“Configuring Port-level CAC” on page 4-43](#).

## How the SA units manage bandwidth

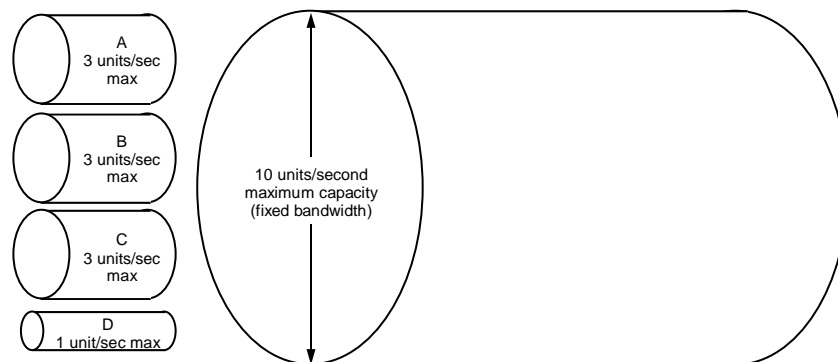
In any system, bandwidth is a commodity limited by physical resources. There are two places where this limit is measured: the physical port into the POD and the switch fabric port, which is the cell highway's connection to the CPOD. The system maintains accounts of the available vs. used bandwidth at both the port and switch fabric levels.

The bandwidth accounting process is somewhat complex. The following example will walk through a very basic model, then extend the concepts to the SA units.

Imagine the bandwidth capacity of the SA unit's switch fabric as a large pipe of diameter X. At any given moment, X units of volume can be passing through the pipe. For this example, we'll say that the pipe can handle a maximum of 10 units per second. The maximum capacity of the pipe is its fixed bandwidth.

Several smaller pipes, representing individual connections, are feeding the large pipe. The sum of the inputs from the small pipes must not exceed the capacity of the large pipe or there will be overflow and some traffic will spill over, unable to be passed through to the other end of the large pipe.

Suppose there are three medium sized pipes (Connections A, B, and C) which can transmit 3 units per second each, and one small pipe (Connection D) which can transmit one unit per second. The maximum input if all pipes are flowing at maximum volume (peak cell rate) simultaneously is 10 units per second, and looks like this:

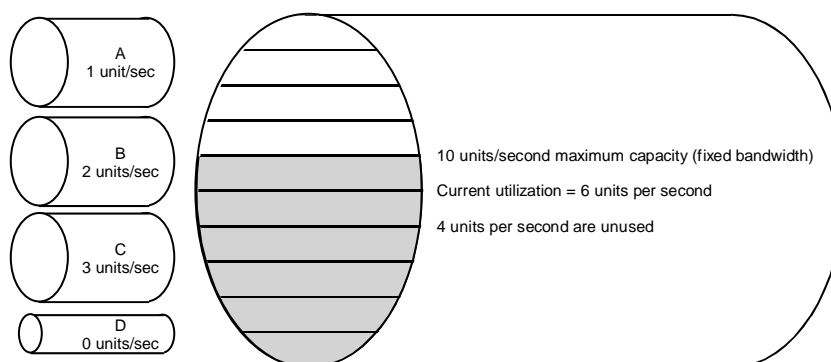


**Figure 1-17. Bandwidth Accounting - Example 1**

In this situation, the large pipe is filled to capacity and can accept no more traffic.

However, suppose that the small pipes do not feed the large pipe at their maximum capacity continuously. Instead, they flow at some average rate (the Sustained Cell Rate), perhaps occasionally delivering a burst of traffic at a higher rate, possibly up to their maximum rate (the Peak Cell Rate). Any time the individual connections are operating at less than their Peak Cell Rate, the larger pipe is not carrying 100% of its capacity. Suppose that at a given moment the small pipes are operating like this:

Pipe (Connection)	Capacity	Current Volume
Connection A	3 units / second	1 unit / second
Connection B	3 units / second	2 units / second
Connection C	3 units / second	3 units / second
Connection D	1 units / second	0 units / second
Large Pipe	10 units / second	6 units / second



**Figure 1-18. Bandwidth Accounting - Example 2**

At this particular moment, the large pipe has 4 units of capacity which are unused and available. It is possible to take advantage of this unused capacity by adding one or more additional pipes (connections). Looking at the current volume of the medium sized pipes, we see that they seem to carry (on average) 2 units / second.

Theoretically, if two more medium-sized pipes were available to feed the large pipe, and they averaged 2 units / second as well, we would be using the full 10 units / second bandwidth of our large pipe. Adding more pipes (connections) allows us to serve more customers.

In reality, adding more pipes makes it possible that several pipes simultaneously bursting above their SCR would exceed the 10 units / second bandwidth of our large pipe. This would leave us unable to accommodate all the traffic we have been asked to transport.

Therefore, we need a mechanism to manage this risk and prevent us from adding an unlimited number of connections on the limited bandwidth of our large pipe. This mechanism is called Bandwidth Accounting.

### ***Bandwidth Accounting - Fixed vs. Variable***

We can use a system of bandwidth accounting to control the number of connections added. We create two accounts, or pools, of bandwidth, called Fixed and Variable. The Fixed Bandwidth pool is equal to the maximum bandwidth of the large pipe. The size of the Variable Bandwidth pool is equal to the Fixed Bandwidth pool times a user-defined multiplier (0 - 2000%). For example, the Fixed Bandwidth pool for a cell highway is 420,000 cells per second<sup>a</sup>. Setting the Variable Bandwidth pool to 200% results in a Variable Bandwidth pool of 840,000 cells per second. This is possible because the Variable Bandwidth pool is strictly an accounting figure and has no relationship to any physical limits.

The Fixed and Variable bandwidth pools are used by CAC when deciding whether a connection request should be granted. CAC checks the system's available resources for each bandwidth pool, Fixed and Variable, against the bandwidth requested for the new connection. If there is insufficient bandwidth in either pool, the connection request is refused until sufficient Fixed and Variable bandwidth is available.

Depending on the connection type, a connection may have an average rate (sustained cell rate, or SCR) and/or a maximum rate (peak cell rate, or PCR). With these parameters in mind, we can view each connection as having a *fixed component* and a *variable component*. The Fixed and Variable bandwidth components of a connection are functions of the service type (CBR, VBR, UBR) and the traffic parameters (PCR, SCR) selected for the connection, and the %Load parameter selected (more about this shortly).

*Constant Bit Rate* (CBR) traffic has only a Fixed Bandwidth component, equal to its Peak Cell Rate. By nature, CBR traffic's bandwidth requirement does not vary, so it has no Variable Bandwidth component.

*Variable Bit Rate* (VBR) traffic, as its name implies, has a bandwidth requirement that varies over time, usually operating at some average rate (the SCR) and sometimes having bursts of traffic above the SCR up to some maximum rate (the PCR). The Fixed component of a VBR connection is equal to its SCR plus the %Load of the Variable component. The Variable component of a VBR connection is equal to the difference between its SCR and its PCR.

- 
- a. The fixed bandwidth pool for the SA devices' switch fabric is 420,000 cells per second per cell highway. In other words, up to 420,000 cells per second can be passed from a single cell highway into the CPOD. This equates to approximately 200 Mbps per cell highway.  
Fixed bandwidth for ports depends on the POD type and the physical interface. Fixed bandwidths for currently-available ATM PODs are listed below:  
DS1 Cell POD: PLCP framing - 3333 cells per second; HEC framing - 3622 cells per second  
E1 Cell POD: PLCP framing - 4210 cells per second; HEC framing - 4528 cells per second  
ATM25 Cell POD: 60377 cells per second  
DS3 Cell POD: PLCP framing - 96000 cells per second; HEC framing - 104226 cells per second  
E3 Cell POD: PLCP framing - 72000 cells per second; HEC framing - 80000 cells per second  
OC-3/STM-1 Cell POD - 353,207 cells per second



*Unspecified Bit Rate* (UBR) traffic has no minimum cell rate and is highly tolerant of cell delay and cell loss. UBR traffic does have a PCR associated with it, usually the maximum line rate, but no other performance parameters, and the PCR and SCR values of a UBR connection are not used in calculating the Fixed and Variable Bandwidth components. For CAC purposes, the Variable component of a UBR connection is set at 100 cells per second. The Fixed component is equal to the %Load parameter times the Variable component.

The following table shows how the values of Fixed and Variable components are calculated for each service type from the PCR and SCR values of a connection.

Service type	Fixed Component equals:	Variable Component equals:
<b>CBR</b>	PCR	(not applicable)
<b>real time VBR</b>	SCR + (%Load * Variable Component)	PCR - SCR
<b>non-real time VBR</b>	SCR + (%Load * Variable Component)	PCR - SCR
<b>UBR</b>	(%Load * Variable Component)	100

The fixed component of each connection is debited against the Fixed Bandwidth pool and the variable component of each connection is debited against the Variable Bandwidth pool. This effectively creates two separate limits on the number of connections which can be established, since when either pool reaches its limit, no new connections may be established.

This accounting system is most useful when a majority of our connections have high variable bandwidth components and we have configured a large Variable Bandwidth pool. In this scenario, it is possible to add many connections to a single pipe and take advantage of the statistical likelihood that bandwidth will be available for a given connection when needed.

However, while we want to take advantage of the statistical gains possible by overbooking connections and using as much of our bandwidth capacity as possible, the consequences of too much overbooking are severe. Should too many connections burst at once, the physical bandwidth available may be consumed and exceeded, unable to pass all the traffic being sent to it. This results in data loss and inability to satisfy the connection commitments we have established.

To help limit excessive overbooking, the system includes a parameter called *Variable to Fixed Loading Percentage* (we'll abbreviate it as %Load). This parameter debits a percentage of each connection's Variable component from the Fixed bandwidth pool, in addition to the regular Fixed component. For instance, consider a connection with a

Fixed bandwidth component of 1 and Variable component of 2 units / second. If the %Load parameter is set at 10%, an additional 0.2 units / second is debited against the Fixed bandwidth pool. If the %Load parameter is set at 100%, an additional 2 units/second is debited against the Fixed bandwidth pool.

As you can see, the higher the %Load value is set, the quicker the the Fixed bandwidth pool is used up, which prevents further connections from being established. This protects against excessive overbooking, by helping to limit the number of connections which may be established.

Extending our original example to an SA unit, the following table shows the cell highway bandwidth accounting for a group of connections.<sup>a</sup> The Fixed Bandwidth pool is set by the physical limitations of the hardware (DS3, OC3 link, etc), and in this example is 420,000 cells/second, the bandwidth of the cell highway. We determine the size of the Variable Bandwidth pool by assigning it some multiple of the fixed bandwidth pool - in this example, we'll use 10%, or 42,000 cells/second.

Connection & Description	Peak Cell Rate	Sustained Cell Rate	Fixed Component	Variable Component
Connection A - real-time VBR connection with service rate = 1 mbps	2594 cells/sec	2358 cells/sec	2382 cells/sec	236 cells/sec
Connection B - non-real-time VBR connection with service rate = 5 mbps	12791 cells/sec	11792 cells/sec	11892 cells/sec	999 cells/sec
Connection C - CBR connection with service rate = 1 mbps	2358 cells/sec	(n/a)	2358 cells/sec	0 cells/sec
Connection D - UBR connection with service rate = 10 mbps	26042 cells/sec	0 cells/sec	10 cells/sec	100 cells/sec
Totals	-----	-----	16,642 cells/sec	1335 cells/sec
Fixed and Variable Bandwidth Pools (Variable = 10% of Fixed)	-----	-----	420,000 cells/sec	42,000 cells/sec
Remaining bandwidth in Fixed and Variable pools after deducting connections A - D	-----	-----	403,358 cells/sec	38,665 cells/sec

---

a. You can view the PCR and SCR for a connection in WebXtend's Add Connection dialog boxes. For example, see the Traffic Descriptors fields in [Figure 5-51 on page 5-70](#).

### **Service Class Bandwidth Calculations and Examples**

**Example 1:** On an SA unit equipped with a DS1 Circuit Emulation IPOD, we establish an unstructured DS1 CES connection (named Connection 1). CES connections are always CBR service type. The %Load variable is set to 10%, and the Variable bandwidth pool is set at 10% of the Fixed bandwidth, or 42,000 cells/second.

A CBR connection has a fixed bandwidth component equal to the Peak Cell Rate and no variable bandwidth component. The system calculates the PCR for this connection to be 4107 cells per second. (The PCR can be viewed in the Add Unstructured CES-IWF window; see [Figure 5-60 on page 5-89](#).)

The ‘balance sheet’ for the switch fabric bandwidth looks like this:

<b>Switch Fabric Bandwidth</b>	<b>Fixed Bandwidth Pool</b>	<b>Variable Bandwidth Pool</b>
<b>Connection 1</b>	4,107 cells/sec	0 cells/sec
<b>Balance Available</b>	415,893 cells/sec	42,000 cells/sec
<b>Total</b>	420,000 cells/sec	42,000 cells/sec

**Example 2:** We establish a non-real time VBR connection named Connection 2 with a rate of 1Mbyte/second. The system calculates the PCR = 2594 and SCR = 2358. The Variable bandwidth pool has been set at 10% of the Fixed bandwidth pool, and the %Load parameter is set to 10%. The fixed bandwidth component is equal to

$$\text{SCR} + (\% \text{Load} * \text{Variable}), \text{ where Variable} = \text{PCR} - \text{SCR}.$$

This works out to  $2358 + (10\% * [2594 - 2358]) = 2358 + (10\% * 236) = 2358 + 24 = 2382$  cells per second debited against the Fixed bandwidth pool. 236 cells/second (the PCR minus the SCR) are debited against the Variable bandwidth pool.

The ‘balance sheet’ for the switch fabric bandwidth looks like this:

<b>Switch Fabric Bandwidth</b>	<b>Fixed Bandwidth</b>	<b>Variable Bandwidth</b>
<b>Connection 2</b>	2,382 cells/sec	236 cells/sec
<b>Balance Available</b>	417,618 cells/sec	41,764 cells/sec
<b>Total</b>	420,000 cells/sec	42,000 cells/sec

Remember that the bandwidth accounting is always performed at two sets of “books”, the port and the switch fabric, and that the two are likely to have different balances, as the switch fabric must account for several different PODs and ports.

## Cell Buffering in the SA Units

Every VC or VP has its own cell buffer accounting. At the time a connection is created, the user specifies the traffic type (CBR, real-time VBR, etc.), telling the system what sort of priority queue to create for this connection, and the depth of this buffer (shallow, medium, or deep).

The depth of a buffer is the number of cells it can accomodate before overflowing, and each depth setting (shallow, medium, or deep) corresponds to an actual number of cell buffers (for instance, shallow = 10 cells, medium = 50 cells, deep = 250 cells). These values are user-configurable for each service type. For example, you could configure the system to allocate 10, 50, or 250 cells for shallow, medium, or deep buffers on CBR priority queues, while allocating 50, 100, or 500 cell buffers for shallow medium, or deep buffers on rt-VBR queues.

Every incoming cell is placed into the priority queue buffer designated for its connection, and the count of cells in that buffer is incremented by one. Each time the a priority queue is serviced (a cell is transported from the buffer to a cell highway) the count of cells in the buffer is decremented.

The PODs and the switch fabric (CPOD) each have a fixed number of cell buffers. These cell buffers are distributed to the priority queues according to user-defined or default percentages. The default cell buffer allocations and priority queue buffer depths are:

Priority Queue	% allocated from total	congestion threshold as a % of allocated	over-subscription as a % of allocated	default cells/buffer shallow/med/high	default congestion thresholds shallow / med / high
<b>CBR</b>	10	80	0	3 / 6 / 8	2 / 4 / 6
<b>rt-VBR</b>	15	70	5	8 / 15 / 25	6 / 12 / 20
<b>nrt-VBR</b>	25	60	20	10 / 25 / 35	8 / 20 / 30
<b>UBR</b>	50	50	400	50 / 500 / 2000	25 / 250 / 1000

The hardware of most PODs supports 6000 input cell buffers. Based on the table above, 600 cell buffers are allocated to CBR priority queues, 900 cell buffers are allocated to rt-VBR priority queues, 1500 cell buffers are allocated to nrt-VBR priority queues, and 3000 cell buffers are allocated to UBR priority queues.

For example, suppose we want to set up a CBR connection with a medium buffer depth. The default settings for CBR priority queue depths are: shallow = 3 cells, medium = 6 cells, and high = 8 cells. Our medium buffer depth CBR connection will have priority queue of 6 cells. The POD has 6,000 buffers available, 10% of which, 600 buffers, are allocated to CBR priority queues. Our connection is allocated 6 of those cell buffers for its priority queue, leaving 594 cell buffers available for the priority queues of other CBR connections.

This distribution model minimizes delay for high-priority, delay-sensitive traffic. Low priority queues are more likely to have to wait for high-priority traffic to pass, so more buffers must be available to accumulate low-priority (such as UBR) traffic until it is selected to move.

### **Oversubscription**

It is important to understand the difference between actual cell buffers and the accounting values used for CAC purposes.

As we saw earlier, each connection established is assigned a number of priority queue cell buffers, based on traffic type and buffer depth parameters. Actual cell buffers are not dedicated to a particular connection; the connection is merely granted access to that number of cell buffers from the priority queue's available buffers. All connections of a given traffic type share the pool of buffers in that priority queue.

Using the example begun in the previous section, the real-time VBR priority queue consists of 900 cell buffers. Suppose that we begin establishing real-time VBR connections, and each is given a cell buffer depth of High (25 buffers). We could establish up to 36 connections and still have sufficient buffers to cover the worst-case demands of all connections.

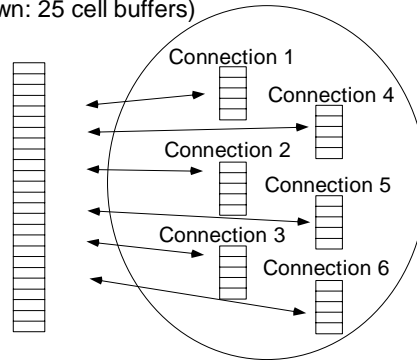
It is, however, unlikely that every connection will require all 25 buffers simultaneously, so at any given moment there are almost always cell buffers available. Overbooking is the idea that we can create more connections than we have actual buffers available for and thus take advantage of inactive cell buffers. You are permitted to oversubscribe (overbook) each type of priority queue by a user-definable percentage. The table above lists the default oversubscription percentages.

For example, the real-time VBR priority queue is allocated 15% of the POD's 6000 cell buffers – 900 cell buffers. By default, the rt-VBR priority queue may be overbooked by 5%, for a total of 995 cell buffers, enabling us to increase the number of established connections. If we have established 36 connections, accounting for 900 cell buffers, and we wish to establish another connection, CAC's accounting reports 95 cell buffers available and will allow the connection to be established. As you can see, this oversubscription factor is used for accounting purposes only, and has no relationship with the number of physical cell buffers.

The *over-subscription as a percentage of allocated* parameter enables you to set a new limit on connections by increasing the number CAC uses when calculating available cell buffers. The pool of buffers assigned to the priority queue as a whole does not change; only the pool of buffers which may be accessed for accounting purposes may be changed.

**Figure 1-19** illustrates the relationship between the cell buffers in a priority queue and the individual connections which may share those buffers.

Priority Queue for a service class.  
This number is determined by  
Priority Queue Allocation  
(example shown: 25 cell buffers)



Each individual connection is assigned a number of cell buffers, determined by the Buffer Depth parameter.

The maximum sum of cell buffers in this pool is determined by the size of the priority queue times the oversubscription factor. (example shows 6 connections x 5 cell buffers/connection = 30 cell buffers. If the oversubscription factor is 40%, 25 cell buffers in the priority queue x 140% = 35 cell buffers max. Connections may be established until this limit is reached.)

**Figure 1-19. Priority queue cell buffers and oversubscription**

Overbooking priority queues allows you to take advantage of statistical gains possible with ATM; a greater number of connections may be supported than we have physical buffers for, based on the statistical probability that there will be buffers available for use at any given moment. However, there is the possibility that multiple connections producing bursts of traffic simultaneously will overrun the priority queue cell buffer allocations and cells will be dropped. Therefore, Quality of Service (QoS) guarantees of zero cell loss cannot be made if overbooking is in use.

### **Output Buffers**

Output buffers are available on ATM cell PODs and operate in a similar fashion to input buffers, with one significant difference. While input cell buffers have four basic priority levels, output buffers are organized into two priorities, a CBR priority queue and an all-others queue shared by real-time VBR, non-real-time VBR, and UBR traffic. The cell buffer distribution percentages used for input priority queues are also used for output priority queues. For example, if a POD has 4000 cells of output buffering and the default allocations explained above are used, the CBR priority queue is allocated 400 cell buffers, the all-others priority queue is allocated the remaining 3600 cell buffers.

## Congestion Thresholds and Congestion Actions

The queues of cell buffers described above are monitored by the system. When the user-defined congestion threshold is exceeded, the priority queue is considered congested, and congestion actions may be taken.

**Example 1: VC congestion.** The CBR connection we established above has a priority queue buffer of 6 cells and a congestion threshold of 4 cells. When four cells are present in the priority queue, it is considered congested, and the hardware will exert the congestion action selected by the user.

**Example 2: Priority Queue Congestion.** The CBR priority queue has a total of 600 buffers in the example above. The congestion threshold is 80%, or 480 cells. When the priority queue reaches this threshold, it is considered congested, and the hardware will exert the congestion action selected by the user for each of the VCs in this priority queue.

There are three types of congestion possible.

1. Cell highway congestion – the aggregate of all the priority buffer pools has been depleted beyond a congestion threshold, affecting all connections on the Cell Highway. Congestion action is turned off after cell buffer pools have recovered to 133% of the congestion threshold.
2. Priority queue congestion – the priority queue congestion threshold has been reached. All connections within this priority queue are affected.
3. VC congestion – the congestion threshold for an individual VC's cell buffer has been reached. Only that individual VC is affected.

The action taken when congestion occurs is configurable for each individual VC. For example, if priority queue congestion occurs, affecting three different connections, each connection may have been configured with a different congestion action. There are several types of congestion actions supported:

1. none – no action is taken.
2. CLP1 discard – cells tagged as CLP1 will be discarded.
3. EFCI – Early Forward Congestion Indication.
4. AAL5 early packet discard (EPD) and partial packet discard (PPD).
5. EFCI with EPD/PPD – a combination of actions 3 & 4.
6. EFCI with CLP1 discard – a combination of actions 2 & 3.

For detailed descriptions of congestion action strategies, refer to standard ATM texts.

## Traffic Policing Details

UPC provides two Generic Cell Rate Algorithms (GCRAs) to police connections. These GCRAs examine each cell flow (CLP 0 and CLP 0+1) according to a “dual leaky bucket” algorithm (refer to available ATM texts for description). Each GCRA can be programmed for policing mode (cells may be discarded or tagged if a connection’s traffic descriptors are violated) or monitoring mode (violations are counted, but no action is taken against non-conforming cells).

The following table shows which cell flows and descriptors each service class must comply with to avoid policing action.

**Table 1-2. Traffic Parameters monitored on each GCRA/Service Class**

	CLP 0 Cell Flow			CLP 0+1 Cell Flow		
Service Class	PCR	SCR	MBS	PCR	SCR	MBS
CBR1				✓		
rt-VBR1				✓	✓	✓
rt-VBR2		✓	✓	✓		
rt-VBR3		✓	✓	✓		
nrt-VBR1				✓	✓	✓
nrt-VBR2		✓	✓	✓		
nrt-VBR3		✓	✓	✓		
UBR1	✓			✓		
UBR2	✓			✓		

For example, the CBR service class’ CLP0+1 cell stream must always conform to the Peak Cell Rate descriptor negotiated at the time the connection was established. If the connection exceeds the PCR parameter, the Usage Parameter Control policing functions will deem the connection to be in violation and take action to bring the connection back into compliance with its service contract. [Table 1-3](#) describes the policing actions which may be taken for each service class.



**Table 1-3. Traffic Policing Actions**

Service Class	Tag/Discard	Discard
CBR1		✓
rt-VBR1		✓
rt-VBR2		✓
rt-VBR3	✓	
nrt-VBR1		✓
nrt-VBR2		✓
nrt-VBR3	✓	
UBR1		✓
UBR2	✓	

The Tag/Discard column refers to traffic types which are policed on both CLP0 and CLP0+1 flows. If the CLP0 flow violates the traffic contract, the cell is tagged. If the CLP0+1 flow violates the traffic contract, the cell is discarded.

Traffic types indicated by a checkmark in the Discard column have non-conforming cells discarded.

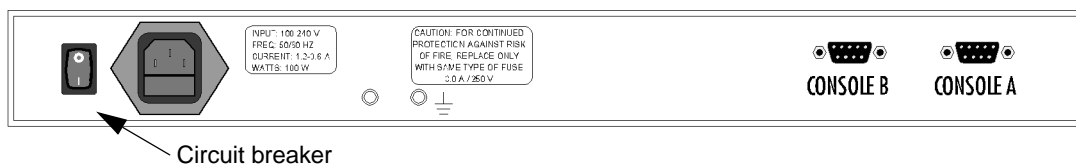
# Getting Started

This chapter describes how to:

- Power up the SA unit ([page 2-3](#))
- Change the IP address of the SA unit ([page 2-6](#))
- Shut down the SA unit ([page 2-18](#))
- Access WebXtend ([page 2-8](#))
- Log off WebXtend ([page 2-18](#))
- Navigate the WebXtend user interface ([page 2-11](#))

## Powering Up the SA 100

To power up the SA 100, toggle on the circuit breaker located on the rear panel of the unit (see [Figure 2-1](#)).

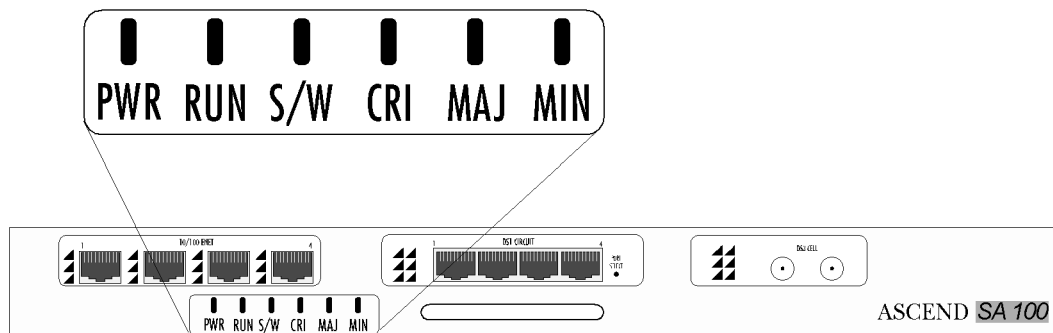


**Figure 2-1. SA 100 Rear Panel (AC power shown)**

After toggling on the circuit breaker, the SA 100 initializes. During initialization, the front panel indicators of the SA 100, shown in [Figure 2-6](#), follow this sequence:

- PWR turns on and remains on as long as the SA 100 is powered.
- For approximately 15 seconds, the chassis front panel indicators turn on and off as they run through their power-up sequence.
- Then, for approximately one minute, RUN blinks once per second, while MIN is lit.
- Finally, the S/W LED is lit, and ST is lit *on the front panel of each IPOD and XPOD* indicating that the unit is ready for normal operation.

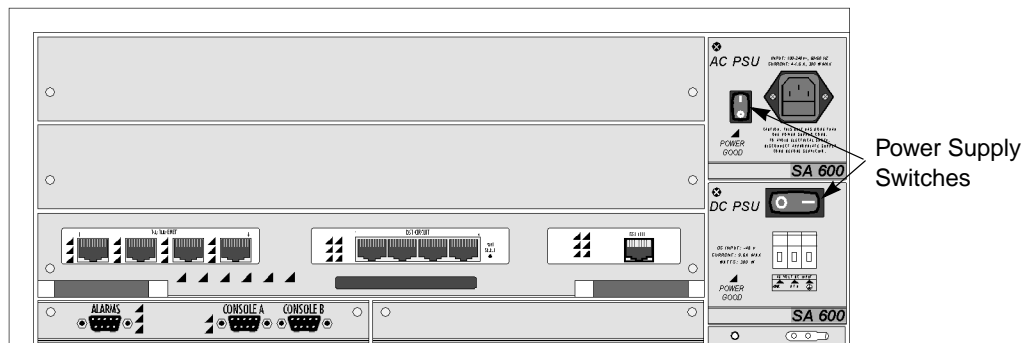
At this point, the SA 100 is ready for use or configuration.



**Figure 2-2. SA 100 Status Indicators**

## Powering Up the SA 600

To power up the SA 600, toggle on the power switch located on the upper power supply, then (if a second power supply is installed) toggle on the power switch on the lower power supply (see [Figure 2-5](#)).

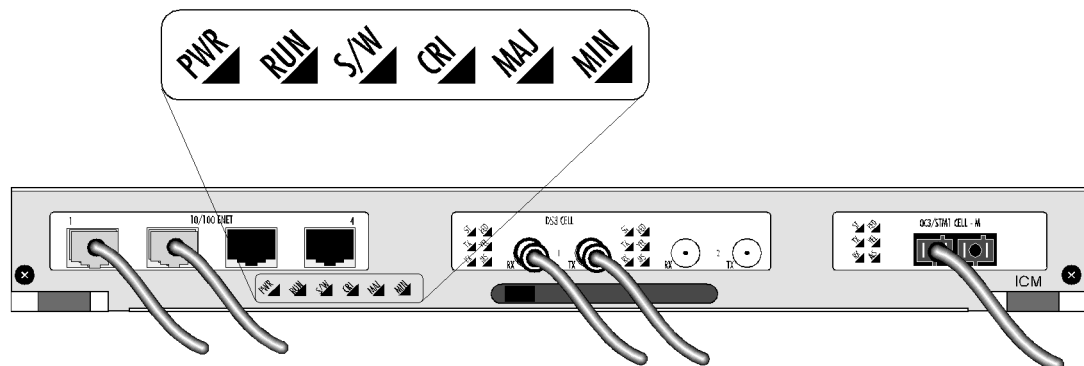


**Figure 2-3. SA 600 Power Switch(es)**

After toggling on the power switch, the SA 600 initializes. During initialization, the front panel indicators of the SA 600 (see [Figure 2-6](#)) follow this sequence:

- PWR turns on and remains on as long as the SA 600 is powered up.
- For approximately 15 seconds, the chassis front panel indicators turn on and off as they run through their power-up sequence.
- Then, for approximately one minute, the RUN indicator blinks once per second, while the MIN indicator is lit.
- Finally, the S/W LED is lit, and ST is lit *on the front panel of each IPOD and XPOD* indicating that the unit is ready for normal operation.

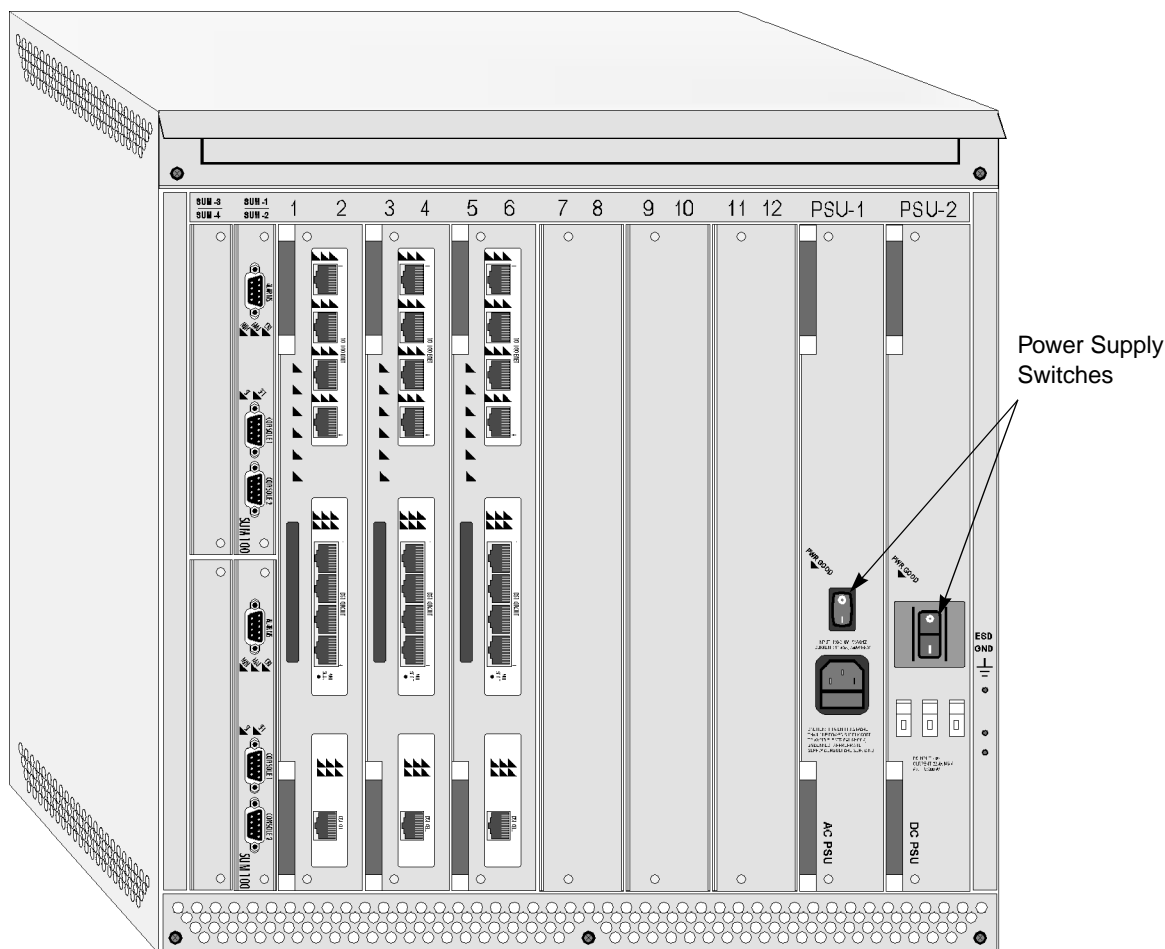
At this point, the SA 600 is ready for use or configuration.



**Figure 2-4. SA 600 Status Indicators**

## Powering Up the SA 1200

To power up the SA 1200, toggle on the power switch located on the upper power supply, then (if a second power supply is installed) toggle on the power switch on the lower power supply (see [Figure 2-5](#)).



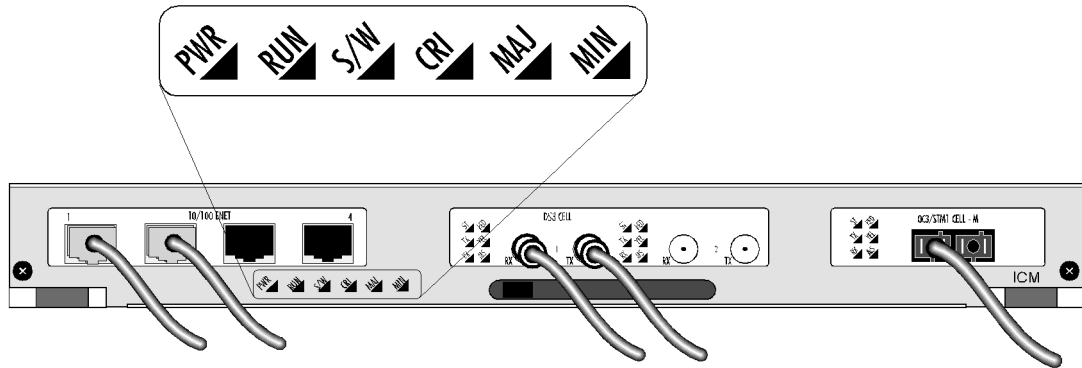
**Figure 2-5. SA 1200 Power Switch(es)**

After toggling on the power switch, the SA 1200 initializes. During initialization, the front panel indicators of the SA 1200, shown in [Figure 2-6](#), follow this sequence:

- PWR turns on and remains on as long as the SA 1200 is powered.
- For approximately 15 seconds, the chassis front panel indicators turn on and off as they run through their power-up sequence.
- Then, for approximately one minute, RUN blinks once per second, while MIN is lit.

- Finally, the S/W LED is lit, and ST is lit *on the front panel of each IPOD and XPOD* indicating that the unit is ready for normal operation.

At this point, the SA 1200 is ready for use or configuration.



**Figure 2-6. SA 1200 Status Indicators**

## Changing the IP address

By default, the IP address of your SA unit is 152.148.126.253. Before using the SA unit in a network environment for the first time, you must change the IP address to match the network topology and the IP address assigned to the node where your SA unit resides.



Before performing this procedure, which uses the SA unit's craft interface, you may want to familiarize yourself with the **"Craft Interface Conventions"** on [page A-7](#).

To change the SA unit's IP address:

7. Prepare your PC terminal emulation software or VT100 terminal as described in **"Setting up the VT100 Terminal"** on [page A-2](#).
8. Make the physical connection from the PC or VT100 terminal to the SA unit's serial port as described in **"Making Craft Interface Connections"** on [page 4-32](#) of the *Hardware Installation Guide*.
9. Power up the SA unit. The SA unit's boot sequence should appear on your terminal screen as described in **"About the SA Unit's Boot Sequence"** on [page A-3](#).
10. Enter your user name at the Login prompt ("root" is the default user name).
11. Enter your password at the Password prompt ("ascend" is the default password). After entering your password, the SA unit displays the Main Menu of the craft interface.
12. Enter **U**.
13. When the Utilities window appears, enter **X**.
14. Enter **sa\_cfg** at the OASOS> prompt.
15. When prompted, enter the new IP address (the current IP address appears in brackets). (Note: The system refers its own IP address as the "fallback IP address".)
16. When prompted, enter the new IP subnet mask (the current IP subnet mask appears in brackets).
17. When prompted, press Enter to leave the Console Port Baud Rate unchanged.  
OASOS displays a list of the parameters followed by:  
  
Is this correct (y/n) [n] ?  
  
Enter **y**.
18. At the OASOS prompt, enter **Exit** to return to the Utilities window.
19. Choose the Cancel button in the Utilities window.

20. Choose the Logoff button in the Main menu.
21. When the Logoff window appears, tab to the Save Configuration box, then press the Space Bar to enter an **X** in the Save Configuration box.
22. Select Yes at the Are You Sure? prompt.
23. Shut down and power up the SA unit.



## Accessing WebXtend

After you change the SA unit's IP address, make an Ethernet connection to the SA unit as described in **“Making the Ethernet Management Connection”** on page 4-31 of the *Hardware Installation Guide* and use WebXtend to perform further configuration and management functions.



If you cannot make a direct Ethernet connection due to distance or lack of an Ethernet port, see **Appendix G, “Managing SA Units Remotely”** for details on managing SA units remotely.

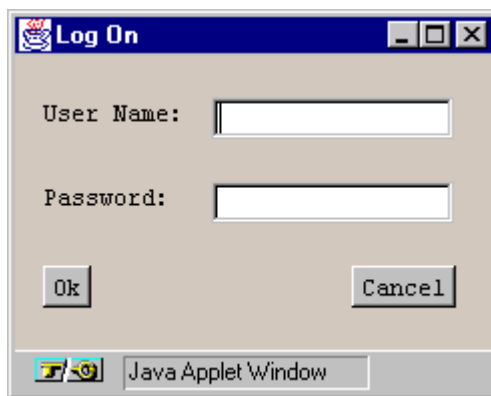
To access WebXtend, start up the Web-browser software on the computer connected to the SA unit. When your Web-browser is up and running, enter the IP address you assigned to the SA unit, using the `http://[IP address]/` format.



The Web-browser you use must be Java-compatible and have Java enabled. See the Release Notes for current browser recommendations.

To access WebXtend using a Web-browser:

1. Enter **http://[IP address]/** in the Location or Address field. When your Web-browser locates the SA unit, it displays the Ascend logo followed by the Log On window (see **Figure 2-7.**)



**Figure 2-7. Log On Window**

2. Enter your user name and password in the appropriate fields (“root” is the default user name, “ascend” is the default password).
3. Choose OK.

If you have logged on successfully, the Main menu of WebXtend appears (see [Figure 2-8](#)). If you entered an incorrect user name and/or password, an error message appears prompting you to try again.



After successfully logging on for the first time, you should immediately create an authorized user profile and delete the default user/password. See [“Setting System Security” on page 3-5](#) for details.



**Figure 2-8. Main Menu**

The Main menu is the starting point for accessing all the functions of WebXtend. You access each function by choosing the appropriate button. [Table 2-1](#) briefly describes the buttons and functions you can access and lists the chapter that describes each function.

**Table 2-1. Main-Menu Buttons and Functions**

<b>Button</b>	<b>Choose this function to...</b>	<b>See Chapter</b>
Administration	Configure SA system-level parameters	3
Monitor Status	Monitor the state of the SA unit	6
Diagnostics	Test the operation of the SA unit	8
Utilities	Save and restore the SA unit configuration and initialize and shut down the SA system	9
Event Management	Customize the SA unit's event and alarm functions and generate event log files	7
Interface Management	Configure the SA unit's ports	4
Service Management	Configure the SA unit's network services	5
Logoff	Exit WebXtend	2

## WebXtend Conventions

To use WebXtend efficiently, you should be familiar with its user interface conventions.

### Navigating Buttons and Fields

There are two ways to navigate the buttons and user-selectable fields that appear in a WebXtend window:

- You can use a mouse connected to your computer.
  - To choose a button or user-selectable field, point and click on the desired button or field.
  - To select an option from a list, point and click on the item. Point and click on the up or down scroll arrows to the right of the desired field to see additional items.
- You can use the Tab, Arrow, and Enter keys.
  - To move between buttons and user-selectable fields, use the Tab key.
  - To scroll through the options in a list, use the Arrow keys.
  - To choose a highlighted button or highlighted option in a user-selectable field, use the Enter key.



A highlighted button has a dotted line bordering its perimeter.  
A highlighted field contains reverse text, i.e., white text on a dark background.

Whether you use a mouse or keys to navigate buttons and fields, the cursor skips over the following buttons and fields because they are not user-selectable:

- Read-only fields, i.e., fields that display information only, contain values but are greyed out and uneditable.
- Gray buttons and fields; blank, gray fields or grey buttons indicate that your SA unit does not support a particular function. For example, if your SA unit does not contain an Ethernet POD, all buttons and fields related to the Ethernet POD are gray.

## Clicking vs. Double-Clicking

In most cases, you only have to click once to select an item in a WebXtend window. The main exception is on the windows displaying the SA unit's front panel. To select a system, slot, POD, or port (to monitor or configure), you must double-click (click twice) on the item to monitor or configure. This action also applies when selecting an item from a list to obtain additional information (for example, to select an individual POD from the Select POD list in the Display Board Status window).

## OK, Cancel, and Apply Buttons

OK, Cancel, and Apply buttons appear in various WebXtend windows. These buttons do the following:

**OK** — Confirms all previous actions you have performed in a window, saves all current configuration additions or changes, and then closes the window.

**Cancel** — Closes the window without saving any configuration additions or changes made in the window.

**Apply** — Enters all previous actions you have performed, saves all current configuration additions or changes, and keeps the window open.

## Events/Alarms Field and Button

In the upper-right corner of each WebXtend full-size window is an Events/Alarms field and button, which do the following:

**Events/Alarms field** — Displays the severity (Critical, Major, or Minor) of the most severe current alarm, if any, detected by the SA unit.

**Events/Alarms button** — Enables you to display a summary of the current events and alarms, if any.

## Window Buttons

Most other buttons on the WebXtend interface are window buttons, which invoke a pop-up window or prompt you to enter information in a secondary window. Enter the required information, then choose OK to return to the previous window.

## Command Buttons

Command buttons are available on some WebXtend screens. Command buttons enable you to issue a command which is immediately executed. A common command is Clear Fields, which clears the fields on the current window.

## Help Field

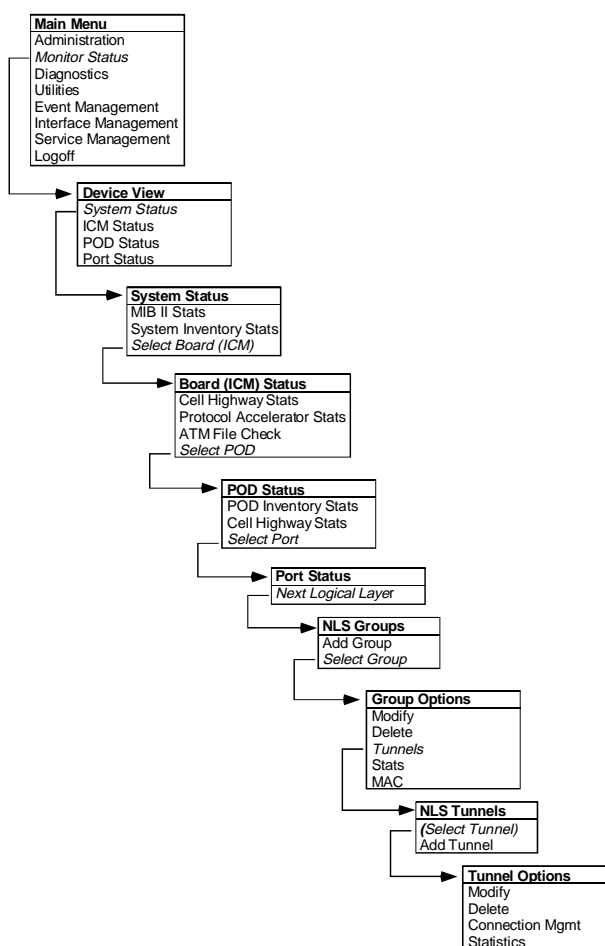
Near the bottom of each WebXtend window is a Help field. This field provides a brief, one-line description of the currently selected button or field. For example, in **Figure 2-8**, the Help field describes the function of the Administration button.

## WebXtend Screen Hierarchy

To use WebXtend efficiently, you should understand the hierarchical layout of the screens and how to move between them.

### Understanding the Program Flow

WebXtend is designed to provide a logical, flowing interface to the SA unit. Beginning at the broadest level (the SA unit as a piece of hardware), the interface guides you through subsequently more detailed levels to the lowest level available (detailed communications parameters). **Figure 2-9** shows an overview of this design.



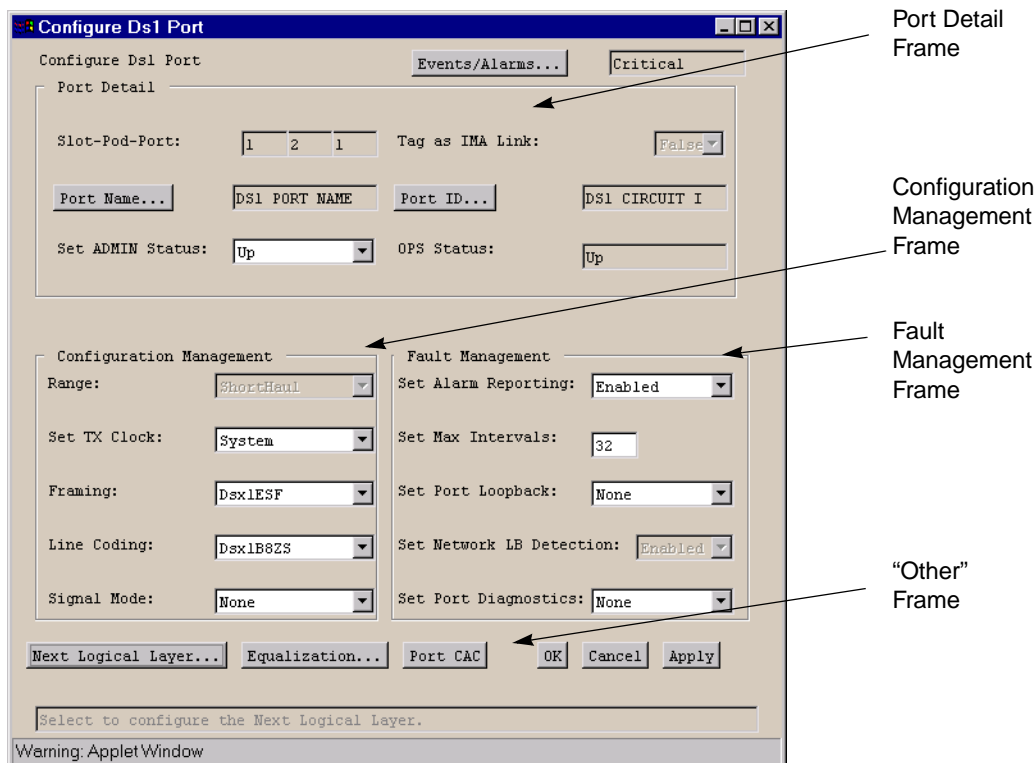
**Figure 2-9. WebXtend Screen Hierarchy Example**

WebXtend's Main menu provides access to various functions. For example, when you choose the Monitor Status button, the system displays the SA unit's front panel, representing the unit as a whole. From this point, you can select a component to view, for example the ICM. At the ICM screen, you can select a POD to view. At the POD screen, you can select a single port to view. At the port screen, you can view various port-level communication details and proceed to the next logical layer, in this case the Native LAN Services screen. At the NLS Groups screen, you can add or select a group, bringing you to the NLS Group Options screen, and so on, reaching a greater level of detail with each window.

In addition to this depth of detail, WebXtend provides further breadth at many layers. Additional windows are often available to provide greater details on a given layer. For example, at the System Status window, you can choose to view MIB II Statistics or System Inventory Statistics, or you can continue drilling down to the board level.

## Understanding the Screens

WebXtend windows are divided into “frames” or sections of related information:



**Figure 2-10. Typical WebXtend Window**

In the example shown, the window contains several frames: Port Detail, Configuration Management, Fault Management, and an unlabeled area at the bottom containing several buttons (the “Other” frame).



The fields in a window are usually organized as follows:

- The frame at the top of the window contains reference information such as the Slot:Pod:Port fields.
- Frames in the middle of the window are usually user-configurable parameters.
- Frames near the bottom of the screen generally contain command buttons that open the next logical layer, or accept or cancel any changes you may have made.

## Common Screen Fields

This manual describes each screen available in WebXtend. In general, you will find a brief description of the window's purpose and contents, along with a screen shot of the window. Following the figure, a table describes the screen fields.

There are some fields that appear on nearly every WebXtend window, typically reference fields such as Slot/Pod/Port. Rather than repeat these fields in every table throughout the manual, [Table 2-2](#) explains these common fields.

**Table 2-2. Common Fields/Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the port's slot, POD, and port numbers.
Port Name	window button	Enables you to specify the port name (32 characters max).
Port ID	window button	Enables you to specify the port ID (32 characters max).
Set ADMIN Status	read/write	Enables you to set the administrative state of the port up or down. Default is up (online). Set to Down (offline) when you run diagnostics. The Testing option is not supported.
OPS Status	read-only	Displays the operational state of the port: up or down.
Events/Alarms	window button	Opens the Events/Alarms Log window.
Clear Fields	command button	Clears any changes you may have made in the current window. Note: the Clear Fields button will not clear any changes that have already been entered by pressing OK.

**Table 2-2. Common Fields/Buttons (Continued)**

Field/Button	Type	Action/Description
Clear Counters	command button	Resets any counters in the current window to zero. Note: the display may not be able to stay current with the real-time counters, so you may never actually see zero appear in a particular field.
Connect Detail	read-only	<p>Displays error codes if any failure is present on this connection; otherwise blank. Common error conditions include:</p> <ul style="list-style-type: none"> <li>• <i>VpvcUsed</i> – "Port / VPI / VCI" of either source or destination is already in use.</li> <li>• <i>vpi-OOR</i> – VPI of either the source or destination is out of range.</li> <li>• <i>vci-OOR</i> – VCI of either the source or destination is out of range.</li> <li>• <i>vpi-Rsvd</i> – PVCs source or destination VPI is within the range reserved for PVPs.</li> <li>• <i>pvp-OOR</i> – PVPs source or destination VPI is outside the range reserved for PVPs.</li> <li>• <i>rate-OOR</i> – PCR/SCR in traffic descriptor is out of range. Depending on service category: PCR is less than SCR, or rate descriptor is non-zero when it should be zero, or rate is zero when it should be non-zero.</li> <li>• <i>desc-OOR</i> – Traffic Descriptor out of range. One or more of these descriptors are not in the list of MIB enumerations: Service Category, Congestion Action, or Buffer Size.</li> <li>• <i>port-bad</i> – Power-on self-test diagnostics have disabled this port.</li> </ul>

## Logging Off WebXtend

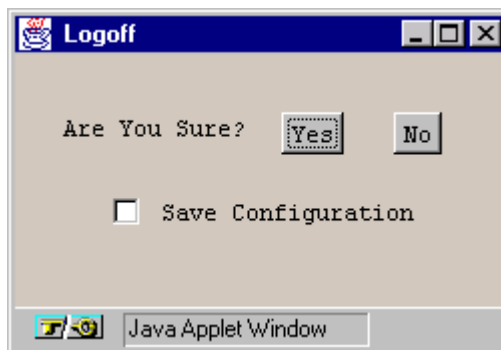
To log off and exit WebXtend:

1. Choose the Logoff button from the Main menu.
2. When the Logoff window appears (see [Figure 2-11](#)), click in the Save Configuration box to preserve any provisioning and configuration work you may have performed during this WebXtend session.



SA units do not save configurations automatically. You must click in the Logoff window's Save Configuration box, then click Yes, to save a configuration. The dialog box reads "Saving..." and shows a progress indicator. When the dialog box closes, it is safe to turn off the unit.

**WARNING:** Turning off an SA unit before it has finished saving configuration data can cause corruption of the configuration file and result in improper operation of the unit the next time it boots up.



**Figure 2-11. Logoff Window**

3. Choose the Yes button.
4. Exit your Web-browser, if desired.

## Shutting Down an SA Unit

To shut down the SA unit, toggle off the power switch(es) (see [Figure 2-5](#)).

## What's Next?

After you are familiar with the basics of WebXtend, you can configure the system-level parameters of the SA unit as described in **Chapter 3, “Configuring the System.”**

# Configuring the System

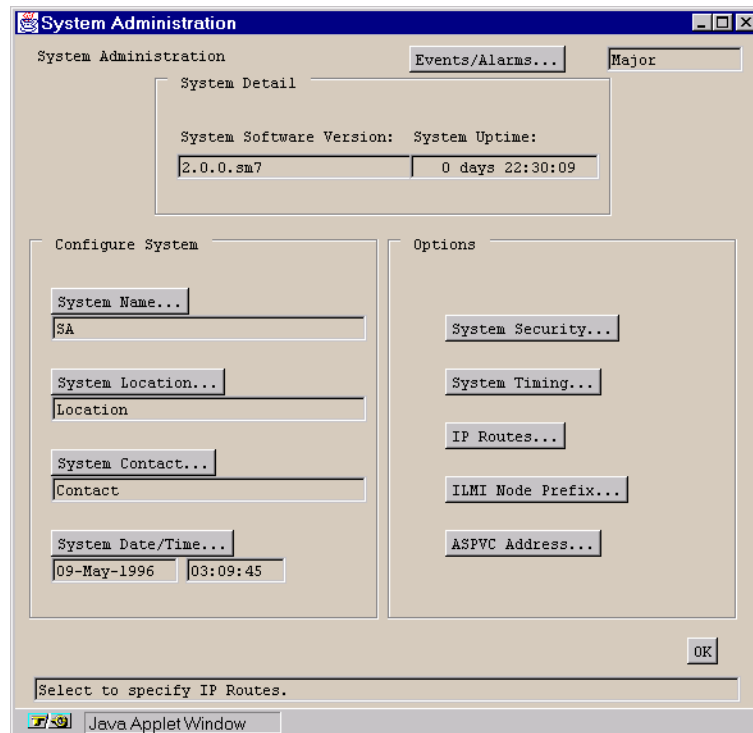
This chapter describes how to configure the following SA unit parameters:

- System name (see [page 3-2](#))
- System location (see [page 3-2](#))
- System contact (see [page 3-2](#))
- System date and time (see [page 3-2](#))
- System security (see [page 3-5](#))
- System timing (see [page 3-8](#))
- IP routing (see [page 3-11](#))
- ILMI node prefixes (see [page 3-14](#))
- Power supply alarm reporting (see [page 3-14](#))
- System CAC parameters (see [page 3-22](#))

## Accessing System Administration Functions

To access System Administration functions and set system parameters:

1. Choose the Administration button from the Main menu. The System Administration window appears (see [Figure 3-1](#)).



**Figure 3-1. System Administration Window**

2. Complete the fields described in [Table 3-1](#).
3. Refer to the sections on Security, System Timing, IP Routes, ILMI Node Prefixes, and ASPVC Address as necessary, completing these procedures.
4. Choose OK to close the System Administration window and save your changes.

**Table 3-1. System Administration Fields and Buttons**

Field/Button	Type	Action/Description
<b>System Detail</b>		
System Software Version	read-only	Displays the level of the program code running in the SA unit.
System Uptime	read-only	Displays the elapsed operating time since the SA unit's last power up.
<b>Configure System</b>		
System Name	read/write	Set/display the name of the SA unit (128 characters max.)
System Location	read/write	Set/display the name of the SA unit's physical site (128 characters max.)
System Contact	read/write	Set/display a contact name, telephone number, e-mail address, etc., for the SA unit (128 characters max.).
System Date/Time	read/write	<p>Set/display the SA unit's system date and time.</p> <p><i>Date</i> – Use DD-MMM-YYYY, where DD is the day of the month (01-31); MMM is the three letter abbreviation representing the month; and YYYY is the numeral representing the year. For example, to set the date to March 8, 1998, enter 08-Mar-1998.</p> <p><i>Time</i> – Use HH:MM:SS, where HH, MM, and SS are the numerals representing hours, minutes, and seconds, respectively. The SA unit's internal clock marks time on a 24-hour basis, representing the hours 1 PM through 11 PM by the numerals 13 through 23; midnight is represented by 00. For example, to set the time to 8:30 PM, enter 20:30:00.</p>
<b>(Other Buttons)</b>		
Security	window button	Enables you to set operator names, passwords, security levels, and access to applications. See <a href="#">“Setting System Security” on page 3-5.</a>
System Timing	window button	Enables you to set the SA unit's clocking parameters. See <a href="#">“Setting System Timing” on page 3-8.</a>
I/P Routes	window button	Opens the I/P Routes window. See <a href="#">“Specifying IP Routes” on page 3-11.</a>
ILMI Node Prefix	window button	Opens the ILMI Node Prefix window. See <a href="#">“Specifying ILMI Node Prefixes” on page 3-14.</a>

**Table 3-1. System Administration Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
ASPVC Addresses	window button	Opens the ASPVC Address Configuration window. See <i>“Specifying ASPVC Addresses” on page 3-19.</i>

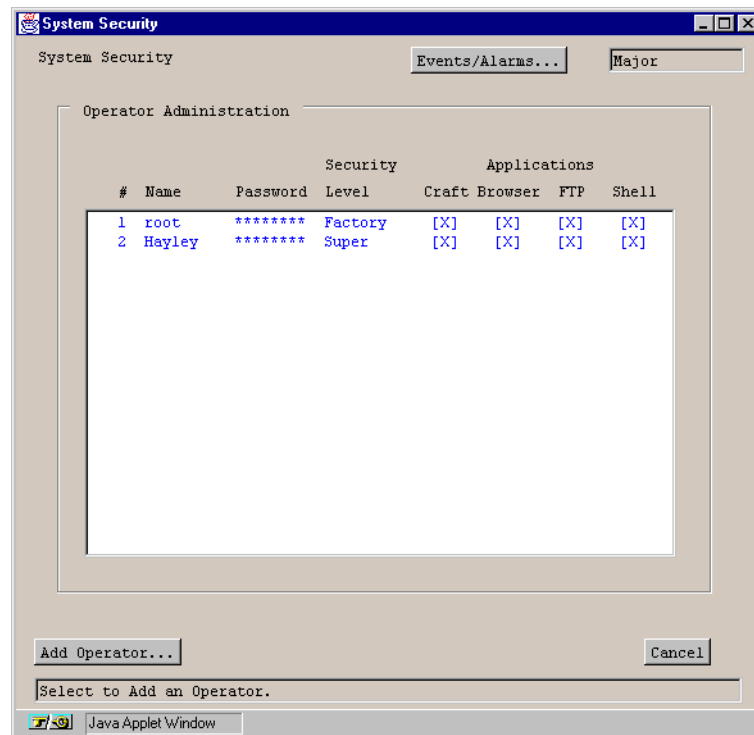


## Setting System Security

SA unit system security is controlled through the creation of operators. You assign passwords and security levels to each operator, and give each operator access to some or all SA applications.

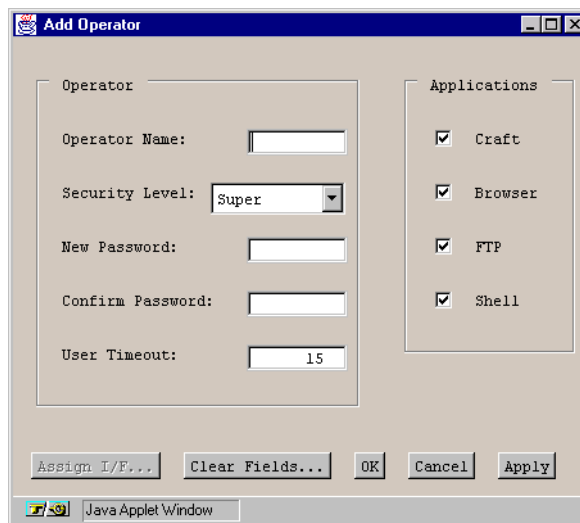
To configure system security parameters by creating or modifying an operator:

1. Choose the Security button from the System Administration window. The System Security window appears (see [Figure 3-2](#)).



**Figure 3-2. System Security Window**

2. The System Security window lists the authorized operators, their security level and the applications they can access. In [Figure 3-2](#) operator Hayley has been added to the system. For security, eight asterisks appear in the Password field instead of the actual password. Hayley has a security level of “Super” and can access all the SA management applications.
3. To add a new operator, choose the Add Operator button. The Add Operator window appears. (See [Figure 3-3](#).)



The 'Add Operator' window is a Java Applet Window with a title bar. It contains two main sections: 'Operator' and 'Applications'. The 'Operator' section has five fields: 'Operator Name' (text input), 'Security Level' (dropdown menu set to 'Super'), 'New Password' (text input), 'Confirm Password' (text input), and 'User Timeout' (text input set to '15'). The 'Applications' section has four checkboxes, all of which are checked: 'Craft', 'Browser', 'FTP', and 'Shell'. At the bottom, there are five buttons: 'Assign I/F...', 'Clear Fields...', 'OK', 'Cancel', and 'Apply'.

**Figure 3-3. Add Operator Window**

4. Complete the fields described in [Table 3-2](#).
5. When you are done, choose OK.
6. To modify or delete an existing operator, select the operator name in the System Security window. The System Security Options window appears ([Figure 3-4](#)).



The 'System Security Options' window is a Java Applet Window with a title bar. It displays a table with three columns: '#', 'Name', and 'Security Level'. The table has one row with the values '2', 'Hayley', and 'Super'. Below the table are three buttons: 'Modify...', 'Delete...', and 'Cancel'.

**Figure 3-4. System Security Options Window**

7. Choose Modify to change the operator's attributes or Delete to delete the operator. Choosing Modify opens the Modify Operator window which enables you to change the user name and application access ([Table 3-2](#) describes these fields). You cannot change passwords and security levels once entered. Choosing Delete prompts you for confirmation before deleting the selected operator.
8. When you have finished modifying or deleting the operator, choose OK to return to the System Security window.
9. Choose OK to close the System Security window and save your changes.

**Table 3-2. Adding an Operator**

Field/Button	Type	Action/Description
Operator Name	read/write	Set/display the current operator's name.
Security Level	read/write	Set/display the current operator's security level. Currently, only the Super security level is supported.  <i>Super</i> — enables the operator to view and modify all SA unit parameters.
New Password	read/write	Set/display the password for the operator. A password may not be changed once it is authenticated in the Confirm Password field and the Add Operator window is closed.
Confirm Password	read/write	Re-enter the password for confirmation.
User Timeout	read/write	Enter the number of minutes the system will wait in an idle state before automatically logging this user off.
Applications	read/write	Set/display the SA applications which the operator can access:  <i>Craft</i> — Enables the operator to configure, monitor, and control the SA unit locally or remotely using a series of menu-driven screens on a VT100 terminal or on a computer running VT100 terminal emulation software.  <i>Browser</i> — Enables the operator to configure, monitor and control the SA unit using the Web browser interface (WebXtend).  <i>FTP</i> — Enables the operator to use the File Transfer Protocol and Zmodem to transfer files to and from the SA unit.  <i>Shell</i> — Enables the operator to access the SA unit's operating system and to configure certain parameters within the SA unit, for example, the IP address and IP subnet mask.
Assign I/F	window button	Select which interfaces the operator can access.  This feature is not currently supported.

## Setting System Timing

The system timing parameters set the primary and secondary reference clocking options of the SA unit.

To configure the System Timing parameters:

1. Choose the System Timing button from the System Administration window. The System Timing window appears (see [Figure 3-5](#)).

The screenshot shows the 'System Timing' window with the following fields and controls:

- System Timing Status:**
  - Primary Source: Recovered
  - Secondary Source: Internal
  - Primary Status: Active
  - Secondary Status: Standby
- Configure Primary:**
  - Set Source: Recovered (dropdown)
  - Set EXT I/F: (empty text box)
  - Set RX I/F: 5, 1, 1 (three separate text boxes)
- Configure Secondary:**
  - Set Source: Internal (dropdown)
  - Set EXT I/F: (empty text box)
  - Set RX I/F: (three empty text boxes)
- Configure Timing Control:**
  - Set Auto Revert: Yes (dropdown)
  - Set Delay: 0 (text box)
  - Manual Override: p, s (two text boxes)
- Buttons:** OK, Cancel, Apply
- Footer:** Select to specify Primary Reference Clock Source. JavaApplet Window

**Figure 3-5. System Timing Window**

2. Complete the fields described in [Table 3-3](#).
3. When you are done, choose OK to return to the System Administration window.

**Table 3-3. System Timing Fields and Buttons**

Field/Button	Type	Action/Description
<b>System Timing Status</b>		
Primary/Secondary Source	read-only	Displays the primary and secondary timing sources: internal clocking or recovered clocking.
Primary/Secondary Status	read-only	Displays the state of the primary and secondary timing: active, standby, failed, or no configuration.
<b>Configure Primary/Secondary</b>		
Set Source	read/write	<p>Select one of the following options:</p> <p><i>Internal</i> – (default) SA unit uses its own internal reference oscillator as the primary reference clock source.</p> <p><i>Recovered</i> (received) – SA unit uses the timing recovered from the interface specified in the Set RX I/F field as the primary reference clock source.</p> <p><b>Note:</b> Never disable alarm reporting on any port used for primary or secondary recovered timing. (External clocking is not currently supported by SA units.)</p>
Set EXT I/F	(disabled)	(Not currently supported.)
Set RX I/F	read/write	Enter the slot, POD and port numbers used for the primary and secondary recovered (received) clocking source.
<b>Configure Timing Control</b>		
Set Auto Revert	read/write	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Yes</i> – the SA unit automatically switches from secondary to primary reference clocking after the primary clock has recovered from a failure. If you select Yes, you must also enter a value in the Set Delay field.</li> <li><i>No</i> – the SA unit will continue using the secondary reference clocking even after the primary clock recovers. With Auto Revert disabled, you must set the Manual Override field to return control to the primary clock.</li> </ul>

**Table 3-3. System Timing Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Delay	read/write	Enter the number of seconds (0 to 30) the SA unit will wait after the primary clock has recovered from a failure before auto-reverting to the primary clock's timing. Zero delay causes the clock to auto-revert immediately.
Manual Override	read/write	Select primary (P) or secondary (S) clocking as the system-timing source, thus overriding all other system-timing parameters (subject to the link status).

## Specifying IP Routes

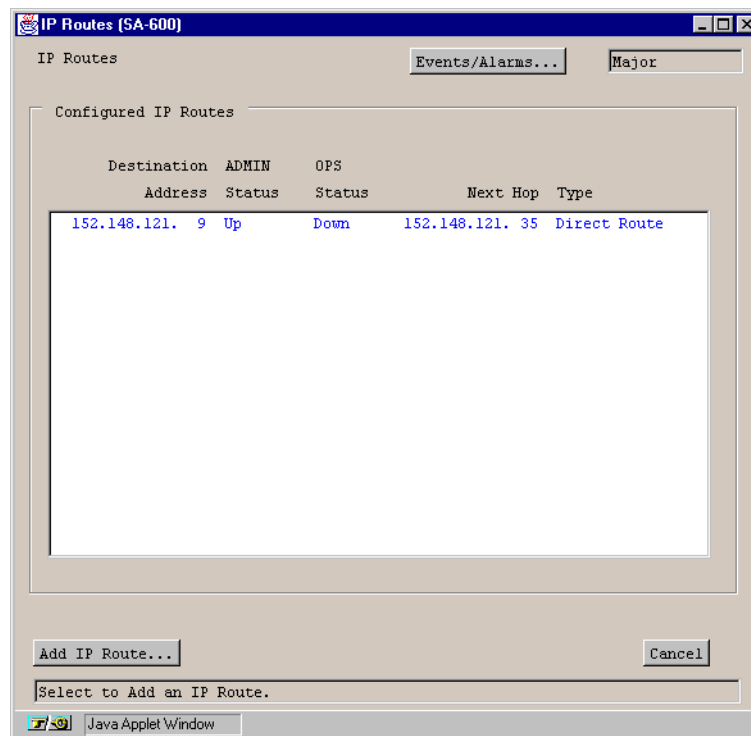
IP Routes establish paths to NMS stations. Establishing an IP route defines a gateway (i.e., an IP router or switch) for the SA unit to use when passing TCP/IP traffic between network segments connected by the gateway.



IP routes are stored outside the nv\_db.dat configuration file which stores other SA unit configuration information. This allows IP routes to be preserved across software upgrades and flash-file system formats.

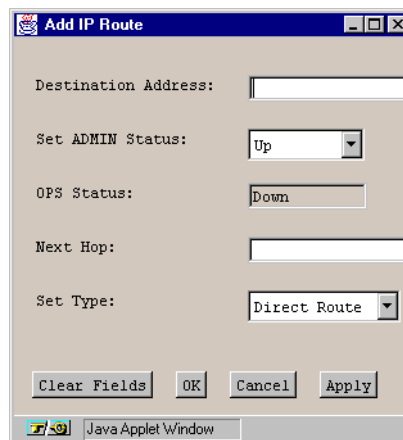
To access the IP Routes parameters and add an IP route:

1. Choose the IP Routes button from the System Administration window. The IP Routes window appears (see [Figure 3-6](#)), showing any existing IP routes.



**Figure 3-6. IP Routes Window**

2. Choose the Add I/P Route button. The Add IP Route window appears (see [Figure 3-7](#)).

A screenshot of a Java Applet window titled "Add IP Route". The window has a light beige background and a blue title bar. It contains several input fields and buttons. The fields are: "Destination Address:" with a text box; "Set ADMIN Status:" with a dropdown menu showing "Up"; "OPS Status:" with a dropdown menu showing "Down"; "Next Hop:" with a text box; and "Set Type:" with a dropdown menu showing "Direct Route". At the bottom, there are four buttons: "Clear Fields", "OK", "Cancel", and "Apply". The status bar at the bottom of the window shows "Java Applet Window".

**Figure 3-7. Add IP Route Window**

3. Complete the fields described in [Table 3-4](#).
4. Choose OK to return to the IP Routes window.

**Table 3-4. Adding an IP Route**

Field/Button	Type	Action/Description
Destination Address	read/write	Enter the destination IP address.
Set ADMIN Status	read/write	Set the administrative state of the IP Route: up or down.
OPS Status	read-only	Display the operational state of the IP Route: up or down.
Next Hop	read/write	Enter the IP address of the next hop.
Set Type	read/write	Select the IP Route Type: Direct Route or Indirect Route.



## Modifying, Deleting, or Connecting IP Routes

To modify, delete, or connect an IP route

1. Double-click the IP route in the IP Routes window (Figure 3-6). The IP Route Options window appears (see Figure 3-8).

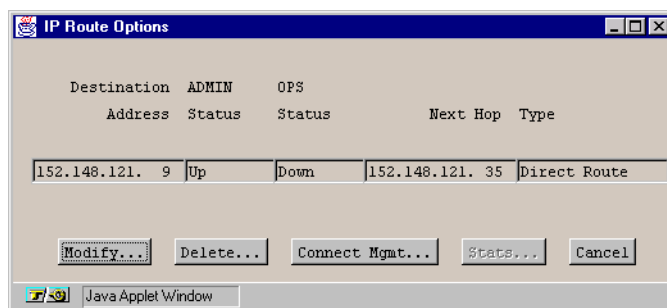


Figure 3-8. IP Route Options Window

2. Select Modify to make any desired changes, then choose OK.
3. Select Delete delete the selected IP route.
4. Select Connect Mgmt to open the Connection Management dialog box (see Figure 3-9 on page 3-13).
5. Set the Connect Status for the IP route to Up or Down by choosing the Connect or Disconnect button.

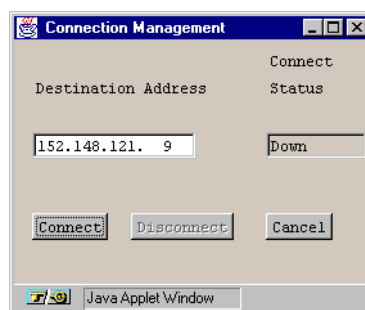


Figure 3-9. Connection Management Window

## Specifying ILMI Node Prefixes

Interim Local Management Interface (ILMI) provides status and communication information to ATM UNI devices and provides for a port keep-alive protocol. WebXtend currently implements the following ILMI functions:

- Address registration based on configured Network and Port Prefix tables
- Rejection of duplicate ATM addresses from DTE devices
- Initiation of link connectivity “keep-alive” messages
- Support for ILMI “gets” for ATM and physical layer statistics

WebXtend implements ILMI in one of three modes: none (ILMI deactivated), DTE mode (SA unit considered user side of UNI), and DCE mode (SA unit considered network side of UNI).

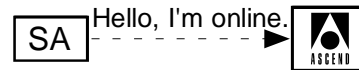


The functions supported by the two active modes depend upon the UNI protocol variant selected when the ATM interface is configured. See **“Configuring ATM UNI Services and Connections”** on page 5-33 for more details.

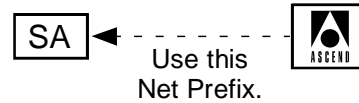
When ILMI is deactivated, net prefixes must be entered manually, and none of the other ILMI functions occur (address registration, keep-alive messages, etc.).

When ILMI is activated in DTE mode, the startup and keep-alive process happens as shown in **Figure 3-10**.

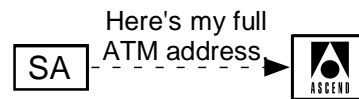
On startup, SA unit sends a cold-start message to the switch over its pre-configured trunk connection.



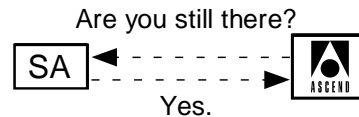
The switch replies with a Net Prefix for the SA unit to use.



The SA unit appends its ESI to the Net Prefix, creating a complete ATM address, and sends this address back to the switch for registration.



Finally, the switch begins a period keep-alive message exchange to ensure that the SA unit is still present.



**Figure 3-10. ILMI Process – DTE mode**

When ILMI is activated in DCE mode, the SA unit plays the role of the network-side ATM switch, reversing the procedures described in [Figure 3-10](#). The SA switch does out Net Prefixes and sends keep-alive messages to attached ATM user-side devices.

## About ILMI Node Prefixes

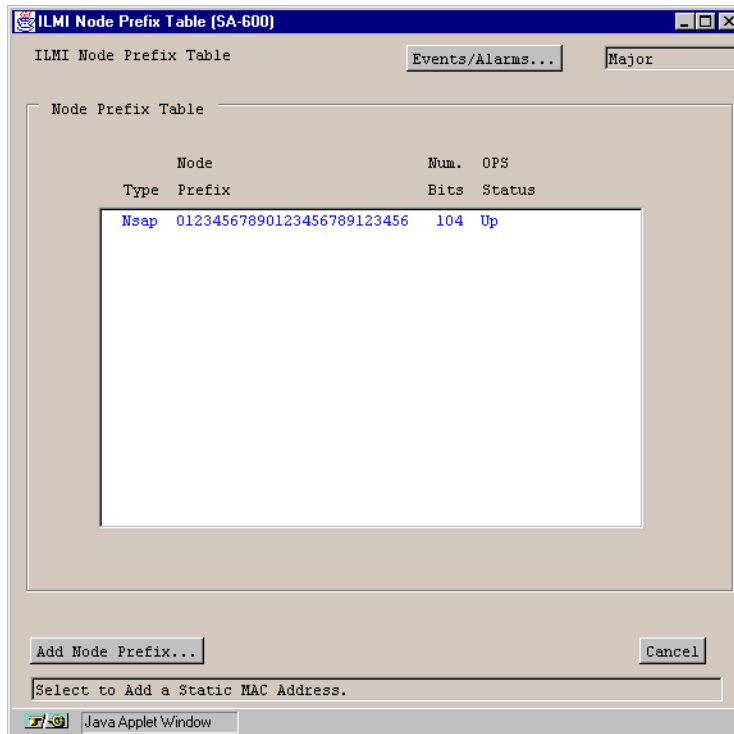
Address information in a switch is used both for determining the proper route for calls and for calling-party screening. When used for route determination, the switch advertises an appropriate subset of its configured node prefixes, port prefixes, and port addresses to all other switches in the network. When used for calling-party screening, the switch uses the configured node prefixes, port prefixes, and/or port addresses to determine whether or not a call should be accepted by the network.

To perform these two functions at a UNI, both the user and the network need to know the ATM addresses that are valid at the UNI. Address registration provides a mechanism for address information to be dynamically exchanged between the user and the network, enabling them to determine the valid ATM addresses that are in effect at a UNI. Address registration applies only to UNI ports on which ILMI is enabled. Any ILMI-eligible node or port prefix will be transferred from all ILMI-enabled UNI-DCE ports to their peer DTE devices.

Node prefixes are not exchanged from “public switch” UNI-DCE ports. Only port prefixes are exchanged from these ports.

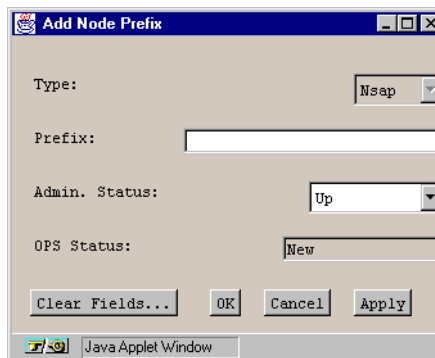
To configure ILMI Node Prefixes:

1. Choose the ILMI Node Prefixes button from the System Administration window. The ILMI Node Prefix Table window appears (see [Figure 3-11](#)).



**Figure 3-11. ILMI Node Prefix Table Window**

2. To add a new ILMI Node Prefix, choose the Add Node Prefix button. The Add Node Prefix window appears (see [Figure 3-12](#)).



**Figure 3-12. Add Node Prefix Window**

3. Complete the fields described in [Table 3-5](#).
4. Choose OK to return to the ILMI Node Prefix Table window.

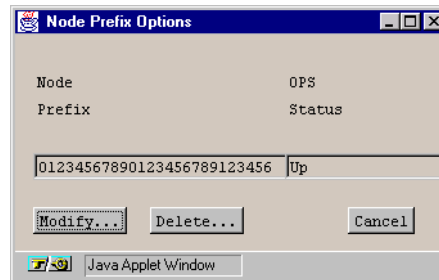
**Table 3-5. Add Node Prefix Fields and Buttons**

Field/Button	Type	Action/Description
Type	read-only	(This field is currently read-only, as only Nsap prefixes are supported.) Select the type of Node Prefix: <i>E.164</i> (not currently supported) - Allows a prefix of up to 16 digits. Prefixes of less than 16 digits will be padded with leading zeros. <i>Nsap</i> - Prefix must be 26 digits. <i>Unknown</i> - (not currently supported)
Prefix	read/write	Enter a node prefix based on the Type selected above.
Admin. Status	read/write	Set the administrative state of the Node Prefix: up or down. (No op not supported.)
OPS Status	read-only	Displays the operational state of the Node Prefix: up or down.

## Modifying or Deleting ILMI Node Prefixes

To modify or delete an ILMI Node Prefix:

1. Double-click the Node Prefix in the ILMI Node Prefix Table window. The Node Prefix Options window appears (see [Figure 3-13](#)).



**Figure 3-13. Node Prefix Options Window**

2. Select Modify to make any desired changes, then choose OK.
3. Select Delete to delete the selected ILMI Node Prefix.

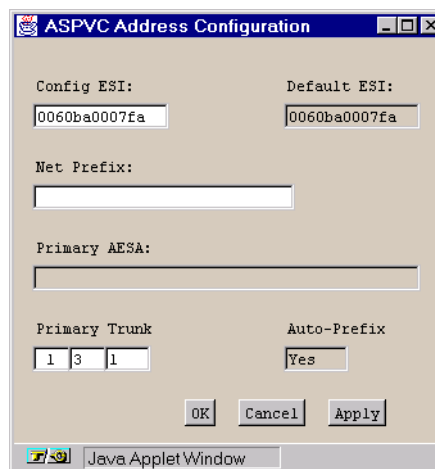
## Specifying ASPVC Addresses

If the SA unit is going to *receive* signalled connections, it must have an ATM End Station Address assigned. (The SA unit may establish signalled connections without having its AESA configured, as the AESA is being used to address the connection to the destination unit only.)

The AESA can be configured automatically using ILMI, if an ATM switch running ILMI is connected to the SA unit's primary trunk. It can also be configured manually if ILMI is disabled or not in use by the ATM switch.

To configure the SA unit's ASPVC Addressing:

1. Choose the ASPVC Addresses button from the System Administration window. The ASPVC Address Configuration window appears (see [Figure 3-14](#)).

The image shows a Java Applet window titled "ASPVC Address Configuration". It contains several input fields: "Config ESI:" and "Default ESI:" both with the value "0060ba0007fa"; "Net Prefix:" which is empty; "Primary AESA:" which is empty; "Primary Trunk" with three input boxes containing "1", "3", and "1"; and "Auto-Prefix" with a "Yes" button. At the bottom are "OK", "Cancel", and "Apply" buttons. The window has a standard Java Applet footer with a small icon and the text "Java Applet Window".

**Figure 3-14. ASPVC Address Configuration Window**

2. Complete the fields described in [Table 3-5](#).
3. Choose OK to return to the System Administration Window.

**Table 3-6. ASPVC Address Configuration Fields and Buttons**

Field/Button	Type	Action/Description
Config ESI	read/write	Displays the Default ESI unless manually edited. The Config ESI should not be changed unless the System Control Module is replaced and you wish to use the original SCM's ESI.
Default ESI	read-only	Displays the System Control Module's MAC address.
Net Prefix	read/write	If Auto Prefix is set to Yes, displays the Net Prefix assigned by the trunk-side ATM switch.  If Auto Prefix is set to No, manually enter the Net Prefix for this unit here.
Primary AESA	read-only	If ILMI is enabled, displays the complete primary AESA as supplied by the trunk-side ATM switch.
Primary Trunk	read/write	Specify the Slot/POD/Port to be used as the primary ATM trunk connection. All A-SPVC and SPVC dial-type connections will be routed out this trunk to the ATM network for switching to their destination.
Auto Prefix	read-only	Displays whether the Net Prefix is obtained automatically (Yes) via ILMI from the ATM switch attached to the primary trunk or entered manually (No) by the user.

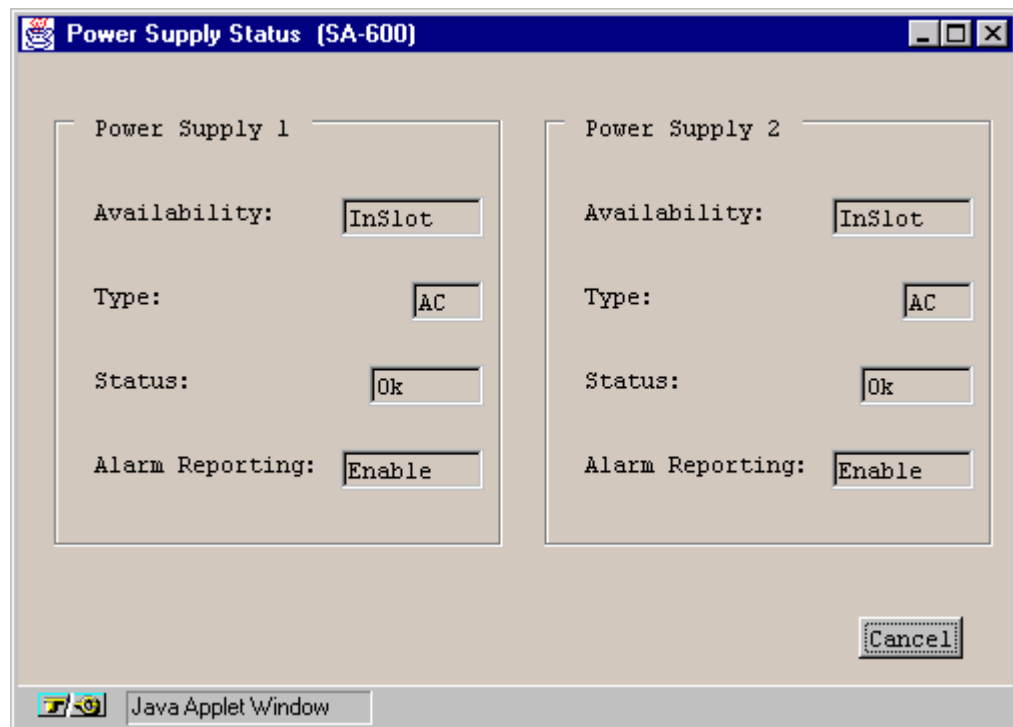


## Configuring Power Supplies on SA 600 and SA 1200 Units

SA 600 and SA 1200 units each support up to two redundant power supplies, which WebXtend can monitor for alarms or failures. You can enable or disable alarm reporting on power supplies.

To configure Power Supply alarm reporting:

1. Select the Interface Management button from the WebXtend Main menu.
2. Double-click on the power supply to configure. The Configure Power Supply Units window appears (see [Figure 3-15](#)).



**Figure 3-15. Configure Power Supply Units Window**

3. Set the Alarm Reporting field for each power supply to Enable or Disable. Enable is the default setting. Disabling Alarm Reporting causes WebXtend to disregard any alarms generated by the selected power supply.
4. Select OK to close the window.

## Configuring Connection Admission Control Parameters

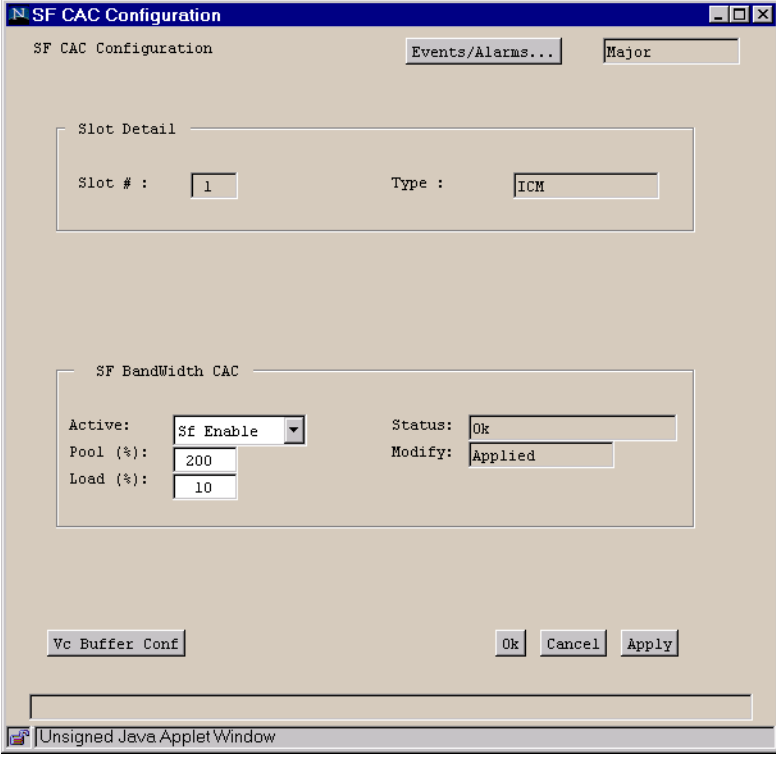
While it is recommended that the SA unit's default Connection Admission Control settings be used for most applications, you can customize the CAC parameters to suit your individual requirements.

(For discussion of CAC theory, see [“Connection Admission Control”](#) on page 1-24.)

### Configuring Switch Fabric CAC

To configure switch fabric CAC:

1. Select the Interface Management button from the WebXtend Main menu.
2. Select System. The Configure System window appears ([Figure 4-2 on page 4-3](#)).
3. Select the CAC button. The SF CAC Configuration window appears ([Figure 3-16](#)).



The image shows a Java applet window titled "SF CAC Configuration". The window has a title bar with standard minimize, maximize, and close buttons. Below the title bar, there are two tabs: "Events/Alarms..." and "Major", with "Major" currently selected. The main content area is divided into two sections. The top section, labeled "Slot Detail", contains two fields: "Slot # :" with a text box containing the value "1", and "Type :" with a text box containing the value "ICM". The bottom section, labeled "SF BandWidth CAC", contains four fields: "Active:" with a dropdown menu showing "Sf Enable", "Status:" with a text box containing "Ok", "Pool (%):" with a text box containing "200", and "Load (%):" with a text box containing "10". There is also a "Modify:" field with a text box containing "Applied". At the bottom of the window, there are three buttons: "Vc Buffer Conf", "Ok", "Cancel", and "Apply". The status bar at the very bottom of the window reads "Unsigned Java Applet Window".

**Figure 3-16. Switch Fabric CAC Configuration Window**

4. [Table 3-7](#) describes the fields and buttons in the SF CAC Configuration window.

**Table 3-7. SF CAC Configuration Fields and Buttons**

Field/Button	Type	Action/Description
<b>Slot Detail</b>		
Slot #	read-only	Displays the currently selected slot number.
Type	read-only	Displays the type of hardware installed in this slot.
<b>SF Bandwidth CAC</b>		
Active	read/write	Enable or disable bandwidth CAC on the switch fabric for the selected ICM.
Pool (%)	read/write	Specify the size of the variable bandwidth pool as a percent of total bandwidth.
Load (%)	read/write	Specify the percent of the variable bandwidth component of a connection to apply against the fixed bandwidth pool.
Status	read-only	Displays a status message indicating if the values entered in the Active, Pool, and Load fields are valid.
Modify	read/write	Indicates whether the system must be rebooted for changes made to take effect. Applied indicates that the changes have been accepted by the system; Applied Pending indicates that the system must be rebooted before the changes will take effect.
VC Buffer Conf(iguration)	window button	Opens the VC Buffer Configuration window to configure per-VC buffer allocation. See <a href="#">“Configuring Per-Virtual Connection Buffers” on page 3-24.</a>

### Configuring Per-Virtual Connection Buffers

When a connection is configured with a service class (CBR, nrt-VBR, etc.) and buffer depth (shallow, medium, high), the combination of service class and buffer depth selections result in a number of buffers and a congestion threshold being assigned. The number of buffers and congestion threshold assigned are determined by the per-VC buffer configuration table.

To configure the per-VC buffers:

1. Select the VC Buffer Conf button from the SF CAC Configuration window (see [Figure 3-16](#)).
2. The VC Buffer Configuration window appears (see [Figure 3-17](#)):

The screenshot shows the 'Vc Buffer Configuration' window. It has a title bar with standard window controls. Below the title bar, there are two tabs: 'Events/Alarms...' and 'Major'. The 'Major' tab is selected. The main area is titled 'Vc Buffer' and contains a table with five columns: 'Priority Q', 'Type', 'Depth', 'Congestion', and 'Status'. The table lists configurations for CBR, Multicast, rt-VBR, nrt-VBR, and UBR/ABR service classes, each with Shallow, Medium, and High buffer depths. At the bottom of the window, there are 'Ok', 'Cancel', and 'Apply' buttons. A status bar at the very bottom indicates 'Please enter a value 2..2000' and 'Unsigned Java Applet Window'.

Priority Q	Type	Depth	Congestion	Status
CBR	Shallow	3	2	Ok
CBR	Medium	6	4	Ok
CBR	High	8	6	Ok
Multicast	Shallow	3	2	Ok
Multicast	Medium	6	4	Ok
Multicast	High	8	6	Ok
rt-VBR	Shallow	8	6	Ok
rt-VBR	Medium	15	12	Ok
rt-VBR	High	25	20	Ok
nrt-VBR	Shallow	10	8	Ok
nrt-VBR	Medium	25	20	Ok
nrt-VBR	High	35	30	Ok
UBR/ABR	Shallow	50	25	Ok
UBR/ABR	Medium	500	250	Ok
UBR/ABR	High	2000	1000	Ok

**Figure 3-17. VC Buffer Configuration Window**

3. [Table 3-8](#) describes the fields and buttons in the VC Buffer Configuration window.

**Table 3-8. VC Buffer Configuration Fields and Buttons**

Field/Button	Type	Action/Description
Priority Q(ueue)	read-only	Displays the name of each VC buffer.
Type	read-only	Displays the depth of each buffer. In conjunction with the Priority Queue name, these two fields list each possible priority queue/buffer depth.
Depth	read/write	Select the number of buffers assigned to the Priority Queue of the indicated depth.  For example, in <a href="#">Figure 3-17</a> , the Real-Time VBR High buffer has a depth of 25.
Congestion	read/write	Select the Congestion threshold for the Priority Queue of the indicated depth. When the threshold is reached, the queue is considered to be congested and the selected congestion control actions will be taken.  The value entered must be greater than zero and less than the value in the Depth field.  For example, in <a href="#">Figure 3-17</a> , the Real-Time VBR High buffer has a Congestion threshold of 20 buffers. When 20 buffers are used, the queue is considered to be congested.
Status	read-only	Displays a status message indicating if the values entered in the Depth and Congestion fields are valid.

## Configuring Priority Queues

You can configure the allocation of cell buffers among the priority queues for the various service classes, as well as setting the congestion thresholds and oversubscription limits.

(For a discussion of Priority Queue theory, see “Priority Queuing” on page 1-18.)



The Multicast and ABR service classes (although seen on the Priority Queue Configuration window) are not currently supported, and are present only for use in future SA product development.

To configure the Priority Queues for an ICM:

1. Select the ICM from the Configure System window (see Figure 4-2 on page 4-3).
2. Select the Prior Queue button from the Configure ICM window (see Figure 4-3 on page 4-5). The Priority Queue Configuration window appears (Figure 3-18).

Queues	Alloc. (%)	Limit (%)	Over Sub. (%)	Modify	Status
CBR	10	80	0	Applied	Ok
Multicast	1	80	0	Applied	Ok
rt-VBR	14	70	5	Applied	Ok
nrt-VBR	25	60	20	Applied	Ok
UBR/ABR	50	50	400	Applied	Ok

Figure 3-18. Priority Queue Configuration Window

**Table 3-9. Priority Queue Configuration Fields and Buttons**

Field/Button	Type	Action/Description
<b>Slot Detail</b>		
Slot #	read-only	Displays the currently selected slot number.
Type	read-only	Displays the type of hardware installed in this slot.
<b>Priority Queue</b>		
Queues	read-only	Displays the name of each class of priority queue.
Alloc(ation) (%)	read/write	Specify the percent of buffers allocated to the priority queue for each service class. The values in this column must add up to 100.
Limit (%)	read/write	Specify the congestion threshold for each service class as a percentage of the allocated buffers.
Oversub(scription) (%)	read/write	Specify the oversubscription to be allowed as a percentage of the priority queue for each service class.
Status	read-only	Displays a status message indicating if the values entered in the Allocation, Limit, and Oversubscription fields are valid.
Modify	read-only	Displays a message indicating whether the values you have changed have been accepted by the SA unit ("Applied"), or if a system reboot is required ("Applied Pending").

## Configuring Cell Highway VPI/VCI Ranges

You may configure the range of values to be used for VPI/VCI parameters on a given cell highway.

(For discussion of VPI/VCI use on Cell Highways, see [“About VPI and VCI Ranges” on page 1-25.](#))

To configure the Cell Highway(s) for a POD:

1. Select the ICM from the Configure System window (see [Figure 4-2 on page 4-3.](#))
2. Select the POD from the Configure ICM window (see [Figure 4-3 on page 4-5.](#))
3. Select the CAC button from the Configure POD window (see [Figure 4-3 on page 4-5.](#)). The Select Cell Highway window appears.
4. Select the desired cell highway (there is only one cell highway for most PODs). The Cell Highway Configuration window appears ([Figure 3-19](#)).

The image shows a Java applet window titled "Cell Hwy Configuration". It has a title bar with standard window controls. Inside, there are three main sections: "Pod Detail", "Cell Highway VP", and "VPI/VCI". The "Pod Detail" section has "Slot-Pod:" with input fields "1" and "3", and "Name:" with input field "xpod". The "Cell Highway VP" section has "Total (bit):" with input field "15", "Max (bit):" with input field "6", "Min (bit):" with input field "3", "VP-Range:" with a dropdown menu showing "Vp Ranges Off", "Modify:" with input field "Applied", and "Status:" with input field "Ok". The "VPI/VCI" section has "VPI bit:" with input field "6" and "VCI bit:" with input field "9". At the bottom right are "Ok", "Cancel", and "Apply" buttons. At the bottom left is a text box with "Select to specify the VP ranges". At the very bottom is a status bar that says "Unsigned Java Applet Window".

**Figure 3-19. Cell Highway Configuration Window**



**Table 3-10. Cell Highway Configuration Fields and Buttons**

Field/Button	Type	Action/Description
<b>POD Detail</b>		
Slot # - POD #	read-only	Displays the currently selected slot and POD number.
Name	read-only	Displays the name of the selected POD.
<b>Highway Cell VP</b>		
Total (bit)	read-only	Total # VP/VC bits available on this cell highway based on the installed hardware.
Max (bit)	read-only	Maximum number of VP bits which may be used to identify a VPI on this cell highway
Min (bit)	read-only	Maximum number of VP bits which may be used to identify a VPI on this cell highway
VP range	read-only	Enable or disable the use of PVPs for ports on this cell highway. To use PVPs, this field must be set to VP Ranges On. See <b>“Configuring Port-level CAC” on page 4-43</b> for further details.
Status	read-only	Displays a status message indicating if the values in the VP Total, Max, and Min fields are valid.
Modify	read-only	Indicates whether the system must be rebooted (“Applied-Pend”) for changes made to take effect or if changes take effect immediately (“Applied”).
<b>VPI/VCI</b>		
VPI bit	read/write	Select the number of VPI bits for this cell highway.
VCI bit	read-only	Displays the number of VCI bits for this cell highway. This field is calculated automatically as the Total VP/VC bits minus the VPI bits.

## **What's Next?**

After you set the SA unit's system-level parameters, you can configure the ports, as described in Chapter 4, "Configuring Ports."

# Configuring Ports

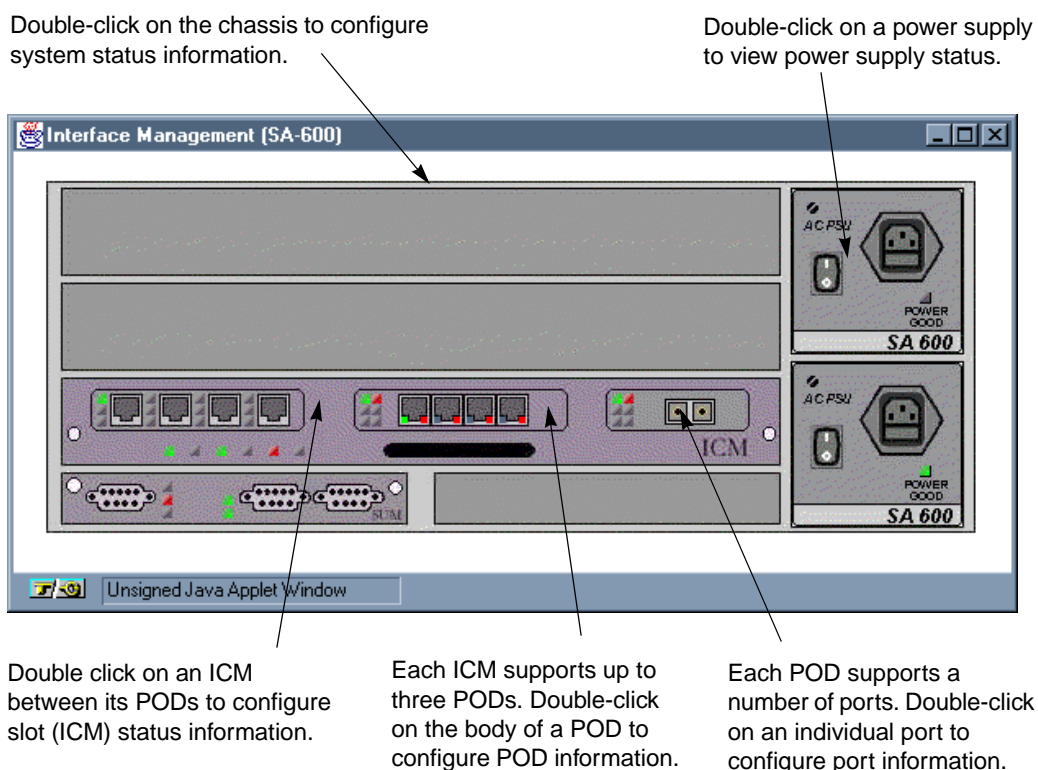
This chapter describes how to configure the following ports:

- Ethernet ports (see [page 4-9](#))
- DS1/E1 ports (see [page 4-11](#))
- DS3/E3 ports (see [page 4-21](#))
- OC-3c/STM-1 ports (see [page 4-30](#))
- Universal Serial ports (see [page 4-55](#))

### Accessing Interface Management Functions

To access the Interface Management functions, choose the Interface Management button from the Main menu.

The Interface Management window appears (see [Figure 4-1](#)), displaying the SA unit's front panel. When you move the mouse pointer over this graphic, callouts appear indicating when the pointer is located over the system, a slot, POD, port, or one of the power supplies. When a callout appears, double-click to select the indicated slot, POD, and/or port.



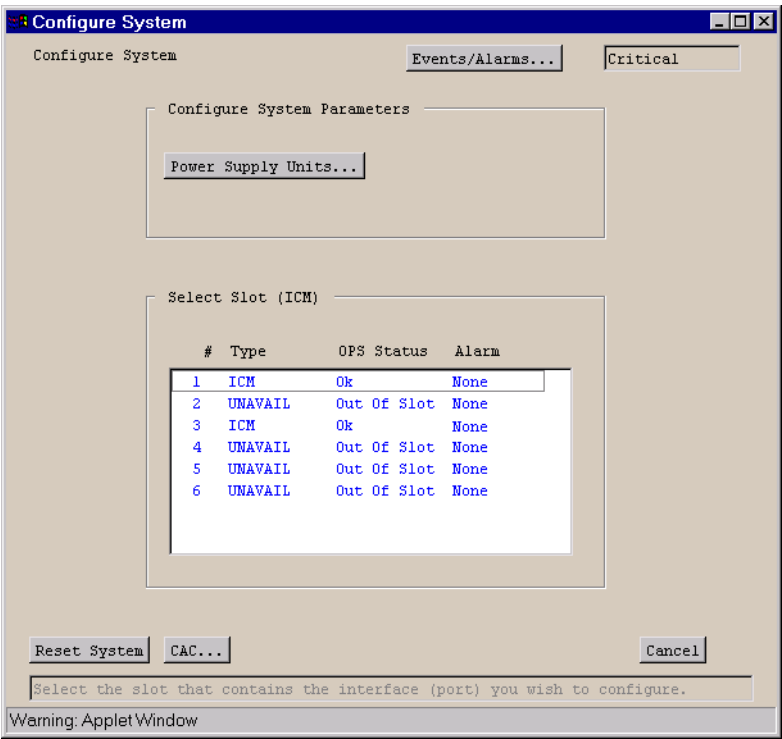
**Figure 4-1. Interface Management Window (SA 600 shown)**

## Selecting an ICM

You can select an ICM in the following ways:

- Select the ICM from the Interface Management window (the callout lists the slot). This method is the quickest and most direct method to select an ICM.
- Select the System object from the Interface Management window (the callout reads *System*).

When the Configure System window appears, select the ICM from the Select Slot list. This method provides additional/expanded information about your selection. (see [Figure 4-2](#).)



**Figure 4-2. Configure System Window**

[Table 4-1](#) describes the fields and buttons in the Configure System window.

**Table 4-1. Configure System Fields and Buttons**

Field/Button	Type	Action/Description
<b>Configure System Parameters</b>		
Power Supply Parameters	window button	Opens the Configure Power Supply window. See <a href="#">“Configuring Power Supplies on SA 600 and SA 1200 Units”</a> on page 3-21.
<b>Select Slot (ICM)</b>		
# (slot number)	read-only	Displays the number of available slots.
Type	read-only	Displays the type of hardware installed in each slot. Currently, ICM is the only option supported. Empty slots are indicated with Unavail(able).
OPS Status	read-only	Displays the OPS status of each slot. Out of slot indicates that nothing is installed in a slot.
Alarm	read-only	Displays the highest level alarm presently detected on a slot.
<b>(Other Buttons)</b>		
Reset System	command button	Reboots the entire SA unit.
CAC	window button	Opens the SF CAC Configuration window for configuring the switch fabric Connection Admission Control parameters. See <a href="#">“Configuring Switch Fabric CAC”</a> on page 3-22.

Selecting the ICM from the Select Slot (ICM) list displays the Configure ICM window (Figure 4-3). [Table 4-2 on page 4-5](#) describes the fields and buttons in the Configure ICM window.

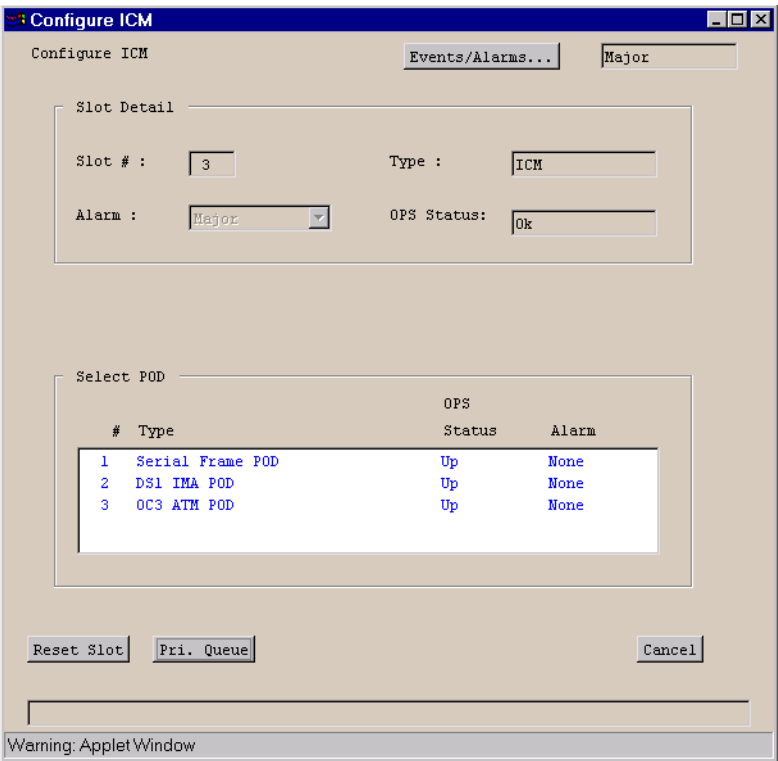


Figure 4-3. Configure ICM Window

Table 4-2. Configure ICM Fields and Buttons

Field/Button	Type	Action/Description
Slot Detail		
Slot #	read-only	Displays the currently selected slot number.
Type	read-only	Displays the type of hardware installed in this slot.
Alarm	read-only	Displays the highest level alarm presently detected on a slot.
OPS Status	read-only	Displays the OPS status of each slot. Out of slot indicates that nothing is installed in a slot.
Select POD		
# (POD number)	read-only	Displays the number of each POD location.
Type	read-only	Displays the type of hardware installed in each POD location.
OPS Status	read-only	Displays the OPS status of each POD.
Alarm	read-only	Displays the highest level alarm presently detected on each POD.

**Table 4-2. Configure ICM Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>(Other Buttons)</b>		
Reset Slot	command button	Resets the currently selected ICM.  Note: If the currently selected ICM is the SCM (System Control Module - the ICM in slot 1), resetting the slot will reboot the entire SA unit.
Prior Queue	window button	Opens the Priority Queue Configuration window for configuring the allocation of cell buffers among priority queues for the various ATM service classes. See <a href="#">“Configuring Priority Queues” on page 3-26.</a>



## Selecting a Port

You can select a port in the following ways:

- Select the *port* directly from the Interface Management window (the callout lists the slot, POD, and port). This method is the quickest and most direct way of selecting a port to configure.

The following methods provide more information concerning your selections. For example, you select a port to configure from the Configure POD window (see [Figure 4-4](#)). This window lists additional port information such as port type, operations status, and alarm conditions.

- Select the *POD* containing the port to configure from the Interface Management window (the callout lists the slot and POD).

When the Configure POD window appears, select the port from the list box.

- Select the *slot* (ICM) from the Interface Management window (the callout only lists the slot).

When the Configure ICM window appears, select the POD containing the port to configure.

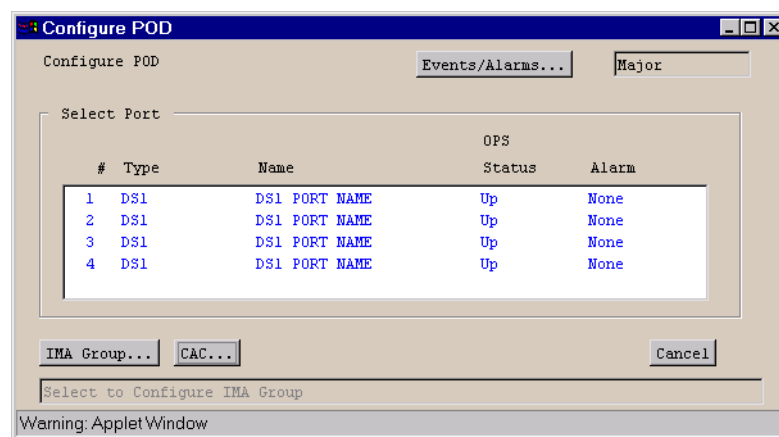
When the Configure POD window appears, select the port from the list box.

- Select the *system* from the Interface Management window (the callout reads *system*).

When the Configure System window appears, use the Select Slot (ICM) field to select the ICM containing the port to configure.

When the Configure ICM window appears, select the POD containing the port to configure.

When the Configure POD window appears, select the port from the list box.



**Figure 4-4. Configure POD Window**

Table 4-3 describes the fields and buttons in the Configure POD window.

**Table 4-3. Configure POD Fields and Buttons**

Field/Button	Type	Action/Description
<b>Select Port</b>		
# (Port number)	read-only	Displays the number of each port location.
Type	read-only	Displays the type of port hardware.
OPS Status	read-only	Displays the OPS status of each port.
Alarm	read-only	Displays the highest level alarm presently detected on each port.
<b>(Other Buttons)</b>		
IMA Group	command button	Available only for IMA PODs, this button opens the IMA Groups window for assigning ports to an IMA group on the POD. See “ <a href="#">Configuring Inverse Multiplex (IMA) Services</a> ” on page 5-46 for details.
CAC	window button	Opens the Cell Highway Configuration window for configuring the VPI/VCI ranges permitted on this POD’s cell highways. See “ <a href="#">Configuring Cell Highway VPI/VCI Ranges</a> ” on page 3-28.

## Configuring an Ethernet Port

To configure an Ethernet port:

1. Select the desired Ethernet port from the Interface Management window, as described in “Selecting a Port” on [page 4-7](#). The Configure Ethernet Port window appears (see [Figure 4-5](#)).

Configure Ethernet Port

Events/Alarms... Major

Port Detail

Slot-Pod-Port: 1 1 1

Port Name... Ethernet Port Port ID... Ethernet Circ

Set ADMIN Status: Up OPS Status: Up

Assigned to NLS Group: ☐ NLS Group Name:

Configuration Management

Set Frame Type: Ethernet Set Rate: Rate 10Mbps

Fault Management

Set Alarm Reporting: Enabled

Service Management... OK Cancel Apply

Select to create/modify a Port Name.

Java Applet Window

**Figure 4-5. Configure Ethernet Port Window**

2. Complete the fields described in [Table 4-4](#).
3. When you are done configuring this port, choose the Service Management button to configure the NLS services as described in “[Configuring Native LAN Services](#)” on [page 5-64](#).
4. Choose OK.

**Table 4-4. Configure Ethernet Port Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the port's slot, POD, and port numbers.
Port Name	window button	Enables you to enter a name for this port (32 characters max).
Port ID	window button	Enables you to enter an ID for this port (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of the port: up (default) or down. Set to down (offline) when you run diagnostics. (The Testing option is not currently supported.)
OPS Status	read-only	Displays the operational state of the port: up or down.
Assigned to NLS Group	read-only	Displays whether the port is assigned to an NLS Group.
NLS Group Name	read-only	Displays the name of the NLS Group this port is assigned to.
<b>Configuration Management</b>		
Set Frame Type	read/write	Specify the type of framing (Ethernet framing) used on the port.
Set Rate	read/write	Set the port's data rate: 10 or 100 Mbps, full- or half-duplex.
<b>Fault Management</b>		
Set Alarm Reporting	read/write	Enable or disable alarm reporting on the port.
<b>(Other Buttons)</b>		
Service Management	window button	Enables you to access and configure NLS services.

## Configuring a DS1 or E1 Port

To configure a DS1 or E1 port:

1. Select the DS1 or E1 port from the Interface Management window (Figure 4-1). The Configure DS1 or E1 Port window appears (see Figure 4-6).

Configure Ds1 Port

Events/Alarms... Critical

Port Detail

Slot-Pod-Port: 1 2 1 Tag as IMA Link: False

Port Name... DS1 PORT NAME Port ID... DS1 CIRCUIT I

Set ADMIN Status: Up OPS Status: Up

Configuration Management

Range: ShortHaul

Set TX Clock: System

Framing: Dsx1ESF

Line Coding: Dsx1B8ZS

Signal Mode: None

Fault Management

Set Alarm Reporting: Enabled

Set Max Intervals: 32

Set Port Loopback: None

Set Network LB Detection: Enabled

Set Port Diagnostics: None

Next Logical Layer... Equalization... Port CAC OK Cancel Apply

Select to configure the Next Logical Layer.

Warning: AppletWindow

Figure 4-6. Configure DS1/E1 Port Window (DS1 shown)



You cannot select IMA DS1/E1 Ports directly from the Interface Management window due to the nature of the physical interface (four ports combined in a single physical interface). Instead, select the IMA DS1/E1 POD to open the Configure POD window, and from the list of ports, select an individual IMA DS1/E1 port to configure.

2. Complete the fields described in Table 4-5. If this is an IMA POD, make sure to set the “Tag as IMA Link” field to True if you want to make this port available to IMA Groups. (IMA PODs enable you to link multiple ports to create a single high-speed aggregate or IMA group. See “Configuring Inverse Multiplex (IMA) Services” on page 5-46 for details.)

3. When you are finished, the next step depends on the type of DS1/E1 POD the port resides on:

- *For ports on a DS1/E1 Cell POD or DS1/E1 IMA POD*, choose the Next Logical Layer button to configure the ATM interface layer of this port, as described in **“Configuring the ATM Interface” on page 4-46**.

When you are finished configuring the ATM interface layer, close the window and configure the other DS1/E1 ports, if any, using the preceding steps.

- *For ports on a DS1/E1 Circuit POD*, choose the Next Logical Layer button to configure the circuit emulation service (CES) connection for this port, as described in **“Configuring Circuit Emulation Services” on page 5-83**.

When you are finished configuring the circuit emulation connection, close the window and configure the other DS1/E1 ports, if any, using the preceding steps.

- *For ports on a DS1/E1 Voice Compression POD*, choose the Next Logical Layer button to configure the Voice Compression service (VCS) connections for this port, as described in **“Configuring Voice Compression Service” on page 5-117**.

When you are finished configuring the VCS connection, close the window and configure the other DS1/E1 ports, if any, using the preceding steps.

4. When you are finished configuring DS1/E1 ports, close the window and go to the applicable sections of this chapter to configure other types of ports, if any.
5. When finished, choose OK.

**Table 4-5. Configure DS1/E1 Port Buttons and Fields**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the port's slot, POD, and port number.
Tag as IMA Link (IMA DS1/E1 PODs only)	read/write	Select True to make the port available to add to an IMA group. Select False to prevent this port from being available to add to an IMA group.  IMA DS1/E1 PODs enable you to link multiple ports to create a single higher-speed aggregate called an IMA Group. See <a href="#">“Configuring Inverse Multiplex (IMA) Services”</a> on page 5-46 for more information.
Port Name	window button	Specify the port name (32 characters max).
Port ID	window button	Specify the port ID (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of the port: up (default) or down. Set to Down (offline) when you run diagnostics. (The Testing option is not currently supported.)
OPS Status	read-only	Displays the operational state of the port: up or down.
<b>Configuration Management</b>		
Range (DS1/E1 Cell POD with CSU only)	read/write	Select the range for the line: ShortHaul or LongHaul. This field determines which window is opened by the Equalization button.
Set TX Clock	read/write	Select the source of transmit timing on the port. Options are:  <i>Loop</i> – The transmit timing is derived from the timing signal coming into this port.  <i>System</i> (default) – System timing provides the transmit timing for this port; configure System Timing in the System Administration window (see <a href="#">page 3-8</a> ).  <i>Local</i> – The POD's internal timing source provides the transmit timing for this port.

**Table 4-5. Configure DS1/E1 Port Buttons and Fields (Continued)**

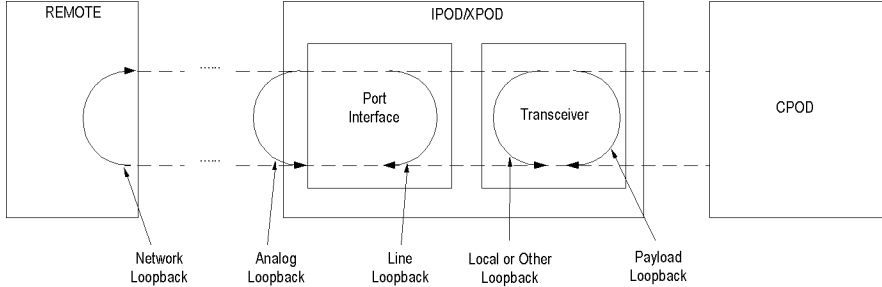
Field/Button	Type	Action/Description
Framing	read/write	<p>Select the type of framing used on the port. Framing provides a method of distinguishing between individual channels by adding one additional bit to each frame.</p> <p><i>Note: Make sure to configure the port to the same framing specifications as the customer premise equipment (CPE).</i></p> <p>Options are:</p> <p><i>Other</i> – This option is for unframed formatting.</p> <p><i>Dsx1ESF</i> (DS1 only and default) – The extended superframe format extends the D4 framing format from 12 to 24 frames and uses modified framing bits to provide a cyclic redundancy check (CRC), secondary channel and data link.</p> <p><i>Dsx1D4</i> (DS1 only) – The D4 framing format consists of twelve frames. It provides end-to-end synchronization and signaling associated with a particular channel.</p> <p><i>Dsx1E1</i> (E1 only and default) – The E1 framing format is the ITU-T Recommendation G.704 multiframe format.</p> <p><i>Dsx1E1 CRC</i> (E1 only) – The E1-CRC framing format is the ITU-T Recommendation G.704 CRC4 multiframe format.</p> <p><i>Dsx1E1 MF</i> (E1 only) – The E1-MF framing format is the ITU-T Recommendation G.704 multiframe format with time slot 16 multiframing enabled.</p> <p><i>Dsx1E1 CRC MF</i> (E1 only) – The E1-CRC-MF framing format is the ITU-T Recommendation G.704 CRC4 multiframe format with time slot 16 multiframing enabled.</p>



**Table 4-5. Configure DS1/E1 Port Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
Line Coding	read/write	<p>Select the type of line coding used on the port. Line coding is the data signal encoding method used on the DS1/E1 interface.</p> <p><i>Note:</i> See your facility service provider for more information about which line code method to use.</p> <p>Options are:</p> <p><i>Dsx1B8ZS</i> (DS1 only and default) – <i>Bipolar with 8 zero substitutions</i> is the ATM Forum standard for ATM cell transmission over a DS1 interface. B8ZS refers to the use of a specified pattern of normal bits and bipolar violation that is used to replace a sequence of eight zero bits. With B8ZS, a special code is placed in and then removed from the pulse stream in substitution for a 0 byte that has been transmitted by the user equipment.</p> <p><i>Dsx1HDB3</i> (E1 only and default) – The ATM Forum standard for ATM cell transmission over an E1 interface. Use this option for optimum E1 performance.</p> <p><i>Dsx1AMI</i> – <i>Alternate Mark Inversion</i>, also known as <i>Jammed Bit</i>, is not supported by the ATM Forum. If you use this method on a DS1 interface, users may experience excessive zeroes alarms on transmission equipment. For an E1 interface, use AMI for physical path verification only, not cell transmission.</p> <p><i>Dsx1JBZS</i> – Not supported.</p> <p><i>Dsx1ZBTSI</i> – Not supported.</p> <p><i>Other</i> – Not supported.</p>
Signal Mode	read/write	<p>Select the signal mode used on the port. Options are:</p> <p><i>None</i> – This disables the signal mode option.</p> <p><i>Robbed bit</i> (DS1 only) – Enables robbed bit signaling.</p> <p><i>Bit Oriented</i> (E1 only) – Enables channel associated (CAS) signaling.</p> <p><i>Message Oriented</i> – Enables common channel signaling (CCS) on channel 24 in DS1 applications and on channel 16 in E1 applications.</p>

**Table 4-5. Configure DS1/E1 Port Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
<b>Fault Management</b>		
Set Alarm Reporting	read/write	Enable/disable alarm reporting on the port. <i><b>Caution:</b> Never disable alarm reporting on any port used for primary or secondary recovered timing.</i>
Set Max Intervals	read/write	Enter the maximum number of 15-minute intervals to store in the interval history table and display in the Monitor Status mode. Valid range is 1 to 96 intervals (15 minutes to 24 hours).
Set Port Loopback	read/write	<p>Select one of the following port loopback options (see <a href="#">Figure 4-7</a>):</p> <p><i>None</i> (default) – Disables the loopback function for normal operation.</p> <p><i>Payload</i> – Payload loopback tests the internal circuitry of this port by routing received data through the port receiver and transmitter circuitry and back out of the port.</p> <p><i>Line</i> – Line loopback tests the port interface by routing received data back out of the port.</p> <p><i>Local</i> – Loops data back towards the CPOD. On an IMA POD, the data is looped back toward the IMA chip.</p> <p><i>Analog</i> – Enables a metallic loopback at the port.</p> <p><i>Network</i> – Generates an inband ‘loop activate’ code to instruct the remote end to perform a line loopback test.</p> <p><i>Other</i> – Presently provides the same function as local loopback.</p>
 <p>The diagram illustrates the data paths for different loopback configurations. It shows three main components: REMOTE, IPD/POD (which contains a Port Interface and a Transceiver), and CPOD. Dashed arrows indicate the direction of data flow.          <ul style="list-style-type: none"> <li><b>Network Loopback:</b> Data flows from REMOTE to the Port Interface and back to REMOTE.</li> <li><b>Analog Loopback:</b> Data flows from the Port Interface back to the Port Interface (local loop).</li> <li><b>Line Loopback:</b> Data flows from the Port Interface back to the Transceiver and then back to the Port Interface.</li> <li><b>Local or Other Loopback:</b> Data flows from the Transceiver back to the Port Interface.</li> <li><b>Payload Loopback:</b> Data flows from the Transceiver back to the Transceiver (internal loop).</li> </ul> </p>		
<b>Figure 4-7. DS1/E1 POD Port Loopbacks</b>		

**Table 4-5. Configure DS1/E1 Port Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
Set Network LB (loopback) Detection (DS1/E1 Cell POD with CSU only)	read/write	Select whether Network Loopback codes will be detected. When enabled, the POD responds to received inband loop activate/deactivate commands by activating or deactivating a line loopback.
Set Port Diagnostics	read/write	Set/display whether alarm/error insertion is enabled or disabled. The options are:  <i>None</i> (default) – Disables the error insertion function.  <i>TxYellow</i> – Enables the insertion of yellow alarms in the transmit path.  <i>TxAIS</i> – Enables the insertion of alarm indication signal (AIS) alarms in the transmit path.  <i>TxE1FasError</i> (E1 only) – Enables the insertion of frame alignment errors in the transmit path.-  <i>TxE1TS16AIS</i> (E1 only) – Enables the insertion of time-slot 16 alarm indication signal (AIS) alarms in the transmit path.  <i>TxE1MASerror</i> (E1 only) – Enables the insertion of multiframe alignment errors in the transmit path.  <i>TxQRSS</i> - Enables QRSS (Quasi-Random Signal Source) transmission for bit-error analysis.
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Enables you to access and configure the ATM interface layer (DS1/E1 Cell POD) as described in <a href="#">“Configuring the ATM Interface” on page 4-46</a> , the CES connections layer (DS1/E1 Circuit POD) as described in <a href="#">“Configuring Circuit Emulation Services” on page 5-83</a> , or the VCS connections layer (VCS POD) as described in <a href="#">“Configuring Voice Compression Service” on page 5-117</a> .
Equalization	window button	Opens the Equalization (Short Haul) or Equalization (Long Haul) window, based on which is selected in the Range field. See <a href="#">“Setting Short-Haul/Long-Haul Equalization” on page 4-19</a> .

**Table 4-5. Configure DS1/E1 Port Buttons and Fields (Continued)**

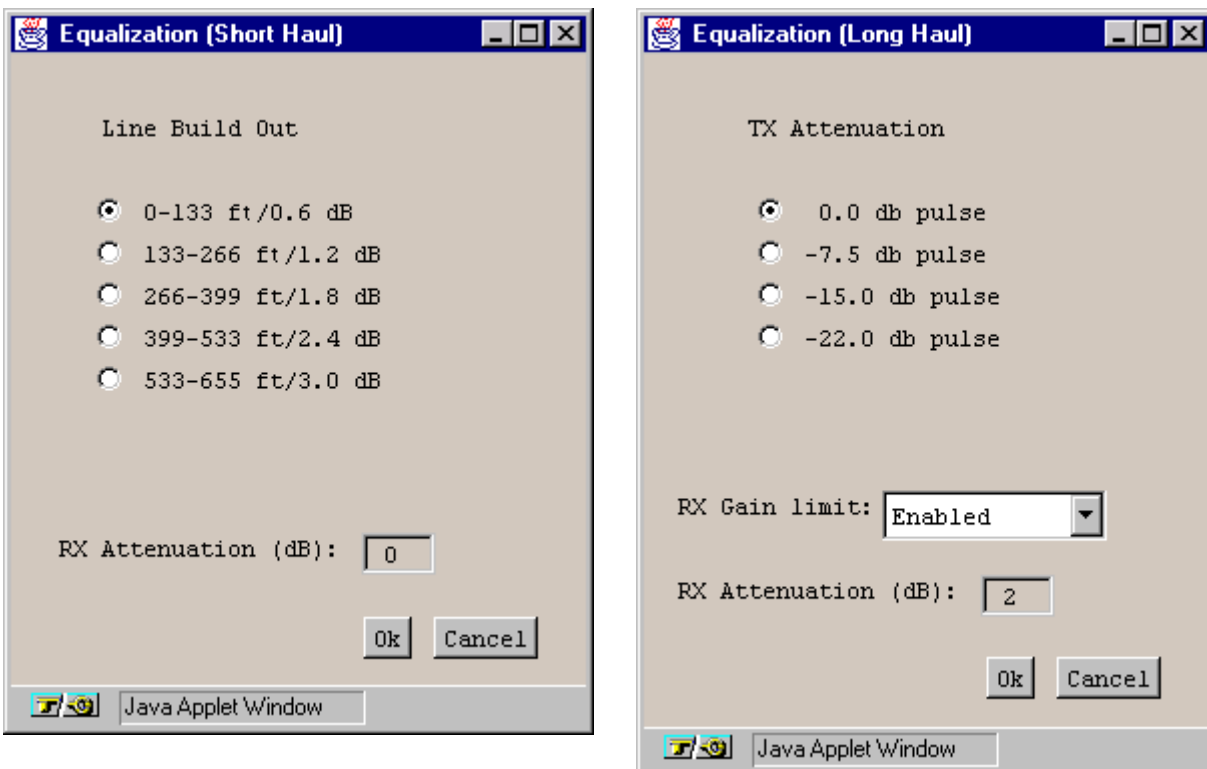
Field/Button	Type	Action/Description
Port CAC (Does not apply to DS1/E1 CES ports)	window button	Enables you to configure port-level CAC parameters. See “ <b>Configuring Port-level CAC</b> ” on page 4-43 for details.

## Setting Short-Haul/Long-Haul Equalization

DS1 ports are assumed to be operating at short range (under approximately 650 feet), with the exception of the DS1/E1 Cell POD with Integral CSU, which supports Long Haul transmission. For Short Haul connections, the line-build out (the length of cable that connects this port to other equipment, such as a router) may be configured. For Long Haul connections, the Transmission Attenuation may be adjusted, and the Receive Gain limit may be enabled or disabled. The Receive Gain limit enables you to boost weak incoming signals or limit strong incoming signals.

To configure the line equalization parameters for a DS1/E1 port:

1. Select the Equalization button from the Configure DS1/E1 Port window.  
Depending on which option is selected in the Range field, the Equalization (Short Haul) or Equalization (Long Haul) window appears (Figure 4-8).



**Figure 4-8. Equalization Short Haul and Long Haul Windows**

2. Complete the fields described in Table 4-6 to set the Equalization parameters.

**Table 4-6. Equalization Buttons and Fields**

Field/Button	Type	Action/Description
Line Build Out (Short Haul only)	read/write	Set/display the required line build-out of the port. The line build-out is the length of cable that connects this port to other equipment (such as a router).
TX Attenuation (Long Haul only)	read/write	Set/display the Transmission Attenuation for the port. Transmission Attenuation may need to be increased depending on the transmission range.
RX Gain Limit (Long Haul only)	read/write	Enable/disable the receive gain limit for the port. Disabling the RX Gain limit provides a boost for weak incoming signals. Enabling the RX Gain limit limits strong incoming signals.
RX Attenuation	read-only	Displays the receive attenuation value of the line in decibels.

## Configuring a DS3/E3 Port

To configure a DS3 port:

1. Select the desired port from the Interface Management window, as described on page 4-7. The Configure DS3/E3 Port window appears (see Figure 4-9 for DS3, Figure 4-10 for E3).

Configure DS3 Port

Events/Alarms... Major

Port Detail

Slot-Pod-Port: 3 1 1

Port Name... DS3 PORT NAME Port ID... DS3 CIRCUIT I

Set ADMIN Status: Up OPS Status: Up

Configuration Management

Line Build Out: Under225ft

Set TX Clock: SystemTiming

Framing: Ds3 Cbit

Line Coding: B3zs

Fault Management

Set Alarm Reporting: Enabled

Set Max Intervals: 32

Set Port Loopback: None

Set Error Insertion: None

FEAC... Next Logical Layer... Port CAC... OK Cancel Apply

Select to create/modify a Port Name.

Warning: AppletWindow

Figure 4-9. Configure DS3 Port Window

**Configure E3 Port (SA-1200)**

Configure E3 Port      Events/Alarms...      Major

**Port Detail**

Slot-Pod-Port:      5      2      1

Port Name...      E3 PORT NAME      Port ID...      E3 CIRCUIT ID

Set ADMIN Status:      Up      OPS Status:      Down

**Configuration Management**

Set TX Clock:      SystemTiming

Framing:      E3 G832

Line Coding:      Hdb3

**Fault Management**

Set Alarm Reporting:      Enabled

Set Max Intervals:      32

Set Port Loopback:      None

Set Error Insertion:      None

Next Logical Layer...      Trail Trace...      Port CAC      OK      Cancel      Apply

Select to create/modify a Port Name.

Warning: AppletWindow

**Figure 4-10. Configure E3 Port Window**

2. Complete the fields described in [Table 4-7](#).
3. When finished, choose OK.



**Table 4-7. Configure DS3/E3 Port Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the port's slot, POD and port number.
Port Name	window button	Specify the port name (32 characters max).
Port ID	window button	Specify the port ID (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of the port: up or down. Default is up (online). Set to Down (offline) to take the port offline. (The Testing option is not currently supported.)
OPS Status	read-only	Displays the operational state of the port: up or down.
<b>Configuration Management</b>		
Line Build Out	read/write	(DS3 only) Select the required line build-out of the port. The line build-out is the length of cable that connects this port to other equipment (such as a router). Options are <i>Under 225 feet</i> (default) <i>Over 225 feet</i> .
Set TX Clock	read/write	Set/display the source of transmit timing on the port. The options are:  <i>Loop</i> – The port transmit timing source is derived from the timing signal coming into this port.  <i>System</i> (default) – System timing provides the transmit timing for this port. The System Timing configuration in the System Administration window determines system timing (see <a href="#">page 3-8</a> ).

**Table 4-7. Configure DS3/E3 Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Framing	read/write	<p>Select the type of framing used on the port. Framing provides a method of distinguishing between individual channels by adding one additional bit to each frame.</p> <p><i>Note: Make sure to configure the port to use the same framing specifications as the external equipment connected to the port.</i></p> <p>Options are:</p> <p><i>Ds3 Cbit</i> (DS3 only and default) – This is the C-bit framing format.</p> <p><i>Ds3 M23</i> (DS3 only) – This is the M.23 framing format.</p> <p><i>E3 G751</i> (E3 only and default) – The G.751 framing format is the ITU-T Recommendation G.751 format.</p> <p><i>E3 G832</i> (E3 only) – The G.832 framing format is the ITU-T Recommendation G.832 format.</p>
Line Coding	read-only	Displays the type of line coding used on the port: B3zs (DS3) or Hdb3 (E3).
<b>Fault Management</b>		
Set Alarm Reporting	read/write	<p>Enable or disable alarm reporting on the port.</p> <p><i>Note: Never disable alarm reporting on any port used for primary or secondary recovered timing.</i></p>
Set Max Intervals	read/write	Enter the maximum number of 15-minute intervals to store in the interval history table and display in the Monitor Status mode. Valid range is 1 to 96 intervals (15 minutes to 24 hours).
Set Port Loopback	read/write	<p>Select one of the following port loopback options (see <a href="#">Figure 4-11</a>):</p> <p><i>None</i> (default) – Disables the loopback function for normal operation.</p> <p><i>Line</i> – Tests the port interface by routing received data back out the port.</p> <p><i>Diagnostic</i> – Tests the port's internal circuitry port by routing transmit data back through the port receiver.</p> <p><i>Payload</i> – Tests the port's internal circuitry by routing received data through the port receiver and transmitter circuitry and back out the port.</p>

**Table 4-7. Configure DS3/E3 Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<p style="text-align: center;">Line Loopback      Diagnostic Loopback      Payload Loopback</p>		
<b>Figure 4-11. DS3/E3 POD Loopbacks</b>		
Set Error Insertion	read/write	<p>Select one of the following alarm/error insertion options:</p> <p><i>None</i> (default) – Disables the error insertion function.</p> <p><i>TxLOS</i> – Enables the insertion of loss of signal (LOS) alarms in the transmit path.</p> <p><i>TxAIS</i> – Enables the insertion of alarm indication signal (AIS) alarms in the transmit path.</p> <p><i>TxFERF</i> – Enables the insertion of far end receive failure (FERF) or yellow alarms in the transmit path.</p> <p><i>TxIdle</i> (DS3 only) – Enables the insertion of idle maintenance signals in the transmit path.</p> <p><i>TxLCV</i> – Enables the insertion of line code violations (LCV) in the transmit path.</p> <p><i>TxPbitErrs</i> (DS3 only) – Enables insertion of P-bit errors in DS3 stream.</p> <p><i>TxCbitErrs</i> (DS3 using C-bit framing only) – Enables the insertion of C-bit parity errors in the DS3 stream.</p> <p><i>TxMbitErrs</i> (DS3 only) – Enables insertion of M-bit errors in DS3 stream.</p> <p><i>TxFbitErrs</i> – Enables the insertion of F-bit errors in the DS3 stream.</p> <p><i>TxFEFE</i> – Enables insertion of Far End Block errors (FEFE) in DS3 stream.</p>

**Table 4-7. Configure DS3/E3 Port Fields and Buttons (Continued)**

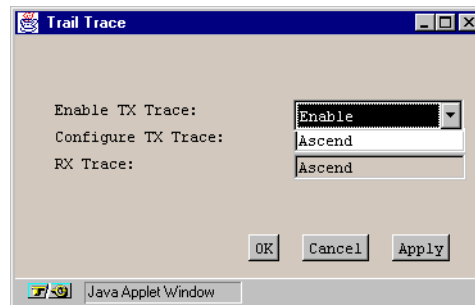
Field/Button	Type	Action/Description
<b>(Other Buttons)</b>		
Trail Trace (E3 only)	window button	(Trail Trace applies only to E3 ports using G 832 framing format.)  Selecting this button opens the Trail Trace window, described in <b>“Trail Trace (E3 only)”</b> on page 4-27.
FEAC (Far End Alarm and Control) (D3 with C-bit framing only)	window button	(FEAC applies only to D3 ports using C-bit framing format.)  Selecting this button opens the Far End Alarm and Control window, described in <b>“Far End Alarm and Control (D3 with C-bit framing only)”</b> on page 4-28.
Next Logical Layer	window button	Enables you to specify the ATM interface layer of this port as described in <b>“Configuring the ATM Interface”</b> on page 4-46.
Port CAC	window button	Enables you to configure port-level CAC parameters. See <b>“Configuring Port-level CAC”</b> on page 4-43 for details.

## Trail Trace (E3 only)

When you configure an E3 port with G832 framing format, you can also configure a trail trace for troubleshooting purposes.

To enable or disable the trail trace, to specify the trace string, or to check the correct return of the trace string:

1. Select the Trail Trace button from the Configure E3 Port window. The Trail Trace window appears (see [Figure 4-12](#)).



**Figure 4-12. Trail Trace Window**

2. Complete the fields described in [Table 4-8](#).

**Table 4-8. Trail Trace Fields**

Field	Type	Action/Description
Enable TX Trace	read-write	Enable or disable TX trace.
Configure TX Trace	read-write	Enter the trace string to be transmitted (16 characters max).
RX Trace	read-only	Displays the trace string received (should be identical to the trace string transmitted).

3. When finished, choose OK.

## Far End Alarm and Control (D3 with C-bit framing only)

When you configure a D3 port with C-bit framing format, you can also configure far-end alarm and control (FEAC) parameters. The FEAC parameters are used for two purposes:

- To send alarm or status information from the far-end terminal back to the near-end terminal; and
- To initiate D3 loopbacks at the far-end terminal from the near-end terminal.

To enable or disable loop processing or far-end loopback:

1. Select the FEAC button from the Configure D3 Port window. The Far End Alarm and Control window appears (see [Figure 4-13](#)).

The screenshot shows a window titled "Far End Alarm and Control". It has a "Port Detail" section with "Slot-Pod-Port:" and three input fields containing "3", "1", and "1". Below is a "Control" section with "Loop Processing:" set to "Disable" and "Far End Loopback:" set to "Deactivate". The "Status" section includes "Local Loopback Status:" (None), "TX FEAC Code:" (None), and "RX FEAC Code:" (None). At the bottom are "OK", "Cancel", and "Apply" buttons. A warning bar at the bottom reads "Warning: AppletWindow".

**Figure 4-13. Far End Alarm and Control Window**

2. Complete the fields described in [Table 4-9](#).
3. When finished, choose OK.

**Table 4-9. Far End Alarm and Control Fields**

Field	Type	Action/Description
Port Detail: Slot-POD-Port	read-only	Displays the Slot-POD-Port numbers of the currently selected port.
Loop Processing	read/write	Specify whether loop processing is enabled or disabled (default). If enabled, the far-end terminal is permitted to set a loopback condition at the near-end terminal.
Far End Loopback	read/write	Specify whether far-end loopback is activated or deactivated (default). When activated, the far-end terminal is instructed to set a loopback condition. The far-end terminal must support FEAC loopback and must be configured to allow far-end loopback control for the loopback condition to be established.
Local Loopback Status	read-only	Displays the current local loopback status: None or Ds3LineLoop.
TX FEAC Code	read-only	Displays the FEAC code being transmitted: <i>None</i> (default) – No FEAC code is being transmitted. <i>DS3 LOS</i> – Loss of Signal error. <i>DS3 OOF</i> – Out-of-Frame error. <i>DS3 AIS Received</i> – Alarm Indication Signal.
RX FEAC Code	read-only	Displays the FEAC code being received. The following codes are considered valid: <i>None</i> (default) – No FEAC code being received. (This is the no alarm condition.) <i>DS3 Eqpt. Failure (SA)</i> – Equipment Failure (Service Affecting). Type I equipment failure, indicating an out-of-service state or defect requiring immediate attention. <i>DS3 LOS</i> – Loss of Signal error. <i>DS3 OOF</i> – Out-of-Frame error. <i>DS3 AIS Received</i> – Alarm Indication Signal error. <i>DS3 Idle Received</i> – Idle error. <i>DS3 Eqpt. Failure (NSA)</i> – Equipment Failure (Non-Service Affecting). Type II equipment failure, indicating an equipment state such as suspended service, not activated, or not available for use. <i>Common Eqpt. Failure (NSA)</i> – Equipment Failure (Non-Service Affecting). Type II equipment failure, indicating an equipment state such as suspended service, not activated, or not available for use.

## Configuring an OC-3c/STM-1 Port

To configure an OC-3c/STM-1 port:

1. Select the desired port from the Interface Management window, as described on [page 4-7](#). The Configure OC-3/STM-1 Port window appears (see [Figure 4-14](#)).

**Configure OC-3 / STM-1 Port**

Configure OC-3 / STM-1 Port    Events/Alarms...    Critical

**Port Detail**

Slot-Pod-Port: 1 3 1    Port Type: SonetLinePlus

Port Name...: SONET PORT NA    Port ID...: SONET LINE CI

Set ADMIN Status: Up    OPS Status: Up

**Configuration Management**

Set Medium Type: Sonet

Medium Line Type: SonetMultiMod

Set Port Laser: On

Set TX Clock: SystemTiming

**Fault Management**

Set Alarm Reporting: Enabled

Set Max Intervals: 32

Set Port Loopback: None

Set Error Insertion: None

Configure Path...    Advanced Options...    Port CAC    OK    Cancel    Apply

Select to create/modify a Port Name.

Warning: AppletWindow

**Figure 4-14. Configure OC-3/STM-1 Port Window**

2. Complete the fields described in [Table 4-11](#).
3. Complete any necessary path information or advanced options as described in “Configuring a Path for an OC-3c/STM-1 Port” on [page 4-38](#) and “Configuring OC-3c/STM-1 Port Advanced Options” on [page 4-36](#).
4. When finished, choose OK.





OC-3 users: If you anticipate high volume usage on your OC-3c/STM-1 port (i.e., using greater than 60 percent of the port's available bandwidth on a regular basis), you should also increase the per-VC buffering settings. See **“Configuring Per-Virtual Connection Buffers”** on page 3-24, for details.

The recommended settings for the VC buffers are:


**Table 4-10. High-Bandwidth Recommended Per-VC Buffering Settings**

Level	Hi-Max	Hi-Thresh	A-Max	A-Thresh	B-Max	B-Thresh	C-Max	C-Thresh
Shallow	10	7	15	12	20	16	50	25
Medium	15	12	20	16	25	20	500	250
High	20	16	25	20	35	30	2000	1000

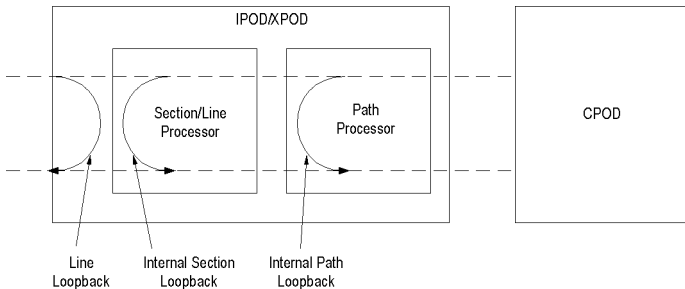
**Table 4-11. Configure OC-3/STM-1 Port Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail Frame</b>		
Slot-POD-Port	read-only	Displays the slot, POD and port numbers.
Port Type	read-only	Displays the type of port.
Port Name	window button	Specify the port name (32 characters max).
Port ID	window button	Specify the port ID (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of the port: up (default) or down. Set to Down to take the port offline. (The Testing option is not supported.)
OPS Status	read-only	Displays the operational state of the port: up or down.
<b>Configuration Management</b>		
Set Medium Type	read/write	Select the type of medium used on the port. Options are: <i>Sonet</i> (default) – Synchronous Optical Network configures the port for OC-3c (North American) applications. <i>Sdh</i> – Synchronous Digital Hierarchy configures the port for STM-1 (international) applications.
Medium Line Type	read-only	Displays the type of line medium on the port: <i>SonetMultiMode</i> (for SONET multimode PODs) or <i>SonetLongSingleMode</i> (for SONET long-reach, single-mode PODs).

**Table 4-11. Configure OC-3/STM-1 Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Port Laser	read/write	<p>Select whether the port laser is enabled or disabled (on or off). This parameter is a safety feature intended to prevent personal injury when you repair or replace the POD or its cables. You must set this option to “on” to transmit incoming traffic out of this port.</p> <p><i><b>Note:</b> When you disable the laser, the CPE or switch at the other end of the connection reports a red port alarm to indicate a loss of signal.</i></p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;">  <p>Before you remove optical cables, set this parameter to <b>off</b>. If the optical connectors are exposed, the transmit laser beam can cause personal injury.</p> </div>
Set TX Clock	read/write	<p>Select transmit timing source for the port. Options are:</p> <p><i>Loop</i> – The port transmit timing source is derived from the timing signal coming into this port.</p> <p><i>Local</i> – The POD’s internal timing source provides the transmit timing for this port.</p> <p><i>System</i> (default) – System timing provides the transmit timing for this port. The System Timing configuration in the System Administration window determines system timing (see <a href="#">page 3-8</a>).</p>
<b>Fault Management</b>		
Set Alarm Reporting	read/write	<p>Enable or disable alarm reporting on the port.</p> <p><i><b>Note:</b> Never disable alarm reporting on any port used for primary or secondary recovered timing.</i></p>
Set Max Intervals	read/write	<p>Enter the maximum number of 15-minute intervals to store in the interval history table and display in the Monitor Status mode. Valid range is 1 to 96 intervals (15 minutes to 24 hours) of activity.</p>

**Table 4-11. Configure OC-3/STM-1 Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Port Loopback	read/write	<p>Select one of the following port loopback options (see <a href="#">Figure 4-15</a>):</p> <p><i>None</i> (default) – Disables the loopback function for normal operation.</p> <p><i>Line</i> – Tests the port interface by routing received data back out of the port.</p> <p><i>Internal Section</i> – Tests the internal circuitry of this port by routing received data through the port receiver and transmitter circuitry and back out the port.</p> <p><i>Internal Path</i> – Tests the port interface by routing received data back out of the port.</p>
 <p>The diagram illustrates the internal structure of an OC-3c/STM-1 POD for loopback testing. It shows a main container labeled 'IPOD/XPOD' which contains two sub-processors: 'Section/Line Processor' and 'Path Processor'. To the right of the IPOD/XPOD is a separate block labeled 'CPOD'. Arrows indicate the flow of data and the points where loopbacks are implemented:         <ul style="list-style-type: none"> <li><b>Line Loopback:</b> An arrow from the input on the left enters the Section/Line Processor, and another arrow loops back from the output of the Section/Line Processor to its input.</li> <li><b>Internal Section Loopback:</b> An arrow from the input enters the Section/Line Processor, and another arrow loops back from the output of the Section/Line Processor to its input, passing through the internal circuitry.</li> <li><b>Internal Path Loopback:</b> An arrow from the input enters the Section/Line Processor, then goes to the Path Processor, and finally loops back from the output of the Path Processor to the input of the Section/Line Processor.</li> </ul>         The CPOD block is shown as a separate component that would receive data from the Path Processor in a normal configuration.       </p>		
<p><b>Figure 4-15. OC-3c/STM-1 POD Loopbacks</b></p>		
Set Error Insertion	read/write	<p>Select one of the following alarm/error insertion options:</p> <p><i>None</i> (default) – Disables the error insertion function.</p> <p><i>TxDigitalLOS</i> – Enables the insertion of digital loss of signal (LOS) alarms in the transmit path.</p> <p><i>TxLineAIS</i> – Enables the insertion of line alarm indication signal (AIS) alarms in the transmit path.</p> <p><i>TxLineRDI</i> – Enables the insertion of line remote defect indication (RDI) or line yellow alarms in the transmit path.</p> <p><i>TxFrameBitErr</i> – Enables the insertion of frame bit errors in the transmit path.</p> <p><i>TxSectBipErr</i> – Enables the insertion of section BIP errors in the transmit path.</p> <p><i>TxLineBipErr</i> – Enables the insertion of line BIP errors in the transmit path.</p>

**Table 4-11. Configure OC-3/STM-1 Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>(Other Buttons)</b>		
Configure Path	window button	Opens a window for configuring OC-3c/STM-1 path. See “ <a href="#">Configuring a Path for an OC-3c/STM-1 Port</a> ” on page 4-38.
Advanced Options*	window button	For ports on all OC-3c/STM-1 PODs except dual port OC-3c/STM-1 IPODs*, opens a window for configuring advanced options (e.g., section trace). See “ <a href="#">Configuring OC-3c/STM-1 Port Advanced Options</a> ” on page 4-36.  * Advanced Options are not available for dual-port OC-3c/STM-1 IPODs.
Port CAC	window button	Enables you to configure port-level CAC parameters.

## Configuring OC-3c/STM-1 Port Advanced Options

You can configure additional features for OC-3/STM-1 POD ports through the Advanced Options function with the exception of dual port OC-3c/STM-1 IPODs, for which this feature is not available.

To access and configure the advanced options:

1. Choose the Advanced Options button in the Configure OC-3/STM-1 Port window. The Configure OC-3/STM-1 Port (Advanced) window appears (see [Figure 4-16](#)).

**Figure 4-16. Configure OC-3/STM-1 Port (Advanced) Window**

2. Complete the fields described in [Table 4-12](#).
3. When finished, choose OK to return to the Configure OC-3/STM-1 Port window.
4. Choose the Configure Path button in the Configure OC-3/STM-1 Port window to configure the paths of this OC-3c/STM-1 port as described in [“Configuring a Path for an OC-3c/STM-1 Port”](#) on page 4-38.

**Table 4-12. Configure OC-3/STM-1 Port (Advanced) Fields and Buttons**

Field/Button	Type	Action/Description
<b>Path Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD, and port numbers.
Medium Type	read-only	Displays the type of medium used: SONET or SDH.
Port Name	read-only	Displays the port name.
Port ID	read-only	Displays the port ID.
ADMIN Status	read-only	Displays the administrative state of the port: up or down.
OPS Status	read-only	Displays the operational state of the port.
<b>Section Advanced Options</b>		
Section Trace Enable TX Trace	read/write	Enable or disable the transmit trace function for this port section.
Section Trace Configure TX Trace	window button	Enables you to set and display the section transmit trace. Choose the Configure TX Trace button. When the Configure Section TX Trace window appears, enter the message you wish to use for tracing, then choose OK. SONET permits trace messages of up to 64 characters. SDH permits trace messages of up to 16 characters in length.
Section Trace Display RX Trace	window button	The field adjacent to this button displays a portion of the RX Trace. If the trace exceeds the field length, select Display RX Trace to open a window displaying the full section receive trace. Click Cancel when you are finished viewing the trace.

## Configuring a Path for an OC-3c/STM-1 Port

To configure a path on an OC-3c/STM-1 port:

1. Choose Configure Path in the Configure OC-3/STM-1 Port window. The Configure OC-3/STM-1 Path window appears (see [Figure 4-17](#)).

Configure OC-3 / STM-1 Path

Events/Alarms... Critical

Path Detail

Slot-Pod-Port: 1 3 1 Path Type: SonetPathPlus

Path Name... SONET Path Na Path ID... SONET Path Ci

Set ADMIN Status: Up OPS Status: Down

Configuration Management

Set Path Label: Atm

Fault Management

Set Alarm Reporting: Enabled

Set Max Intervals: 32

Error Insertion: None

Advanced Options... Next Logical Layer... OK Cancel Apply

Select to create/modify a Path Name.

Java Applet Window

**Figure 4-17. Configure OC-3/STM-1 Path Window**

2. Complete the fields described in [Table 4-13](#).
3. When you are finished, choose the Next Logical Layer button to configure the ATM interface layer of this port, as described in [“Configuring the ATM Interface” on page 4-46](#).
4. When you are finished with step 3, the next step depends on the type of OC-3c/STM-1 POD the port resides on:
  - *For ports on dual port OC-3c/STM-1 IPODs:*

When you are finished configuring the ATM interface layer, choose the applicable button (OK, Cancel or Apply) and configure the other OC-3c/STM-1 ports, if any, using the preceding steps.

When you are finished configuring the other OC-3c/STM-1 ports, go to the applicable sections of this chapter to configure other types of ports, if any.
  - *For ports on all other OC-3/STM-1 PODs:*

When you are finished configuring the ATM interface layer, choose the Advanced Options button to configure the path of this OC-3c/STM-1 port on



an advanced level, as described in the next section, “Configuring a Path for an OC-3c/STM-1 Port - Advanced Options” on page 4-41.

5. Choose OK when finished to return to the Configure OC-3/STM-1 Port window.

**Table 4-13. Configure OC-3/STM-1 Path Fields and Buttons**

Field/Button	Type	Action/Description
<b>Path Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD, and port numbers.
Path Type	read-only	Displays the type of path.
Path Name	window button	Specify the path name (32 characters max).
Path ID	window button	Specify the path ID (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of this path upon powering up. Default is up (online). Set to Down (offline) when you run diagnostics. (The Testing option is not supported.)
OPS Status	read-only	Displays the operational state of the port.
<b>Configuration Management</b>		
Set Path Label	read/write	Specify the C2 path overhead byte:  <i>Unequipped</i> – Sets the C2 path overhead byte to 0 hex.  <i>Atm</i> (default) – Asynchronous Transmit Mode sets the C2 path overhead byte to 13 hex.
<b>Fault Management</b>		
Set Alarm Reporting	read/write	Select whether alarm reporting is enabled or disabled on the port.  <i>Note: Never disable alarm reporting on any port used for primary or secondary recovered timing.</i>
Set Max Intervals	read/write	Enter the maximum number of 15-minute intervals to store in the interval history table and display in the Monitor Status mode. Valid range is 1 to 96 intervals (15 minutes to 24 hours) of activity.

**Table 4-13. Configure OC-3/STM-1 Path Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Error Insertion	read/write	<p>Select one of the following alarm/error insertion options:</p> <p><i>None</i> (default) – Disables the error insertion function.</p> <p><i>TxPathAIS</i> – Enables the insertion of line alarm indication signal (AIS) alarms in the transmit path.</p> <p><i>TxPathRDI</i> – Enables the insertion of line remote defect indication (RDI) or line yellow alarms in the transmit path.</p> <p><i>TxPathBipErr</i> – Enables the insertion of path BIP errors in the transmit path.</p> <p><i>TxHcsBitErr</i> – Enables the insertion of HCS bit errors in the transmit path.</p>
<b>(Other Buttons)</b>		
Advanced Options*	window button	<p>For ports on all OC-3c/STM-1 PODs except dual port OC-3c/STM-1 IPODs*, enables you to configure advanced options (e.g., path trace). See <a href="#">“Configuring a Path for an OC-3c/STM-1 Port - Advanced Options”</a> on page 4-41.</p> <p>* Advanced Options are not available for dual-port OC-3c/STM-1 IPODs.</p>
Next Logical Layer	window button	<p>Enables you to configure the ATM interface layer. See <a href="#">“Configuring the ATM Interface”</a> on page 4-46.</p>

## Configuring a Path for an OC-3c/STM-1 Port - Advanced Options

You can configure advanced path information for an OC-3c/STM-1 port through the Configure OC-3/STM-1 Path (Advanced) window. This applies to all OC-3c/STM-1 PODs except dual-port OC-3c/STM-1 IPODs; Advanced Options are not available on dual-port OC-3c/STM-1 IPODs.

To configure advanced path options on an OC-3c/STM-1 port:

1. Choose the Advanced Options button in the Configure OC-3/STM-1 Path window. The Configure OC-3/STM-1 Path (Advanced) window appears (see [Figure 4-18](#)).

Configure OC-3 / STM-1 Path (Advanced)

Events/Alarms... Critical

Path Detail

Slot-Pod-Port: 1 3 1 Path Type: SonetPathPlus

Path Name: SONET Path Na Path ID: SONET Path Ci

Set ADMIN Status: Up OPS Status: Down

Path Advanced Options

Path Trace

Enable TX Trace: Enable

Configure TX Trace... SAHARA

Display RX Trace... YYYYYYYYYYYYYY

OK Cancel Apply

Select to display the path Receive Trace.

Java Applet Window

**Figure 4-18. Configure OC-3/STM-1 Path (Advanced) Window**

2. Complete the fields described in [Table 4-14](#).
3. When finished, choose OK to return to the Configure OC-3/STM-1 Port window.

**Table 4-14. Configure OC-3/STM-1 Path (Advanced) Fields and Buttons**

Field/Button	Type	Action/Description
<b>Path Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD and port numbers.
Path Type	read-only	Displays the type of path.
Path Name	read-only	Displays the path name.
Path ID	read-only	Displays the path ID.
Set ADMIN Status	read/write	Sets the administrative state of this path upon powering up. Default is up (online). Set to Down to take the port offline.
OPS Status	read-only	Displays the operational state of the port.
<b>Path Advanced Options</b>		
Path Trace: Enable TX Trace	read/write	Specify whether the transmit trace function is enabled or disabled.
Path Trace: Configure TX Trace	window button	Enables you to set and display the path transmit trace. Choose the Configure TX Trace button. When the Configure Path TX Trace window appears, enter the message you wish to use for tracing, then click OK. SONET permits trace messages of up to 64 characters; SDH trace messages may be up to 16 characters in length.
Path Trace: Display RX Trace	window button	The field adjacent to this button displays a portion of the RX Trace. If the trace exceeds the field length, select Display RX Trace to display the full path receive trace. Choose Cancel when you are finished viewing the trace.

## Configuring Port-level CAC

Port-level Connection Admission Control parameters may be configured for the ports on an ATM cell POD.

Port-level CAC configuration has two components, CAC Bandwidth and Virtual Path Identifier configuration.

CAC Bandwidth configuration consists of setting the size of the variable bandwidth pool as a percent of the port's fixed bandwidth pool, and setting the variable to fixed load percentage, which debits a portion of each connection's variable bandwidth from the fixed bandwidth pool.

Virtual Path Identifier configuration involves reserving a range of VPIs for use by Permanent Virtual Paths.

Most applications call for using Permanent Virtual Channel connections rather than Permanent Virtual Path connections. To make available the maximum number of Virtual Path Identifier values to PVC connections, Permanent Virtual Paths are, by default, disabled on the SA units.

Should you wish to use Permanent Virtual Paths, PVPs may be enabled and a range of VPI values reserved for use by PVPs. This range of values may not be used for PVC connections.



Remember: Before a range of VPIs may be reserved for use by PVPs on an ATM UNI port, you must enable VP ranges at the Cell Highway level (see [Figure 3-19](#)).

To reserve a range of PVPs on a port:

1. Select the ICM from the Configure System window (see [Figure 4-2 on page 4-3](#)).
2. Select the POD from the Configure ICM window (see [Figure 4-3 on page 4-5](#)).
3. At the Configure POD window, select the CAC button and in the Cell Hiway Configuration window ([Figure 3-19](#)), set the VP Range field to Vp Ranges On. Select OK to return to the Configure POD window.
4. Select the Port from the Configure POD window ([Figure 4-4 on page 4-7](#)). The Configure Port window appears.
5. Select the CAC button from the Configure Port window. The Port CAC Configuration window appears ([Figure 4-19](#)).

The image shows a Java applet window titled "Port CAC Configuration". It has a menu bar with "Events/Alarms..." and "Major". Below the menu bar is a "Port Detail" section with "Slot-Pod-Port" fields containing "1", "3", and "1", and a "Port ID..." field containing "DS3 CIRCUIT I". The main area is divided into two panels: "CAC" and "VP". The "CAC" panel has "BW Pool(%):" set to "200", "BW Load(%):" set to "10", "Active:" set to "Enable" (via a dropdown), and "Status:" set to "Ok". The "VP" panel has "Vp Minimum:" set to "0", "Vp Maximum:" set to "63", "Start Reserved:" set to "0", "End Reserved:" set to "0", "Modify:" set to "Applied", and "Status:" set to "Vp Ranges Disabled". At the bottom are "Ok", "Cancel", and "Apply" buttons. A status bar at the very bottom says "Please enter a value 0..2000" and "Unsigned Java Applet Window".

**Figure 4-19. Port CAC Configure Window**

6. Enter a Start Reserved and End Reserved value to designate a range of VPI values for use by PVPs. The VPI values in this range are unavailable for use by PVCs. Select Apply or OK to accept your changes.

Table 4-15 describes the fields and buttons in the Port CAC Configuration window.

**Table 4-15. Port CAC Configuration Fields and Buttons**

Field/Button	Type	Action/Description
<b>POD Detail</b>		
Slot # - POD # - Port #	read-only	Displays the currently selected slot, POD, and port number.
Port ID	read-only	Displays the name of the selected POD.
<b>CAC</b>		
BW Pool (%)	read/write	Specify the size of the variable bandwidth pool as a percent of the fixed bandwidth pool.
BW Load (%)	read/write	Specify the value of the Variable to Fixed Load percentage.
Active	read/write	Enable or disable CAC bandwidth accounting on this port.
Status	read-only	Displays the status of CAC on this port.
<b>VP (Applies only to ATM Cell PODs using PVPs)</b>		
Vp Minimum	read-only	Displays the minimum VPI value; always 0.
Vp Maximum	read-only	Displays the maximum VPI value. Determined by the number of VPI bits on the Cell Highway Configuration screen (Figure 3-19).
Start Reserved	read-write (read-only if VP Ranges is disabled)	Enter the lowest VPI value to be reserved for PVPs.  If VP Ranges is disabled, this field is read-only and displays 0.
End Reserved	read-write (read-only if VP Ranges is disabled)	Enter the highest VPI value to be reserved for PVPs.  If VP Ranges is disabled, this field is read-only and displays 0.
Modify	read/only	Indicates whether the system must be rebooted for changes made to take effect.
Status	read-only	Indicates whether VP ranges are enabled or disabled. If VP ranges are disabled, the VP Min/VP Max and Start Reserved/End Reserved values above will be read-only.

## Configuring the ATM Interface

After configuring an ATM Cell Port (DS1 Cell, DS3, OC3-c/STM-1, IMA), the ATM interface must be configured.

To configure the ATM interface:

1. Choose the Next Logical Layer button in the specific Configure Port or Configure Path window. The Configure ATM Interface window appears (see [Figure 4-20](#)).

Configure ATM Interface

Events/Alarms... Critical

Interface Detail

Interface Name... ATM INTERFACE Interface ID... ATM CIRCUIT 1

ADMIN Status: Up OPS Status: Up

Slot-Pod-Port: 1 3 1

Configuration Management

Cell Delineation: HcsBased

Cell Scrambling: Enable

Cell Fill Option: Idle

Cell Shaping Rate:

SAP Configuration

Type: Config AtmfUniPvcOnly Actual AtmfUniPvcOnly

Side: Config User Actual User

ILMI: None

Admin: Enabled

Oper :

Advanced... ILMI Port Prefix...

Service Management...

OK Cancel Apply

Select to create/modify an Interface Name.

Warning: AppletWindow

**Figure 4-20. Configure ATM Interface Window**

2. Complete the fields described in [Table 4-16](#).
3. When finished, choose OK to return to the previous window.



**Table 4-16. Configure ATM Interface Fields and Buttons**

Field/Button	Type	Action/Description
<b>Interface Detail</b>		
Slot-POD-Port	read-only	Displays the interface's slot, POD and port numbers.
Interface Name	read/write	Specify the interface name (32 characters max).
Interface ID	read/write	Specify the interface ID (32 characters max).
ADMIN Status	read/write	Set the administrative state for this interface on power-up. Default is up (online). Set to Down (offline) when you run diagnostics. (The Testing option is not supported.)
OPS Status	read-only	Displays the operational state of the interface.
<b>Configuration Management</b>		
Cell Delineation	read/write          read-only	<b>DS3/E3 interfaces only:</b> displays the cell delineation or cell synchronization method for this interface. Options are:  <i>HcsBased</i> – Enables HCS-based cell delineation.  <i>PlcpFrame</i> – Enables Physical Layer Convergence Protocol cell delineation.  <b>For all other interfaces,</b> displays the type of cell delineation: HcsBased.
Cell Scrambling	read/write	Specify whether the cell scrambling function is enabled, disabled, or not applicable.
Cell Fill Option	read/write	Specify the cell fill option to transmit idle cells or unassigned cells when no data cells are queued for transmission.
Cell Shaping Rate	read/write	(For OC-3/STM-1 Cell POD with Bulk Cell Shaping only)  If the Cell Fill Option (above) is enabled, enter the cell shaping rate in 1 Mbps increments. The outgoing ATM cell stream will be shaped to this rate.  The valid range is 1 – 150. Selections from 1 – 100 Mbps provide uniform distribution of cells into the cell stream. Selections from 101 – 150 Mbps transmit cells in a non-uniform distribution.

**Table 4-16. Configure ATM Interface Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Fault Management</b>		
Alarm Reporting	read/write	Enable or disable alarm reporting on the interface.  <i>Note: Never disable alarm reporting on any port used for primary or secondary recovered timing.</i>
<b>SAP Configuration</b> (applies only to SAP-eligible ports; i.e., ATM ports on Slot 1)		
Type: Config	read/write	Select the ATM Forum UNI variant for this ATM interface. This determines the connection setup procedures which will be used for this ATM interface.  <i>AtmfUni3Dot0</i> (default) – selects ATM Forum UNI 3.0 signaling.  <i>AtmfUni3Dot1</i> – selects ATM Forum UNI 3.1 signaling.  <i>AtmfIisp3Dot0</i> – selects ATM Forum Interim Inter-Switch Protocol 3.0 signaling.  <i>AtmfIisp3Dot1</i> – selects ATM Forum Interim Inter-Switch Protocol 3.1 signaling.  <i>AtmfUniPvcOnly</i> – disables signaling; connections must be made using provisioned VPI/VCI values.
Type: Actual	read-only	Displays the actual UNI variant in effect at this port. Will match the Config Type above unless the UNI variant selected cannot be applied.  Similar to the Admin and Oper Status fields, the Actual field serves as a check on the Config field, providing a verification that what you have selected is actual in use.  For example, only two ports may be configured for signalling, so a third port configured for signalling would display <i>AtmfUniPvcOnly</i> in this field, and permit only PVC dial-type connections on this port.
Side: Config	read/write	Specify this ATM Interface as <i>User-side</i> (DTE) or <i>Network-side</i> (DCE).  ( <i>Other</i> is not currently supported.)

**Table 4-16. Configure ATM Interface Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Side: Actual	read-only	Displays the actual network side in effect at this port. Will match the Side:Config selection above unless the side selected cannot be applied.  Similar to the Admin and Oper Status fields, the Actual field serves as a check on the Config field, providing a verification that what you have selected is actual in use.
ILMI	read/write	Enable or disable ILMI on this ATM interface:  <i>None</i> – Disables all ILMI components on this interface.  <i>ILMI</i> – Enables ILMI address registration and keep-alive message functions on this ATM interface.
Oper	read-only	Displays the operational state of ILMI on this port.
Advanced	window button	Not currently supported.
Port Prefix Table	window button	Enables you to access and configure the ILMI Port Prefix Table. See “ <a href="#">Setting ILMI Port Prefixes</a> ” on page 4-52.
<b>(Other Buttons)</b>		
Service Management	window button	Enables you to configure ATM UNI connections. See “ <a href="#">Configuring ATM UNI Connections</a> ” on page 5-37.

## About Signaling Protocols, User/Network Side, and ILMI

A Service Access Point (SAP) is the point (a selected interface) at which the one ATM device communicates with another ATM device. With regard to the SA devices, it is the point at which the SA unit meets the network-side ATM switch. Service Access Points are used to exchange the call setup messages required by all signalled connections. The SAP Configuration settings in the Configure ATM Interface dialog box have important implications on the function of the box as a whole and the kinds of dial types available when configuring connections.

In an SA unit, the primary trunk is one ATM port on the System Control Module, usually on the XPOD. The primary trunk is configured as a SAP by selecting an ATM Forum signaling variant. The primary trunk is used for outbound signaling applications. The initiating call setup messages for all signalled connections (A-SPVC's and SPVC's) are passed out the SAP designated as the primary trunk, and, conversely, the primary trunk SAP recognizes and handles any incoming call setup messages received. Call setup messages received on ports not configured as a SAP are not recognized and are ignored.

Multiple SAPs may be configured to provide a readily available backup should the primary trunk port fail. By changing the Slot-POD-Port defined as the primary trunk in the ASPVC Address Configuration window to a previously configured SAP, you can quickly restore any switched connections lost in the failure of the primary trunk.

Selecting a signaling variant on the SAP and configuring the SA unit as user-side or network-side affects the function of ILMI (if enabled). The relationship between Protocol Variant, User/Network Side and ILMI are described in [Table 4-17](#), below.

**Table 4-17. Signaling Protocols and ILMI**

Protocol Variant Selected	UNI Side Selected	If ILMI is On:	Interpretation
UNI 3.0 or 3.1	User	SA unit considered DTE, Address registration On	The SA unit is considered the user-side ATM device, receiving its net prefix from and registering its address with the network-side device.
UNI 3.0 or 3.1	Network	SA unit considered DCE, Address registration On	The SA unit is considered the network-side ATM device. It doles out net prefixes to attached user-side devices, and maintains a table of registered user-side addresses.
IISP 3.0 or 3.1	Either	SA unit considered DCE, Address registration not supported.	The SA unit supports ILMI keep-alive messages to attached user-side ATM devices, but does not perform address registration functions.

ILMI provides an automated method for generating an SA unit's ATM address. The ATM address is required if signalled connections are going to be placed *to* an SA unit. Without a destination ATM address, an ASPVC Orig or SPVC connection cannot be directed through the network, and, unless the destination SA unit knows its own ATM address, it will not respond to call setup requests directed to that address.

If ILMI is enabled, it will attempt to contact the network-side ATM switch connected to the SAP. Assuming there is an ATM switch connected to the primary trunk's ATM port, and that switch is also running ILMI, the SA unit will request and receive a net prefix from the ATM switch. The SA unit appends its ESI to the net prefix to create an AESA (ATM End Station Address), which it sends back to the ATM switch. From this point on, any call setup requests for this AESA will be directed to the SA unit.

If ILMI is disabled, the SA unit can still receive and reply to call setup requests if an AESA is manually established for the SA unit. A net prefix must be obtained from the network-side ATM switch port to which the SA unit is connected. This net prefix is entered into the Net Prefix field of the ASPVC Address Configuration dialog box. The SA unit will append its ESI to the net prefix to create an AESA. The ATM switch will direct any messages addressed with the net prefix out the port to the SA unit. The SA unit will recognize its AESA and reply appropriately to any messages directed to this AESA. (See [“Specifying ASPVC Addresses” on page 3-19](#) for details.)

## Setting ILMI Port Prefixes

Interim Local Management Interface (ILMI) is a Management Information Base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep-alive protocol. WebXtend currently implements the following ILMI functions:

- Address registration based on configured Network and Port Prefix tables
- Rejection of duplicate ATM addresses from DTE devices
- Initiation of link connectivity “keep-alive” messages
- Support for ILMI “gets” for ATM and physical layer statistics

### About ILMI Prefixes

Address information in a switch is used both for determining the proper route for calls and for calling-party screening. When used for route determination, the switch advertises an appropriate subset of its configured node prefixes, port prefixes, and port addresses to all other switches in the network. When used for calling-party screening, the switch uses the configured node prefixes, port prefixes, and/or port addresses to determine whether or not a call should be accepted by the network.

To perform these two functions at a UNI, both the user and the network need to know the ATM addresses that are valid at the UNI. Address registration provides a mechanism for address information to be dynamically exchanged between the user and the network, enabling them to determine the valid ATM addresses that are in effect at a UNI. Address registration applies only to UNI ports on which ILMI is enabled. Any ILMI-eligible node or port prefix will be transferred from all ILMI-enabled private UNI-DCE ports and all ILMI-enabled public end-system UNI-DCE ports to their peer DTE devices.

Node prefixes are not exchanged from “public switch” UNI-DCE ports. Only port prefixes are exchanged from these ports.

To configure ILMI Port Prefixes:

1. Choose the Port Prefix Table button from the Configure ATM Interface window. The ILMI Port Prefix Table window appears (see [Figure 4-21](#)).

**Figure 4-21. ILMI Port Prefix Table Window**

2. To add a new ILMI Port Prefix, choose the Add Port Prefix button. The Add Port Prefix window appears (see [Figure 4-22](#)).

**Figure 4-22. Add Port Prefix Window**

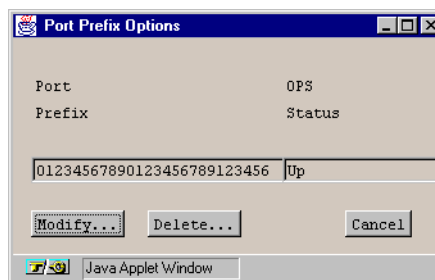
3. Complete the fields described in [Table 4-18](#).
4. Choose OK to return to the ILMI Port Prefix Table window.

**Table 4-18. Add Port Prefix Fields and Buttons**

Field/Button	Type	Action/Description
Type	read/write	Select the type of Port Prefix: <i>E.164</i> (not currently supported) - Allows a prefix of up to 16 digits. Prefixes of less than 16 digits will be padded with leading zeros. <i>Nsap</i> - Prefix must be 26 digits. <i>Unknown</i> - (not currently supported)
Prefix	read/write	Enter a port prefix based on the Type selected above.
Admin. Status	read/write	Set the administrative state of the Port Prefix: up or down. (No op not supported.)
OPS Status	read-only	Displays the operational state of the Port Prefix: up or down.

### Modifying or Deleting ILMI Port Prefixes

To modify or delete an ILMI Port Prefix, double-click the Port Prefix in the ILMI Port Prefix Table window. The Port Prefix Options window appears (Figure 4-23), enabling you to modify or delete the selected prefix.



**Figure 4-23. Port Prefix Options window**

Selecting Modify presents a Modify dialog box similar to the Add Port Prefix dialog box. Make any desired changes, then choose OK.

Selecting Delete prompts you for confirmation before deleting the selected ILMI Port Prefix.



## Configuring a Universal Serial Port

There are two serial-port PODs available, a Universal Serial Frame IPOD and a Universal Serial Circuit Emulation Service POD. The two serial PODs have the same physical interface, and thus are configured through identical Configure Port dialog boxes.

To configure a Universal Serial port:

1. Select the serial port from the Interface Management window, as described in “Selecting a Port” on [page 4-7](#). The Configure Universal Serial Port window appears (see [Figure 4-24](#)).

**Figure 4-24. Configure Universal Serial Port Window**

2. Complete the fields described in [Table 4-19](#).
3. When you are done configuring this port, choose the Next Logical Layer button to configure connections and interworking functions. See “[Configuring Universal Serial Frame Service](#)” on [page 5-102](#) for information on configuring frame service interworking functions, or “[Configuring Circuit Emulation Services](#)” on [page 5-83](#) for information on configuring CES interworking functions.
4. After configuring the US service and returning to this window, choose OK.

**Table 4-19. Configure Universal Serial Port Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD, and port number.
Port Name	window button	Specify the port name (32 characters max).
Port ID	window button	Specify the port ID (32 characters max).
Set ADMIN Status	read/write	Set the administrative state of the port: up (default) or down. Set to Down (offline) when you run diagnostics.
OPS Status	read-only	Displays the operational state of the port: up or down.
<b>Configuration Management</b>		
Service Type	read/write	Specify the service type used on the port: <i>HDLC Encapsulation</i> (default) – selects High-Level Data Link Control communications. This service type provides encapsulation and tunneling on all HDLC frames on a point to point basis. <i>SDLC Encapsulation</i> – selects Synchronous Data Link Control communications. This service type provides encapsulation and tunneling on all SDLC frames on a point to point basis.
Physical Interface	read-only	Displays the physical interface (cable type) which has been auto-detected by the port: <i>None</i> (default) – No cable is connected to interface. <i>Rs232</i> – RS232 cable connected to interface. <i>Rs449</i> – RS449 cable connected to interface. <i>Rs530</i> – RS530 cable connected to interface. <i>V35</i> – V.35 cable connected to interface. <i>X21</i> – X.21 cable connected to interface. <i>Unknown</i> – The POD is unable to identify the cable connected to interface.

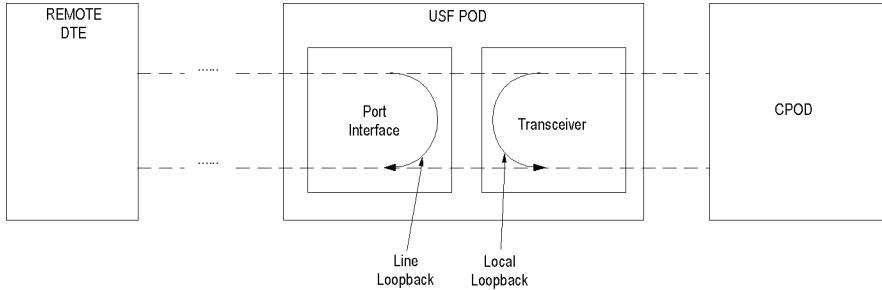
**Table 4-19. Configure Universal Serial Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Tx Clock	read/write	<p>Select a transmit timing source for the port from the following options:</p> <p><i>Internal</i> (default) - The POD's internal timing source provides the transmit timing for this port.</p> <p><i>External</i> – The transmit timing is derived from the timing signal recieved by this port.</p> <p><i>Split</i> – not supported.</p>
Timing Phase	read/write	Specify the Timing Phase for this port: normal (default) or inverted.
Clock Rate	read/write	<p>Specify the clock rate (data rate) of the interface.</p> <p><i>PortBPS 2400</i> (default) – Selects a service rate of 2400 bps.</p> <p><i>PortBPS 4800</i> – Selects a service rate of 4800 bps.</p> <p><i>PortBPS 9600</i> – Selects a service rate of 9600 bps.</p> <p><i>PortBPS 19200</i> – Selects a service rate of 19200 bps.</p> <p><i>PortBPS 38400</i> – Selects a service rate of 38400 bps.</p> <p><i>PortBPS 64K</i> – Selects a service rate of 64 kbps.</p> <p><i>PortBPS 128K</i> – Selects a service rate of 128 kbps.</p> <p><i>PortBPS 256K</i> – Selects a service rate of 256 kbps.</p> <p><i>PortBPS 384K</i> – Selects a service rate of 384 kbps.</p> <p><i>PortBPS 512K</i> – Selects a service rate of 512 kbps.</p> <p><i>PortBPS 768K</i> – Selects a service rate of 768 kbps.</p> <p><i>PortBPS 1024K</i> – Selects a service rate of 1024 kbps.</p> <p><i>PortBPS 1536K</i> – Selects a service rate of 1536 kbps.</p> <p><i>PortBPS 2048K</i> – Selects a service rate of 2048 kbps.</p> <p><i>PortBPS 4096K</i> – Selects a service rate of 4096 kbps.</p>

**Table 4-19. Configure Universal Serial Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Flow Control	read/write	Specify the flow control to use on this port: <i>None</i> (default) – no flow control. <i>CtsRts</i> – Clear to Send/Request to Send flow control. <i>DsrDtr</i> – Data Set Ready/Data Terminal Ready flow control.
LOS Detection	read/write	Select the conditions which register a Loss of Signal alarm for the port. The options are: <i>Dtr</i> (default) – LOS alarm occurs when the POD detects a loss of DTR (DCE ports). <i>Rts</i> – LOS alarm occurs when the POD detects a loss of RTS (DCE ports). <i>DtrORrts</i> – LOS alarm occurs when the POD detects a loss of either DTR or RTS (DCE ports). <i>DtrANDrts</i> – LOS alarm occurs when the POD detects a loss of both DTR and RTS (DCE ports). <i>Dsr</i> – LOS alarm occurs when the POD detects a loss of DSR (DTE ports). <i>Cts</i> – LOS alarm occurs when the POD detects a loss of CTS (DTE ports). <i>DsrORcts</i> – LOS alarm occurs when the POD detects a loss of either DSR or CTS (DTE ports). <i>DsrANDcts</i> – LOS alarm occurs when the POD detects a loss of both DSR and CTS (DTE ports). <i>None</i> – LOS alarm detection disabled.
<b>SDLC Configuration</b>		
Line Encoding	read/write	Select a line encoding method for this port: <ul style="list-style-type: none"> <li><i>Nrz</i> (default) – Non-Return to Zero.</li> <li><i>Nrzi</i> – Non-Return to Zero Inverted.</li> </ul>
Minimum Flag Bytes	read/write	Specify the minimum number of flags between frames: 1 or 2. Default = 2.
Idle Pattern	read/write	Select the idle pattern for this port: Space (default) or Mark

**Table 4-19. Configure Universal Serial Port Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Fault Management</b>		
Set Alarm Reporting	read/write	Enable or disable alarm reporting on the port.
Set Port Loopback	read/write	<p>Set/display whether port loopback is disabled or enabled for testing purposes (see <a href="#">Figure 4-25</a>). Select one of the following:</p> <p><i>None</i> (default) – Disables the loopback function for normal operation.</p> <p><i>Line</i> – Tests the port interface by routing received data back out of the port.</p> <p><i>Local</i> – Loops data back towards the CPOD.</p>
 <p>The diagram illustrates the data flow for port loopbacks. On the left is a box labeled 'REMOTE DTE'. In the center is a larger box labeled 'USF POD' which contains two sub-components: 'Port Interface' and 'Transceiver'. On the right is a box labeled 'CPOD'. Dashed lines represent data paths: one from REMOTE DTE to Port Interface, and another from Transceiver to CPOD. Below the USF POD box, two curved arrows indicate loopback paths: 'Line Loopback' from the Port Interface back to itself, and 'Local Loopback' from the Transceiver back to itself.</p>		
<b>(Other Buttons)</b>		
Next Logical Layer	window button	<p>Opens a window for configuring universal serial service connections. See <a href="#">“Configuring Universal Serial Frame Service”</a> on page 5-102 for information on configuring frame service interworking functions, or <a href="#">“Configuring Circuit Emulation Services”</a> on page 5-83 for information on configuring CES interworking functions.</p>

**Figure 4-25. Universal Serial POD Port Loopbacks**

## **What's Next?**

After you configure the SA unit's ports, you can configure network services through the Service Management functions, as described in Chapter 5, "Configuring Network Services."

# Configuring Network Services and Connections

This chapter describes how to configure the following network services, including establishing connections and interworking functions.

If you're new to using WebXtend and want some background information about setting up connections, read [“Selecting a Network Service and Managing Connections” on page 5-2](#) and [“About Connections and Dial Types” on page 5-10](#).

For specific examples of setting up connections of various dial types, see [“Connection Setup Examples” on page 5-17](#).

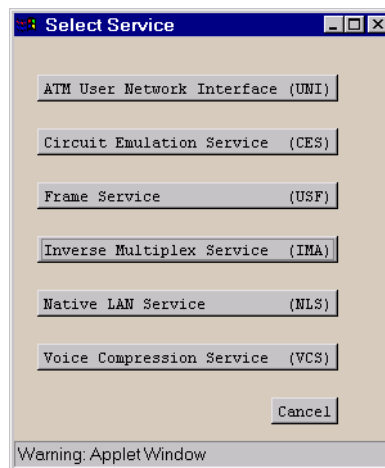
If you're familiar with connection setup procedures and just want the details, see the following sections:

- ATM User Network Interface (UNI) Service (see [page 5-33](#))
- Inverse Multiplexing (IMA) Services (see [page 5-46](#))
- Native LAN Service (NLS) (see [page 5-64](#))
- Circuit Emulation Service (CES) (see [page 5-83](#))
- Frame Service (USF) (see [page 5-102](#))
- Voice Compression Service (VCS) (see [page 5-117](#))

## Selecting a Network Service and Managing Connections

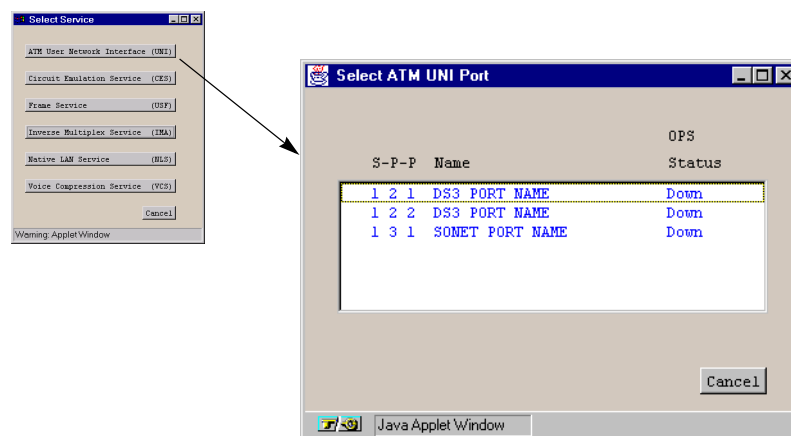
You can select a network service by choosing the Service Management button from the Main menu. (Using the Service Management button is the most direct means to select network services and set up connections, but there are other ways; see [“Alternate Methods of Selecting a Network Service”](#) on page 5-9.)

When the Select Service window appears (see [Figure 5-1](#)), select the service type.



**Figure 5-1. Select Service Window**

Selecting a service from the Select Service window displays the Select Port window, a list of all ports supporting that service type. For example, selecting ATM User Network Interface on an SA unit might display the following ports:



**Figure 5-2. Select Port Window (ATM UNI shown)**

Selecting a port from the list opens the Connections window for that port (see [Figure 5-3](#)). The Connections window for a selected port lists all connections and interworking functions which have been established on the port.



The Connections window is the central point for setting up connections and accessing connection information. All connection management and connection monitoring functions (covered in Chapter 6) are handled from the Connections window.

#### Common Fields in Connection Window

**Port Detail** shows information on the selected port. Some fields may be read/write, enabling you to configure port-level connection attributes (apply to all connections on this port). May offer function buttons to view additional information.

**Configured Connections** list shows all connections which have been configured on this port. Note that connections may have been set up from another port with this port as Endpoint B.

Selecting a connection opens the Connection Options window for that connection, for modifying connection parameters, deleting the connection or viewing statistics about the connection.

Additional buttons allow you to add connections/interworking functions on this port or to view additional information.

Name	Svc Dial Type	Connect Status	Connect Detail
ATM UNI Conn 1	UNI Pvc Orig	Up	Ok
NLS Tunnel 1	NLS Pvc Orig	Up	Ok
CES Conn 1	CES Pvc Orig	Up	Ok
CES Conn 2	CES Pvc Orig	Up	Ok
CES Conn 3	CES Pvc Orig	Up	Ok
CES Conn 4	CES Pvc Orig	Up	Ok

Figure 5-3. Connections Window (ATM UNI shown)

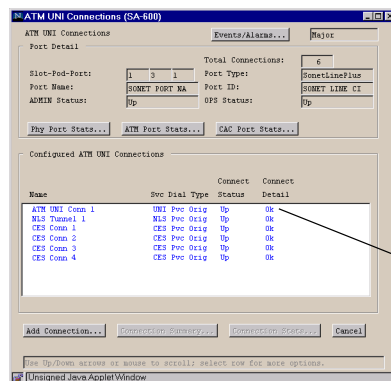


The title of the Connections window depends upon the type of port selected. For instance, the Connections window of an ATM cell port (DS1, DS3, OC-3/STM-1, etc.) is titled ATM UNI Connections. The Connections window of a CES port is titled Configure CES Connections. The Connections window of an Ethernet port is titled Native LAN Service (NLS) Tunnels. (Ethernet connections are referred to as “tunnels”.) Though titled differently and displaying some port-type-specific information and buttons depending on service type, the purpose of all Connections windows is similar: enabling you to add new connections and to access existing connections to modify connection parameters, delete the connection, or view a connections’ statistics. The various services supported by the SA units are described throughout the rest of this chapter and the Connections window for each service type is described in detail.

Selecting a connection from the Configured Connections list opens the Connection Options window, an example of which is shown in [Figure 5-4](#):

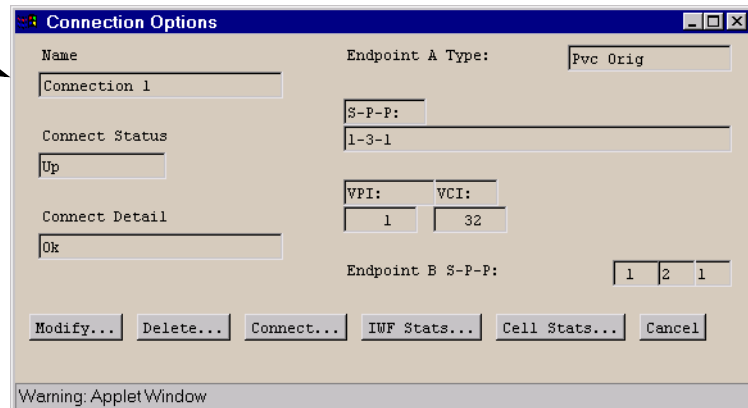
## Configuring Network Services and Connections

### Selecting a Network Service and Managing Connections



**Endpoint A Type and identifiers** display the type and identity of connection at this end. (The currently selected port is always considered Endpoint A of any connection being viewed.)

**Endpoint B S-P-P** displays the slot, POD, and port at the opposite end of the connection.



#### Common Fields in Connection Options

**Name** displays the name assigned to this connection.

**Connect Status** displays the connection status, Up or Down.

**Connect Detail** displays error conditions (if any) for the connection.

**Modify** opens the Add/Modify Connection window to change the connections' parameters.

**Delete** prompts you for confirmation, then deletes the connection.

**Connect** enables you to set the connection's status to Up (active) or Down (inactive).

**IWF Stats** applies to interworking function connections only, and displays statistics on the interworking function side of the connection.

**Cell Stats** displays statistics on the ATM cell side of the connection.

**Figure 5-4. Connection Options Window Example (ATM UNI shown)**

From the Connection Options window, you can modify, delete, or temporarily enable or disable a connection, as well as monitor interworking function statistics or cell statistics. [Table 5-1](#) describes the buttons and fields in the Connection Options windows.

**Table 5-1. Connection Options Fields and Buttons**

Field/Button	Type	Description
Name	read-only	Displays the name of the currently selected ATM connection.
Connect Status	read-only	Displays the state of the ATM connection: Up or Down.
Connect Detail	read-only	Displays an error code if any failure is present on this connection, or blank if no failure exists. See <b>“Common Fields/Buttons”</b> on page 2-16 for a list of error codes.
Endpoint A Type	read-only	Displays the dial type for this connection: <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI. <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI. <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle. <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle. <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read-only	Displays Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
Handle (applies to ASPVC dial type only)	read-only	Displays the ASPVC Handle associated with this connection.
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual channel identifier of endpoint B for this connection.

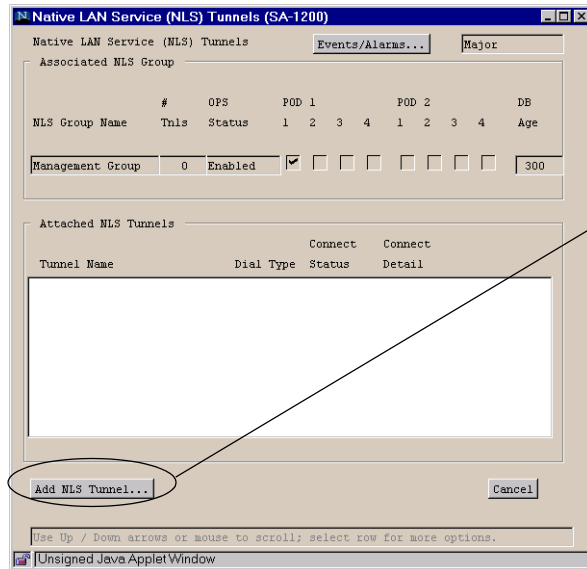
**Table 5-1. Connection Options Fields and Buttons (Continued)**

Field/Button	Type	Description
Endpoint B	read-only	Displays the Slot-POD-Port for the other end of this connection:
<b>(Other Fields and Buttons)</b>		
Modify	window button	Enables you to modify the selected connection by opening the Add/Modify window.
Delete	window button	Enables you to delete the selected connection after prompting you for confirmation.
Connect Mgmt	window button	Enables you to set the selected ATM connection's status to Up or Down (active or inactive).
IWF Stats	window button	<p>Enables you to view statistics on the interworking function (CES, USF, or VCS) side of the selected connection. See <b>Chapter 6, "Monitoring an SA Unit,"</b> for information on viewing IWF statistics.</p> <p>Does not apply to ATM UNI connections since all statistics are cell statistics. Not available for NLS interworking functions since statistics are available at the group level.</p>
Cell Stats	window button	Enables you to view statistics on the ATM side of the selected connection. See <b>Chapter 6, "Monitoring an SA Unit,"</b> for information on viewing ATM statistics.

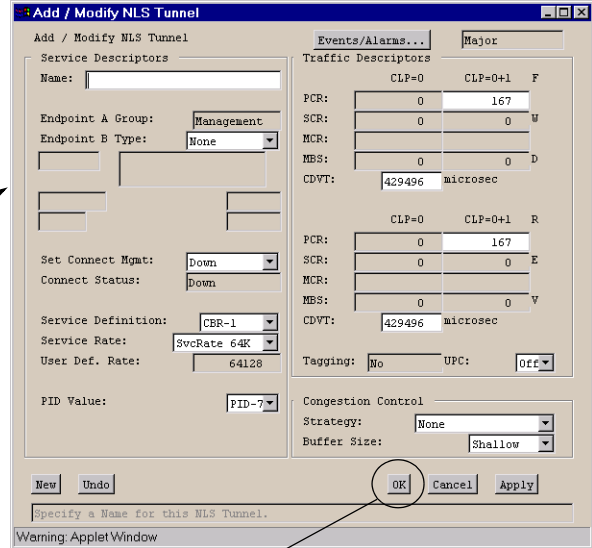
## Setting up Connections

The general procedure for setting up connections is shown in **Figure 5-5**. The procedure is explained beginning at the Connections window (i.e., after selecting a service and an individual port). The individual dialog boxes you will need to complete at each step are covered in complete detail throughout the rest of this chapter.

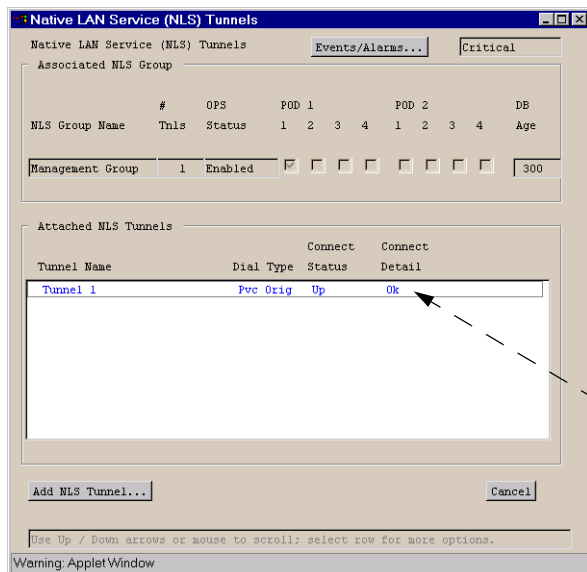
1. Beginning at the Endpoint A Connections window, select the Add button.



2. Complete the Add Connection dialog box to configure the new connection's parameters.



3. The connection or interworking function is created at the Endpoint A port...



...and is mirrored at the Endpoint B port.

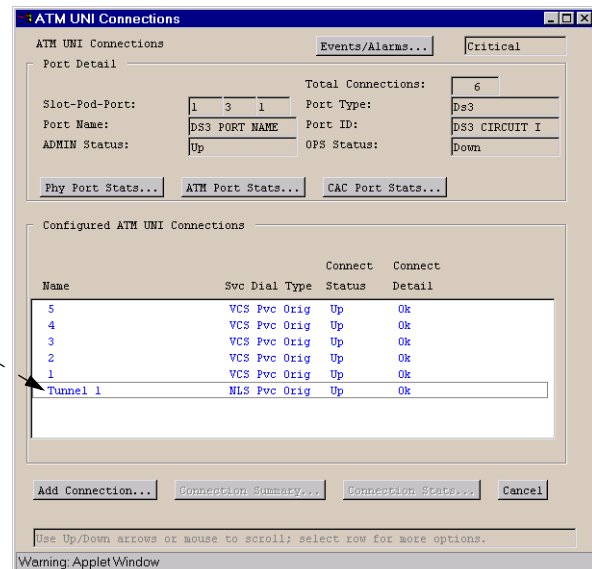


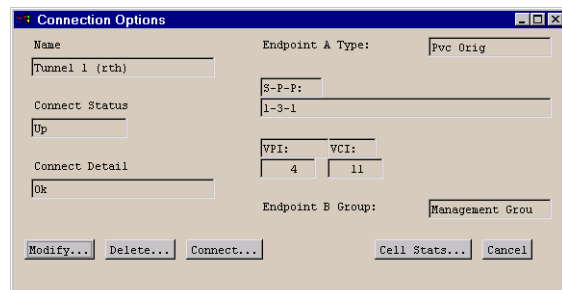
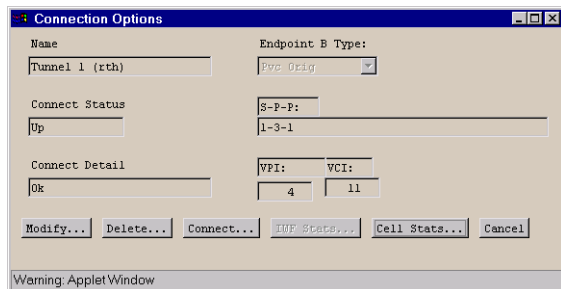
Figure 5-5. Connection Setup and Mirroring Example

As shown in **Figure 5-5**, creating a connection causes that connection to appear in the Configured Connections list both at the originating endpoint and at the destination endpoint. This reflection at the second endpoint is called “mirroring” and enables you to view each connection from either endpoint.

The Endpoint A and Endpoint B designations, however, are always presented with regard to the port selected. The selected port is always considered Endpoint A and the other port is always considered Endpoint B, regardless of which port the connection was set up on initially. To illustrate this, **Figure 5-6** shows the Connection Options windows displayed when Tunnel 1 is selected from the Configured NLS Tunnels window and the Connection Options window displayed in **Figure 5-5**.

The Connection Options window opened from the Configured NLS Tunnels list shows Endpoint B as S-P-P 1-3-1...

...the mirrored end of the connection opened from the Configured ATM UNI Connections list shows Endpoint B as Management Group.



**Figure 5-6. Connection Options Example**

Now that you’ve seen a general overview of the connection setup process, the following sections discuss the various dial-types which may be used to create connections and then provide more detailed examples of how to set up each kind of connections.

## Alternate Methods of Selecting a Network Service

Although the Service Management window provides the quickest, most direct route to the Connections windows from the Main Menu, there are other ways of accessing the Connections window for a port. You can also select a network service after configuring or monitoring a port as follows:

**ATM UNI** — After configuring the ATM interface of a DS1/E1, DS3/E3 Cell, or OC-3c/STM-1 Cell port, (described in [“Configuring the ATM Interface” on page 4-46](#)), configure the ATM UNI Connections by choosing the Service Management button in the Configure ATM Interface window.

**Native LAN** — After configuring the ports of an Ethernet POD, configure the Native LAN Service (NLS) by choosing the Service Management button in the Configure Ethernet Port window.

**CES** — After configuring the ports of a Circuit Emulation Service (CES) POD, configure the Circuit Emulation Service by choosing the Next Logical Layer button in the Configure Port window.

**Frame Service** — After configuring the ports of a Universal Serial Frame (USF) POD, configure the Frame Service by choosing the Next Logical Layer button in the Configure Port window.

**Inverse Multiplex Service** — After configuring the ports of an IMA POD, configure the IMA Service by choosing the Next Logical Layer button in the Configure Port window.

**Compressed Voice** — After configuring the ports of a Voice Compression POD, configure the Compressed Voice service by choosing the Next Logical Layer button in the Configure Port window.

## About Connections and Dial Types

Connections provide a path from one endpoint to another. The means used to identify the endpoints and establish the connection is called the dial type. The SA devices support several kinds of dial types:

- PVP – Permanent Virtual Path. A traditional non-switched manually-provisioned connection between the SA unit and the next network hop, identified by a Virtual Path Identifier (VPI).
- PVC – Permanent Virtual Channel. A traditional non-switched manually-provisioned connection between the SA unit and the next network hop, identified by both a Virtual Path Identifier and a Virtual Channel Identifier (VCI).
- A-SPVC – Adaptation Soft PVC. A PVC connection using switching functions between two SA units across an ATM network. The end system's ATM address is used to route the connection through the network to the destination SA unit. At the destination SA unit, the connection is passed to the destination interworking function identified with a unique 'handle'.
- SPVC – Switched PVC. A special case in which switching is used over most of the connection's path and a designated Permanent Virtual Connection is used for the final hop. This case exists only between an SA unit and an Ascend CBX 500 or GX 550 ATM switch. The switch's ATM address is used to establish the switched connection from the SA unit to the CBX 500/GX 550, and a specified VPI/VCI is used to reach the next hop beyond the switch.

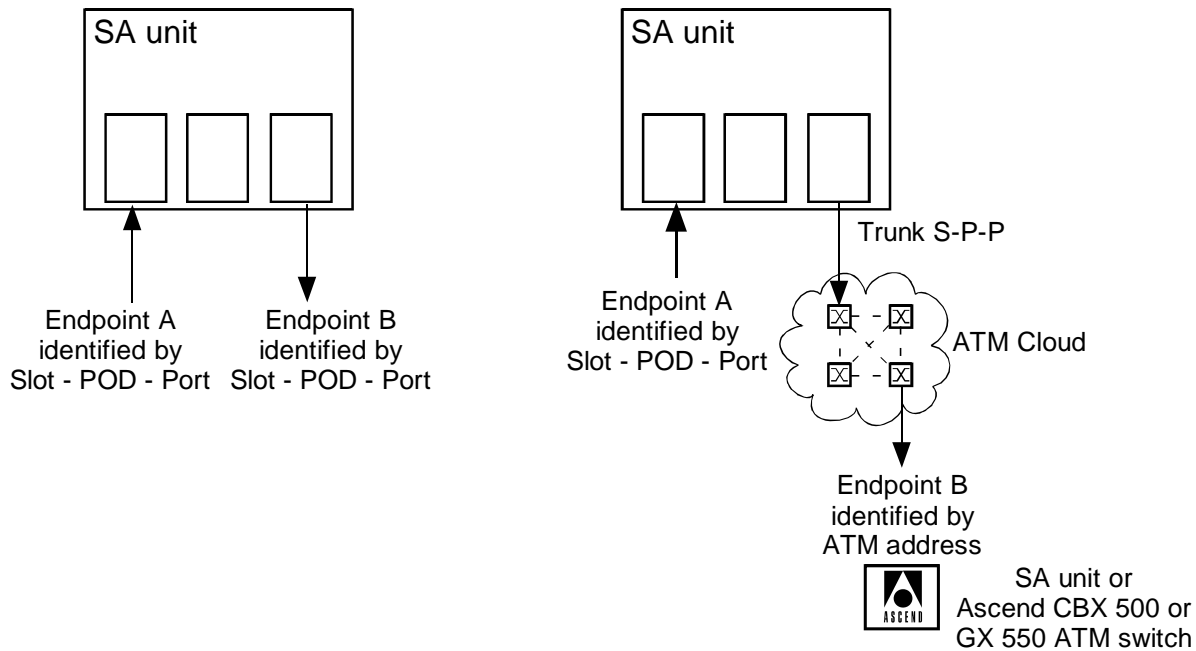
For a summary of the various dial types, see [“Dial-Type Addressing Formats Summary” on page 5-16](#).

## Switched Connections and Trunks

Unlike traditional PVP/PVC connections, which have Endpoint B defined as a Slot/POD/Port on the same SA unit as Endpoint A, the two switched dial types (A-SPVCs and SPVCs) have an Endpoint B outside the SA unit, usually at the other side of an ATM network. To direct the connection out of the SA unit and on to the next hop, switched connections always use a pre-defined trunk connecting the SA unit to the ATM network. All switched connections are automatically sent from their incoming POD to the trunk POD/Port. [Figure 5-7](#) compares traditional PVP/PVC connections with switched connections using a trunk.

The SA unit's primary trunk is configured using the ASPVC Address Configuration window (see [“Specifying ASPVC Addresses” on page 3-19](#) for details). The primary trunk can be configured to use switching per ATM Forum UNI 3.0, UNI 3.1, IISP 3.0, or IISP 3.1 signalling variants, using the Configure ATM Interface window (see [“Configuring the ATM Interface” on page 4-46](#) for details).



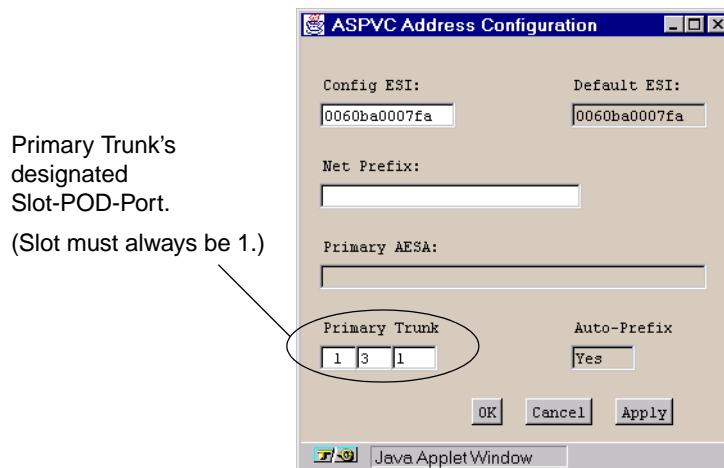


#### PVP/PVC Connections

#### A-SPVC and SPVC Connections

**Figure 5-7. Traditional PVP/PVC vs Switched Connections**

The Trunk is a designated Port on an ATM Cell POD (OC-3/STM-1, IMA, DS1/E1 ATM, DS3/E3, etc). The trunk must be located on the System Control Module (the ICM in Slot 1), and is usually Port 1 of the XPOD (POD 3), so the default trunk is 1-3-1. **Figure 5-8** shows the setting of the default trunk POD in the ASPVC Address Configuration window (accessed from the System Administration window).

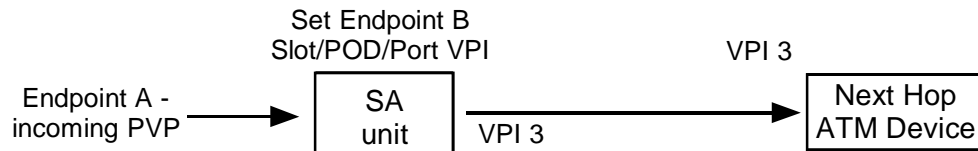


**Figure 5-8. ASPVC Address Configuration – Default Primary Trunk**

## PVP Dial Type

Permanent Virtual Paths may only be used to connect one ATM UNI to another ATM UNI. Both sides of the connection must be ATM UNI PVPs.

In traditional Permanent Virtual Path addressing, you assign an Endpoint B slot/POD/port and VPI (see [Figure 5-9](#)). The connection is made to the next hop on the ATM network, and the VPI value remains fixed until the connection is deleted.



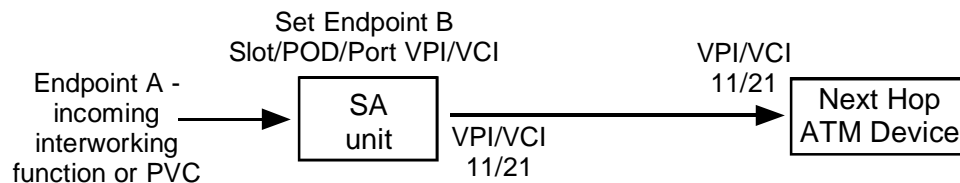
**Figure 5-9. PVP Dial Type**

See [“Example 1: PVP” on page 5-17](#) for a step-by-step example of configuring a PVP connection.

## PVC Orig Dial Type

Permanent Virtual Connections may be used to mesh non-ATM connections (interworking functions) into ATM connections, or one ATM-UNI PVC connection to another PVC connection.

In traditional PVC addressing, you assign an Endpoint B slot/POD/port and VPI/VCI (see [Figure 5-9](#)). The connection is made to the next hop on the ATM network, and the VPI/VCI values remain fixed until the connection is deleted.



**Figure 5-10. Traditional PVC Dial Type**

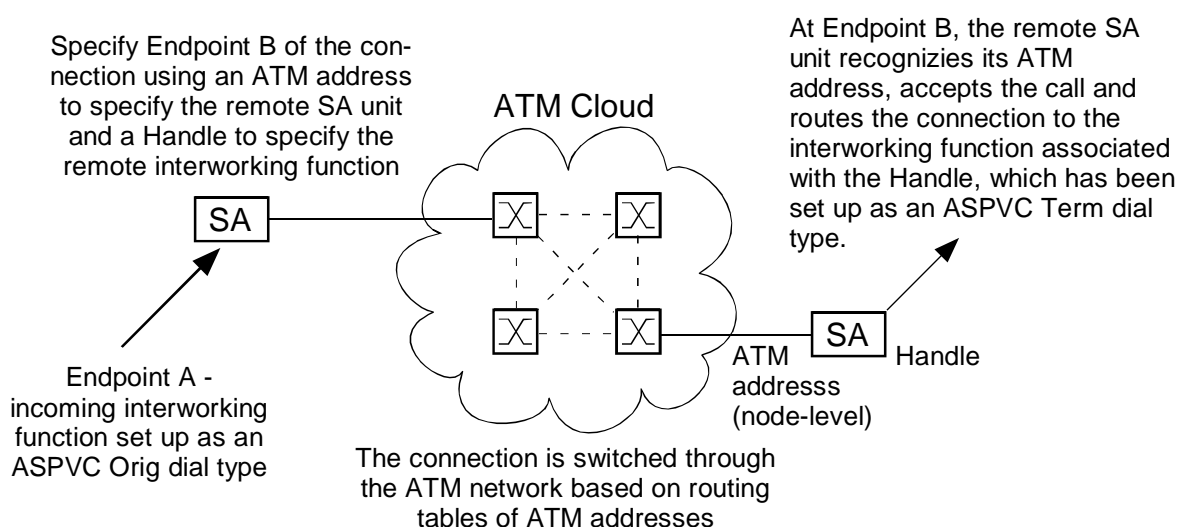
See [“Example 2: PVC \(CES to ATM\)” on page 5-20](#) for a step-by-step example of configuring a PVC interworking function.

See [“Example 3: PVC \(ATM to ATM\)” on page 5-22](#) for a step-by-step example of configuring an ATM PVC connection.

## A-SPVC Dial Type

The Adaptation Service Permanent Virtual Circuit (A-SPVC) dial type uses an ATM address to indicate a specific destination SA unit, and a 'handle' to designate a specific service instance (interworking function) on the remote SA unit (see [Figure 5-9](#)). The A-SPVC also differs from a PVP/PVC in that no slot/POD/port is specified for Endpoint B. It is assumed that Endpoint B is always routed out the slot/POD/port which has been configured as the trunk.

The remote end of an A-SPVC must be pre-configured as a termination. The interworking function and its slot/POD/port are associated with a unique identifier (its handle), and given a dial type of A-SPVC Term. The connection remains idle until it receives a call setup request from an originating SA unit and interworking function.



**Figure 5-11. A-SPVC Dial Type**

Setting up an A-SPVC connection involves three steps:

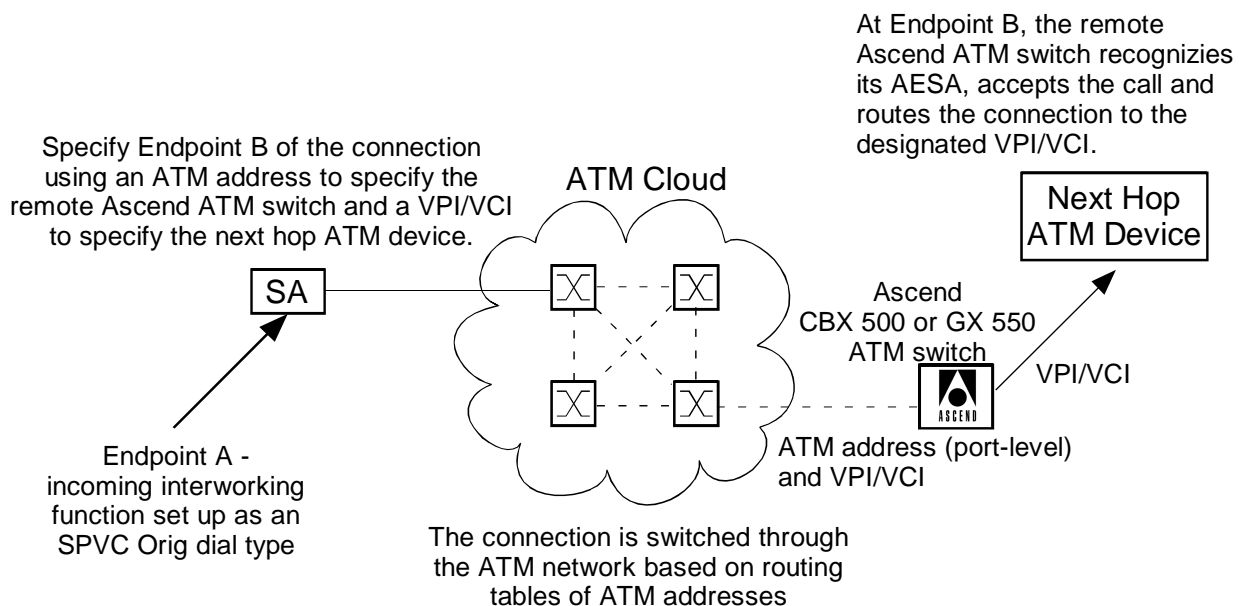
1. Configure the trunks at Endpoint A and Endpoint B. (This is done at the unit level so it usually only needs to be done once.)
2. Set up the remote end (Endpoint B) of the connection as an A-SPVC Term dial type. (A Handle identifier is automatically assigned.)
3. Set up the local end (Endpoint A) of the connection as an A-SPVC Orig dial type, specifying the ATM address of the remote SA node and the individual Handle to connect to.

With these three steps complete, whenever the connection status is set to UP, a call setup request is switched through the network to establish the connection.

See [“Example 4: A-SPVC” on page 5-24](#) for a step-by-step example of configuring an A-SPVC connection.

## SPVC Dial Type

A special case called Switched PVC (SPVC) exists when a connection is being made to a remote Ascend CBX 500 or GX 550 ATM switch. In the case of an SPVC dial type, you address the connection by specifying the ATM address of the remote Ascend switch, and assign a VPI/VCI for the switch to use on the UNI side for the next hop (our ultimate destination ATM device). The final hop beyond the Ascend ATM switch will need to be separately configured to accept the incoming connection's VPI/VCI and service parameters.



**Figure 5-12. SPVC Dial Type**

To set up an SPVC connection, the Ascend ATM switch at the remote end must be properly configured. (This manual does not discuss configuration of non-SA devices; refer to the users manual which accompanied the device.)

Assuming the Ascend ATM switch has been properly configured, follow the procedure below to set up an SPVC connection.

1. Configure the trunk at Endpoint A. (This is done at the unit level so it usually only needs to be done once.)
2. Set up the local end (Endpoint A) of the connection as an SPVC Orig dial type, specifying the ATM address of the remote Ascend switch and the VPI/VCI to use from the Ascend switch out to the UNI (next hop).
3. Set up the PVC at the destination unit.

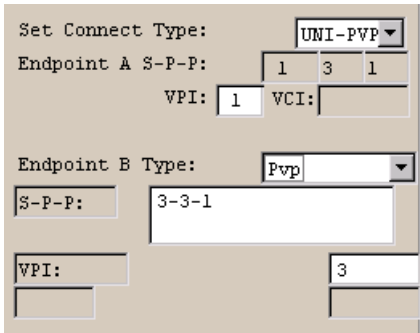
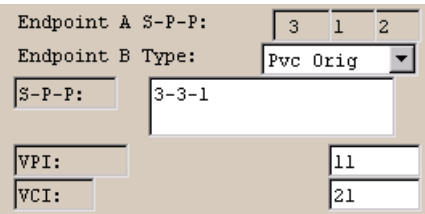
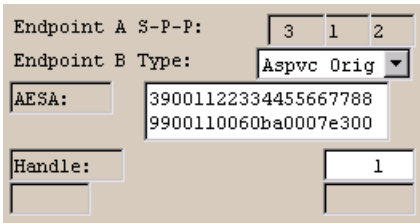
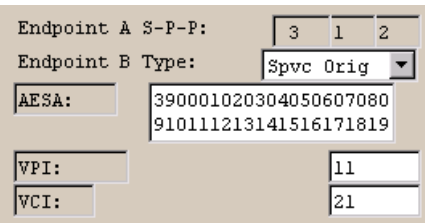
See **“Example 5: SPVC”** on page 5-31 for a step-by-step example of configuring an SPVC connection.

From this point on, whenever the connection status is set to UP, a call setup request is passed through the network establishing a connection between the SA unit and the Ascend ATM switch. The connections between the two are switched; the connection from the Ascend ATM switch to the final destination is set up by the Ascend ATM switch as a PVC using the specified VPI/VCI.

## Dial-Type Addressing Formats Summary

As described in the previous section, SA units may use a variety of dial types to establish connections. Each dial type uses a different addressing convention. [Table 5-2](#) summarizes the various addressing conventions and shows how to use each one when establishing a new connection or interworking function.

**Table 5-2. Dial-Type Addressing Formats**

Type	Addressing Format Example	Comments
PVP		<p>Connection based on Endpoint B Slot-POD-Port, VPI.</p> <p>PVPs are only used to connect one UNI PVP to another UNI PVP.</p> <p>PVP Ranges must be enabled before any PVPs may be established. See <a href="#">“Configuring Port-level CAC” on page 4-43</a>.</p>
PVC Orig		<p>Connection based on Endpoint B Slot-POD-Port, VPI/VCI.</p> <p>The PVC dial type is used to connect one UNI PVC to another UNI PVC or to connect a non-ATM (adaptation service) interworking function to an ATM PVC connection.</p>
ASPVC		<p>Connection based on Endpoint B AESA and Handle.</p> <p>The ASPVC Term side should be set up first to obtain the target AESA and Handle.</p> <p>Complete the ASPVC Orig side addressing as shown, using the AESA and Handle obtained from the ASPVC Term side.</p> <p>Signalling must be enabled on both SA units.</p>
SPVC		<p>Connection based on Endpoint B AESA and VPI/VCI.</p> <p>Signalling must be enabled on both SA units.</p> <p>The Endpoint B AESA must correspond to an Ascend CBX 500 or GX 550 ATM switch. The switch's ATM address is used to establish the switched connection from the SA unit to the CBX 500/GX 550, and a specified VPI/VCI is used to reach the next hop beyond the switch.</p>

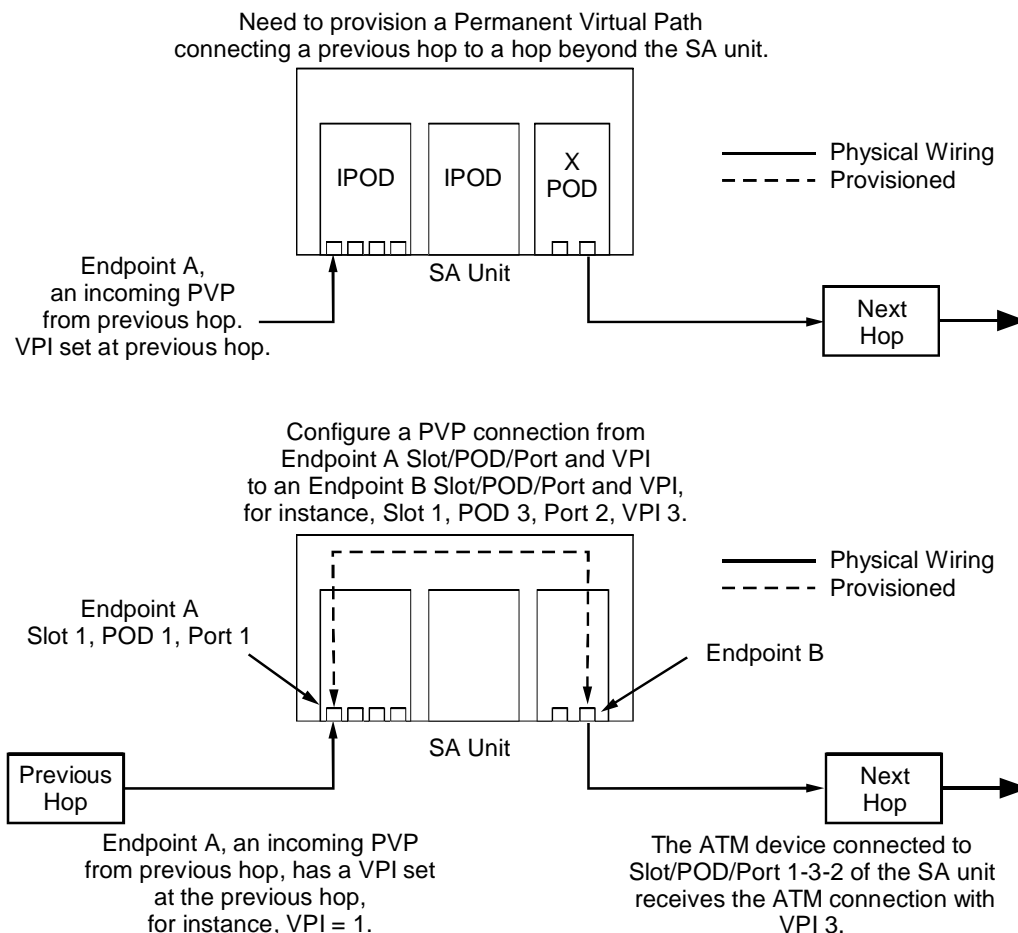
## Connection Setup Examples

This section provides several examples of how connections with different dial types are set up using WebXtend. The examples assume that the port configuration discussed in Chapter 4 has been completed correctly and that any necessary physical connections between the SA units and/or the ATM network have been made.

These examples are intended as a brief overview of setting up various dial-type connections. They are not intended to serve as a complete tutorial. It is expected that you will use the rest of Chapter 5 to guide you in the setup of connections required by your system, and in completing the fields specific to each connection type and interworking function.

### Example 1: PVP

You have an SA unit with an ATM port connected from the previous hop, and another ATM cell port connected to the next hop. Suppose that you wish to establish a permanent virtual path between two SA units, as shown in [Figure 5-13](#).



**Figure 5-13. PVP Connection Required**

To establish this connection, log in to the SA unit, select Service Management > ATM UNI, then select the Endpoint A Slot/POD/Port. At the ATM UNI Connections dialog, select Add Connection, then complete the Add ATM UNI Connection dialog box, as shown below in [Figure 5-14](#).



By default, PVPs are disabled on SA units. This is because most applications call for PVCs rather than PVPs. Disabling PVPs makes the maximum number of VPI values available for use by PVCs. To use PVPs, you must enable VP ranges, then assign a range of VPI values for use by PVPs. VPI values in this range are unavailable for use by PVCs. See [“Configuring Port-level CAC”](#) on page 4-43 for more details.

1. Set the Endpoint A Type of “UNI-PVP” and enter the VPI for this connection.
2. Set the Endpoint B Type to “PVP” and enter the Endpoint B Slot/POD/Port as shown, with the slot, POD, and port separated with dashes.
3. Enter the Endpoint B Virtual Path Identifier.
4. Make sure Connection Management is set to “Up”
5. Make sure the correct Service Definition and Rate are selected. If you enter a User Defined Rate, make sure it is in Bits per Second.
6. Select OK to accept the connection.

**Figure 5-14. PVP Connection Setup Procedure**

The resulting PVP is shown in the Configured Connections field in the Configure ATM UNI Connection dialog box, as shown in [Figure 5-15](#).



The screenshot shows the 'ATM UNI Connections' window. The 'Port Detail' section displays the following information:

Slot-Pod-Port:	5 3 1	Total Connections:	0
Port Name:	DS3 PORT NAME	Port Type:	Ds3
ADMIN Status:	Up	Port ID:	DS3 CIRCUIT I
		OPS Status:	Up

Below the 'Port Detail' section are three buttons: 'Phy Port Stats...', 'ATM Port Stats...', and 'CAC Port Stats...'. The 'Configured ATM UNI Connections' section contains a table with the following data:

Name	Svc	Dial Type	Connect Status	Connect Detail
Connection 1	UNI	Pvp	Up	Ok

At the bottom of the window are four buttons: 'Add Connection...', 'Connection Summary...', 'Connection Stats...', and 'Cancel'. A warning message at the very bottom reads: 'Warning: AppletWindow'.

**Figure 5-15. PVP Connection Setup Results**

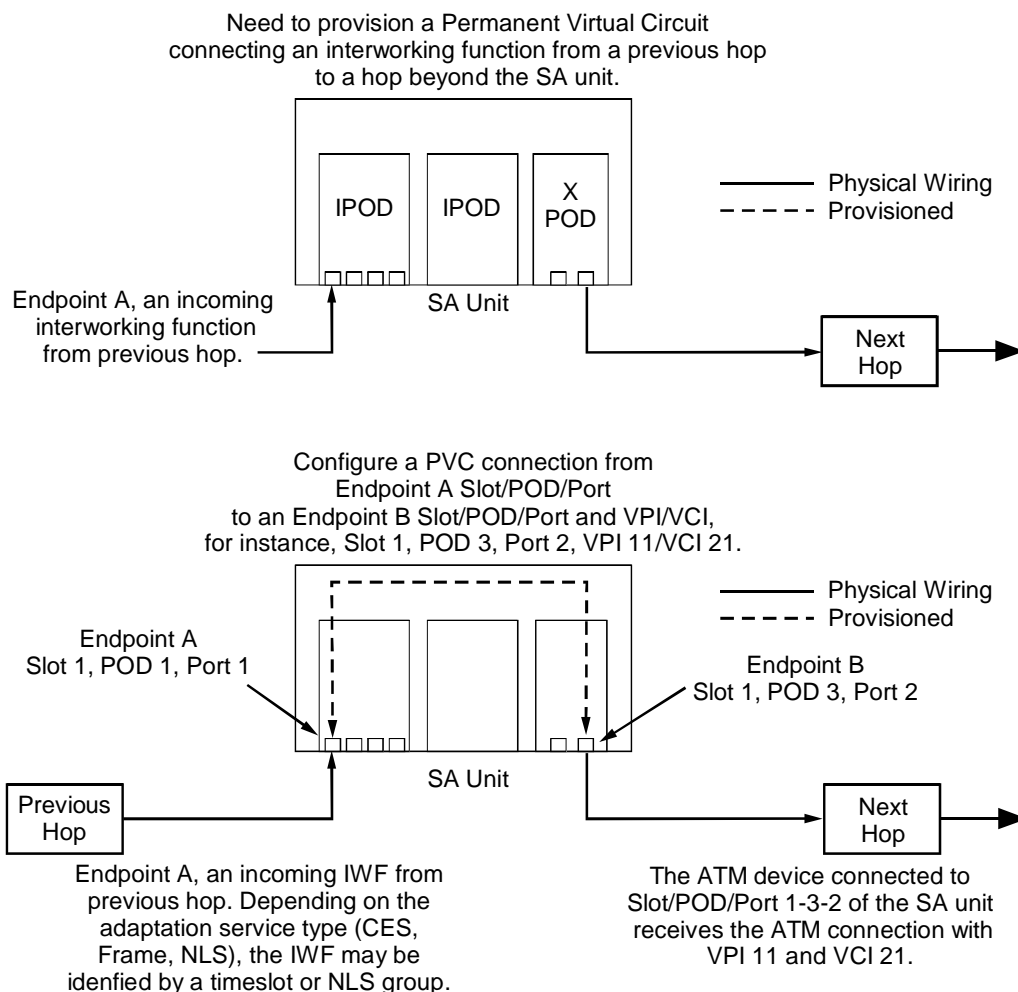
The connection will be reflected (“mirrored”) at the ATM UNI Connections window for Endpoint B as well.



When viewing a connection from the trunk side, the endpoints will appear to be reversed. Because connections are always bi-directional, WebXtend presents whichever end of a connection you are presently viewing as Endpoint A.

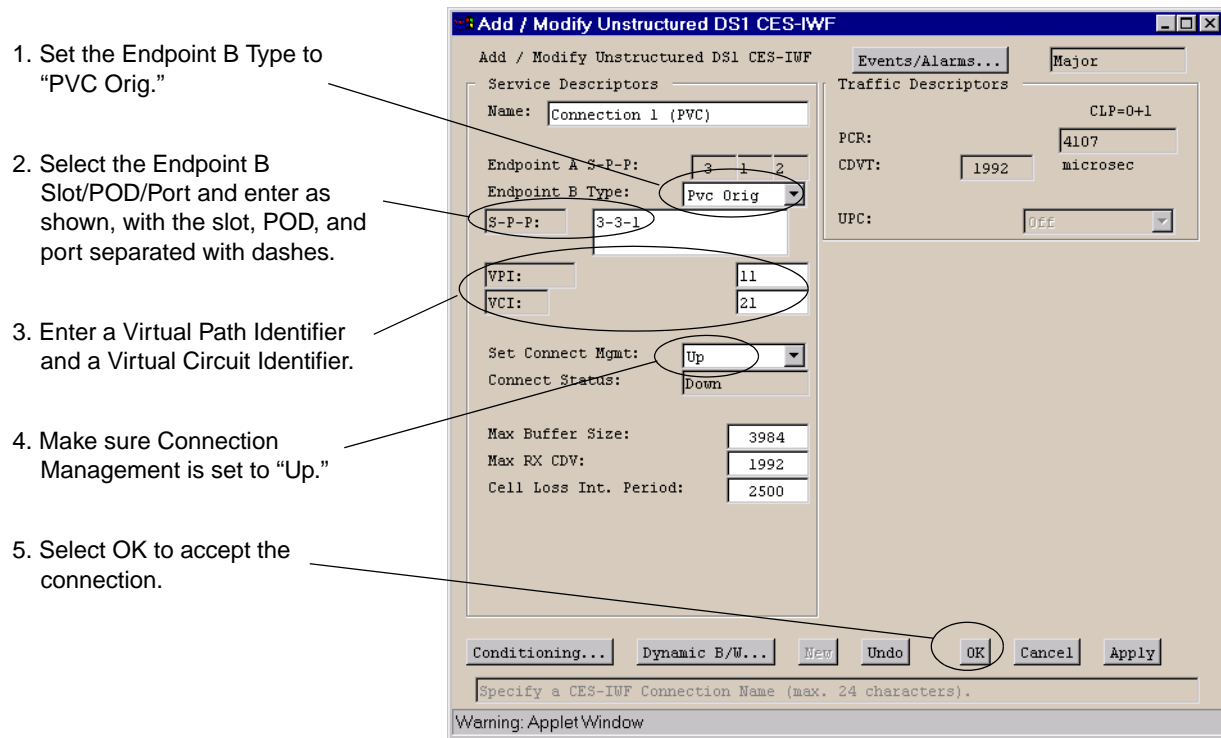
## Example 2: PVC (CES to ATM)

Permanent Virtual Circuits are a more discrete connection unit than Permanent Virtual Paths (a PVP actually consists of groups of PVCs), but the provisioning procedure is nearly identical. Also, a PVC may be an interworking function, meshing a non-ATM service to an ATM-UNI connection. Suppose that you have an interworking function (in this case a DS1 timeslot) that you wish to interwork to a permanent virtual circuit to the next hop device, as shown in [Figure 5-16](#).



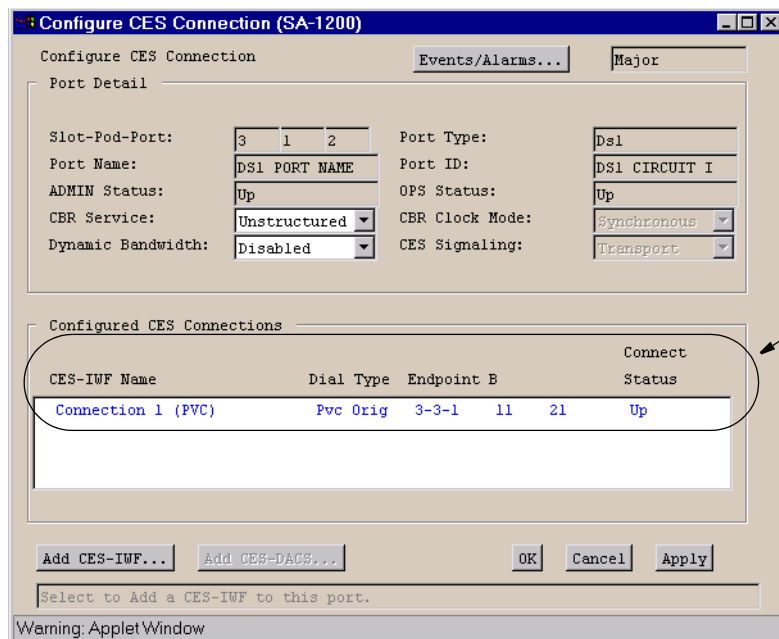
**Figure 5-16. IWF/PVC Connection Required**

To establish this connection, log in to the SA unit and select Service Management > Circuit Emulation Service. Select the Endpoint A port, and at the Configure CES Connections window, select the Add CES-IWF button. Finally, complete the Add CES-IWF dialog box, as shown below in [Figure 5-17](#).



**Figure 5-17. PVC Connection Setup Procedure**

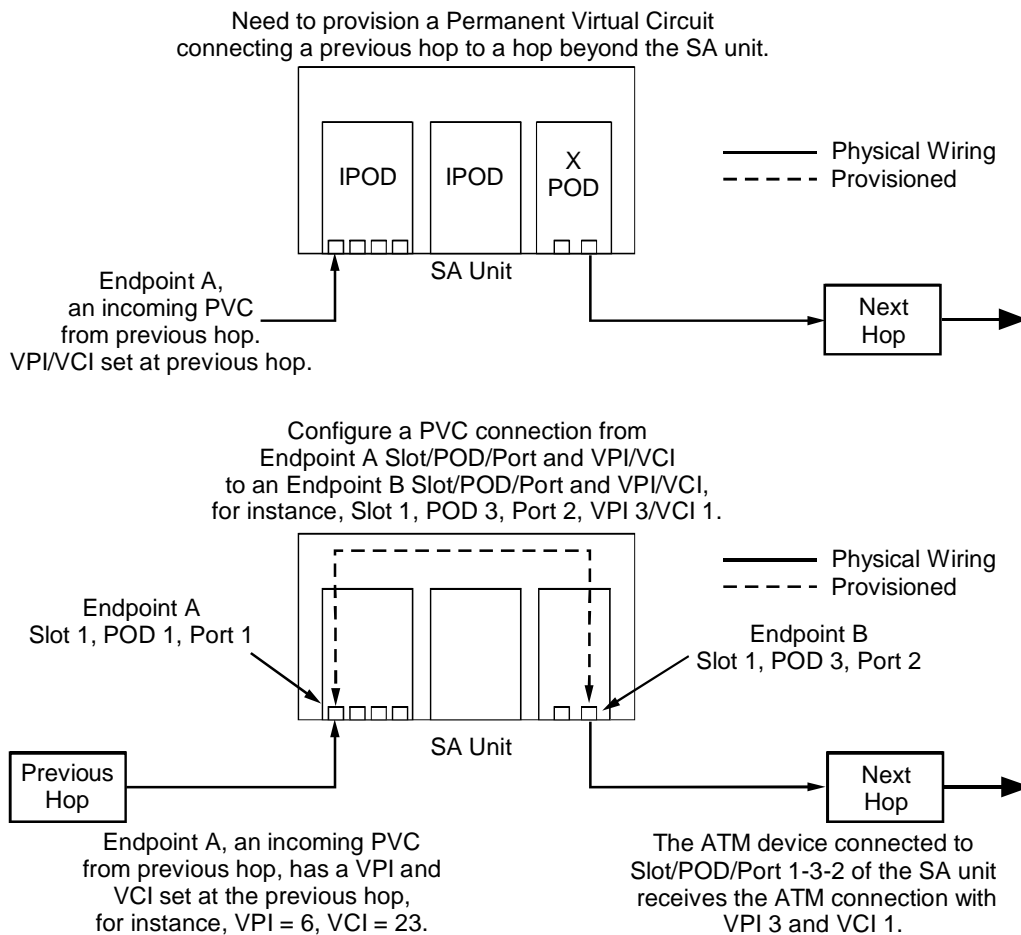
The resulting CES-IWF is shown in the Configured Connections field in the Configure CES-IWF dialog box, as shown in [Figure 5-18](#).



**Figure 5-18. PVC Connection Setup Results**

### Example 3: PVC (ATM to ATM)

Permanent Virtual Circuits being established between two ATM ports require slightly different configuration than an IWF connection being established as shown in Example 2. Suppose that you wish to establish a permanent virtual circuit between an ATM-UNI PVC at one SA unit and another ATM-UNI port at a second SA unit, as shown in **Figure 5-19**.



**Figure 5-19. ATM-UNI PVC Connection Required**

To establish this connection, log in to the SA unit. Select Service Management > ATM UNI, then select the Endpoint A port from the list of ATM UNI ports. At the ATM UNI Connections window, select the Add Connection button. Finally, complete the Add ATM-UNI Connection dialog box, as shown below in **Figure 5-20**.

1. Set the Connect Type to "UNI-PVC."
2. Endpoint A is the currently selected Slot/POD/Port. Enter the VPI and VCI for the incoming connection.
3. Set the Endpoint B type to PVC Orig and enter the Endpoint B S-P-P and VPI/VCI.
4. Make sure Connection Management is set to "Up."
5. Make sure the correct Service Definition and Rate are selected. If you enter a User Defined Rate, make sure it is in Bits per Second.
6. Select OK to accept the connection.

**Figure 5-20. ATM-UNI PVC Connection Setup Procedure**

The resulting ATM-UNI Connection is shown in the Configured Connections field in the ATM UNI Connections dialog box, as shown in [Figure 5-21](#).

**Figure 5-21. ATM-UNI PVC Connection Setup Results**

### Example 4: A-SPVC

Suppose that you wish to establish a connection from one CES interworking function at a local SA unit to a CES-IWF at a remote SA unit across an ATM network. You would like to take advantage of the switching capabilities of the network rather than provision each hop manually. The A-SPVC satisfies this requirement.

To set up a CES-IWF between two SA units using an A-SPVC:

1. Choose one SA unit to be the Terminating unit (called party) and one SA unit to be the Originating unit (calling party).
2. Log in to the Terminating unit, and at the main menu, select Administration > ASPVC Address, displaying the Configure ASPVC Address dialog box.

1. If the Net Prefix box is empty, enter a 13-byte hex Net Prefix, then click Apply.
2. The unit will append its ESI to the Net Prefix and display the results in the Primary AESA. Copy the AESA for use later when configuring the Orig side of the A-SPVC.
3. Check the Primary Trunk - make sure the correct Slot/POD/Port are shown.
4. Select OK to accept the connection.

ASPVC Address Configuration

Config ESI: 0060ba0007fa Default ESI: 0060ba0007fa

Net Prefix:

Primary AESA:

Primary Trunk: 1 | 3 | 1 Auto-Prefix: Yes

OK Cancel Apply

Java Applet Window

**Figure 5-22. A-SPVC Remote-side Connection Setup – ASPVC Address Configuration**

- a. If the Net Prefix has not been configured, enter a 13-byte hexadecimal Net Prefix now. Click Apply to append the ESI to the Net Prefix and create the complete AESA.
  - b. Check the Primary Trunk. By default, its Slot/POD/Port should be 1-3-1.
  - c. Choose OK to close the Configure ASPVC Address dialog box. Close the Administration dialog box.
3. From the main menu, select Interface Management, and drill down to the Primary Trunk port. From the port level, select the Configure Path button, then at the Configure Path window, select Next Logical Layer to reach the Configure ATM Interface screen.

1. Select a UNI signalling variant. The same Type must be selected for both ends of the connection.

2. Designate this side of the UNI as User or Network. (See the network considerations below for more details.)

3. Select OK to accept the changes.

**Figure 5-23. A-SPVC Remote-side Connection Setup – SAP Configuration**

- a. In the SAP Configuration field, set the Type to your desired ATM Forum UNI variant. Both sides of the connection must be set to the same UNI variant.
- b. In the SAP Configuration field, set the Side of the ATM connection for this SA unit according to the network considerations below:

**If the SA units are connected back-to-back:** If the two SA units are connected directly to each other via their trunk PODs (a back-to-back configuration), one unit **MUST** be set to User and the other unit **MUST** be set to Network. While it doesn't make a difference which is User and which is Network, they must be set to opposite values. The ATM User-Network Interface relationship requires a User-side and a Network-side to function correctly.

**If the SA units are connected across an ATM switch or a network of ATM switches:** Set the Type variable on both units to User, as the ATM switch should be considered the Network side of the UNI.

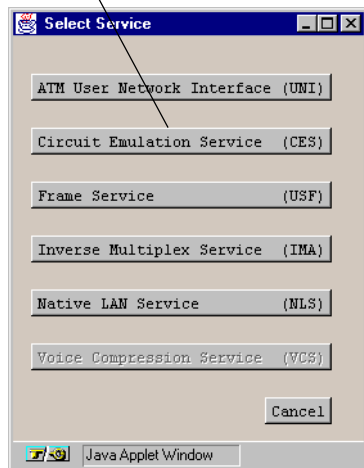


*Tip:* After you select the UNI variant and side and click OK, you'll see the TX LED on the trunk POD begin to flash. The RX LED on the trunk POD of the opposite SA unit will also begin to flash as the units seek to connect.

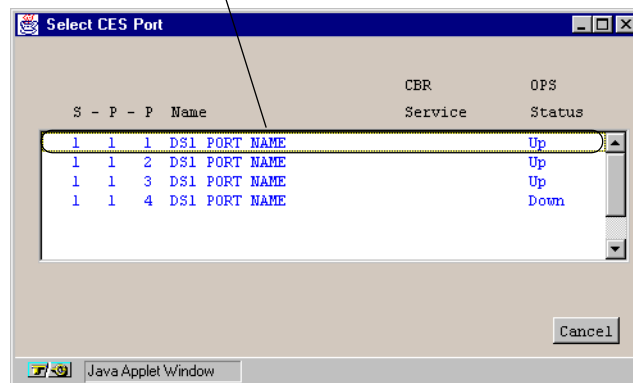
- c. Choose OK to close the Configure ATM Interface window. Close any other open windows and return to the main menu.

4. At the main menu, select Service Management > Circuit Emulation Service to open the Select CES Port window, displaying the CES ports in your SA unit. Select the CES port you wish to establish the interworking function on.

1. Select Service Emulation Service...



2. Select the desired port for the CES-IWF.



**Figure 5-24. A-SPVC Remote-side Connection Setup – Selecting the CES Port**

5. At the Configure CES Connection window, make any desired selections in the Port Detail frame (such as Structured/Unstructured, DBA Enabled, etc.), then select Add CES-IWF to open the Add/Modify DS1 CES-IWF window.



6. Configure the CES-IWF as shown below, then select OK to accept the connection.

1. Set the Endpoint B Type to "A-SPVC Term."

Tip: After you select OK or Apply, this SA unit's ATM address (in this case, a 40-digit AESA) is displayed, and a unique handle is assigned corresponding to this slot/POD/port and interworking function. You'll need these numbers to configure the originating end of the connection.

2. Make sure Connection Management is set to "Up"

3. Select OK to accept the interworking function.

Service Descriptors

Name: Connection 1 (Remote)

Endpoint A S-P-P: 3 1 2

Endpoint B Type: Aspvc Term

AESA: 390011223344556677889900110060ba0007e300

Handle: 1

Set Connect Mgmt: Up

Connect Status: Down

Traffic Descriptors

CLP=0+1: 4107

CDVT: 1992

UPC: Off

Max Buffer Size: 3984

Max RX CDV: 1992

Cell Loss Int. Period: 2500

Conditioning... Dynamic B/W... New Undo OK Cancel Apply

Select to specify the status of this connection.

Warning: Applet Window

**Figure 5-25. A-SPVC Remote-side Connection Setup – Interworking function**

7. At the Configure CES-IWF window, you'll see the connection listed in the Configured CES-IWF Connections field. Select it to open the Connection Options window. Make note of the Handle assigned to this CES-IWF; you'll need it shortly to configure the Originating side of the ASPVC. Also, select and copy the AESA; you'll be able to paste it into the Endpoint B field when configuring the Originating side.

This completes the configuration of the remote half (Terminating side) of the connection. The CES-IWF will sit idle until the SA unit receives a call setup request from an A-SPVC Orig asking for a connection to this handle number.

Setting up the local half of the connection completes the equation by creating an entity to place this call setup request. Configure the Originating half of the connection as follows:

1. Log in to the Originating unit, and at the main menu, select Administration > ASPVC Address, displaying the Configure ASPVC Address dialog box.

1. If the Net Prefix box is empty, enter a 13-byte hex Net Prefix, then click Apply.

2. The unit will append its ESI to the Net Prefix and display the results in the Primary AESA.

3. Check the Primary Trunk - make sure the correct Slot/POD/Port are shown.

4. Select OK to accept the connection.

ASPVC Address Configuration

Config ESI: 0060ba0007fa Default ESI: 0060ba0007fa

Net Prefix:

Primary AESA:

Primary Trunk: 1 3 1 Auto-Prefix: Yes

OK Cancel Apply

Java Applet Window

**Figure 5-26. A-SPVC Originating-side Connection Setup – ASPVC Address Configuration**

- a. If the Net Prefix has not been configured, enter a 13-byte hexadecimal Net Prefix now. Click Apply to append the ESI to the Net Prefix and create the complete AESA.
- b. Check the Primary Trunk. By default, its Slot/POD/Port should be 1-3-1.
- c. Choose OK to close the Configure ASPVC Address dialog box. Close the Administration dialog box.

2. From the main menu, select Interface Management, and drill down to the Primary Trunk port. From the port level, select the Configure Path button, then at the Configure Path window, select Next Logical Layer to reach the Configure ATM Interface screen.

1. Select a UNI signalling variant. The same Type must be selected for both ends of the connection.
2. Designate this side of the UNI as User or Network. (See the network considerations below for more details.)
3. Select OK to accept the changes.

Figure 5-27. A-SPVC Originating-side Connection Setup – SAP Configuration

- a. In the SAP Configuration field, set the Type to your desired ATM Forum UNI variant. This must match the Type set at the Term side, as both sides of the connection must be set to the same UNI variant.
- b. In the SAP Configuration field, set the Side of the ATM connection for this SA unit according to the network considerations below:

**If the SA units are connected back-to-back:** If the two SA units are connected directly to each other via their trunk PODs (a back-to-back configuration), one unit **MUST** be set to User and the other unit **MUST** be set to Network. Set the Orig unit to the opposite Side of the UNI that you configured the Term side with.

**If the SA units are connected across an ATM switch or a network of ATM switches:** Set the Type variable on both units to User, as the ATM switch should be considered the Network side of the UNI.



*Tip:* After you select the UNI variant and side and click OK, you'll see the TX and RX LEDs on the trunk POD both SA units flashing.

- c. Choose OK to close the Configure ATM Interface window. Close any other open windows and return to the main menu.
3. At the main menu, select Service Management > Circuit Emulation Service to open the Select CES Port window, displaying the CES ports in your SA unit. Select the CES port you wish to establish the interworking function on.
4. At the Configure CES Connection window, make any desired selections in the Port Detail frame (such as Structured/Unstructured, DBA Enabled, etc.), then select Add CES-IWF to open the Add/Modify DS1 CES-IWF window.
5. Configure the CES-IWF as shown below, then select OK to accept the connection.

1. Set the Endpoint B Type to "A-SPVC Orig."
2. Enter the Endpoint B ATM address (in this case, an AESA), and the handle assigned at the remote SA unit.  
*Tip: Since you copied the AESA from the Term unit, paste it in here to avoid mistakes typing out 40 digits.*
3. Make sure Connection Management is set to "Up."
4. Select OK to accept the connection.

The screenshot shows the 'Add / Modify Unstructured DS1 CES-IWF (SA-600)' dialog box. The 'Service Descriptors' tab is selected. The 'Name' field is 'Connection 1 (Local)'. The 'Endpoint A S-P-P' field shows '3 1 2'. The 'Endpoint B Type' dropdown is set to 'Aspvc Orig'. The 'AESA' field contains a 40-digit hexadecimal string: '39001122334455667788 9900110060ba0007e300'. The 'Handle' field is '1'. The 'Set Connect Mgmt' dropdown is set to 'Up'. The 'Connect Status' dropdown is set to 'Down'. The 'Max Buffer Size' is '3984', 'Max RX CDV' is '1992', and 'Cell Loss Int. Period' is '2500'. The 'Traffic Descriptors' tab shows 'Events/Alarms...' set to 'Critical', 'CLP=0+1', 'PCR' set to '4107', 'CDVT' set to '1992 microsec', and 'UPC' set to 'OFF'. At the bottom are buttons for 'Conditioning...', 'Dynamic B/W...', 'New', 'Undo', 'OK', 'Cancel', and 'Apply'. A status bar at the bottom says 'Warning: AppletWindow'.

**Figure 5-28. A-SPVC Originating-side Connection Setup – Interworking function**

When both the originating and terminating sides of the connection are configured and their connection management status is Up, the connection is active and data may pass.

The resulting connection is displayed in the Configured CES Connection field of the Configure CES Connections dialog box.



It is important to remember that if the Terminating side of the A-SPVC is deleted, its handle is also deleted. If the Term-side interworking function is then re-configured, a new and different handle will be assigned, rendering the Originating side handle invalid, and the connection will not function. Modifying the CES-IWF to correspond with the new handle will restore the connection.

### **Example 5: SPVC**

In this example, the requirement is to establish an NLS tunnel from a local SA unit to a remote third-party ATM device across an ATM network consisting of Ascend GX 550 ATM switches. You would like to take advantage of the switching capabilities of the network rather than provision each hop manually. The SPVC satisfies this requirement. The GX 550 ATM switch is capable of establishing a connection based on an SPVC connection request from an SA unit; unlike an A-SPVC, no remote (terminating) setup is required.



Prior to setting up an SPVC connection, make sure the SA unit's primary trunk has been properly configured as described in Example 4 on [page 5-28](#).

To set up an NLS tunnel across the ATM cloud using an SPVC:

1. Log in to the SA unit, and at the main menu, select Service Management > Native LAN Service. Select the desired ICM from the Select Board window.
2. At the NLS Groups window, do one of the following:
  - a. Select an existing NLS group from the Configured NLS Groups field, or
  - b. Create a new group, then select it from the Configured NLS Groups field.
3. At the NLS Group Options screen, select Tunnels to display the Native LAN Service Tunnels window.
4. Select Add Tunnel to display the Add/Modify NLS Tunnel window. Configure the tunnel as shown below:

1. Set the Endpoint B Type to "SPVC Orig."
2. Enter the Endpoint B ATM address (in this case, an AESA, the address of the GX 550 port connected to our desired next hop).
3. Enter the VPI and VCI to be used by the remote ATM switch to route the connection to its next hop.
4. Set the Connection Management to "Up."
5. Make sure the correct Service Definition and Rate are selected. If you enter a User Defined Rate, make sure it is in Bits per Second.
6. Select OK to accept the connection.

Warning: Applet Window

**Figure 5-29. SPVC Remote-side Connection Setup**

When the connection status is set to Up, a call setup request will be placed to the remote Ascend GX 550 switch to establish a PVC on the switch port associated with the AESA and using the provided VPI/VCI.

The next hop ATM device will need to be provisioned to accept this connection on its VPI/VCI.

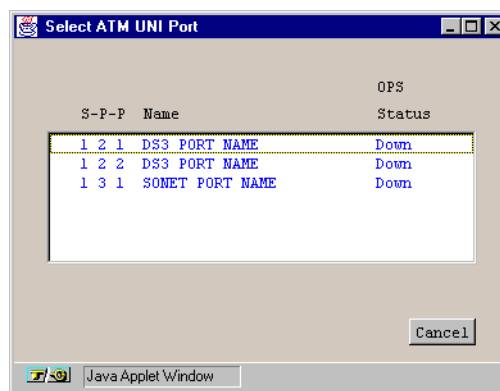
The resulting connection is displayed in the Configured NLS Tunnels field of the Configure NLS Tunnels dialog box.

## Configuring ATM UNI Services and Connections

To configure ATM User Network Interface (UNI) services on a particular port, you must access the port's Connections window from either the Main menu via the Service Management button, or from the port's Configure ATM Interface window.

*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears (Figure 5-1 on page 5-2).
2. Choose the ATM User Network Interface (UNI) button. The Select ATM UNI Port window appears (see Figure 5-30).



**Figure 5-30. Select ATM UNI Port Window**

3. Select the port you want to configure. The ATM UNI Connections window appears (see Figure 5-31).

*From the Configure ATM Interface window:*

4. After you configure the ATM interface of a DS1/E1, DS3/E3 Cell or OC-3c/STM-1 Cell port, as described in “Configuring the ATM Interface” on page 4-46, choose the Service Management button. The ATM UNI Connections window appears (see Figure 5-31).

The screenshot shows the 'ATM UNI Connections (SA-600)' window. It has a title bar with standard window controls. Inside, there's a tabbed interface with 'ATM UNI Connections' selected. To the right of the tabs are 'Events/Alarms...' and 'Major' buttons. The 'Port Detail' section contains fields for 'Slot-Pod-Port' (1 3 1), 'Port Name' (SONET PORT NA), 'ADMIN Status' (Up), 'Total Connections' (6), 'Port Type' (SonetLinePlus), 'Port ID' (SONET LINE CI), and 'OPS Status' (Up). Below these are three buttons: 'Phy Port Stats...', 'ATM Port Stats...', and 'CAC Port Stats...'. The 'Configured ATM UNI Connections' section features a table with columns: Name, Svc Dial Type, Connect Status, and Connect Detail. The table lists six connections, all with 'Up' status and 'Ok' detail. At the bottom are buttons for 'Add Connection...', 'Connection Summary...', 'Connection Stats...', and 'Cancel'. A footer note says 'Use Up/Down arrows or mouse to scroll; select row for more options.' The window title bar at the bottom reads 'Unsigned Java AppletWindow'.

Name	Svc Dial Type	Connect Status	Connect Detail
ATM UNI Conn 1	UNI Pvc Orig	Up	Ok
NLS Tunnel 1	NLS Pvc Orig	Up	Ok
CES Conn 1	CES Pvc Orig	Up	Ok
CES Conn 2	CES Pvc Orig	Up	Ok
CES Conn 3	CES Pvc Orig	Up	Ok
CES Conn 4	CES Pvc Orig	Up	Ok

**Figure 5-31. ATM UNI Connections Window**

5. Complete the fields described in [Table 5-3](#) to add, modify, make, or break an ATM UNI service connection.



**Table 5-3. ATM UNI Connections Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Total Connections	read-only	Displays the number of defined connections on the port.
Slot-POD-Port	read-only	Displays the slot, POD, and port number.
Port Type	read-only	Displays the type of port.
Port Name	read-only	Displays the port name (32 characters max).
Port ID	read-only	Displays the port ID (32 characters max).
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
Phy Port Stats	window button	Enables you to view the physical port statistics.
ATM Port Stats	window button	Enables you to view the ATM port statistics.
CAC Port Stats	window button	Enables you to view the Connection Admission Control (CAC) port statistics.
<b>Configured ATM UNI Connections</b>		
Name	read-only	Displays the user designation of each configured connection on this port.
Svc	read-only	Displays the service type for Endpoint A of the connection: NLS, CES, FFS, UNI, or VCS.
Dial Type	read-only	Displays the dial type configured for each configured VCS interworking function on this port: PVC Orig, PVP, ASPVC Term, ASPVC Orig, or SPVC Orig.
Connect Status	read-only	Displays the connection state of each configured connection on this port: Up or Down.

**Table 5-3. ATM UNI Connections Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Connect Detail	read-only	<p>Displays error codes if any failure is present on this interworking function. Possible error conditions include:</p> <p><i>VpvcUsed</i> - "Port / VPI / VCI" of either source or destination is already used.</p> <p><i>vpi-OOR</i> - VPI of either the source or destination is out of range.</p> <p><i>vci-OOR</i> - VCI of either the source or destination is out of range.</p> <p><i>vpi-Rsvd</i> - PVCs source or destination VPI within range reserved for PVPs.</p> <p><i>rate-OOR</i> - PCR/SCR in traffic descriptor out of range. Depending on service category: PCR is less than SCR, rate descriptor is non-0 when it should be 0, or rate is 0 when it should be non-0.</p> <p><i>desc-OOR</i> - Traffic Descriptor out of range. One or more of these descriptors is not in the list of MIB enumerations: Service Category, Congestion Action, or Buffer Size.</p> <p><i>port-bad</i> - The power-on self-test results have disabled this port.</p>
<b>(Other Buttons)</b>		
Add Connection	window button	Enables you to add an ATM UNI connection. See <b>"Adding a Connection"</b> on page 5-38.
Connection Summary	window button	<p>(This feature not currently supported.)</p> <p>Enables you to view a summary of the configuration data related to all the connections on this port (see <b>"Viewing Connection Statistics via the Connections Summary Window"</b> on page 6-95).</p>
Connection Stats	window button	<p>(This feature not currently supported.)</p> <p>Enables you to view connection statistics for all the connections on this port (see <b>"Viewing Connection Statistics via the Connections Statistics Window"</b> on page 6-96).</p>

## Configuring ATM UNI Connections

This section describes how to:

- Add an ATM UNI service connection (see [page 5-38](#))
- Modify an ATM UNI service connection (see [page 5-44](#))
- Enable or Disable an ATM UNI service connection (see [page 5-44](#))
- Delete an ATM UNI service connection (see [page 5-45](#))

## Adding a Connection

To add and configure a connection:

1. Choose the Add Connection button from the ATM UNI Connections window (Figure 5-31 on page 5-34). The Add/Modify ATM UNI Connection window appears (see Figure 5-32).

**Figure 5-32. Add/Modify ATM UNI Connection Window**

2. Complete the fields described in Table 5-4 to select the parameters for the new connection.
3. When you are finished defining this connection, choose OK.

**Table 5-4. Add/Modify ATM UNI Connection Fields**

Field/Button	Type	Action/Description
<b>Service Descriptors</b>		
UNI Connection Name	read/write	Specify a name for this connection.
Set Connect Type	read/write	Select the Endpoint A type of ATM UNI connection: PVC or PVP.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port number) of endpoint A of the connection.
Endpoint A VPI	read/write	Specify the virtual path identifier of endpoint A for this connection.
Endpoint A VCI	read/write	Specify the virtual channel identifier of endpoint A for this connection.
Endpoint B Type	read/write	<p>Select the dial type for Endpoint B of this connection:</p> <p><i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.</p> <p><i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI.</p> <p><i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.</p> <p><i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.</p> <p><i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.</p>
(Address field) S-P-P or AESA	read/write	Specify Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual channel identifier of endpoint B for this connection.

**Table 5-4. Add/Modify ATM UNI Connection Fields (Continued)**

Field/Button	Type	Action/Description
Handle (ASPVC Term and ASPVC Orig dial types only)	read/write or read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only). For ASPVC Orig dial type, specify the handle being called (read/write).
Set Connect Mgmt	read/write	Specify the administrative state of the connection (up or down). <i>up</i> (default) – Activates the connection. <i>down</i> – Deactivates the connection.
Connect Status	read-only	Displays the operational state of the connection: Up or Down.
Service Definition	read/write	Select the type of service for this connection:  <i>CBR-1</i> (default) – Selects constant bit rate service for handling digital information, such as video and digitized voice and is represented by a continuous stream of bits. Constant bit rate service requires guaranteed throughput rates and service levels.  <i>RT-VBR1</i> – Selects real time variable bit rate 1 service for packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.  <i>RT-VBR2</i> – Selects real time variable bit rate 2 service.  <i>RT-VBR3</i> – Selects real time variable bit rate 3 service.  <i>NRT-VBR1</i> – Selects non-real time variable bit rate 1 service for packaging the transfer of long, bursty data streams over a pre-established ATM connection. Selectsservice is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of non-real time VBR.  <i>NRT-VBR2</i> – Selects non-real time variable bit rate 2 service.  <i>NRT-VBR3</i> – Selects non-real time variable bit rate 3 service.  <i>UBR1</i> – Selects unspecified bit rate 1 service for LAN traffic applications primarily. The CPE should compensate for any delay or lost cell traffic.  <i>UBR2</i> – Selects unspecified bit rate 2 service.

**Table 5-4. Add/Modify ATM UNI Connection Fields (Continued)**

Field/Button	Type	Action/Description
Service Rate	read/write	Specify the connection data rate: <i>Rate 64KB</i> (default) – Selects a service rate of 64 Kbps. <i>Rate 384KB</i> – Selects a service rate of 384 Kbps. <i>Rate 1536KB</i> – Selects a service rate of 1536 Kbps/1.536 Mbps. <i>Rate 1MB</i> – Selects a service rate of 1 Mbps. <i>Rate 2MB</i> – Selects a service rate of 2 Mbps. <i>Rate 5MB</i> – Selects a service rate of 5 Mbps. <i>Rate 10MB</i> – Selects a service rate of 10 Mbps. <i>Rate 40MB</i> – Selects a service rate of 40 Mbps. <i>Rate 50MB</i> – Selects a service rate of 50 Mbps. <i>Rate 100MB</i> – Selects a service rate of 100 Mbps. <i>Rate 150MB</i> – Selects a service rate of 150 Mbps. <i>User Defined</i> – Selects a user-defined service rate, and makes available the User Defined Rate field.
User Defined Rate (available only if User Defined is selected in the Service Rate field)	read/write	Specify a service rate in bits per second.
<b>Traffic Descriptors (Forward or Reverse)</b> <b>note: if traffic descriptors are changed, Service Rate field changes to User Defined.</b>		
PCR (CLP=0)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0.
SCR (CLP=0)	read/write	Specify the forward/reverse sustainable cell rate, where the cell loss priority is 0.
MCR (CLP=0)		Not supported.
MBS (CLP=0)	read/write	Specify the forward/reverse maximum burst size, where the cell loss priority is 0.
PCR (CLP=0+1)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0+1.
SCR (CLP=0+1)	read/write	Specify the forward/reverse sustainable cell rate, where the cell loss priority is 0+1.
MCR (CLP=0+1)		Not supported.

**Table 5-4. Add/Modify ATM UNI Connection Fields (Continued)**

Field/Button	Type	Action/Description
MBS (CLP=0+1)	read/write	Specify the forward/reverse maximum burst size, where the cell loss priority is 0+1.
CDVT (microsec)	read/write	Specify the forward/reverse cell delay variation tolerance in microseconds for this connection.
<b>Traffic Descriptors (Forward and Reverse)</b>		
Tagging	read-only	Displays the method of changing a high-priority cell to a low-priority cell for this connection.
UPC	read/write	Specify whether usage parameter control is enabled or disabled on this connection.
<b>Congestion Control</b>		
Strategy	read/write	<p>Specify the type of congestion control on this connection:</p> <p><i>None</i> (default) – Selects no strategy for handling congestion.</p> <p><i>SetEFCI</i> – Uses the explicit forward congestion indicator to determine if congestion (or impending congestion) exists in a node. When selected, the congested node modifies the EFCI bit in the ATM cell header to indicate congestion.</p> <p>If the equipment connected to the SA unit can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve the congestion. EFCI is only set in the UBR queue and affects all connections in the queue of the physical port, therefore, do not select this option if you do not want to use the EFCI strategy on this physical port.</p> <p><i>EarlyPacketDi</i> (Early Packet Discard) – Drops a whole packet to relieve congestion under AAL5 adaptation.</p> <p><i>DropCLP1</i> – Drops low-priority cells (CLP=1) to relieve congestion.</p>



**Table 5-4. Add/Modify ATM UNI Connection Fields (Continued)**

Field/Button	Type	Action/Description
Buffer Size	read/write	Specify the buffer size allocated for controlling congestion on this connection:  <i>Shallow</i> (default) – Provides the smallest buffer for handling congestion on this connection.  <i>Medium</i> – Provides a moderately sized buffer for handling congestion on this connection.  <i>High</i> – Provides the largest buffer for handling congestion on this connection.
New	command button	Saves the current connection and opens a new instance of the Add/Modify ATM UNI Connection window to create a new connection.
Undo	command button	Undoes any unsaved changes. Unsaved changes are those which have not been saved by selecting Apply or OK.

## Modifying a Connection

To modify a connection:

1. Select the connection from the list in the ATM UNI Connections window (Figure 5-31). The Connection Options window appears (see Figure 5-33):

The screenshot shows the 'Connection Options' dialog box. The 'Name' field contains 'Connection 1'. The 'Endpoint A Type' is set to 'Pvc Orig'. The 'S-P-P' field contains '1-3-1'. The 'VPI' field contains '1' and the 'VCI' field contains '32'. The 'Endpoint B S-P-P' field contains '1 2 1'. The 'Connect Status' is set to 'Up' and the 'Connect Detail' is set to 'Ok'. At the bottom, there are buttons for 'Modify...', 'Delete...', 'Connect...', 'IWF Stats...', 'Cell Stats...', and 'Cancel'. A warning bar at the bottom of the window reads 'Warning: Applet Window'.

**Figure 5-33. Connection Options - ATM-UNI**

2. Choose the Modify button. The Add/Modify ATM UNI Connection window appears (see Figure 5-32).
3. Modify the connection parameters described in Table 5-4, then choose OK.

## Enabling and Disabling a Connection

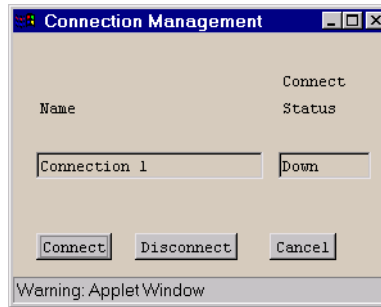
When you add an ATM UNI connection, it is automatically set to a connect state of Up, in which the connection is active. The connect state of a connection is effectively an on/off switch for the connection. You can deactivate a connection temporarily by setting its Connect State to Down, then turn the connection back on by setting the Connect State to Up. You can control the state of a connection from the Add/Modify ATM UNI Connection window or from the Connection Management window, both accessed from the Connection Options window.

*From the Add/Modify ATM UNI Connection window:*

To enable or disable a connection from the Add/Modify ATM UNI Connection window (Figure 5-32 on page 5-38), set the Set Connect Mgmt parameter to Up or Down, then choose OK.

*From the Connection Management window:*

To enable or disable an ATM UNI connection from the Connection Management window (Figure 5-35), select the Connect or Disconnect button.



**Figure 5-34. Connection Management Window**

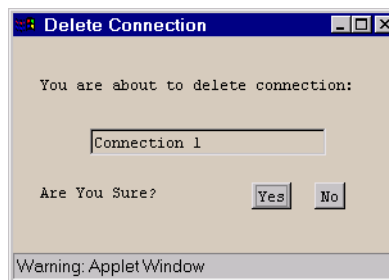


Disconnecting a connection (setting its Connect Status to Down) does not remove the connection configuration from the SA unit's database. You can reconnect it at any time, using the procedure described above.

## Deleting a Connection

To delete a connection:

1. Select the connection from the Configured ATM UNI Connections list in the ATM UNI Connections window. The Connection Options window appears (Figure 5-33).
2. Choose the Delete button to remove the connection from the port configuration. The Delete Connection (see Figure 5-35) window appears, asking you to confirm this action.



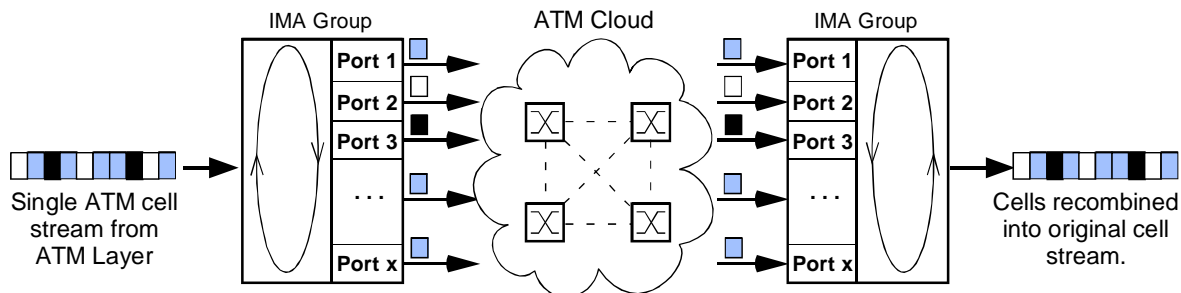
**Figure 5-35. Delete Connection Window**

3. Choose the Yes button. The connection is removed from the SA unit's database and disappears from the list of configured ATM UNI connections in the ATM UNI Connections window.

## Configuring Inverse Multiplex (IMA) Services

Inverse Multiplexing over ATM (IMA) is not strictly a connection service by itself, but rather an adjunct tool to configure a special type of ATM UNI port. Inverse Multiplexing over ATM allows you to ‘group’ several DS1/E1 ATM ports into a single logical connection with a bandwidth equal to the sum of the combined ports. This grouping of ports into a single virtual connection is called an IMA Group. Since the IMA Groups must be configured prior to any connections being configured across an IMA port, IMA Service is accessible from the Select Service menu.

Figure 5-36 shows the theory behind IMA’s operation: several individual DS1 or E1 circuits act in concert as a single high-speed data pipe to satisfy bandwidth requirements greater than DS1/E1 but less than DS3/E3.



Cells being transmitted are distributed across the ports (links) in a round-robin sequence. At the receiving end, the cells from each link are recombined into the original ATM cell stream.

**Figure 5-36. IMA Operation Example**

An IMA Group has an effective bandwidth equal to the bandwidths of the combined ports, minus a small percent for management and control. For an XPOD (4 IMA ports), the maximum aggregate speed of a four-port group is approximately 6.0 Mbps for a DS1 POD or 7.6 Mbps for an E1 POD. For an IPOD (8 IMA ports), the maximum aggregate speed of an eight-port group is approximately 12.0 Mbps for a DS1 POD or 15.2 Mbps for an E1 POD.

You can calculate the maximum aggregate speed of an IMA group with the following formulas, where M is the frame size selected and N is the number of links in the IMA group.

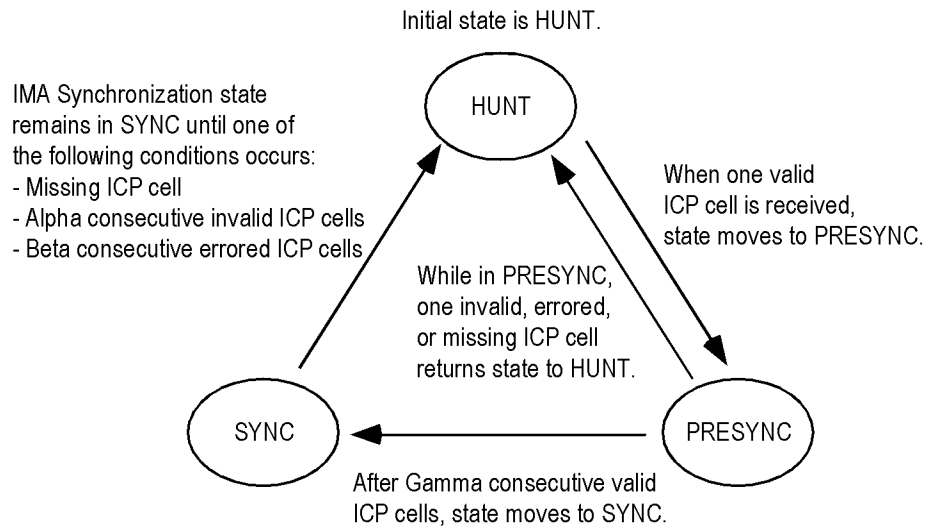
For a DS1 POD IMA Group:

$$1.536M \times \frac{M-1}{M} \times \frac{2048}{2049} \times N$$

For an E1 POD IMA Group:

$$1.920M \times \frac{M-1}{M} \times \frac{2048}{2049} \times N$$

When an IMA link is set to the Up operational state, the IMA Frame Synchronization process begins attempting to synchronize its links so that it can begin passing data. Once synchronization is achieved, the links pass data unless an error occurs, restarting the synchronization process. Each link goes through a Hunt-Presync-Sync cycle to establish synchronization with its opposite end, shown in [Figure 5-37](#).



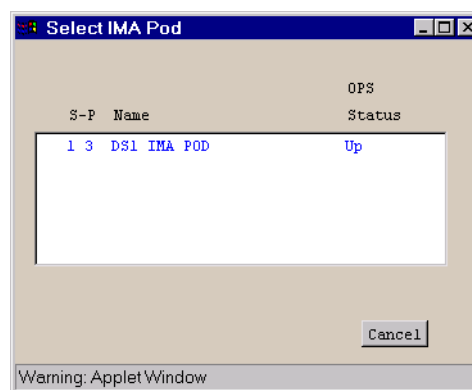
**Figure 5-37. IMA Frame Synchronization Process**

Configuring IMA service on an IMA POD consists of tagging IMA ports as IMA links (see [“Configuring a DS1 or E1 Port” on page 4-11](#) for details on tagging an IMA port as an IMA link), creating an IMA group and assigning ports to the group, and configuring the operational parameters so that the separate links function as one unit.

To configure IMA services:

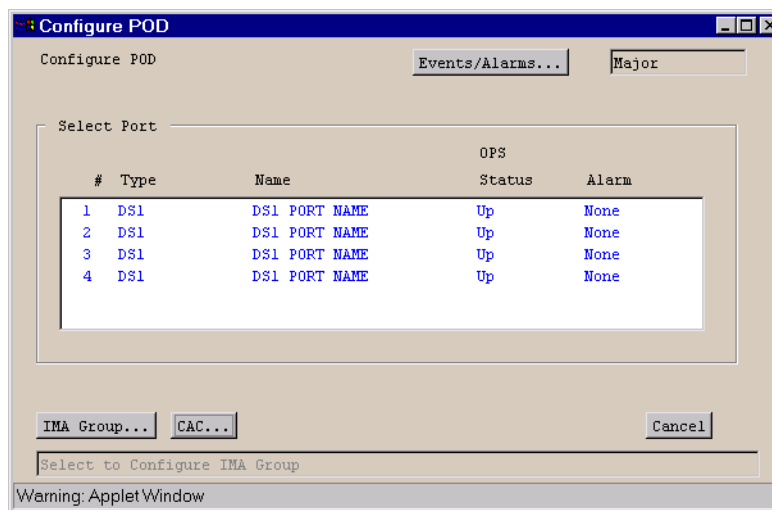
*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears.
2. Choose the Inverse Multiplex Service (IMA) button. The Select IMA POD window appears (see [Figure 5-38](#)).



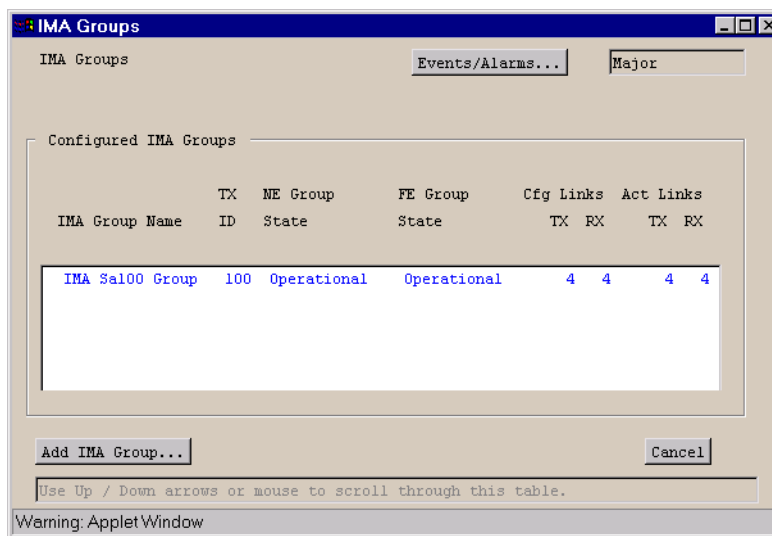
**Figure 5-38. Select IMA POD Window**

3. Select the IMA POD whose service you want to configure. The Configure POD window appears (see [Figure 5-39](#)).



**Figure 5-39. Configure POD Window**

4. Select the IMA Group button. The IMA Groups window appears (see [Figure 5-40](#)), listing any existing IMA groups.



**Figure 5-40. IMA Groups Window**

5. Select the Add IMA Group button to create a new IMA group. The Add/Modify IMA Group window appears (see [Figure 5-41](#)).

**Figure 5-41. Add/Modify IMA Group Window**

6. Complete the fields described in [Table 5-5](#) to define the IMA group and assign one or more of the IMA DS1/E1 ports to the group.



You can assign from one to four IMA ports to an IMA group on an IMA XPOD, and from one to eight IMA ports to an IMA group on an IMA IPOD. You should assign all available ports to a group, as unassigned ports are idle and unused.

**Table 5-5. Add/Modify IMA Group Buttons and Fields**

Field/Button	Type	Action/Description
<b>IMA Group Descriptors</b>		
Group Name	read/write	Enter an IMA Group name (32 characters max).
ADMIN Status	read/write	Set the administrative state of the IMA group: up (default) or down. Set to Down (offline) when you run diagnostics. (Testing mode is not currently supported.)
NE (Near End) Group State	read-only	Displays the operational state of the near-end of the IMA group: operational or non-operational.

**Table 5-5. Add/Modify IMA Group Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
TX IMA ID	read/write	Specify the transmission identification number to be assigned to this IMA group (must be an integer from 0-255.)
Min. TX Links	read/write	Specify the minimum number of transmit links that must be active to move the IMA group into the operational state.
Min. RX Links	read/write	Specify the minimum number of receive links that must be active to move the IMA group into the Operational state.
<b>Select Links</b>		
Add	read/write	Select IMA DS1/E1 ports to add to or remove from this group. Links marked with an X are included in this group. Selecting a link from this list opens the Configure IMA Link window ( <a href="#">Figure 5-42 on page 5-53</a> ); select the Add Link to Group parameter to add the selected link to this IMA group.  Note: only ports whose “Tag as IMA Link” parameter is set to True appear in this list.
Link Name	read-only	Displays the link name.
S-P-P	read-only	Displays the slot, POD, and port numbers of each link.
<b>IMA Group Tuning</b>		
Symmetry	read/write	Select the symmetry to be used by this IMA group. Options are:  <i>SymmetricOperation</i> (default) – The IMA interface is required to configure each IMA link in both transmit and receive directions. ATM cells can only be transmitted and received over links that are active in both directions.  <i>AssymmetricOperation</i> – (not currently supported) The IMA interface is required to configure each IMA link in both transmit and receive directions. ATM cells can be transmitted over a link in the transmit direction while the link is not active in the receive direction.  <i>AssymmetricConfiguration</i> – (not currently supported) The IMA interface is not required to configure all IMA links in both transmit and receive directions. ATM cells can be transmitted over a link in the transmit direction while the link is not active in the receive direction.



**Table 5-5. Add/Modify IMA Group Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
NE Transmit Clock Mode	read/write	Select the near-end transmit clock mode for this IMA Group. Options are:  <i>CTC</i> (default) – Common Transmit Clock. The same transmit clock is used for all IMA links.  <i>ITC</i> – (not currently supported) Independent Transmit Clock. The transmit clock on at least one link is derived from a different clock source than another link.
TX Frame Length	read/write	Select the transmission frame length for this IMA Group. Options are:  <i>M32</i> – IMA frames of 32 ATM cells. <i>M64</i> – IMA frames of 64 ATM cells. <i>M128</i> (default) – IMA frames of 128 ATM cells. <i>M256</i> – IMA frames of 256 ATM cells.  <i>Note:</i> Frames consist of <i>M-1</i> data cells and one OAM cell.
Max. Delay (ms)	read/write	Enter the maximum delay differential in milliseconds that this IMA Group will allow among its links. Range 0-25 msec.
Alpha	read/write	Enter the number of consecutive invalid ICP cells that must be detected before moving to the IMA HUNT state. The range is 1–2; the default value is 2.  See <a href="#">Figure 5-37 on page 5-47</a> for an illustration of the IMA frame synchronization mechanism.  <i>Note:</i> See the ATM Forum Technical Committee's <i>Inverse Multiplexing for ATM (IMA) specification for additional information on IMA state.</i>
Beta	read/write	Enter the number of consecutive errored ICP cells that must be detected before moving to the IMA HUNT state. The range is 1–5; the default value is 2.
Gamma	read/write	Enter the number of consecutive valid ICP cells that must be detected before moving to the IMA SYNC state from the PRESYNC state. The range is 1–5; the default value is 1.
Tx Test	read/write	Select whether transmit test is enabled or disabled.
Tx Test LID	read/write	Select the link on which Tx Test Pattern will be sent.

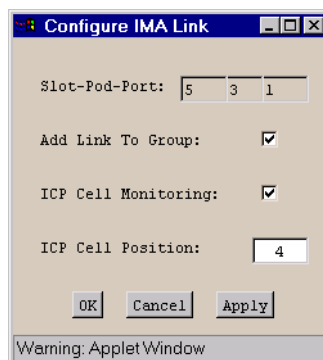
**Table 5-5. Add/Modify IMA Group Buttons and Fields (Continued)**

Field/Button	Type	Action/Description
Tx Test Pattern	read/write	Enter the test pattern for IMA group loopback. Select a value between 0 and 255 to designate a specific pattern. This pattern will be transmitted on the link selected by Tx Test LID and returned by the far end on <i>all</i> active links.
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Opens the Configure ATM Interface window, enabling you to access and configure the ATM interface. (See <a href="#">“Configuring the ATM Interface”</a> on page 4-46.)

## Configuring IMA Links

To configure the attributes of an individual IMA link (IMA DS1/E1 port):

1. Select the IMA DS1 or E1 from the Add or Modify IMA Group window's Add/Remove Links field (see [Figure 5-41](#)). The Configure IMA Link window appears ([Figure 5-42](#)):



**Figure 5-42. Configure IMA Link Window**

2. Complete the fields described in [Table 5-6](#).

**Table 5-6. Configure IMA Link Buttons and Fields**

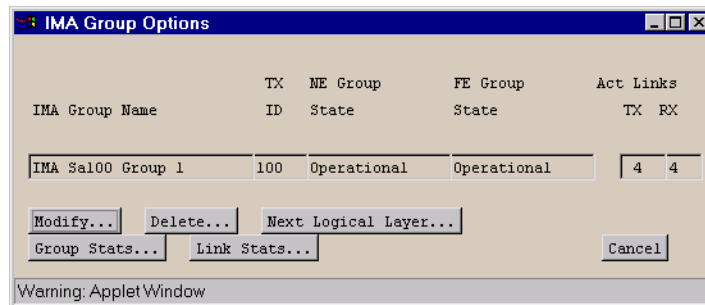
Field/Button	Type	Action/Description
<b>IMA Link Descriptors</b>		
Slot-Pod-Port	read-only	Displays the link's slot, POD and port numbers.
Add Link to Group	read/write	Check this box to add this IMA link to the current IMA group.
ICP Cell Monitoring	read/write	Check this box to enable ICP cell monitoring on this IMA link. Default is selected.
ICP Cell Position	read/write	Displays the position in the IMA frame where the ICP (OAM) cell is located during transmission.  This value must be between 0 and M, where M is the frame size. Default is 1.

3. Choose OK to close the window and return to the Add or Modify IMA Group window.

## Modifying an IMA Group

To modify an IMA group:

1. Select an IMA group from the list of Configured IMA Groups in the IMA Groups window (Figure 5-40). The IMA Group Options window appears (see Figure 5-43).



**Figure 5-43. IMA Group Options Window**

2. Select the Modify button. The Add/Modify IMA Group window appears.
3. Make any desired changes, referring to the parameters listed in Table 5-5 on page 5-49.
4. Choose OK to close the window when finished.

## Deleting an IMA Group

To delete an IMA group:

1. Select the IMA group from the list of Configured IMA Groups in the IMA Groups window (Figure 5-40). The IMA Group Options window appears (Figure 5-43).
2. Choose the Delete button. The Delete IMA Group window appears, asking you to confirm this action.
3. Choose OK to confirm. The system deletes the group and returns you to the IMA Group Options window.

## Viewing IMA Group Statistics

To view statistics regarding an IMA group or an individual link in an IMA group:

1. Select an IMA group from the list of Configured IMA Groups in the IMA Groups window (Figure 5-40). The IMA Group Options window appears (Figure 5-43).
2. Select the Group Stats button. The IMA Group Statistics window appears (see Figure 5-44).

The screenshot shows the 'IMA Group Statistics' window. It has a title bar with standard window controls. Inside, there's a tabbed interface with 'Events/Alarms...' and 'Major' tabs. The 'IMA Group Summary' section contains a table with columns: IMA Group Name, Status, NE Group, FE Group, and Last Change. The table has one row for 'IMA Sa100 Grou' with status 'p', NE Group 'perational', FE Group 'perational', and Last Change '5-Aug-1998 :58:01'. Below this, the 'imaGroup...' section contains various fields: Failure Status (NoFailure), TX Test Status (Disabled), Symmetry (SymmetricOperation), LID (1), Pattern (255), TX Cells (84122944), RX Cells (72629189), UASs (589), Fails (3), Run. Secs (364), ACR (14492), TX IMA ID (100), RX IMA ID (100), Alpha Value (2), Minimum # Links (1), Beta Value (2), Links Configured (4), Gamma Value (1), Links Active (4), Clock Mode (CTC), Allowed Delay (25), Timing Ref (0), Observed Delay (0), Frame (M128), and Least Delay (0). At the bottom, there are 'Clear Counters' and 'Cancel' buttons, and a text field with 'Select to return to the previous screen.' A warning bar at the very bottom says 'Warning: Applet Window'.

**Figure 5-44. IMA Group Statistics Window**

Table 5-7 describes the fields in the IMA Group Statistics window.

**Table 5-7. IMA Group Statistics Fields and Buttons**

Field/Button	Type	Description
<b>IMA Group Summary</b>		
IMA Group Name	read-only	Displays the name of the IMA group.
OPS Status	read-only	Displays the operational state of the IMA group: up or down.
NE (Near End), FE (Far End) Group State	read-only	<p>Displays the state of the near end and far end of this IMA group:</p> <p><i>Operational</i> - IMA group is operating properly at the near end.</p> <p><i>Startup</i> - Local end is in startup, waiting to see the far end in startup.</p> <p><i>Startup Ack</i> - A transitional state when both near and far ends are in startup.</p> <p><i>Insufficient Links</i> - The group does not have a sufficient number of links to operate.</p> <p><i>Blocked</i> - The group is blocked; a group can be blocked for maintenance purposes while sufficient links are active in both directions.</p> <p><i>ConfigAborted</i> - The far end has attempted to use unacceptable configuration parameters.</p>
Last Change	read-only	Displays the time and date of the last change to the IMA group state.

**Table 5-7. IMA Group Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
<b>IMA Group</b>		
Failure Status	read-only	Displays the failure status for this IMA group. <i>noFailure</i> – IMA group is up. <i>startUpNe</i> – Start up near-end failure. <i>startUpFe</i> – Start up far-end failure. <i>invalidMValueNe</i> – Invalid transmission frame length near-end. <i>invalidMValueFe</i> – Invalid transmission frame length far-end. <i>failedAssymmetricNe</i> – Assymmetric failure near-end. <i>failedAssymmetricFe</i> – Assymmetric failure far-end. <i>insufficientLinksNe</i> – Insufficient links near-end. <i>insufficientLinksFe</i> – Insufficient links far-end. <i>blockedNe</i> – Connection blocked at near-end. <i>blockedFe</i> – Connection blocked at far-end. <i>otherFailure</i> – Unrecognized failure.
TX Test Status	read-only	Displays whether the TX Test is currently enabled or disabled.
Symmetry	read-only	Displays the symmetry mode for this IMA group: Symmetric Operation (default), Assymmetric Operation, or Assymmetric Configuration.
LID	read-only	Displays the Tx Test Link Identifier for this IMA group.
Pattern	read-only	Displays the Tx Test Pattern for this IMA group.
TX Cells	read-only	Displays the number of cells transmitted by this IMA group.
(TX Cells)		
Fails	read-only	Displays the number of transmission cell failures.
ACR	read-only	Displays the current cell rate (in cells per second) provided by this IMA group, considering all the transmit links in the Active state.
RX Cells	read-only	Displays the number of cells received by this IMA group.

**Table 5-7. IMA Group Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
(RX Cells)		
Fails	read-only	Displays the number of receive cell failures.
ACR	read-only	Displays the current cell rate (in cells per second) provided by this IMA group, considering all the receive links in the Active state.
UASs	read-only	Displays the number of unavailable seconds recorded on this IMA group.
Run. Secs	read-only	Displays the length of time (in seconds) this IMA group has been in its current state (up or down).
TX IMA ID	read-only	Displays the IMA ID currently in use by the local IMA group.
(TX IMA)		
Minimum # Links	read-only	Displays the minimum number of transmit links required to be active to move the IMA group into the operational state.
Links Configured	read-only	Displays the number of links configured to transmit in this IMA group.
Links Active	read-only	Displays the number of configured transmit links that are also active.
Clock Mode	read-only	Displays the synchronization mode being used by the local IMA group.
Timing Ref	read-only	Displays the LID of the transmit timing reference link being used by the near end for IMA cell clock recovery from the ATM layer.
Frame	read-only	Displays the frame length being used by the IMA group in the transmit direction.
RX IMA ID	read-only	Displays the IMA ID currently in use by the remote IMA group.
(RX IMA)		
Minimum # Links	read-only	Displays the minimum number of receive links required to be active to move the IMA group into the operational state.
Links Configured	read-only	Displays the number of links configured to receive in this IMA group.



**Table 5-7. IMA Group Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
Links Active	read-only	Displays the number of configured receive links that are also active.
Clock Mode	read-only	Displays the synchronization mode being used by the remote IMA group.
Timing Ref	read-only	Displays the LID of the receive timing reference link being used by the near end for IMA cell clock recovery toward the ATM layer.
Frame	read-only	Displays the frame length being used by the IMA group in the transmit direction.
Alpha Value	read-only	Displays the number of consecutive invalid ICP cells that must be detected before moving from IMA SYNC to the IMA HUNT state. The default value is two.
Beta Value	read-only	Displays the number of consecutive errored ICP cells that must be detected before moving from IMA SYNC to the IMA HUNT state. The default value is two.
Gamma Value	read-only	Displays the number of consecutive valid ICP cells that must be detected before moving to the IMA SYNC state from the PRESYNC state. The default value is one.
Allowed Delay	read-only	Displays the maximum number of milliseconds of delay differential among the links that will be tolerated on this group.
Observed Delay	read-only	Displays the maximum differential delay in milliseconds observed among the receive links currently available in the IMA group.
Least Delay	read-only	Displays the index of the link in this IMA group that has the smallest link propagation delay. (This value is valid only if there is at least one link included in the IMA group.)

## Viewing IMA Link Statistics

To view statistics regarding an individual link within an IMA group:

1. Select an IMA group from the list of Configured IMA Groups in the IMA Groups window (Figure 5-40). The IMA Group Options window appears (Figure 5-43).
2. Select the Link Stats button. The Select IMA Link window appears (see Figure 5-45).

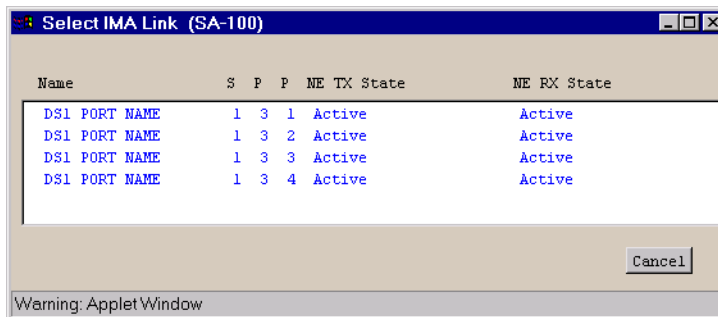


Figure 5-45. Select IMA Link Window

3. Select an individual link from the list box. The IMA Link Statistics window appears (see Figure 5-46).

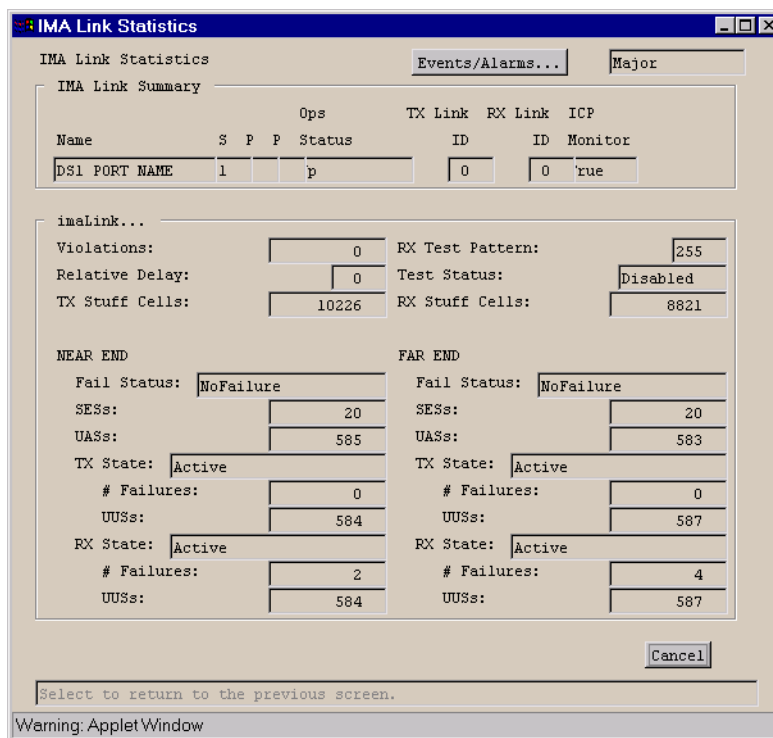


Figure 5-46. IMA Link Statistics Window

Table 5-8 describes the fields in the IMA Link Statistics window.

**Table 5-8. IMA Link Statistics Fields and Buttons**

Field/Button	Type	Description
<b>IMA Link Summary</b>		
Name	read-only	Displays the name of this IMA link.
S-P-P	read-only	Displays the location (slot, POD and port numbers) of the port.
OPS Status	read-only	Displays the operational status of the IMA link: up or down.
TX Link ID	read-only	Displays the outgoing Link ID currently in use by the link on the local end. (This value has meaning only if the link belongs to an IMA group.)
RX Link ID	read-only	Displays the incoming LID currently in use by the link on the remote end. (This value has meaning only if the link belongs to an IMA group.)
ICP Monitor	read-only	Displays whether the link is selected for ICP Cell monitoring.
<b>imaLink</b>		
Violations	read-only	Displays the count of errored, invalid or missing ICP cells during a non-SES-IMA condition.
Relative Delay	read-only	Displays the latest measured delay on this link relative to the link in the same IMA group with the least delay. Value is displayed in milliseconds.
TX Stuff Cells	read-only	Displays the number of stuff cells transmitted. Stuff cells are transmitted whenever there is no data cell waiting for transmission.
RX Test Pattern	read-only	Displays the received test pattern.
Test Status	read-only	Displays whether a test is currently underway (Enabled) or not (Disabled).
RX Stuff Cells	read-only	Displays the number of stuff cells received.
Near End:		
Fail Status	read-only	Displays the current link failure status of the near-end receive link.
SESS	read-only	Displays the count of one-second intervals containing several IV-IMA defects or one or more link defects (LOS, OOF/LOF, LCD), LIF, or LODS defects during a non-UAS-IMA condition.

**Table 5-8. IMA Link Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
UASs	read-only	Displays the count of unavailable seconds at the near-end. Unavailability begins at the onset of 10 contiguous SES-IMA and ends at the presence of 10 contiguous seconds with non-SES-IMA.
TX State	read-only	Displays the current state of the near-end transmit link.
# Failures	read-only	Displays the number of times the near-end transmit link has gone down due to a failure condition.
UUSs	read-only	Displays the count of unusable/fault seconds at the near-end transmit link.
RX State	read-only	Displays the current state of the near-end receive link.
# Failures	read-only	Displays the number of times the near-end receive link has gone down due to a failure condition.
UUSs	read-only	Displays the count of unusable/fault seconds at the near-end receive link.
Far End:		
Fail Status	read-only	Displays the current link failure status of the far-end receive link as reported via ICP cells.
SESs	read-only	Displays the count of one-second intervals containing one or more IMA-RDI defects.
UASs	read-only	Displays the count of unavailable seconds at the far end. Unavailability begins at the onset of 10 contiguous SES-IMA-FE and ends at the presence of 10 contiguous seconds with non-SES-IMA-FE.
TX State	read-only	Displays the current state of the far-end transmit link as reported via ICP cells.
# Failures	read-only	Displays the number of times the far-end transmit link has gone down due to a failure condition.
UUSs	read-only	Displays the count of unusable/fault seconds at the far-end transmit link.
RX State	read-only	Displays the current state of the far-end receive link as reported via ICP cells.
# Failures	read-only	Displays the number of times the far-end receive link has gone down due to a failure condition.

**Table 5-8. IMA Link Statistics Fields and Buttons (Continued)**

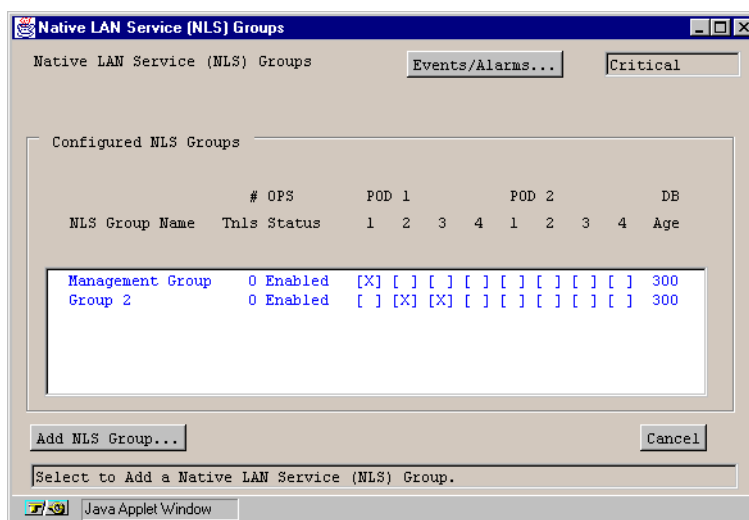
Field/Button	Type	Description
UUSs	read-only	Displays the count of unusable/fault seconds at the far-end receive link.

## Configuring Native LAN Services

Ethernet Native LAN Services (NLS) require configuration at two levels. First, ports must be assigned to an NLS Group. Second, once an NLS Group has been created, NLS Tunnels (connections) may be added to the Group. To configure Native LAN Service:

*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears (Figure 5-1 on page 5-2).
2. Choose the Native LAN Service (NLS) button. The Native LAN Service (NLS) Groups window appears (see Figure 5-47).



**Figure 5-47. Native LAN Service (NLS) Groups Window**

*From the Configure Ethernet Port window:*

3. After configuring the ports of a 10/100 Ethernet POD (“Configuring an Ethernet Port” on page 4-9), you can configure the Native LAN Service (NLS) by choosing the Service Management button in the Configure Ethernet Port window. The Native LAN Service (NLS) Groups window appears (see Figure 5-47).

From this window you can add a new group or modify existing groups.

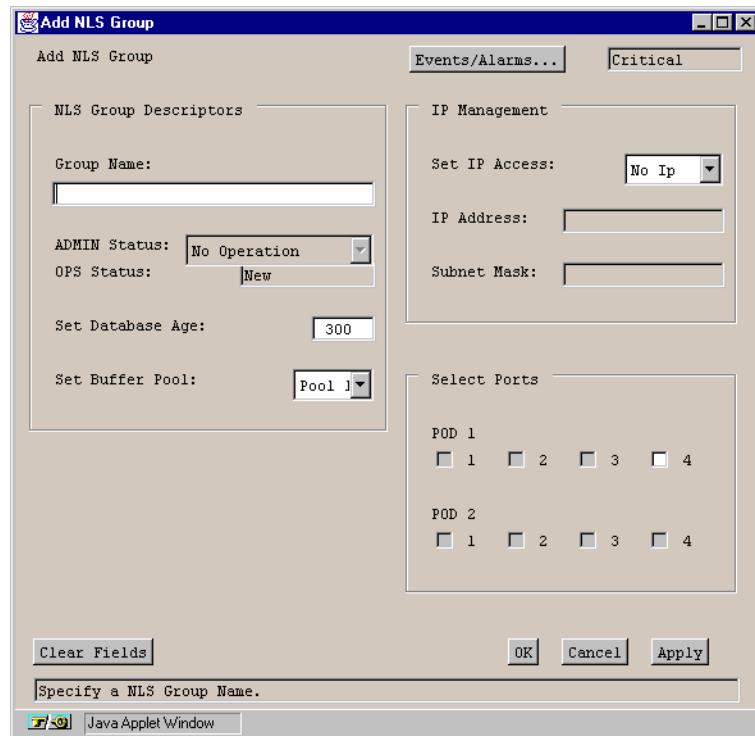
To add a new NLS group, proceed with section “Adding an NLS Group” on page 5-65.

To modify an existing NLS group, proceed with section “Modifying an NLS Group” on page 5-68.

## Adding an NLS Group

To add a Native LAN Services Group:

1. In the Native LAN Service (NLS) Groups window (Figure 5-47), choose the Add NLS Group button. The Add NLS Group window appears (see Figure 5-48).



The "Add NLS Group" window is a Java Applet Window with a title bar. It contains several sections for configuring a new NLS group. At the top, there are buttons for "Events/Alarms..." and "Critical". The main area is divided into three columns. The left column, titled "NLS Group Descriptors", contains fields for "Group Name" (a text box), "ADMIN Status" (a dropdown menu set to "No Operation"), "OPS Status" (a dropdown menu set to "New"), "Set Database Age" (a text box set to "300"), and "Set Buffer Pool" (a dropdown menu set to "Pool 1"). The middle column, titled "IP Management", contains fields for "Set IP Access" (a dropdown menu set to "No Ip"), "IP Address" (a text box), and "Subnet Mask" (a text box). The right column, titled "Select Ports", contains two sections: "POD 1" and "POD 2", each with four checkboxes labeled 1, 2, 3, and 4. At the bottom left is a "Clear Fields" button. At the bottom right are "OK", "Cancel", and "Apply" buttons. A status bar at the very bottom says "Specify a NLS Group Name." and "Java Applet Window".

**Figure 5-48. Add NLS Groups Window**

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

**Table 5-9. Add NLS Group Fields**

Field	Type	Action/Description
<b>NLS Group Descriptors</b>		
Group Name	read/write	Enter a name for this group.
Set ADMIN Status	read/write	<p>(This function not currently supported; NLS Groups are automatically set to UP Admin Status when created.)</p> <p>Specify the administrative state of the connection (up or down) after choosing the OK or Apply button.</p> <p><i>Up</i> (default) – Activates the connection when you click the OK or Apply button.</p> <p><i>Down</i> – Deactivates the connection when you click the OK or Apply button.</p>
OPS Status	read-only	Displays the operational state of the connection: Up or Down.
Set Database Age	read/write	Specify the default age (in seconds) of MAC addresses in the forwarding table.
Set Buffer Pool	read/write	<p>Specify the buffer pool for this NLS group:</p> <ul style="list-style-type: none"> <li>Mgmt (<i>Note: the Mgmt pool is intended for internal device functions. Do not assign to NLS Groups.</i>)</li> <li>Comms (<i>Note: the Comms pool is intended for internal device functions. Do not assign to NLS Groups.</i>)</li> <li>Pool 1</li> <li>Pool 2.</li> </ul> <p>By assigning Pool 1 and Pool 2 to different NLS groups, you can provide independent buffer pools for different customers.</p>
<b>IP Management</b>		
Set IP Access	read/write	Specify whether this group will have IP Access: No IP (default) or IP.
IP Address	read/write	<p>Specify the IP addresses for this group.</p> <p><b>Note:</b> This field is not available if No IP is selected in the Set IP Access field.</p>



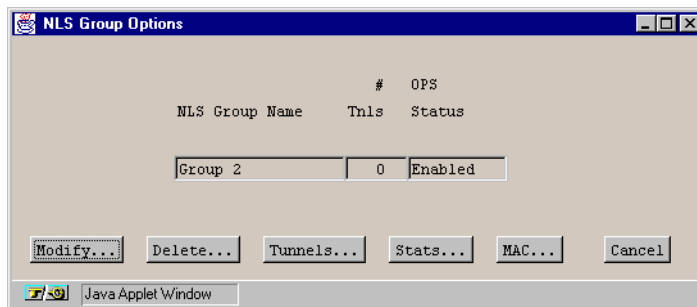
**Table 5-9. Add NLS Group Fields (Continued)**

Field	Type	Action/Description
Subnet Mask	read/write	Specify the IP subnet mask for this group. <i>Note: This field is not available if No IP is selected in the Set IP Access field.</i>
<b>Select Ports</b>		
POD 1 Ports 1–4	read/write	Assign POD1 ports to this group by placing a check mark in the box for each port.
POD 2 Ports 1–4	read/write	Assign POD2 ports to this group by placing a check mark in the box for each port.

## Modifying an NLS Group

To modify an NLS group:

1. Select the group from the list of defined groups in the NLS Groups window (Figure 5-47). The NLS Group Options window appears (see Figure 5-49):



**Figure 5-49. NLS Group Options Window**

2. Choose the Modify button. The Add/Modify NLS Group window appears (Figure 5-48).
3. Make any desired changes. (See Table 5-9 for fields information.)
4. When you have finished modifying the group, choose OK.

## Deleting an NLS Group

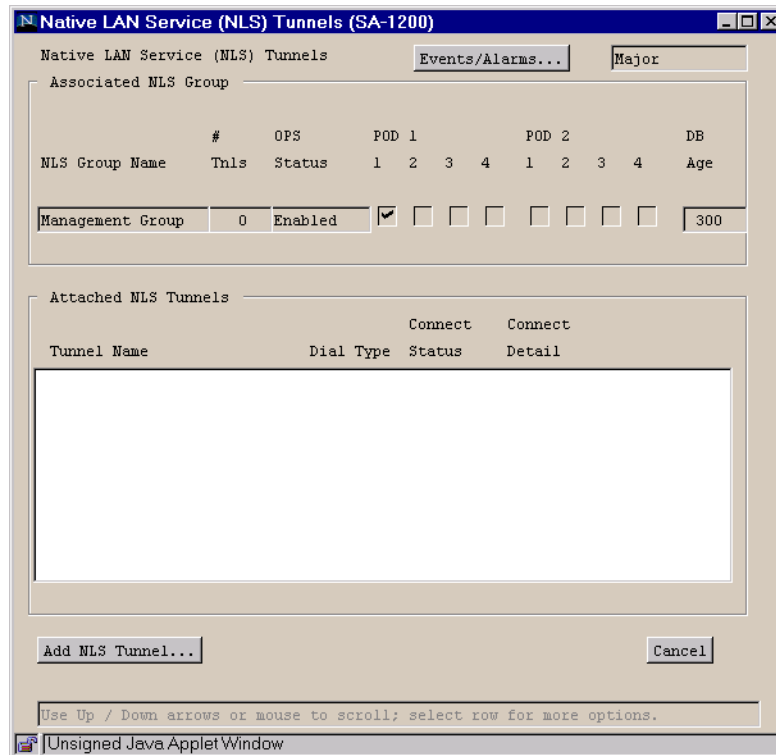
To delete an NLS group:

1. Select the group from the list of defined Groups in the NLS Groups window (Figure 5-47). The NLS Group Options window appears (Figure 5-49).
2. Choose the Delete button. The Delete NLS Group window appears, prompting you for confirmation.
3. Choose OK. The system deletes the group and returns you to the NLS Group Options window.

## Creating Tunnels for an NLS Group

To define tunnels for an NLS group:

1. Select a group from the list in the NLS Groups window (Figure 5-47). The NLS Group Options window appears (Figure 5-49).
2. Choose the Tunnels button. The Native LAN Service (NLS) Tunnels window appears (see Figure 5-50).



The screenshot shows the 'Native LAN Service (NLS) Tunnels (SA-1200)' window. It has a title bar with standard window controls. Inside, there are two tabs: 'Native LAN Service (NLS) Tunnels' (selected) and 'Events/Alarms...'. Below the tabs is a 'Major' dropdown menu. The main area is divided into two sections. The top section, 'Associated NLS Group', contains a table with columns: 'NLS Group Name', '#', 'OPS', 'Status', 'POD 1' (with sub-columns 1, 2, 3, 4), 'POD 2' (with sub-columns 1, 2, 3, 4), and 'DB Age'. A row is visible for 'Management Group' with values 0, Enabled, a checked checkbox, and several empty checkboxes, ending with a value of 300. The bottom section, 'Attached NLS Tunnels', has a table with columns: 'Tunnel Name', 'Dial Type', 'Status', and 'Detail'. It also has 'Connect' buttons above the 'Status' and 'Detail' columns. Below this table is a large empty rectangular area. At the bottom of the window are 'Add NLS Tunnel...' and 'Cancel' buttons. A status bar at the very bottom says 'Use Up / Down arrows or mouse to scroll; select row for more options.' and 'Unsigned Java Applet Window'.

**Figure 5-50. NLS Tunnels Window**

3. Choose the Add NLS Tunnel button. The Add/Modify NLS Tunnel window appears (see Figure 5-51).

**Add / Modify NLS Tunnel**

Events/Alarms... Major

Service Descriptors

Name:

Endpoint A Group:

Endpoint B Type:

Set Connect Mgmt:

Connect Status:

Service Definition:

Service Rate:

User Def. Rate:

PID Value:

Traffic Descriptors

	CLP=0	CLP=0+1	F
PCR:	0	167	
SCR:	0	0	W
MCR:			
MBS:	0	0	D
CDVT:	429496 microsec		

	CLP=0	CLP=0+1	R
PCR:	0	167	
SCR:	0	0	E
MCR:			
MBS:	0	0	V
CDVT:	429496 microsec		

Tagging:  UPC:

Congestion Control

Strategy:

Buffer Size:

New Undo OK Cancel Apply

Specify a Name for this NLS Tunnel.

Warning: AppletWindow

**Figure 5-51. Add/Modify NLS Tunnel Window**

- Complete the fields described in [Table 5-10](#), then choose OK.

**Table 5-10. Add/Modify NLS Tunnel Fields**

Field	Type	Action/Description
<b>Service Descriptors</b>		
Name	read/write	Enter a name for this tunnel (32 chars max.).
Endpoint A Group	read-only	Displays the name of the group for Endpoint A.
Endpoint B Type	read/write	<p>Select the dial type for this connection:</p> <p><i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.</p> <p><i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI.</p> <p><i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.</p> <p><i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.</p> <p><i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.</p>
(Address field) S-P-P or AESA	read/write	Specify Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read/write or read-only	<p>For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).</p> <p>For ASPVC Orig dial type, specify the handle being called (read/write).</p>
Set Connect Mgmt	read/write	<p>Specify the administrative state of the connection (up or down).</p> <p><i>Up</i> (default) – Activates the connection.</p> <p><i>Down</i> – Deactivates the connection.</p>

**Table 5-10. Add/Modify NLS Tunnel Fields (Continued)**

Field	Type	Action/Description
Connect Status	read-only	Displays the operational state of the connection: Up or Down.
Service Definition	read/write	<p>Select the type of service for this connection:</p> <p><i>CBR-1</i> (default) – Selects constant bit rate service for handling digital information, such as video and digitized voice and is represented by a continuous stream of bits. Constant bit rate service requires guaranteed throughput rates and service levels.</p> <p><i>RT-VBR1</i> – Selects real time variable bit rate 1 service for packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.</p> <p><b>Note:</b> <i>RT-VBR</i> and <i>NRT-VBR</i> service definitions apply to the ATM side of the connection only. The NLS-side shaping mechanism treats all <i>RT</i>- and <i>NRT-VBR</i> services as <i>VBR</i>.</p> <p><i>RT-VBR2</i> – Selects real time variable bit rate 2 service.</p> <p><i>RT-VBR3</i> – Selects real time variable bit rate 3 service.</p> <p><i>NRT-VBR1</i> – Selects non-real time variable bit rate 1 service for packaging the transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of non-real time VBR.</p> <p><i>NRT-VBR2</i> – Selects non-real time variable bit rate 2 service.</p> <p><i>UBR1</i> – Selects unspecified bit rate 1 service for LAN traffic applications primarily. The CPE should compensate for any delay or lost cell traffic.</p> <p><i>UBR2</i> – Selects unspecified bit rate 2 service for LAN traffic applications primarily.</p> <p><i>ABR</i> – Selects automatic bit rate service (not currently supported).</p>

**Table 5-10. Add/Modify NLS Tunnel Fields (Continued)**

Field	Type	Action/Description
Service Rate	read/write	Specify the data rate of the connection. <i>User Defined</i> – Allows you to specify a custom service rate in the User Def Rate field. <i>Rate 56KB</i> – Selects a service rate of 56 Kbps. <i>Rate 64KB</i> – Selects a service rate of 64 Kbps. <i>Rate 128KB</i> – Selects a service rate of 128 Kbps. <i>Rate 256KB</i> – Selects a service rate of 256 Kbps. <i>Rate 384KB</i> – Selects a service rate of 384 kbps. <i>Rate 512KB</i> – Selects a service rate of 512 Kbps. <i>Rate 1544KB</i> – Selects a service rate of 1544 Kbps/1.544 Mbps. <i>Rate 2M</i> – Selects a service rate of 2 Mbps. <i>Rate 10M</i> (default) – Selects a service rate of 10 Mbps. <i>Rate 34M</i> – Selects a service rate of 34 Mbps. <i>Rate 45M</i> – Selects a service rate of 45 Mbps. <i>Rate 100M</i> – Selects a service rate of 100 Mbps.
User Def Rate	read/write	If User Defined is selected as the service rate, this field becomes available. Enter a custom service rate in bits per second.
PID Value	read/write	Specify PID-1 or PID-7 to enable/disable error checking. PID-1 preserves the Ethernet CRC across the network. PID-7 regenerates the CRC locally.
<b>Traffic Descriptors (Forward and Reverse)</b>		
PCR (CLP=0)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0.
SCR (CLP=0)	read/write	Specify the forward/reverse sustainable cell rate, where the cell loss priority is 0.
MCR (CLP=0)		Not supported.

**Table 5-10. Add/Modify NLS Tunnel Fields (Continued)**

Field	Type	Action/Description
MBS (CLP=0)	read/write	Specify the forward/reverse maximum burst size, where the cell loss priority is 0.
PCR (CLP=0+1)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0+1.
SCR (CLP=0+1)	read/write	Specify the forward/reverse sustainable cell rate, where the cell loss priority is 0+1.
MCR (CLP=0+1)		Not supported.
MBS (CLP=0+1)	read/write	Specify the forward/reverse maximum burst size, where the cell loss priority is 0+1.
CDVT (microsec)	read/write	Specify the forward/reverse cell delay variation tolerance in microseconds for this connection.
Tagging	read-only	Displays the method of changing a high-priority cell to a low-priority cell for this tunnel.
UPC	read/write	Specify whether usage parameter control is enabled or disabled on this tunnel.
<b>Congestion Control</b>		
Strategy	read/write	<p>Specify the type of congestion control on this connection:</p> <p><i>None</i> (default) – Selects no strategy for handling congestion.</p> <p><i>SetEFCI</i> – Uses the explicit forward congestion indicator to determine if congestion (or impending congestion) exists in a node. The congested node modifies the EFCI bit in the ATM cell header to indicate congestion.</p> <p>If the equipment connected to the SA unit can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve the congestion. EFCI is only set in the UBR queue and affects all connections in the queue of the physical port. Do not select this option unless you want to use the EFCI strategy on this physical port.</p> <p><i>EarlyPacketDi</i> – Drops a whole packet to relieve congestion under AAL5 adaptation.</p> <p><i>DropCLP1</i> – Drops low-priority cells (CLP=1) to relieve congestion.</p>



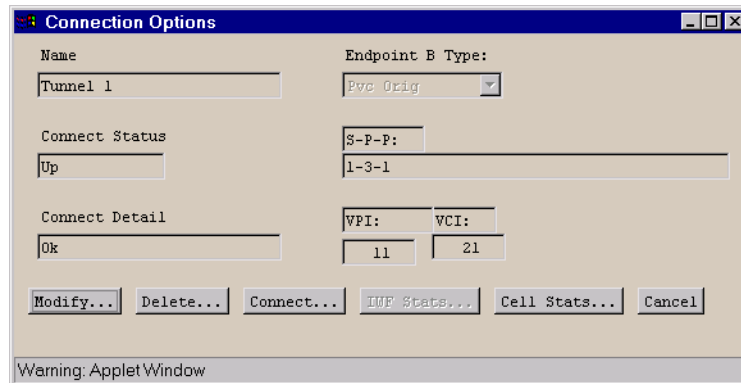
**Table 5-10. Add/Modify NLS Tunnel Fields (Continued)**

Field	Type	Action/Description
Buffer Size	read/write	Specify the buffer size allocated for controlling congestion on this connection:  <i>Shallow</i> (default) – Provides the smallest buffer for handling congestion on this connection.  <i>Medium</i> – Provides a moderately sized buffer for handling congestion on this connection.  <i>High</i> – Provides the largest buffer for handling congestion on this connection.
New	command button	Saves the current NLS tunnel and opens a new instance of the Add/Modify NLS Tunnel window to create a new NLS tunnels.
Undo	command button	Undoes any unsaved changes. Unsaved changes are those which have not been saved by selecting Apply or OK.

## Modifying an NLS Tunnel

Once you have created one or more NLS tunnels, you can modify their attributes. To modify an NLS tunnel:

1. Select the tunnel from the list of tunnels in the NLS Tunnels window. The Connection Options window appears (see [Figure 5-52](#)), showing the tunnel name, Endpoint B type and addressing information, connection status, and connection details (error code).



**Figure 5-52. Connection Options Window (NLS Tunnel)**

2. Choose the Modify button. The Add/Modify NLS Tunnel window appears ([Figure 5-51](#)).
3. Make any desired changes (see [Table 5-10](#) for field information).
4. When you have finished modifying the tunnel, choose OK.

## Enabling and Disabling an NLS Tunnel

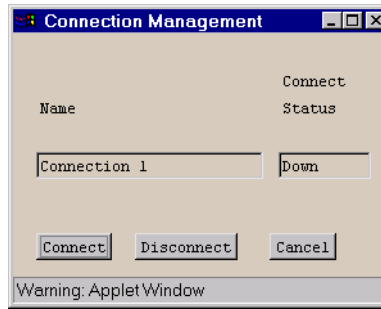
When you add an NLS Tunnel, it is automatically set to a connect state of Up, in which the connection is active. The connect state of a connection is effectively an on/off switch for the connection. You can deactivate a connection temporarily by setting its Connect State to Down, then turn the connection back on by setting the Connect State to Up. You can control the state of a connection from the Add/Modify NLS Tunnel window or from the Connection Management window, both accessed from the NLS Tunnel Options window.

*From the Add/Modify NLS Tunnel window:*

To enable or disable an NLS tunnel from the Add/Modify NLS Tunnel window ([Figure 5-51 on page 5-70](#)), set the Set Connect Mgmt parameter to Up or Down, then choose OK.

*From the Connection Management window:*

To enable or disable an NLS Tunnel from the Connection Management window ([Figure 5-53 on page 5-77](#)), select the Connect or Disconnect button.



**Figure 5-53. Connection Management Window**



Disconnecting a tunnel (setting its Connect Status to Down) does not remove the connection configuration from the SA unit's database. You can reconnect it at any time, using the procedure described above.

## Deleting an NLS Tunnel

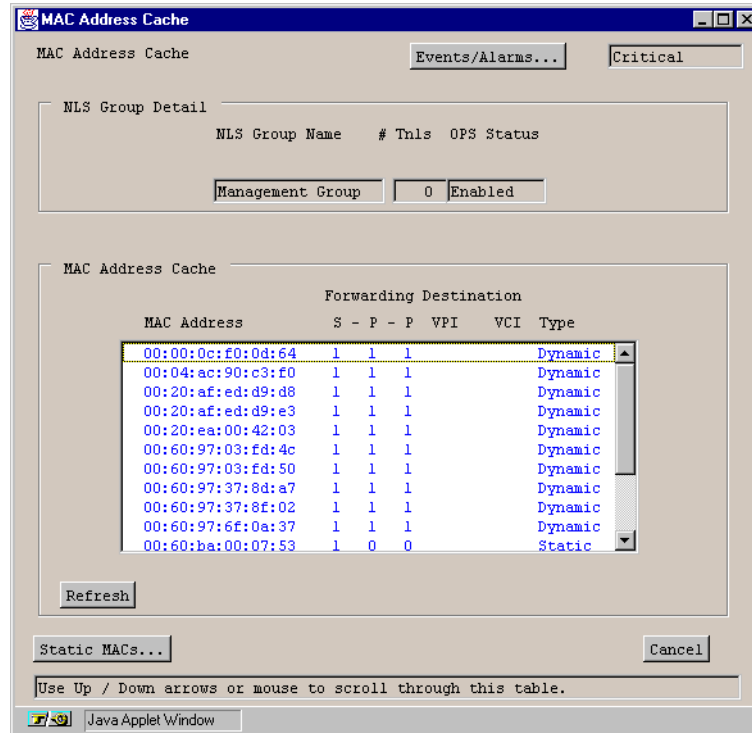
To delete an NLS tunnel:

1. Select the tunnel from the list of tunnels in the NLS Tunnels window (Figure 5-50). The Connection Options window appears (Figure 5-52).
2. Choose the Delete button. The Delete NLS Tunnel window appears, prompting you for confirmation.
3. Choose OK. The system deletes the tunnel returns you to the Connection Options window.

## Viewing MAC Address Cache Information

To view the MAC address cache information:

1. Select the group from the list of groups in the NLS Groups window (Figure 5-47). The NLS Group Options window appears (Figure 5-49).
2. Choose the MAC button. The MAC Address Cache window appears (see Figure 5-54).



**Figure 5-54. MAC Address Cache Window**

Table 5-11 describes the fields and buttons on the MAC Address Cache window.



Note that one MAC address has a Slot-POD-Port of 1-0-0, an exception to the usual Slot-POD-Port designation. Each Ethernet port is given a static MAC address at startup and designated S-P-P 1-0-0. This MAC address (like all static MAC addresses) never ages out from the MAC address table, nor can it be deleted by the user.

**Table 5-11. MAC Address Cache Fields and Buttons**

Field/Button	Type	Action/Description
<b>NLS Group Detail</b>		
NLS Group Name	read-only	Displays NLS group name.
# Tnls	read-only	Displays the number of tunnels established for this NLS group.
OPS Status	read-only	Displays the operational state of the group: up or down.
<b>MAC Address Cache</b>		
MAC Address	read-only	Displays MAC addresses in cache.
Forwarding Destination fields:		
S-P-P	read-only	Displays the forwarding destination (slot, POD, port numbers) of this MAC address.
VPI	read-only	Displays forwarding destination VPI of this MAC address.
VCI	read-only	Displays forwarding destination VCI of this MAC address.
Type	read-only	Displays the MAC address type.
Refresh	command button	Refreshes the data displayed in this window.
Static MACs	command button	Displays the Static MAC addresses screen. See <b>“Defining Static MAC Addresses”</b> on page 5-80 for details.

## Defining Static MAC Addresses

Static MAC addresses (MAC addresses that never “age out” from the MAC address table) may be assigned within each NLS Group. To view assigned static MAC addresses, choose the Static MACs button from the MAC Address Cache window. The Static MAC Addresses window appears (see [Figure 5-55](#)), showing the current NLS group name, number of tunnels and OPS status, along with a table of static MAC addresses, forwarding destinations, and connection types.

The Static MAC Addresses window displays the following information:

**Static MAC Addresses** (Title Bar)

Events/Alarms... Critical

**NLS Group Detail**

NLS Group Name	# Tnls	OPS Status
Management Group	0	Enabled

**Static MAC Address Table**

MAC Address	Forwarding Destination							
	S	-	P	-	P	VPI	VCI	Type

Add MAC... Cancel

Use Up / Down arrows or mouse to scroll through this table.

Java Applet Window

**Figure 5-55. Static MAC Adresses Window**

To add a static MAC address:

1. Choose the Add MAC button in the Static MAC Addresses window. The Add Static MAC Address window appears (see [Figure 5-56](#)):

**Figure 5-56. Add Static MAC Address Window**

2. Complete the fields described in [Table 5-12](#), then choose OK. The new static MAC address is added to the table of addresses in the Static MAC Addresses window.

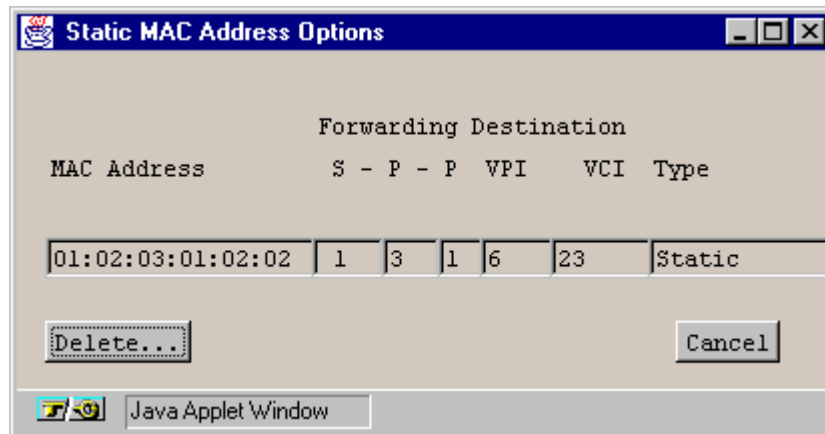
**Table 5-12. Add Static MAC Address Fields**

Field	Type	Action/Description
<b>Port Detail</b>		
MAC Address	read-write	Specify the new static MAC address, six two-character hexadecimal numerals separated by colons. For example, 01:02:03:04:05:06.
Forwarding Destination fields:		
S-P-P	read-write	Specify the forwarding destination (slot, POD, port numbers) of this MAC address.
VPI	read-write	Specify the forwarding destination VPI of this MAC address.
VCI	read-write	Specify the forwarding destination VCI of this MAC address.
Type	read-only	Always displays Static, the type of MAC address being added.

## Deleting Static MAC Addresses

To remove a static MAC address from the database:

1. Select the address from the Static MAC Addresses Table in the Static MAC Addresses window. The Static MAC Address Options window appears (see [Figure 5-57](#)):



**Figure 5-57. Static MAC Address Options Window**

2. Choose the Delete button to delete the displayed MAC address from the table. A warning dialog box appears, prompting you for confirmation.
3. Choose Yes to confirm deletion of this static MAC address.

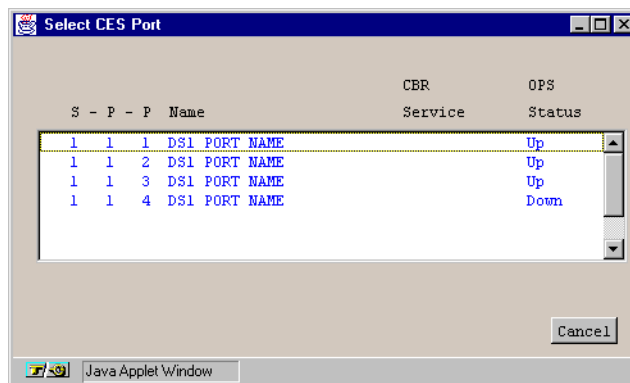


## Configuring Circuit Emulation Services

To configure Circuit Emulation Services:

*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears (Figure 5-1 on page 5-2).
2. Choose the Circuit Emulation (CES) button. The Select CES Port window appears (see Figure 5-58).



**Figure 5-58. Select CES Port Window**

3. Select the port you want to configure. The Configure CES Connection window appears (see Figure 5-59).

*From the Configure DS1 or E1 Port window:*

4. After you configure the ports of a DS1/E1 Circuit POD, as described in "Configuring a DS1 or E1 Port" on page 4-11, choose the Next Logical Layer button in the Configure DS1/E1 Port window. The Configure CES Connection window appears (see Figure 5-59).

*From the Configure Universal Serial Port window:*

5. After you configure the ports of a Universal Serial Circuit POD, as described in "Configuring a Universal Serial Port" on page 4-55, choose the Next Logical Layer button in the Configure Universal Serial Port window. The Configure CES Connection window appears (see Figure 5-59).

**Configure CES Connection**

Events/Alarms... Major

**Port Detail**

Slot-Pod-Port: 3 1 2 Port Type: Dsl  
Port Name: DS1 PORT NAME Port ID: DS1 CIRCUIT I  
ADMIN Status: Up OPS Status: Up  
CBR Service: Structured CBR Clock Mode: Synchronous  
Dynamic Bandwidth: Enabled CES Signaling: Transport

**Configured CES Connections**

CES-IWF Name	Dial Type	Status	Detail
--------------	-----------	--------	--------

Add CES-IWF... Add CES-DACS... OK Cancel Apply

Select the type of CBR Service for this port.

Warning: AppletWindow

**Figure 5-59. Configure CES Connection Window**

6. Complete the fields described in [Table 5-13](#) to configure the Circuit Emulation Service.

**Table 5-13. Configure CES Connection Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the location (slot, POD and port numbers) of the port.
Port Type	read-only	Displays the type of port.
Port Name	read-only	Displays the user designation of the port.
Port ID	read-only	Displays the user identification of the port.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
CBR Service	read/write	<p>Select the constant bit rate service of the port:</p> <p><i>Unstructured</i> (default) – Specifies unstructured constant bit rate service, which permits only one CES-IWF per port. (Note: Unstructured is not supported for Universal Serial CES PODs.)</p> <p><i>Structured</i> – Specifies structured constant bit rate service, which permits more than one CES-IWF per port.</p>
CBR Clock Mode	read-only	Specify the clock mode of the constant bit rate service of the port. Synchronous is the only clock mode currently supported.
Dynamic Bandwidth (Structured CBR Service only)	read/write	<p>Set Dynamic Bandwidth Allocation to Enabled or Disabled on this port.</p> <p><i>Enabled</i> (default) – Permits operation of the DBA function on any CES-IWF for which DBA is enabled.</p> <p><i>Disabled</i> – Prevents the DBA function from operating, i.e., each CES-IWF function's transmitter will remain enabled at all times, never allowing free bandwidth to be utilized by the DBA function.</p> <p>This setting acts as a global DBA control mechanism for the entire port. To enable or disable DBA on individual IWFs, see <a href="#">“Configuring Dynamic Bandwidth Allocation” on page 5-96.</a></p>

**Table 5-13. Configure CES Connection Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
CES Signalling (Structured CBR Service only)	read/write	Specify whether signalling information is preserved across the ATM network for this port:  <i>Transport</i> (default) – signalling information is preserved across the ATM network.  <i>Terminate</i> – signalling information is not preserved across the ATM network.
<b>Configured CES Connections</b>		
CES-IWF Name	read-only	Displays the user designation of each configured circuit emulation interworking function on this port. Choosing a CES-IWF from this list opens the window for “optioning” your selection. Optioning includes the ability to modify, delete, connect, disconnect, and obtain statistics on the CES-IWF.
Dial Type	read-only	Displays the dial type configured for each configured VCS interworking function on this port: PVC Orig, PVP, ASPVC Term, ASPVC Orig, or SPVC Orig.
Connect Status	read-only	Displays the state of the connection of each configured circuit emulation interworking function on this port: Up or Down.

**Table 5-13. Configure CES Connection Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Connect Detail	read-only	<p>Displays error codes if any failure is present on this interworking function. Possible error conditions include:</p> <p><i>VpvcUsed</i> - "Port / VPI / VCI" of either source or destination is already used.</p> <p><i>vpi-OOR</i> - VPI of either the source or destination is out of range.</p> <p><i>vci-OOR</i> - VCI of either the source or destination is out of range.</p> <p><i>vpi-Rsvd</i> - PVCs source or destination VPI within range reserved for PVPs.</p> <p><i>rate-OOR</i> - PCR/SCR in traffic descriptor out of range. Depending on service category: PCR is less than SCR, rate descriptor is non-0 when it should be 0, or rate is 0 when it should be non-0.</p> <p><i>desc-OOR</i> - Traffic Descriptor out of range. One or more of these descriptors is not in the list of MIB enumerations: Service Category, Congestion Action, or Buffer Size.</p> <p><i>port-bad</i> - The power-on self-test results have disabled this port.</p>
Add CES-IWF	window button	Opens the Add/Modify CES-IWF window. See <a href="#">"Adding a CES-IWF Connection" on page 5-89</a> .
Add CES-DACs	window button	Not currently supported.

## Configuring CES Interworking Functions

The following sections describe how to:

- Add a CES interworking function to a port ([page 5-89](#))
- Modify a CES interworking function ([page 5-99](#))
- Enable or Disable a CES interworking function ([page 5-100](#))
- Delete a CES interworking function ([page 5-101](#))

## Adding a CES-IWF Connection

To add and configure a CES interworking function to a port (if the selected port is on a Universal Serial CES POD, see note at bottom of this page):

1. Choose the Add CES-IWF button on the Configure CES Connection window.

Depending on how you configured the Set CBR Service parameter in the Configure CES Connection window, the following occurs:

- If you Set CBR Service to “Unstructured” (the default), the Add/Modify Unstructured DS1 or E1 CES-IWF window appears (see [Figure 5-60](#)). (The DS1 and E1 windows are similar.)

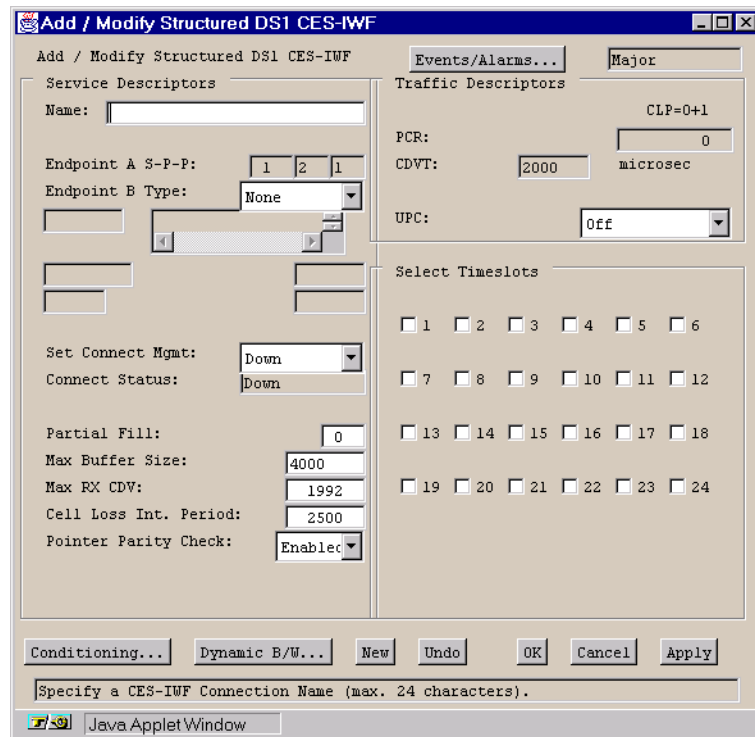
The screenshot shows a Java Applet window titled "Add / Modify Unstructured DS1 CES-IWF". The window is divided into two main panes. The left pane, labeled "Service Descriptors", contains fields for "Name", "Endpoint A S-P-P" (with values 1, 2, 1), "Endpoint B Type" (set to "None"), "Set Connect Mgmt" (set to "Down"), "Connect Status" (set to "Down"), "Max Buffer Size" (3984), "Max RX CDV" (1992), and "Cell Loss Int. Period" (2500). The right pane, labeled "Traffic Descriptors", contains fields for "CLP=0+1", "PCR" (4107), "CDVT" (1992), "microsec", and "UPC" (set to "Off"). At the bottom of the window, there are buttons for "Conditioning...", "Dynamic B/W...", "New", "Undo", "OK", "Cancel", and "Apply". Below these buttons is a text field labeled "Specify a CES-IWF Connection Name (max. 24 characters)". The window is running on a Java Applet, as indicated by the "JavaAppletWindow" label at the bottom.

**Figure 5-60. Add/Modify Unstructured CES-IWF Window (DS1 shown)**

- If you Set CBR Service to “Structured”, the Add/Modify Structured DS1 or E1 CES-IWF window appears (see [Figure 5-61](#)). (The DS1 and E1 windows are similar.)



The Universal Serial CES POD supports only one Structured CES-IWF per port. Unstructured interworking functions are not supported by the Universal Serial CES POD.



The image shows a Java Applet Window titled "Add / Modify Structured DS1 CES-IWF". The window is divided into two main sections: "Service Descriptors" on the left and "Traffic Descriptors" on the right. The "Service Descriptors" section includes fields for "Name", "Endpoint A S-P-P" (with values 1, 2, 1), "Endpoint B Type" (set to "None"), "Set Connect Mgmt" (set to "Down"), "Connect Status" (set to "Down"), "Partial Fill" (set to 0), "Max Buffer Size" (set to 4000), "Max RX CDV" (set to 1992), "Cell Loss Int. Period" (set to 2500), and "Pointer Parity Check" (set to "Enabled"). The "Traffic Descriptors" section includes "CLP=0+1" (set to 0), "PCR" (set to 0), "CDVT" (set to 2000), "UPC" (set to "Off"), and a "Select Timeslots" section with checkboxes for timeslots 1 through 24. At the bottom of the window, there are buttons for "Conditioning...", "Dynamic B/W...", "New", "Undo", "OK", "Cancel", and "Apply". A text field at the bottom prompts the user to "Specify a CES-IWF Connection Name (max. 24 characters)".

**Figure 5-61. Add/Modify Structured DS1 CES-IWF Window**

2. Complete the fields described in [Table 5-14](#), as appropriate.



**Table 5-14. Add/Modify Unstructured/Structured CES-IWF Fields and Buttons**

Field/Button	Type	Action/Description
<b>Service Descriptors</b>		
CES-IWF Name	read/write	Specify the user designation of this circuit emulation interworking function (24 characters max).
Endpoint A S-P-P	read only	Displays the location (slot-POD-port numbers) of endpoint A of this circuit emulation interworking function.
Endpoint B Type	read/write	Select the dial type for this connection: <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI. <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI. <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle. <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle. <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read/write	Specify Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read/write or read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only). For ASPVC Orig dial type, specify the handle being called (read/write).

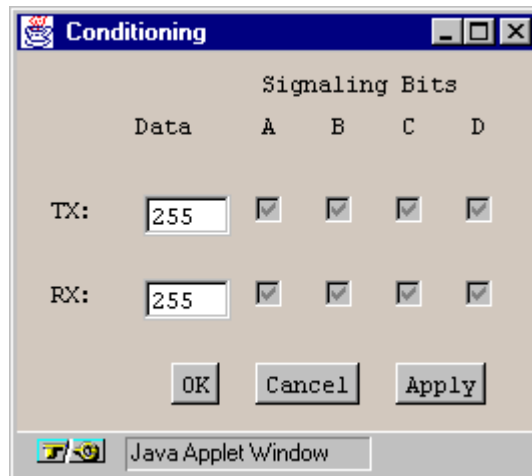
**Table 5-14. Add/Modify Unstructured/Structured CES-IWF Fields and Buttons**

Field/Button	Type	Action/Description
Set Connect Mgmt	read/write	Specify the administrative state of the connection of this circuit emulation interworking function.  <i>Up</i> (default) – The connection comes up after you choose the OK or Apply button.  <i>Down</i> – The connection is inoperative after you choose the OK or Apply button.
Connect Status	read-only	Displays the operational state of the connection of this circuit emulation interworking function: Up or Down.
Partial Fill (Structured only)	read/write	Sets/displays the number of user octets per cell for this circuit emulation interworking function: 0 to 47 (0 disables this function). (The minimum number of user octets depends on the number of DS0s and the selected signaling type.)
Max Buffer Size	read/write	Specify the maximum size of the reassembly buffer in 10 microsecond increments. The default of 1250 equals 12500 microseconds. As a general rule, set this parameter to twice the value of the Max RX CDV parameter.
Max RX CDV	read/write	Specify the maximum received-cell arrival jitter in microseconds. (Default is 1992 microseconds.)
Cell Loss Int. Period	read/write	Specify the cell loss integration period in milliseconds. (Default is 2500 milliseconds.)
Pointer Parity Check (Structured only)	read/write	Specify whether the pointer parity check is enabled (default) or disabled.
<b>Traffic Descriptors</b>		
PCR (CLP=0+1)	read-only	Displays the peak cell rate, where the cell loss priority is 0+1.
CDVT (microsec)	read-only	Displays the cell delay variation timing in microseconds.
UPC	read/write	Specify whether usage parameter control is enabled or disabled (on or off). (Default is off.)
<b>Select Timeslots (Structured only)</b>		
1 - 24 (DS1 only) 0-31 (E1 only)	read/write	Select the timeslots for this circuit emulation interworking function: 1 to 24 for DS1 ports, 0 to 31 for E1 ports. Timeslots previously assigned to another interworking function are unavailable.

**Table 5-14. Add/Modify Unstructured/Structured CES-IWF Fields and Buttons**

Field/Button	Type	Action/Description
Conditioning	window button	Enables you to configure the transmit and received data conditioning.
Dynamic B/W (Structured only)	window button	Enables you to configure the dynamic bandwidth allocation for this CES-IWF.
Clear Fields	command button	Enables you to clear any data you have entered in the Service Descriptor fields.
New (Structured only)	command button	Saves the current CES-IWF and opens a new instance of the Add/Modify CES-IWF window to create a new interworking function.  The New button is not available in the Add/Modify Unstructured DS1 CES-IWF window because only one interworking function is supported for Unstructured CES connections.
Undo	command button	Undoes any unsaved changes. Unsaved changes are those which have not been saved by selecting Apply or OK.

3. When you finish setting parameters, choose the Conditioning button. The Conditioning window appears (Figure 5-62).



**Figure 5-62. Conditioning Window**

*For unstructured CBR, follow steps 4 and 5 only. For structured CBR, skip steps 4 and 5 and continue with step 6.*

4. Enter the TX and RX Data parameters as required and choose OK. With unstructured constant bit rate service, signaling bit conditioning is not an option, therefore you cannot select the TX and RX Signaling Bits parameters A-B-C-D.

Conditioning serves the following functions:

- When the SA unit discovers that the local DS1/E1 circuit is down (a loss of frame condition), it sends the contents of the TX Data conditioning parameter to the remote interworking function (to replace the lost live traffic).
  - When the SA unit discovers that the remote end of the interworking function is down, it sends the contents of the RX Data conditioning parameter over the DS1/E1 circuit (to replace the lost live traffic). It also continues to send the same signaling (the signaling is “frozen”) that was present at the time the SA unit discovered that the remote end was down.
5. When you are finished, choose OK to close the Conditioning window and return to the Add/Modify Unstructured DS1/E1 CES-IWF window.
  6. Enter the TX and RX Data parameters as required.
  7. Configure the signaling bit conditioning according to the type of channel associated signaling (CAS) that is associated with the structured constant bit rate service:
    - With basic CAS, signaling bit conditioning is not an option. Therefore you cannot select TX and RX Signaling Bits parameters A-B-C-D.
    - With D4 CAS, two-bit signaling bit conditioning is available. Therefore you may enter the TX and RX Signaling Bits parameters A-B, but not parameters C-D.

- With ESF CAS, four-bit signaling bit conditioning is available. Therefore you may enter TX and RX Signaling Bits parameters A-B-C-D.

If signaling bit conditioning is an option (D4 and ESF CAS), the SA unit sends the contents of the Signaling Bits parameter over the DS1/E1 circuit after the cell loss integration period has expired, which by default is 2.5 seconds after the SA unit discovered that the remote end was down.

8. When you are finished, choose OK to close the Conditioning window and return to the Add/Modify Structured DS1/E1 CES-IWF window.
9. If desired, configure Dynamic Bandwidth Allocation by choosing the Dynamic B/W button from the Add/Modify Structured DS1/E1 CES-IWF window. See **“Configuring Dynamic Bandwidth Allocation”** on page 5-96 for details.

## Configuring Dynamic Bandwidth Allocation

Structured CES interworking functions can take advantage of Dynamic Bandwidth Allocation to send idle cells out the trunk port when the selected CES-IWF is not in use. The Dynamic Bandwidth Allocation function monitors the selected IWF, and when it senses that the IWF is not in use, DBA disables the IWF's transmitter and begins sending idle cells out the trunk port. If DBA senses the IWF's return to in-use status, it re-enables the IWF's transmitter.

Dynamic Bandwidth Allocation of CES interworking functions is accomplished by allowing combinations of various control sources to control the transmitter of individual IWFs. Using the Dynamic Bandwidth dialog box, you can select the control sources which determine whether an IWF is in-use or not in-use. If multiple control sources are selected, *all* DS0s within the CES-IWF must meet *all* selected criteria for the IWF to be considered not in-use and the Dynamic Bandwidth Allocation function to operate. **Table 5-15** shows when a transmitter is enabled or disabled based on the selected control sources.

**Table 5-15. Transmitter Control Sources**

Control Source	Transmitter Enabled When...	Transmitter Disabled When...
Signaling codes	at least one channel is 'off-hook'	NO channels are 'off-hook'
LOS Alarm	LOS alarm is inactive	LOS alarm is active
Cell Loss Status	No cell loss is reported	Cell loss is reported

As **Table 5-15** shows, an IWF's transmitter can be enabled or disabled. When an interworking function is in-use, its transmitter is enabled, sending AAL1 cells toward the switch fabric and out the trunk port. When an IWF is not in-use, the transmitter is disabled, no cells are sent toward the switch fabric, and DBA sends idle cells out the trunk port. Bandwidth previously used for the IWF can be used for other lower-priority services.

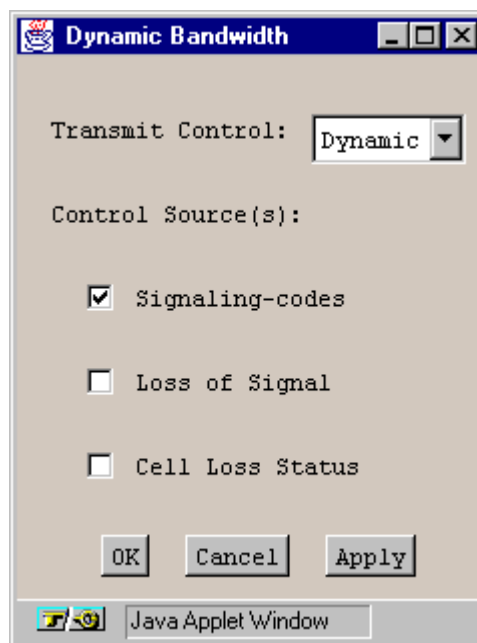


There is no interaction with connection management system - all connections in the cross-connect table remain intact.

To configure Dynamic Bandwidth Allocation on a structured CES-IWF:

1. Select the Dynamic Bandwidth button from the Add/Modify Structured DS1/E1 CES-IWF window. The Dynamic Bandwidth window appears (Figure 5-63).

► The CES-IWF must have been set to Dynamic Bandwidth: Enabled in the Configure CES Connection window, or the Dynamic Bandwidth button will be greyed out in the Add/Modify Structured DS1/E1 CES-IWF window. The DBA setting in the Configure CES Connection window acts as a global DBA control mechanism; if it is disabled, *all* DBA is disabled. (DBA applies only to Structured DS1 and Structured E1 CES interworking functions.)



**Figure 5-63. Dynamic Bandwidth Window.**

2. Complete the fields described in Table 5-16, DS1 or E1 as appropriate, then choose the OK button to return to the Add/Modify Structured DS1/E1 CES-IWF window.

**Table 5-16. Dynamic Bandwidth Fields and Buttons**

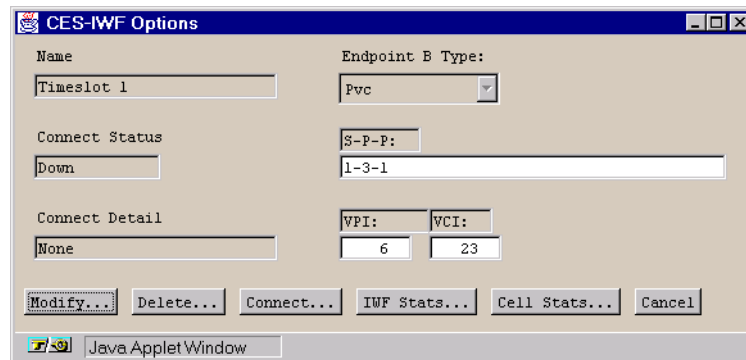
Field/Button	Type	Action/Description
Transmit Control	read/write	<p>Specify the Dynamic Bandwidth Allocation transmit control:</p> <p><i>Enabled</i> (default) – The IWF transmitter is always enabled.</p> <p><i>Disabled</i> – The IWF transmitter is always disabled.</p> <p><i>Dynamic</i> –The IWF transmitter is controlled by the selected Control Source(s) (see below).</p>
Control Sources	read/write	<p>Control sources determine whether an IWF is in-use or not-in-use. The criteria of all selected control sources must be satisfied for a port to be considered not-in-use.</p> <p>Select one or more Control Source(s):</p> <p><i>Signaling-codes</i> (applies to structured IWF with CAS Super-Frame or Extended Super Frame framing formats only) – The IWF is considered in-use if one or more DS0 in the bundle have a signaling code of off-hook.</p> <p><i>Loss-of-Signal</i> – The IWF is considered in-use whenever the loss-of-signal alarm is not active. When the loss-of-signal alarm is active, the IWF is considered not-in-use.</p> <p><i>Cell Loss</i> –The IWF is considered in-use whenever the cell-loss status is ‘no loss.’ When cell-loss status is ‘loss,’ the IWF is considered not-in-use.</p>



## Modifying a CES-IWF Connection

To modify a CES-IWF:

1. Select the CES-IWF from the connections list in the Configure CES Connection window. The Connection Options window appears (see [Figure 5-64](#)).



**Figure 5-64. Connection Options Window (CES-IWF)**

2. Choose the Modify button to change the settings in the CES-IWF configuration.

The window that appears depends on how you configured the Set CBR Service parameter in the Configure CES Connection window.

- If you set CBR Service to Unstructured (default), the Add/Modify Unstructured DS1/E1 CES-IWF window appears (see [Figure 5-60](#)).
- If you set CBR Service to Structured, the Add/Modify Structured DS1/E1 CES-IWF window appears (see [Figure 5-61](#)).

3. Make any desired changes to the interworking function. See [Table 5-14](#) for details of each parameter.
4. When you have finished making your changes, choose OK.

## Enabling and Disabling a Connection

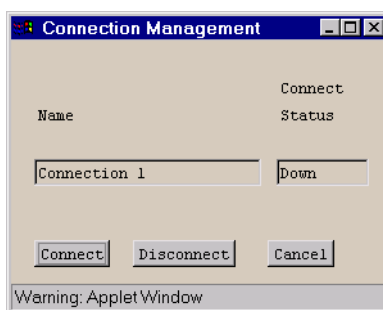
When you add a CES IWF, it is automatically set to a connect state of Up, in which the connection is active. The connect state of an IWF is effectively an on/off switch for the connection. You can deactivate a connection temporarily by setting its Connect State to Down, then turn the connection back on by setting the Connect State to Up. You can control the state of a connection from the Add/Modify CES-IWF window or from the Connection Management window, both accessed from the Connection Options window.

*From the Add/Modify CES-IWF window:*

To enable or disable a connection from the Add/Modify CES-IWF window (Figure 5-60 or Figure 5-61), set the Set Connect Mgmt parameter to Up or Down, then choose OK.

*From the Connection Management window:*

To enable or disable a CES-IWF from the Connection Management window (Figure 5-65), select the Connect or Disconnect button.



**Figure 5-65. Connection Management Window**



Disconnecting an IWF by setting its Connect Status to Down does not remove the connection configuration from the SA unit's database. You can reconnect it at any time, using the procedure described above. To remove a CES-IWF from the SA unit's database, see [“Deleting a CES-IWF Connection” on page 5-101](#).

## **Deleting a CES-IWF Connection**

To remove the configuration of a CES-IWF from the SA unit's database:

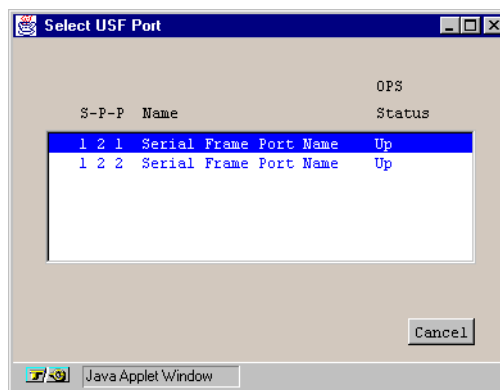
1. Select the CES-IWF from the Configured CES Connections list in the Configure CES Connection window.
2. When the Connection Options window appears, choose the Delete button.
3. When the Delete CES Connection window appears, choose the Yes button.

## Configuring Universal Serial Frame Service

To configure Frame services:

*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears (Figure 5-1 on page 5-2).
2. Choose the Frame Service button. The Select USF Port window appears (see Figure 5-66).



**Figure 5-66. Select USF Port Window**

3. Select the port you want to configure and the Configure USF Connections window appears (see Figure 5-67).

*From the Configure Universal Serial Frame Port window:*

4. After you configure the ports of a Universal Serial Frame POD, as described in "Configuring a Universal Serial Port" on page 4-55, choose the Next Logical Layer button in the Configure Universal Serial Frame Port window and the Configure USF Connections window appears (see Figure 5-67).

Configure USF Connection

Events/Alarms... Major

Port Detail

Slot-Pod-Port: 1 2 1 Port Type: RvxPort

Port Name: Serial Frame Port ID: Serial Frame

ADMIN Status: Up OPS Status: Up

Configured USF Connections

Tunnel Name	Dial Type	Connect Status	Connect Detail
-------------	-----------	----------------	----------------

Add USF-IWF... Cancel

Use Up / Down arrows or mouse to scroll; select row for more options.

Warning: AppletWindow

**Figure 5-67. Configure USF Connection Window**

5. See [Table 5-17](#) for descriptions of the fields and buttons in the Configure USF Connection window.
6. Choose the Add USF-IWF button to configure a new USF interworking function. See [“Configuring USF Interworking Functions”](#) on page 5-106.



Only one USF-IWF connection per Universal Serial Frame port is supported.

**Table 5-17. Configure USF Connection Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD and port number.
Port Type	read-only	Displays the type of port.
Port Name	read-only	Displays the user designation of the port.
Port ID	read-only	Displays the user identification of the port.
ADMIN Status	read-only	Displays the administrative state of the port: up or down.
OPS Status	read-only	Displays the operational state of the port: up or down.
<b>Configured USF Connections</b>		
Tunnel Name	read-only	Displays the user designation of each configured USF interworking function on this port. Choosing a USF-IWF from this list opens the window for “optioning” your selection. Optioning includes the ability to modify, delete, connect, disconnect and obtain statistics concerning the USF-IWF.
Dial Type	read-only	Displays the dial type for this connection: <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI. <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle. <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle. <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
Connect Status	read-only	Displays the state of the connection of each configured USF interworking function on this port: up or down.

**Table 5-17. Configure USF Connection Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Connect Detail	read-only	<p>Displays error codes if any failure is present on this USF connection. Possible error conditions include:</p> <p><i>VpvcUsed</i> - "Port / VPI / VCI" of either source or destination is already used.</p> <p><i>vpi-OOR</i> - VPI of either the source or destination is out of range.</p> <p><i>vci-OOR</i> - VCI of either the source or destination is out of range.</p> <p><i>vpi-Rsvd</i> - PVCs source or destination VPI within range reserved for PVPs.</p> <p><i>rate-OOR</i> - PCR/SCR in traffic descriptor out of range. Depending on service category: PCR is less than SCR, rate descriptor is non-0 when it should be 0, or rate is 0 when it should be non-0.</p> <p><i>desc-OOR</i> - Traffic Descriptor out of range. One or more of these descriptors is not in the list of MIB enumerations: Service Category, Congestion Action, or Buffer Size.</p> <p><i>port-bad</i> - The power-on self-test results have disabled this port.</p>
<b>Other Buttons</b>		
Add USF-IWF	window button	Opens the Add USF-IWF window for adding and configuring a new USF interworking function.

## Configuring USF Interworking Functions

This section describes how to:

- Add an USF-IWF connection (see [page 5-107](#))
- Modify an USF-IWF connection (see [page 5-114](#))
- Enable or Disable an USF-IWF connection (see [page 5-115](#))
- Delete an USF-IWF connection (see [page 5-116](#))



## Adding a USF-IWF Connection

To add and configure a connection:

1. Choose the Add USF-IWF button from the Configure USF Connection window (see [Figure 5-67 on page 5-103](#)). The Add/Modify USF-IWF window appears (see [Figure 5-68](#)).

**Add / Modify USF IWF**

Events/Alarms... Major

**Service Descriptors**

Name:

Endpoint A S-P-P:

Endpoint B Type:

Set Connect Mgmt:

Connect Status:

Service Definition:

Service Rate:

User Def. Rate:

CRC Length:

Header Length:

Frame Error Threshold:

**Traffic Descriptors**

	CLP=0	CLP=0+1	F
PCR:	0	10666	
SCR:	0	0	W
MCR:			
MBS:	0	0	D
CDVT:	94	microsec	

	CLP=0	CLP=0+1	R
PCR:	0	10666	
SCR:	0	0	E
MCR:			
MBS:	0	0	V
CDVT:	94	microsec	

Tagging:  UPC:

**Congestion Control**

Strategy:

Buffer Size:

Specify a Name for this NLS Tunnel.

Warning: AppletWindow

**Figure 5-68. Add/Modify USF IWF Window**

2. Complete the fields described in [Table 5-18](#) to select the parameters for the new connection.
3. When you are finished defining this connection, choose OK.

**Table 5-18. Add/Modify USF-IWF Fields and Buttons**

Field/Button	Type	Action/Description
<b>Service Descriptors</b>		
Name	read/write	Specify a name for this connection.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the connection.
Endpoint B Type	read/write	Select the dial type for this connection:  <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.  <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.  <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.  <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read/write	Specify Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read/write or read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).  For ASPVC Orig dial type, specify the handle being called (read/write).

**Table 5-18. Add/Modify USF-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Connect Mgmt	read/write	Specify the administrative state of the connection.  <i>up</i> (default) – Activates the connection when you click the OK or Apply button.  <i>down</i> – Deactivates the connection when you click the OK or Apply button.
Connect Status	read-only	Displays the operational state of the connection: up or down.
Service Definition	read/write	Select the type of service of the connection:  <i>CBR-1</i> – Selects constant bit rate service for handling digital information, such as video and digitized voice and is represented by a continuous stream of bits. Constant bit rate service requires guaranteed throughput rates and service levels.  <i>RT-VBR1</i> – Selects real time variable bit rate 1 service for packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.  <i>RT-VBR2</i> – Selects real time variable bit rate 2 service.  <i>RT-VBR3</i> – Selects <i>real time variable bit rate 3</i> service.  <i>NRT-VBR1</i> (default) – Selects non-real time variable bit rate 1 service for packaging the transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of non-real time VBR.  <i>NRT-VBR2</i> – Selects non-real time variable bit rate 2 service.  <i>NRT-VBR3</i> – Selects non-real time variable bit rate 3 service.  <i>UBR1</i> – Selects unspecified bit rate 1 service for LAN traffic applications primarily. The CPE should compensate for any delay or lost cell traffic.  <i>UBR2</i> – Selects unspecified bit rate 2 service.

**Table 5-18. Add/Modify USF-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Service Rate	read/write	Specify the data rate of the connection. <i>Rate 64KB</i> – Selects a service rate of 64 Kbps. <i>Rate 384KB</i> – Selects a service rate of 384 Kbps. <i>Rate 1536KB</i> – Selects a service rate of 1536 Kbps/1.536 Mbps. <i>Rate 1MB</i> – Selects a service rate of 1 Mbps. <i>Rate 2MB</i> – Selects a service rate of 2 Mbps. <i>Rate 5MB</i> – Selects a service rate of 5 Mbps. <i>Rate 10MB</i> – Selects a service rate of 10 Mbps. <i>Rate 40MB</i> – Selects a service rate of 40 Mbps. <i>Rate 50MB</i> – Selects a service rate of 50 Mbps. <i>Rate 100MB</i> – Selects a service rate of 100 Mbps. <i>Rate 150MB</i> – Selects a service rate of 150 Mbps. <i>User Defined</i> (default) – Selects a user-defined service rate, and makes available the User Defined Rate field.
User Defined Rate (available only if User Defined is selected in the Service Rate field)	read/write	Specify a service rate in bits per second. Defaults to the service rate defined in the Configure USF Port dialog.
CRC Length	read/write	Specify the size of the CRC for the connection: <i>CRC16</i> (default) – Selects a 16-bit CRC. <i>CRC32</i> – Selects a 32-bit CRC.
Header Length	read/write	(This parameter is not currently supported.) Specify the header length for this connection.
Frame Error Threshold	read/write	(This parameter is not currently supported.) Specify the number of frame errors (discarded frames, bad CRC, etc.) required to generate a frame error alarm.

**Table 5-18. Add/Modify USF-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Traffic Descriptors</b> <b>(Forward or Reverse)</b> <b>note: if traffic descriptors are changed, Service Rate field changes to User Defined.</b>		
PCR (CLP=0)	read-only	Displays the forward/reverse peak cell rate, where the cell loss priority is 0.
SCR (CLP=0)	read-only	Displays the forward/reverse sustainable cell rate, where the cell loss priority is 0.
MCR (CLP=0)		Not supported.
MBS (CLP=0)	read-only	Displays the forward/reverse maximum burst size, where the cell loss priority is 0.
PCR (CLP=0+1)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0+1.
SCR (CLP=0+1)	read-only	Displays the forward/reverse sustainable cell rate, where the cell loss priority is 0+1.
MCR (CLP=0+1)		Not supported.
MBS (CLP=0+1)	read-only	Displays the forward/reverse maximum burst size, where the cell loss priority is 0+1.
CDVT (microsec)	read/write	Specify the forward/reverse cell delay variation tolerance for this connection in microseconds.
<b>Traffic Descriptors</b> <b>(Forward and Reverse)</b>		
Tagging	read-only	Displays the method of changing a high-priority cell to a low-priority cell for this connection.
UPC	read/write	Specify whether usage parameter control is enabled or disabled on this connection.

**Table 5-18. Add/Modify USF-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Congestion Control</b>		
Strategy	read/write	<p>Specify the type of congestion control on this connection:</p> <p><i>None</i> (default) – This selects no strategy for handling congestion.</p> <p><i>SetEFCI</i> – The <i>Set EFCI</i> option uses the explicit forward congestion indicator to determine if congestion (or impending congestion) exists in a node. When selected, the congested node modifies the EFCI bit in the ATM cell header to indicate congestion.</p> <p>If the equipment connected to the SA unit can use the EFCI bit to adjust its transmission rate, it may lower the connection cell rate to relieve the congestion. EFCI is only set in the UBR queue and affects all connections in the queue of the physical port, therefore, so not select this option if you do not want to use the EFCI strategy on this physical port.</p> <p><i>EarlyPacketDi</i> (Early Packet Discard) – Drops a whole packet to relieve congestion under AAL5 adaptation.</p> <p><i>DropCLP1</i> – Drops low-priority cells (CLP=1) to relieve congestion.</p> <p><i>SetEFCIandEPD</i> – Combines the Set EFCI and Early Packet Discard congestion control options.</p> <p><i>SetEFCIandCLP1</i> – Combines the Set EFCI and EDrop CLP1 congestion control options.</p>
Buffer Size	read/write	<p>Specify the buffer size allocated for controlling congestion on this connection:</p> <p><i>Shallow</i> (default) – Provides the smallest buffer for handling congestion on this connection.</p> <p><i>Medium</i> – Provides a moderately sized buffer for handling congestion on this connection.</p> <p><i>High</i> – Provides the largest buffer for handling congestion on this connection.</p>
New	command button	(The New button is not available in the Add/Modify USF-IWF window because only one interworking function is supported per USF port.)

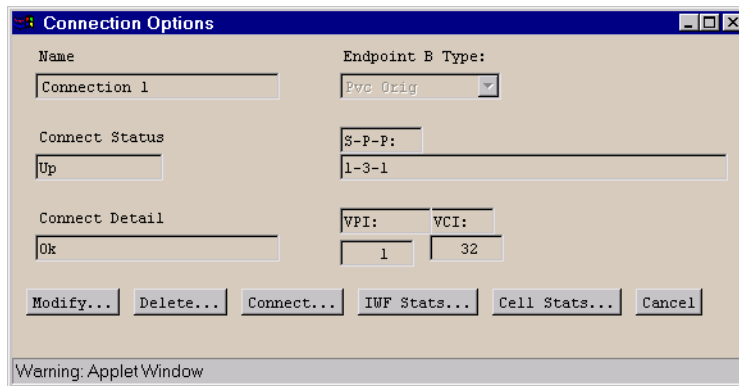
**Table 5-18. Add/Modify USF-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Undo	command button	Undoes any unsaved changes. Unsaved changes are those which have not been saved by selecting Apply or OK.

## Modifying a USF-IWF Connection

To modify a USF-IWF:

1. Select the IWF from the Configured USF Connections list in the Configure USF Connection window (Figure 5-67). The Connection Options window appears (see Figure 5-69):



**Figure 5-69. Connection Options Window (USF-IWF)**

2. Choose the Modify button. The Add/Modify USF-IWF window appears (Figure 5-68).
3. Modify the connection parameters (see Table 5-17), then choose OK.



## Enabling and Disabling a Connection

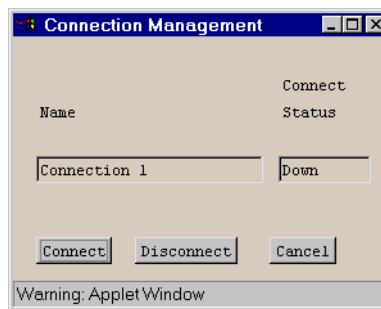
When you add a USF IWF connection, it is automatically set to a connect state of Up, in which the connection is active. The connect state of an IWF is effectively an on/off switch for the connection. You can deactivate a connection temporarily by setting its Connect State to Down, then turn the connection back on by setting the Connect State to Up. You can control the state of a connection from the Add/Modify USF-IWF window or from the Connection Management window, both accessed from the Connection Options window.

*From the Add/Modify USF-IWF window:*

To enable or disable a connection from the Add/Modify USF-IWF window (Figure 5-68 on page 5-107), set the Set Connect Mgmt parameter to Up or Down, then choose OK.

*From the Connection Management window:*

To enable or disable a USF-IWF from the Connection Management window (Figure 5-70), select the Connect or Disconnect button.



**Figure 5-70. Connection Management Window**



Disconnecting an IWF by setting its Connect Status to Down does not remove the connection configuration from the SA unit's database. You can reconnect it at any time, using the procedure described above. To remove a USF-IWF from the SA unit's database, see **"Deleting a USF-IWF Connection"** on page 5-116.

## **Deleting a USF-IWF Connection**

To remove the configuration of a USF-IWF connection from the SA unit's database:

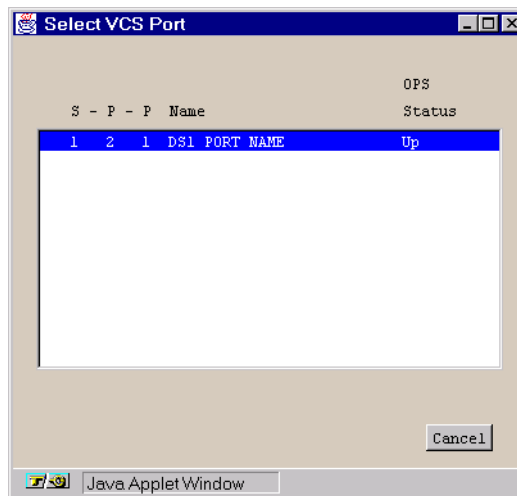
1. Select the USF-IWF from the list in the Configure USF Connection window.
2. When the Connection Options window appears, choose the Delete button.
3. When the Delete USF-IWF window appears, choose the Yes button.

## Configuring Voice Compression Service

To configure Voice compression services:

*From the Main menu:*

1. Choose the Service Management button. The Select Service window appears (Figure 5-1 on page 5-2).
2. Choose the Voice Compression button. The Select VCS Port window appears (see Figure 5-71).



**Figure 5-71. Select VCS Port Window**

3. Select the port you want to configure and the Configure VCS Connection window appears (see Figure 5-72).

*From the Configure DS1 Port window:*

4. After you configure the port of a DS1 Voice Compression POD, as described in “Configuring a DS1 or E1 Port” on page 4-11, choose the Next Logical Layer button in the Configure DS1 Port window and the Configure VCS Connections window appears (see Figure 5-72).

Configure VCS Connection

Events/Alarms... Critical

Port Detail

Slot-Pod-Port: 1 2 1 Port Type: DS1

Port Name: DS1 PORT NAME Port ID: DS1 CIRCUIT I

ADMIN Status: Up OPS Status: Up

PCM Coding Scheme: U Law

VCS Port Stats...

Configured VCS Connections

VCS-IWF Name	Dial Type	Status	Connect Detail
1	Pvc Orig	Up	Ok

Add VCS-IWF... OK Cancel Apply

Select to specify the operating status of this connection.

Warning: AppletWindow

**Figure 5-72. Configure VCS Connection Window**

5. See [Table 5-19](#) for descriptions of the fields and buttons in the Configure VCS Connection window.
6. Choose the Add VCS-IWF button to configure a new VCS interworking function. See [“Adding a VCS-IWF Connection” on page 5-122](#).

**Table 5-19. Configure VCS Connection Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the slot, POD and port number.
Port Type	read-only	Displays the type of port.
Port Name	read-only	Displays the user designation of the port.
Port ID	read-only	Displays the user identification of the port.
ADMIN Status	read-only	Displays the administrative state of the port: up or down.
OPS Status	read-only	Displays the operational state of the port: up or down.
PCM Coding Scheme	read-only	Displays the companding law in use for this VCS port, based on the POD hardware.  <i>U Law</i> – selected for DS1 POD. <i>A Law</i> – selected for E1 POD.
VCS Port Stats	window button	Opens the VCS Ports Statistics window. See <b>“Viewing VCS Port Statistics”</b> on page 6-107 for details.
<b>Configured VCS Connections</b>		
VCS-IWF Name	read-only	Displays the user designation of each configured VCS interworking function on this port. Choosing a VCS-IWF from this list opens the Connection Options window for “optioning” your selection. Optioning includes the ability to modify, delete, connect, disconnect and obtain statistics concerning the VCS-IWF.
Dial Type	read-only	Displays the dial type configured for each configured VCS interworking function on this port: PVC Orig, PVP, ASPVC Term, ASPVC Orig, or SPVC Orig.
Connect Status	read-only	Displays the state of the connection of each configured VCS interworking function on this port: up or down.
Connect Detail	read-only	

**Table 5-19. Configure VCS Connection Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Add VCS-IWF	window button	Opens the Add VCS-IWF window for adding and configuring a new VCS interworking function. See <a href="#">page 5-122</a> .

## Configuring VCS Interworking Functions

This section describes how to:

- Add an VCS-IWF connection (see [page 5-122](#))
- Modify an VCS-IWF connection (see [page 5-127](#))
- Enable or Disable a VCS-IWF connection (see [page 5-128](#))
- Delete an VCS-IWF connection (see [page 5-128](#))

## Adding a VCS-IWF Connection

To add a VCS-IWF connection:

1. Choose the Add VCS-IWF button from the Configure VCS Connection window (see [Figure 5-72 on page 5-118](#)). The Add/Modify VCS-IWF window appears (see [Figure 5-73](#)).

**Add / Modify VCS-IWF**

Service Descriptors

VCS-IWF Name: 1

Endpoint A S-P-P: 1 2 1

Endpoint B Type: Pvc Orig

S-P-P: 1-3-1

VPI: 1

VCI: 32

Set Connect Mgmt: Up

Connect Status: Up

Service Category: Chr 1

Dispatch Delay Factor: 1

Compression...

Traffic Descriptors

CLP=0 CLP=0+1

PCR: 0 1540

SCR: 0 0

MCR: 0 0

MBS: 0 0

CDVT: 0 microsec

UPC: Off

Timeslots

Timeslot	Channel ID	Near End	Far End
1	0	0	
2	1	1	
3	2	2	
4	3	3	
5	4	4	
6	5	5	

Add Timeslot...

Conditioning... Dynamic B/W... New Undo OK Cancel Apply

Specify a VCS-IWF Connection Name (max. 24 characters).

Warning: AppletWindow

**Figure 5-73. Add/Modify VCS-IWF Window**

2. Complete the fields described in [Table 5-20](#) to select the parameters for the new connection.
3. When you are finished defining this connection, choose OK.



**Table 5-20. Add/Modify VCS-IWF Fields and Buttons**

Field/Button	Type	Action/Description
<b>Service Descriptors</b>		
VCS-IWF Name	read/write	Specify a name for this interworking function.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the interworking function.
Endpoint B Type	read/write	<p>Select the dial type for this connection:</p> <p><i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.</p> <p><i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI.</p> <p><i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.</p> <p><i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.</p> <p><i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.</p>
(Address field) S-P-P or AESA	read/write	Specify Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read/write	Specify the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read/write or read-only	<p>For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).</p> <p>For ASPVC Orig dial type, specify the handle being called (read/write).</p>

**Table 5-20. Add/Modify VCS-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Set Connect Mgmt	read/write	Specify the administrative state of the connection.  <i>up</i> (default) – Activates the connection when you click the OK or Apply button.  <i>down</i> – Deactivates the connection when you click the OK or Apply button.
Connect Status	read-only	Displays the operational state of the connection: up or down.
Service Category	read-write	Select the type of service for this IWF:  <i>CBR-1</i> – Selects constant bit rate service for handling digital information, such as video and digitized voice and is represented by a continuous stream of bits. Constant bit rate service requires guaranteed throughput rates and service levels.  <i>RT-VBR1</i> – Selects real time variable bit rate 1 service for packaging special delay-sensitive applications, such as packet video, that require low cell delay variation between endpoints.  <i>RT-VBR2</i> – Selects real time variable bit rate 2 service.  <i>RT-VBR3</i> – Selects <i>real time variable bit rate 3</i> service.  <i>NRT-VBR1</i> (default) – Selects non-real time variable bit rate 1 service for packaging the transfer of long, bursty data streams over a pre-established ATM connection. This service is also used for short, bursty data, such as LAN traffic. CPE protocols adjust for any delay or loss incurred through the use of non-real time VBR.  <i>NRT-VBR2</i> – Selects non-real time variable bit rate 2 service.  <i>NRT-VBR3</i> – Selects non-real time variable bit rate 3 service.  <i>UBR1</i> – Selects unspecified bit rate 1 service for LAN traffic applications primarily. The CPE should compensate for any delay or lost cell traffic.  <i>UBR2</i> – Selects unspecified bit rate 2 service.

**Table 5-20. Add/Modify VCS-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Dispatch Delay Factor	read-only	The Dispatch Delay Factor is the number of voice payloads per subframe. Currently, this value is always 1.
Compression	window button	Opens the VCS-IWF Compression window for selecting a compression scheme for this IWF.
<b>Traffic Descriptors (Forward or Reverse)</b> <b>note: if traffic descriptors are changed, Service Rate field changes to User Defined.</b>		
PCR (CLP=0)	read-only	Displays the forward/reverse peak cell rate, where the cell loss priority is 0.
SCR (CLP=0)	read-only	Displays the forward/reverse sustainable cell rate, where the cell loss priority is 0.
MCR (CLP=0)		Not supported.
MBS (CLP=0)	read-only	Displays the forward/reverse maximum burst size, where the cell loss priority is 0.
PCR (CLP=0+1)	read/write	Specify the forward/reverse peak cell rate, where the cell loss priority is 0+1.
SCR (CLP=0+1)	read-only	Displays the forward/reverse sustainable cell rate, where the cell loss priority is 0+1.
MCR (CLP=0+1)		Not supported.
MBS (CLP=0+1)	read-only	Displays the forward/reverse maximum burst size, where the cell loss priority is 0+1.
CDVT (microsec)	read/write	Specify the forward/reverse cell delay variation tolerance for this connection in microseconds.
<b>Traffic Descriptors (Forward and Reverse)</b>		
Tagging	read-only	Displays the method of changing a high-priority cell to a low-priority cell for this connection.
UPC	read/write	Specify whether usage parameter control is enabled or disabled on this connection.

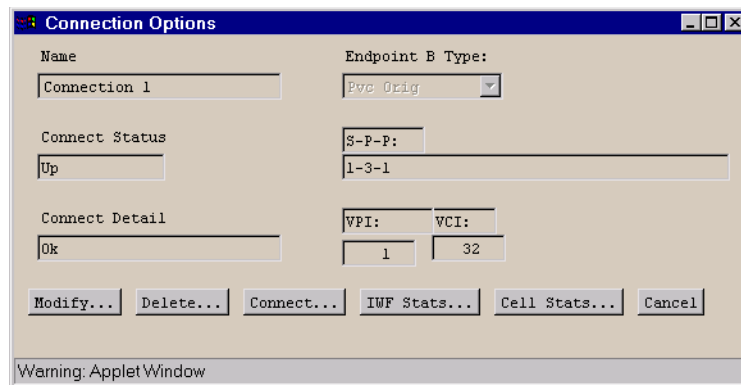
**Table 5-20. Add/Modify VCS-IWF Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Timeslots</b>		
Timeslot	read-only	Displays the configured timeslots for this IWF. Select a timeslot to open the Add/Modify Timeslot window.
Near End Channel ID	read-only	Displays the Near End Channel ID assigned to this timeslot.
Far End Channel ID	read-only	Displays the Far End Channel ID assigned to this timeslot.
Conditioning	n/a	Does not apply to VCS ports.
Dynamic Bandwidth	n/a	Does not apply to VCS ports.
New	command button	Saves the current interworking function and opens a new instance of the Add/Modify VCS-IWF window to create a new VCS interworking function.
Undo	command button	Undoes any unsaved changes. Unsaved changes are those which have not been saved by selecting Apply or OK.

## Modifying a VCS-IWF Connection

To modify a VCS-IWF:

1. Select the IWF from the Configured VCS Connections list in the Configure VCS Connection window (Figure 5-72). The Connection Options window appears (see Figure 5-74):



**Figure 5-74. Connection Options Window (VCS-IWF)**

2. Choose the Modify button. The Add/Modify VCS-IWF window appears (Figure 5-73).
3. Modify the connection parameters (see Table 5-20), then choose OK.

## Enabling and Disabling a Connection

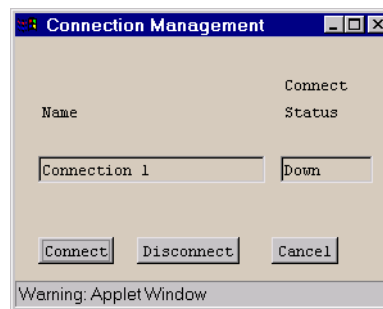
When you add a VCS IWF connection, it is automatically set to a connect state of Up, in which the connection is active. The connect state of an IWF is effectively an on/off switch for the connection. You can deactivate a connection temporarily by setting its Connect State to Down, then turn the connection back on by setting the Connect State to Up. You can control the state of a connection from the Add/Modify VCS-IWF window or from the Connection Management window, both accessed from the Connection Options window.

*From the Add/Modify VCS-IWF window:*

To enable or disable a connection from the Add/Modify VCS-IWF window (Figure 5-73 on page 5-122), set the Set Connect Mgmt parameter to Up or Down, then choose OK.

*From the Connection Management window:*

To enable or disable a VCS-IWF from the Connection Management window (Figure 5-75), select the Connect or Disconnect button.



**Figure 5-75. Connection Management Window**



Disconnecting an IWF by setting its Connect Status to Down does not remove the connection configuration from the SA unit's database. You can reconnect it at any time, using the procedure described above. To remove a VCS-IWF from the SA unit's database, see [“Deleting a VCS-IWF Connection” on page 5-128](#).

## Deleting a VCS-IWF Connection

To remove the configuration of a VCS-IWF connection from the SA unit's database:

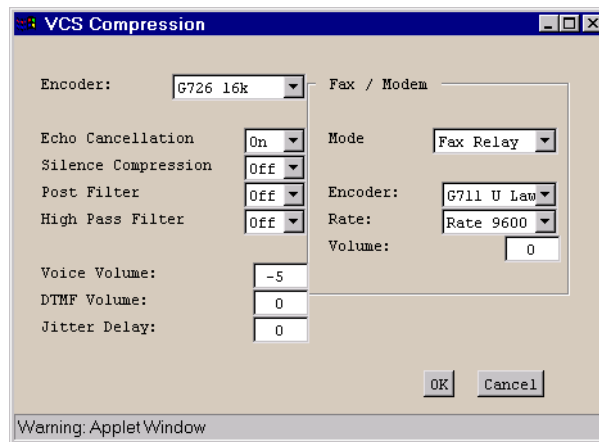
1. Select the VCS-IWF from the list in the Configure VCS Connection window.
2. When the Connection Options window appears, choose the Delete button.
3. When the Delete VCS-IWF window appears, choose the Yes button.

## Setting VCS Compression Options

The traffic on a VCS-IWF may be compressed or modified using a number of options such as various types of encoders, echo cancellation feature, silence suppression, and more.

To configure the compression options for a VCS-IWF:

1. Select the Compression button from the Add/Modify VCS-IWF window (Figure 5-73). The VCS Compression window appears (see Figure 5-76):



**Figure 5-76. VCS Compression Window**

2. Modify the compression parameters (see Table 5-21), then choose OK.

**Table 5-21. VCS Compression Fields and Buttons**

Field/Button	Type	Action/Description
Encoder	read/write	Select the compression algorithm for encoding this VCS-IWF.  (The encoders conform to ITU-standard compression methods.)
Echo Cancellation	read/write	Set echo cancellation to On or Off for this VCS-IWF.
Silence Compression	read/write	Set Silence Compression to On or Off for this VCS-IWF.
Post Filter	read/write	Set the post filter to On or Off for this VCS-IWF. Applies to G.723 and G.729 compression only. Disabling the post filter may improve voice quality when multiple tandem is expected in the channel.

**Table 5-21. VCS Compression Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
High Pass Filter	read/write	Set the high pass filter to On or Off for this VCS-IWF. Applies to G.723 and G.729 compression only. Disabling the high pass filter may improve voice quality when multiple tandem is expected in the channel.
Voice Volume	read/write	Specify the voice volume in dB for the DS0s on this VCS-IWF. Valid range is -31 – 31. To mute, set Voice Volume to -32.
DTMF Volume	read/write	Specify the volume of the DTMF tones in dB for the DS0s on this VCS-IWF. Valid range is -31 – 31. To mute, set DTMF Volume to -32.
Jitter Delay	read/write	Specify the nominal jitter buffer delay (the length of the jitter buffer for incoming packets) in milliseconds. Valid range is 0 – 150.
<b>Fax</b>		
Mode	read/write	Specify the action to be taken when an incoming fax or modem call is detected.  <i>Fax-modem-bypass</i> causes the detection of a modem or FAX to be handled by switching to an alternate voice coder.  <i>Fax-relay</i> causes the detection of FAX calls to be handled by demodulating the FAX tones and transferring the binary data.  <i>None</i> causes no special action to be taken upon detection of FAX or modem.
Encoder	read/write	Select the Encoding algorithm to use when the Fax mode is set to Fax Modem Bypass.
Rate	read/write	Select the maximum allowable FAX transmission rate in bps: 2400, 4800, 7200, 9600, 12000, or 14400.
Volume	read/write	Specify the FAX volume in dB for the DS0s on this VCS-IWF. Valid range is -31 – 31. To mute, set to -32.



## Configuring VCS Timeslots

Each VCS-IWF consists of one or more timeslots, each timeslot representing a single 64 Kbps voice channel (DS0). The number of timeslots actually supported is a function of the POD hardware and the number of DSP mezzanine boards installed. The base DS1 Voice Compression POD handles up to eight timeslots, and may be expanded with 1 or 2 mezzanine boards, each supporting an additional 8 timeslots. The maximum number of timeslots which may be supported by a DS1 Voice Compression POD with two mezzanine boards is 24.



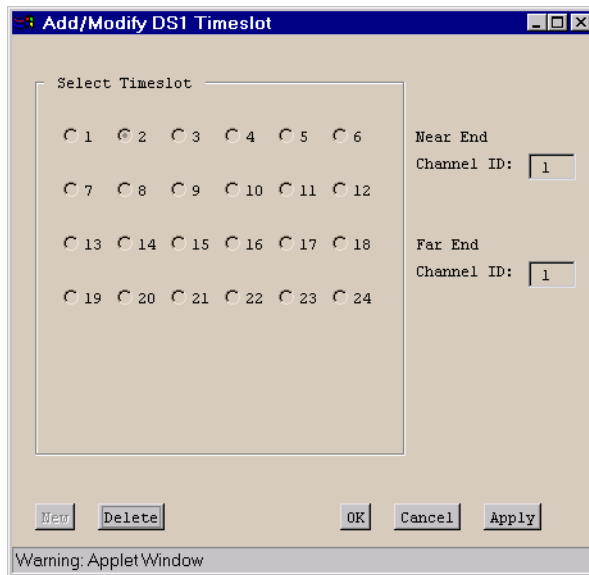
The number of Timeslots is fixed based on the POD hardware. Timeslots assigned to one VCS-IWF are not available to any other VCS-IWF.

Each timeslot is given a unique Channel ID (CID). If you are using only two SA units communicating solely with each other across an ATM cloud, you may find it convenient to accept default values for the Near End and Far End CIDs.

However, the near-end and far-end Channel IDs may be different. For example, consider the case of two remote offices needing to communicate with a central office. Each remote office is using an SA unit equipped with a base Voice Compression POD (no DSP mezzanine cards). Each POD can use near end CID's 0–7. The central office is using an SA unit equipped with a Voice Compression POD and two DSP mezzanine cards, providing CIDs 0–23. Each remote SA unit uses Near End CIDs 0–7, but associates these to a different set of Far End CIDs at the central office's SA unit. Unit A associates Near End CIDs 0–7 with Far End CIDs 0–7, and Unit B associates Near End CIDs 0–7 with Far End CIDs 8–15. At the central office SA unit, the Voice Compression POD has two interworking functions set up (one for each remote office), and the timeslots for these interworking functions are numbered 0–15. Timeslots 0–7 are associated with CIDs 0–7 at Unit A, and Timeslots 8–15 are associated with CIDs 0–7 at Unit B.

To configure a VCS-IWF's timeslots and their Channel IDs:

1. Select the Add Timeslot button from the Add VCS-IWF window's Timeslots field, or select an existing timeslot from the list in the Timeslots field (Figure 5-73). The Add/Modify DS1 Timeslot window appears (see Figure 5-77):



**Figure 5-77. Add/Modify DS1 Timeslot Window**

2. If you selected Add Timeslot, the Select Timeslot radio button will indicate next available Timeslot. For instance, if you have previously configured Timeslots 1, 2, and 3, selecting Add Timeslot will display Timeslot 4 and the Near End and Far End Channel IDs will display the next available channel ID number. You may change the Timeslot number to any available timeslot, and you may alter the Near End/Far End Channel IDs. (For ease of setup, this is not recommended unless necessary - see the example above.)

If you selected a previously configured timeslot from the Timeslots field in the Add/Modify VCS-IWF window, the Select Timeslot window will show the timeslot you've selected and its Near and Far End Channel IDs. Previously configured timeslots may not be modified. To change the parameters of a previously configured timeslot, you must delete it and create a new timeslot with the desired Timeslot number and Near End/Far End Channel IDs.

3. Configure the Timeslots as necessary (see Table 5-22 for field and button details, then choose OK.

**Table 5-22. Add/Modify DS1 Timeslot Fields and Buttons**

Field/Button	Type	Action/Description
Select Timeslot (1 – 24)	read/write for new timeslots; read-only for existing timeslots	For existing timeslots, displays the number of the currently selected timeslot.  When creating a new timeslot, enables you to select an individual timeslot from the field of available timeslots. (Previously configured timeslots are greyed out.)
Near End Channel ID	read/write for new timeslots; read-only for existing timeslots	For existing timeslots, displays the Near End Channel ID of the currently selected timeslot.  When creating a new timeslot, enables you to specify a Channel ID for the near end of the selected timeslot.  The valid range of Channel IDs depends on the number of DSP mezzanine boards installed on the POD:  Base POD range = 0 – 7.  Base POD + 1 DSP board range = 0 – 15.  Base POD + 2 DSP boards range = 0 – 23.
Far End Channel ID	read/write for new timeslots; read-only for existing timeslots	For existing timeslots, displays the Far End Channel ID of the currently selected timeslot.  When creating a new timeslot, enables you to specify a Channel ID for the far end of the selected timeslot.  The valid range of Far End Channel IDs depends on the number of DSP mezzanine boards installed on far end POD; see Near End Channel ID above for details on CID ranges.
New	command button	Saves the current timeslot and opens a new instance of the Add/Modify DS1 Timeslot window, with the next available Timeslot selected and the next available Near End/Far End Channel IDs specified.
Delete	command button	Deletes the current Timeslot.

## What's Next?

After you have configured network services, you can use WebXtend's monitoring functions to check the system, as described in [Chapter 6, "Monitoring an SA Unit."](#)

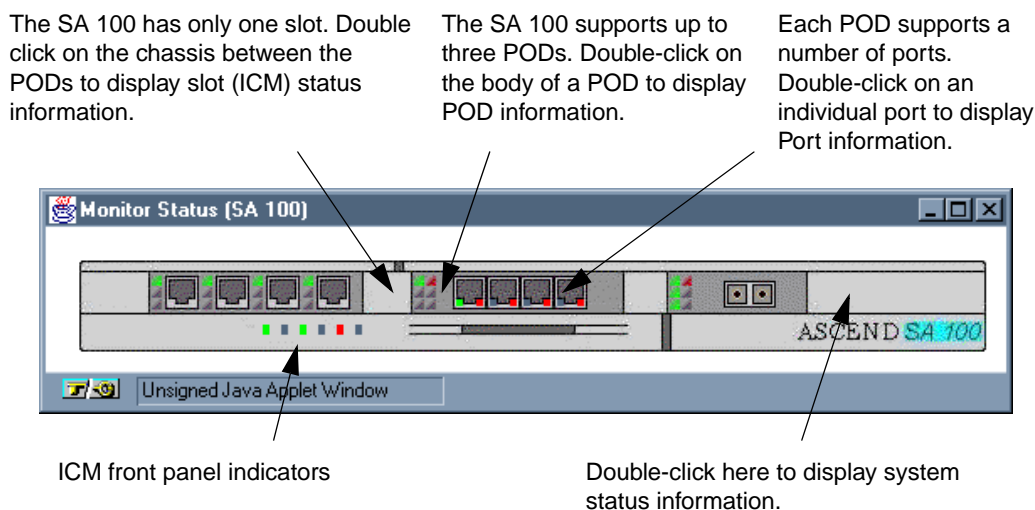
## Monitoring an SA Unit

This chapter describes how to monitor an SA 100, SA 600, or SA 1200 at the following levels:

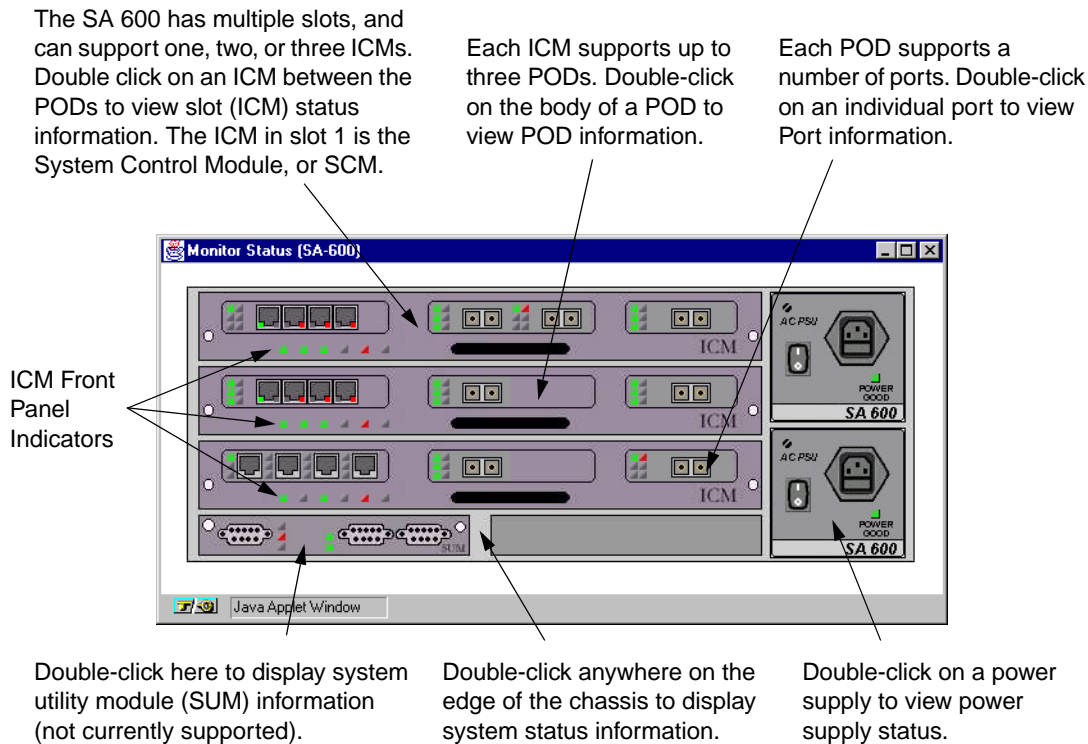
- System (see [page 6-6](#))
- Slots (see [page 6-13](#))
- Protocol Option Devices (PODs) (see [page 6-29](#))
- Ports (see [page 6-40](#))
- Logical layers
- Connections (see [page 6-84](#) for ATM-UNI connections; [page 6-98](#) for NLS connections; [page 6-101](#) for CES-IWF connections; [page 6-103](#) for USF connections; and [page 6-105](#) for VCS-IWF connections)

## Accessing Monitoring Functions

To access the monitoring functions, choose the Monitor Status button from the Main menu. The Monitor Status window appears, displaying a graphical representation of the SA unit's front panel. **Figure 6-1**, **Figure 6-2**, and **Figure 6-3** show the Monitor Status window for an SA 100, SA 600, and SA 1200, respectively.



**Figure 6-1. Monitor Status Window – SA 100**

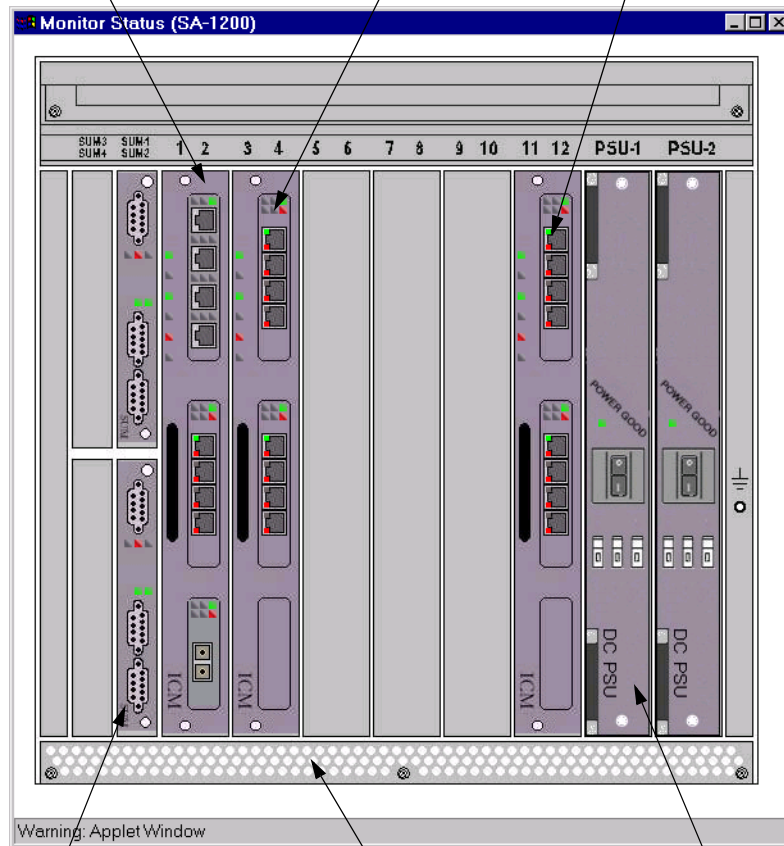


**Figure 6-2. Monitor Status Window – SA 600**

The SA 1200 has multiple slots, and can support up to six ICMs. Double click on an ICM between the PODs to view slot (ICM) status information. The ICM in slot 1 is the System Control Module, or SCM.

Each ICM supports up to three PODs. Double-click on the body of a POD to view POD information.

Each POD supports a number of ports. Double-click on an individual port to view Port information.



Double-click here to display system utility module (SUM) information (not currently supported).

Double-click anywhere on the edge of the chassis to display system status information.

Double-click on a power supply to view power supply status.

**Figure 6-3. Monitor Status Window – SA 1200**

If you move the mouse pointer over this window, callouts appear when the pointer is located over a slot, POD, and/or port, or the system as a whole. Double-clicking the mouse while a callout appears enables you to display status information for the indicated system, slot (ICM), POD, port or power supply.

## ICM Front Panel Indicators

The Monitor Status window displays the current state of the indicator lights on each ICM. Although the labels are not visible in WebXtend, [Table 6-1](#) describes the six indicators on each ICM (read from left to right). For descriptions of the POD front panel indicators, see [“Monitoring PODs” on page 6-29](#).

**Table 6-1. ICM Front Panel Indicators**

Indicator (left to right on ICMs)	Name	Color	Description
PWR	Power	green	Lit when the SA unit has power.
RUN	Running	green	Blinks when the SA unit is running.
S/W	Software	green	Lit when the SA unit’s software is fully operational.
CRI	Critical Alarm	red	Lit when the SA unit detects a critical alarm.*
MAJ	Major Alarm	red	Lit when the SA unit detects a major alarm.*
MIN	Minor Alarm	yellow	Lit when the SA unit detects a minor alarm.*

\*only the most severe alarm detected is displayed. For example, if both a Critical and a Minor alarm are presently detected, only the CRI indicator will be lit.



## SUM Front Panel Indicators (SA 600 and SA 1200 only)

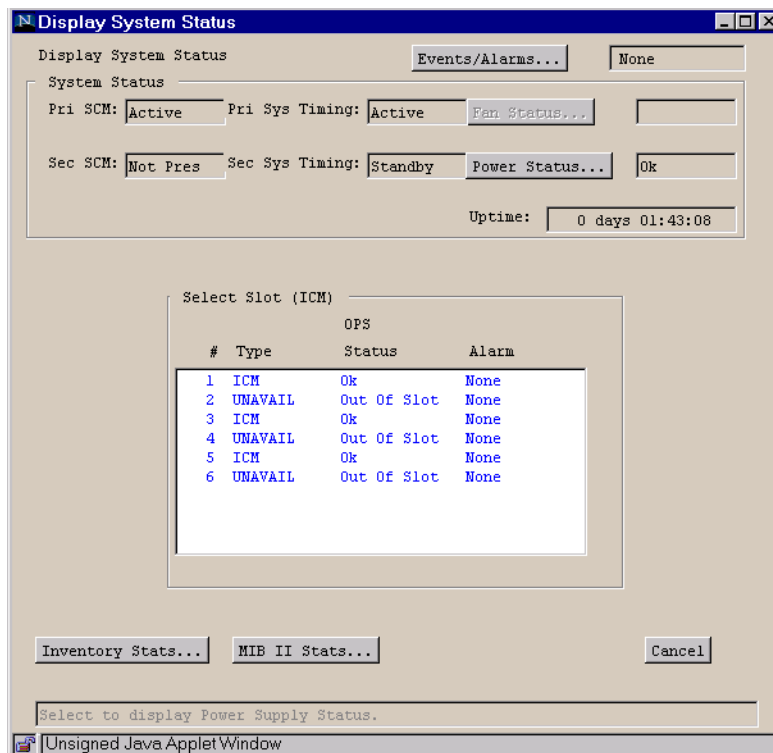
The Monitor Status window also displays the current state of the indicator lights on each SUM. Although the labels are not visible in WebXtend, [Table 6-2](#) describes the five indicators on each SUM.

**Table 6-2. SUM Status Indicators**

Indicator Position	Label	Description
top left	CRI	A critical alarm is the most severe alarm currently detected by the SA unit.
middle left	MAJ	A major alarm is the most severe alarm currently detected by the SA unit.
bottom left	MIN	A minor alarm is the most severe alarm currently detected by the SA unit.
top right	ST	When lit, indicates the operational SUM. (Multiple SUMs are not currently supported; the left hand SUM slot should always contain the currently operational SUM.)
bottom right	SFT	Displays the cumulative software status of the SA unit; green indicates all ICMs are operational; red indicates that one or more slots are non-operational.

## Monitoring System-Level Status

To monitor status at the system level, choose System from the Monitor Status window by double-clicking the blank panels below the PODs or the blank panels to the extreme left or right of the row of PODs (the System callout appears). The Display System Status window appears (see [Figure 6-4](#)).



**Figure 6-4. Display System Status Window**

[Table 6-3](#) describes the buttons and fields in the Display System Status window.

**Table 6-3. Display System Status Fields and Buttons**

Field/Button	Type	Description
<b>System Status</b>		
Pri SCM (System Control Module)	read-only	Displays the state of the primary system control module: Active, No Cfg, or Failed. (The primary SCM is the ICM located in slot 1.)
Pri Sys Timing	read-only	Displays the state of primary system timing: Active, No Cfg, or Failed.
Fan Status	window button	Not supported.
Fan Status	read-only	Not supported.
Sec SCM	read-only	Displays the state of the secondary system control module. A secondary SCM is not currently supported; therefore, this field displays “Not Pres(ent).”
Sec Sys Timing	read-only	Displays the state of secondary system timing: Active, No Cfg, or Failed.
Power Status	window button	(SA 600 and SA 1200 only) Opens the Power Supply Status window, enabling you to view additional information on the SA unit’s power supplies. See <a href="#">“Viewing Power Supply Status Information (SA 600 and SA 1200 only)” on page 6-9.</a>
Power Status	read-only	(SA 600 and SA 1200 only) Displays the state of the SA unit’s power supplies.
Uptime	read-only	Displays the amount of time (days, hours, minutes, seconds) that the SA unit has been operating since it last powered up.
<b>Select Slot (ICM)</b>		
#	read-only	Displays the slot numbers of the SA unit.
Type	read-only	Displays the type of each installed board. Slots containing no ICM display “unavailable.”
OPS Status	read-only	Displays the operational status of each board. Slots containing no ICM display “out of slot.”
Alarm	read-only	Displays the current highest-level alarm, if any, associated with each board.

**Table 6-3. Display System Status Fields and Buttons (Continued)**

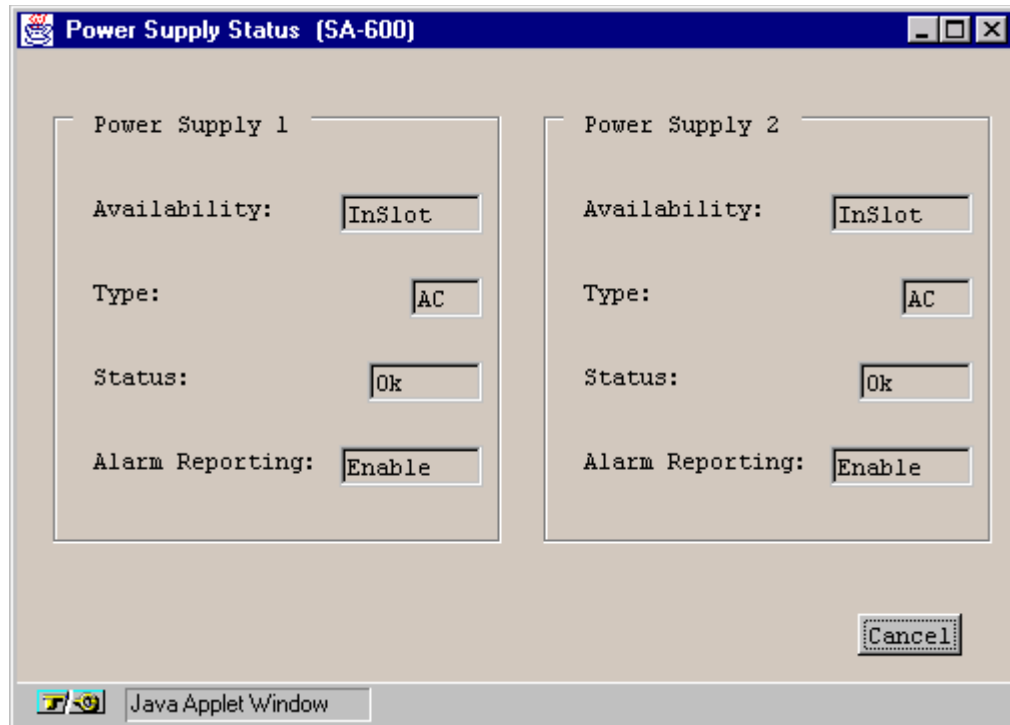
Field/Button	Type	Description
<b>(Other Buttons)</b>		
Inventory Status	window button	Enables you to display rack and backplane information. See “ <b>Viewing System Inventory Information</b> ” on page 6-11.
MIB II Stats	window button	Opens the MIB II Statistics window, enabling you to view information on various Management Information Base groups. See “ <b>Viewing System MIB Statistics</b> ” on page 6-12.

## Viewing Power Supply Status Information (SA 600 and SA 1200 only)

To display status information on the SA 600 or SA 1200 power supplies:

- Double-click on either power supply in the Monitor Status window; or
- Select the Power Status button from the Display System Status window.

Either action opens the Power Supply Status window (see [Figure 6-5](#)), displaying information on installed power supplies.



**Figure 6-5. Power Supply Status Window (SA 600 shown)**

[Table 6-4](#) describes the fields in the Power Supply Status window.

**Table 6-4. Power Supply Status Fields**

Field	Type	Description
<b>Power Supply 1</b>		
Availability	read-only	Displays the state of the upper power supply: InSlot or Unavailable.
Type	read-only	Displays the type of the upper power supply: AC or DC.
Status	read-only	Displays the status of the voltage leaving the upper power supply: OK or Fail.
Alarm Reporting	read-only	Displays whether alarm reporting is enabled or disabled for the upper power supply.
<b>Power Supply 2</b>		
Availability	read-only	Displays the state of the lower power supply: InSlot or Unavailable.
Type	read-only	Displays the type of the lower power supply: AC or DC.
Status	read-only	Displays the status of the voltage leaving the lower power supply: OK or Fail.
Alarm Reporting	read-only	Displays whether alarm reporting is enabled or disabled for the lower power supply.

## Viewing System Utility Module (SUM) Status Information (SA 600 and SA 1200 only)

The Monitor Status window displays the indicators on the System Utility Module (SUM) installed in the SA 600 or SA 1200. (Table 6-2 describes the SUM indicators).

A future enhancement of WebXtend will enable you to view status information on the System Utility Module(s).

## Viewing System Inventory Information

To display “inventory” information about the system, choose the Inventory Stats button on the Display System Status window. The System Inventory Statistics window appears (see Figure 6-6), providing information on the rack type and backplane type for the SA unit (described in Table 6-5).

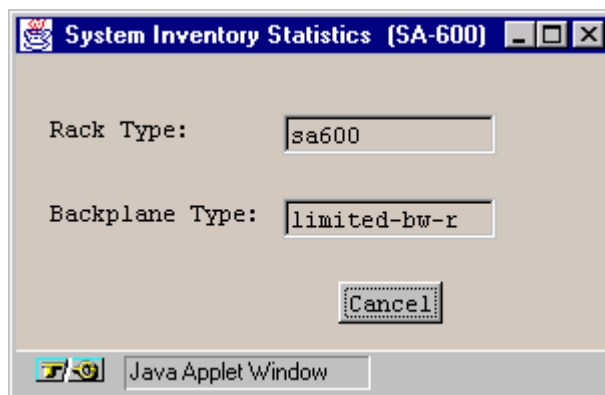


Figure 6-6. System Inventory Statistics (SA 600 shown)

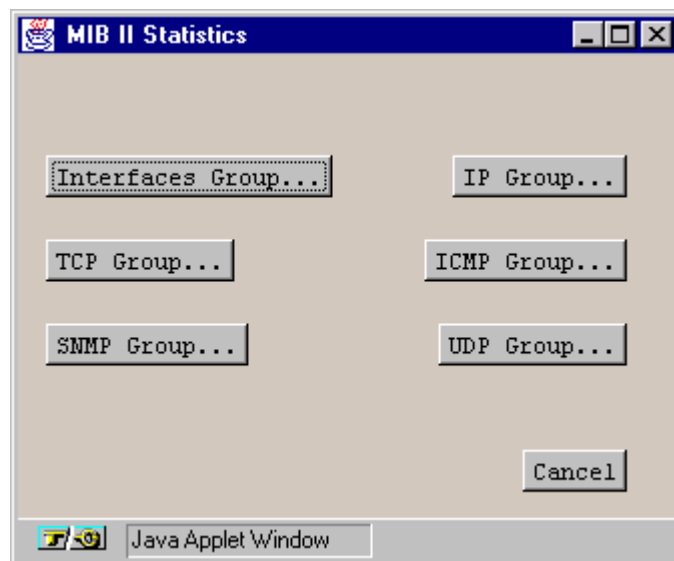
Table 6-5. System Inventory Statistics

SA Unit	Rack Type	Backplane Type
SA 100	sa100	sf-1200-r3
SA 600	sa600	sf-3100-r3
SA 1200	sa1200	sf-6800-r2

## Viewing System MIB Statistics

A MIB is a database of information maintained by the agent that the management can query or set. For details, see RFC-1213, which defines MIB II for use with network management protocols in TCP/IP-based internets. For SA product-specific MIB parameters, see the [Ascend Broadband Access Enterprise MIB](#) (product code #80055).

To display Management Information Base (MIB) statistics about the system, choose the MIB II Stats button on the Display System Status window. The MIB II Statistics window appears (see [Figure 6-7](#)).



**Figure 6-7. MIB II Statistics Window**

Select the button for the group of statistics you want to view (described in [Table 6-6](#).)

**Table 6-6. MIB II Statistics Buttons**

Button	Displays statistics for:
Interfaces Group	MIB II Interface Group.
TCP Group	MIB II TCP Group.
SNMP Group	MIB II SNMP Group.
IP Group	MIB II IP Group.
ICMP Group	MIB II ICMP Group.
UDP Group	MIB II UDP Group.



## Monitoring a Slot



In this section, the terms slot, board, and ICM are used interchangeably. For example, “monitoring the slot” is the same as “monitoring the ICM.”

The Interface Control Module (ICM) in Slot 1 provides control functions for the entire SA unit, and is referred to as the System Control Module (SCM).

- The SA 100 chassis supports only one ICM, so that ICM is always the SCM.
- The SA 600 chassis contains six slots, each of which may accommodate an interface control module (ICM). Currently, a maximum of three ICMs is supported; these ICMs must be installed in slots 1, 3, and 5.
- The SA 1200 chassis contains twelve slots, each of which may accommodate an ICM. Currently a maximum of six ICMs is supported; these ICMs must be installed in slots 1, 3, 5, 7, 9, and 11.

To monitor an ICM, you first select its slot in one of two ways:

- Choose a slot from the Monitor Status window (the callout displays *Slot: #*).
- Choose the system from the Monitor Status window (the callout displays *system*).  
When the Display System Status window appears, select Slot 1 from the Select Slot (ICM) list.

The Display ICM Status window appears (see [Figure 6-8](#)).

Display ICM Status

Events/Alarms... Critical

ICM Status

Slot #: 1 Board Type: ICM

ADMIN Status: Up OPS Status: Ok

Proc Util... 15 PC Card... None

Processor Memory: 16777216 SAR Memory: 4194304

Inventory...

Select POD

#	Type	# Ports	OPS Status	Description
1	IP0D-10-100-ENET	4	Up	Ethernet POD
2	IP0D-DS1-CELL	4	Up	DS1 ATM POD
3	XP0D-DS1-CELL	1	Up	DS1 ATM POD

Cell Hwy Stats... Pro Accel Stats... ATM File Check... Cancel

Select to display Processor Utilization table.

Unsigned Java Applet Window

**Figure 6-8. Display ICM Status Window**

**Table 6-7** describes the fields and buttons in the Display ICM Status window.

**Table 6-7. Display Board Status Fields and Buttons**

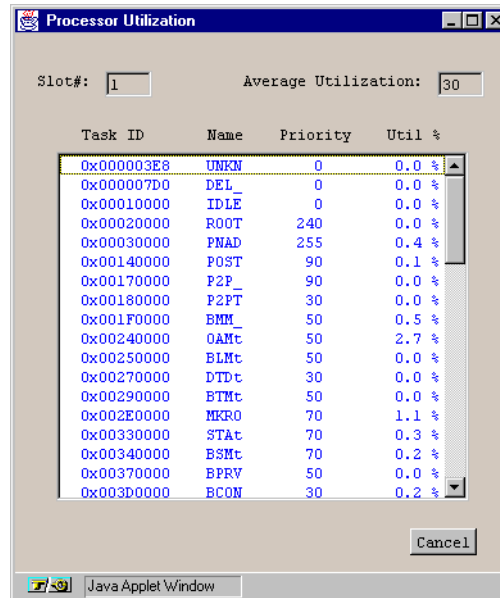
Field/Button	Type	Description
<b>Board Status</b>		
Slot #	read-only	Displays the slot number of the selected ICM.
Board Type	read-only	Displays the type of the board (always ICM).
ADMIN Status	read-only	Displays the administrative state (up or down) of the ICM.
OPS Status	read-only	Displays the operational state (up or down) of the ICM.
Proc Util	window button	Opens a window that displays how the microprocessor on the ICM is being used. See <a href="#">“Viewing Microprocessor Utilization” on page 6-17.</a>
Proc Util	read-only	Displays a percentage indicating how much of the ICM’s microprocessor capacity is being used.
PC Card	window button	Not currently supported.
PC Card	read-only	Not currently supported.
Processor Memory	read-only	Displays the memory available at the ICM’s CPU in bytes.
SAR Memory	read-only	Displays the memory available at the Protocol Accelerator in bytes.
Inventory	window button	Enables you to display a variety of “inventory” information concerning the ICM. See <a href="#">“Viewing Slot Inventory Information” on page 6-19.</a>
<b>Select POD</b>		
#	read-only/ selectable item	Displays the POD number (1, 2, or 3) of each POD installed in the ICM. Choose a POD from the list to view its status information (see <a href="#">“Monitoring PODs” on page 6-29.</a> ).
Type	read-only	Displays the type of each POD installed in the ICM.
# Ports	read-only	Displays the number of ports on each POD installed in the ICM.
OPS Status	read-only	Displays the operational state (up or down) of each POD installed in the ICM.

**Table 6-7. Display Board Status Fields and Buttons (Continued)**

Field/Button	Type	Description
Description	read-only	Displays a brief description of each POD installed in the ICM.
<b>(Other Buttons)</b>		
Cell Hwy Stats	window button	Enables you to pick a cell highway to monitor. Cell highways are circuits on the ICM that are used to relay packets between the CPOD and the IPOD(s), XPOD, and ICM. See <a href="#">“Viewing Slot Cell Highway Statistics”</a> on page 6-22.
Pro Accel Stats	window button	Enables you to display the status of the ICM Protocol Accelerator. See <a href="#">“Viewing Protocol Accelerator Statistics”</a> on page 6-26.
ATM File Check	window button	Enables you to display the status of ATM files. See <a href="#">“Viewing ATM File Check Information”</a> on page 6-27.

## Viewing Microprocessor Utilization

To display how the microprocessor capacity on the ICM is being used, choose the Proc Util button in the Display Board Status window. The Processor Utilization window (see [Figure 6-9](#)) shows how the microprocessor is being used by the system.



**Figure 6-9. Processor Utilization Window**

[Table 6-8](#) describes the Processor Utilization fields.

**Table 6-8. Processor Utilization Fields**

<b>Field (read-only)</b>	<b>Description</b>
Slot#	Displays the slot number of the ICM on which the microprocessor is located.
Average Utilization	<p>Displays a percentage indicating how much of the microprocessor's capacity is being used. This field indicates whether the microprocessor is functioning properly.</p> <p>Normally, this field is in the upper 90s. If the field is inordinately low, it may indicate a problem in the microprocessor or the SA unit's software. However, in such a case, it is likely that WebXtend will fail before you can view this screen.</p>
Task ID	Displays the hexadecimal number assigned to each function performed by the microprocessor.
Name	Displays the acronym of the name assigned to each function performed by the microprocessor.
Priority	Displays the priority assigned to each function, the highest number receiving the highest priority.
Util %	<p>Displays the percentage of the microprocessor's capacity being devoted to each function performed by the microprocessor. This field indicates whether the microprocessor is functioning properly.</p> <p>The majority of functions performed by the microprocessor use less than 10% of the microprocessor's capacity (most functions require less than 1%). The Util % field jumps to a high reading immediately after a task is performed (e.g., when you open a window, the Util % field for the MENU task may rise over 80%). When the Processor Utilization window is updated (every 5 seconds), the Util % for a performed task should reduce. If the Util % field remains high for an extended period of time, it may indicate a problem in the SA unit.</p>

## Viewing Slot Inventory Information

Each ICM and CPOD (a daughter-board of the ICM) contains unique identity information, such as serial number, assembly number, and manufacture date. These statistics are grouped into a category called “inventory” information.

To display inventory information about the ICM, choose the Inventory button on the Display Board Status window. The Board Inventory Statistics window appears (see [Figure 6-10](#)) displaying ICM/CPOD inventory information. [Table 6-9](#) describes the fields in this window. All fields in this window are read-only, with the exception of the Revision Status: Severity pull downs.

The screenshot shows a Java Applet window titled "Board Inventory Statistics". It contains two main sections: "ICM Statistics" and "CPOD Statistics". Each section displays various identification numbers, revision levels, and dates. At the bottom of each section is a "Revision Status" box with "Status" and "Severity" pull-down menus. The ICM section shows a status of "Error", while the CPOD section shows "Ok". Navigation buttons (OK, Cancel, Apply) are at the bottom right, and a severity selection prompt is at the bottom left.

Board Inventory Statistics			
Board Inventory Statistics		Events/Alarms...	Major
<b>ICM Statistics</b>			
Serial #:	1000000289	BOM Rev:	X5G
Assembly #:	750A010000	CFG Rev:	004
Manu. Date:		07-Oct-1997	
Warr. Date:			
Customer Code:		Revision Status	
CLEI Code:	BDIUAA0AAA	Status:	Error
		Severity:	Default
<b>CPOD Statistics</b>			
CPOD Type:	cpod-200-1	H/W Rev:	1
Serial #:	3000000124	BOM Rev:	00
Assembly #:	750A030200	CFG Rev:	001
Manu. Date:		04-Nov-1997	
Warr. Date:			
Customer Code:		Revision Status	
CLEI Code:	BDIUBC0AAA	Status:	Ok
		Severity:	Default
<div>OK Cancel Apply</div>			
Select the Severity Level of this event.			

**Figure 6-10. Board Inventory Statistics Window**

[Table 6-9](#) describes the fields in this window. All fields in this window are read-only, with the exception of the Revision Status: Severity pull downs.

**Table 6-9. Board Inventory Statistics Fields**

Field	Description
<b>ICM Statistics</b>	
Serial #	Displays ICM serial number.
BOM Rev	Displays bill of material (BOM) revision level of the ICM.
Manu. Date	Displays date that the ICM was manufactured.
Assembly #	Displays ICM assembly part number.
CFG Rev	Displays ICM software configuration revision level.
Warr. Date	Displays ICM warranty date (not supported).
Customer Code	Displays ICM customer code (not supported).
CLEI Code	Displays ICM's Common-Language Equipment Identification.
Revision Status: Status	Displays whether the ICM's revision level is valid to operate with the current software revision.
Revision Status: Severity	<p>Selects the severity level of the alarm associated with an out-of-rev ICM: default, info, minor, major, or critical.</p> <p>The default setting (recommended) compares the revision level of the ICM against a database of component revision levels and reports an alarm based on the revision level of the ICM in relation to the installed software. For example, a recent ICM might elicit only an informational alarm, while a very old revision ICM might elicit a critical alarm.</p>
<b>CPOD Statistics</b>	
CPOD Type	Displays the CPOD type installed on the ICM.
H/W Rev	Displays the CPOD hardware revision level.
Manu. Date	Displays date that the CPOD was manufactured.
Serial #	Displays CPOD serial number.
BOM Rev	Displays bill of material revision level of the CPOD.
Warr. Date	Displays CPOD warranty date (not supported).
Assembly #	Displays CPOD assembly part number.
CFG Rev	Displays CPOD software configuration revision level.
Customer Code	Displays customer code for the CPOD (not supported).
CLEI Code	Displays CPOD's Common-Language Equipment Identification.



**Table 6-9. Board Inventory Statistics Fields (Continued)**

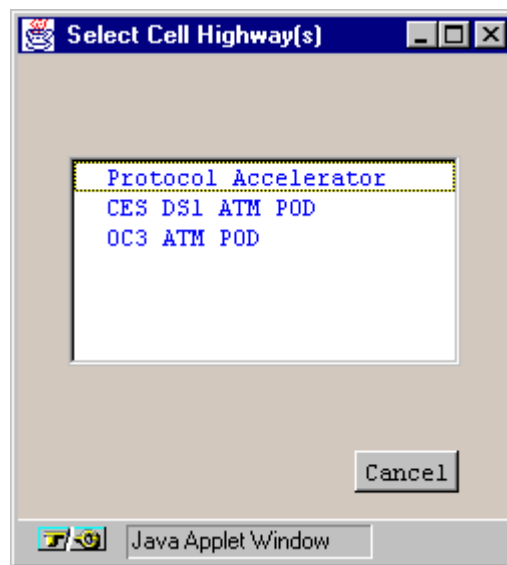
<b>Field</b>	<b>Description</b>
Revision Status: Valid Rev	Displays whether the CPOD's revision level is valid to operate with the current software revision.
Revision Status: Severity	<p>Selects the severity level of the alarm associated with an out-of-rev CPOD: default, info, minor, major, or critical.</p> <p>The default setting (recommended) compares the revision level of the CPOD against a database of component revision levels and reports an alarm based on the revision level of the CPOD in relation to the installed software. For example, a recent CPOD might elicit only an informational alarm, while a very old revision CPOD might elicit a critical alarm.</p>

## Viewing Slot Cell Highway Statistics

Cell highways are the circuits on each ICM used to relay cells between the CPOD and the IPOD(s), XPOD, and Protocol Accelerator. (For more information on cell highways, see [“Connections” on page 1-11.](#))

To display cell highway statistics:

1. Choose the Cell Hwy Stats button in the Display Board Status window. The Select Cell Highway(s) window appears (see [Figure 6-11](#)).



**Figure 6-11. Select Cell Highway(s) Window**

2. Select the cell highway you want to view. The items in the list represent one end of the cell highway with the ICM's CPOD at the other end. For example, if OC3 ATM POD appears in the list, it represents the cell highway between an OC-3C/STM-1 ATM POD and the CPOD.

The Cell Highway/Priority Queue Stats window appears (see [Figure 6-12](#)), displaying a variety of statistics about the selected cell highway. See [Table 6-10](#) for a description of the fields and buttons in this window.

Cell Highway / Priority Queue Stats

Events/Alarms... Major

Detail

Cell Highway(s):  
Protocol Accelerator

Slot#-POD#: 1

Cell Highway Statistics

	Total Congestion Threshold	Empty Cell Buffers	Buffer Congestion State
Hwy 1	100	512	Not Congested
Hwy 2			

Priority Queue

	Queue Priority	Max Queue Size	Congestion Threshold	Max Queue Depth	Congestion State
Hwy 1	High Priority	97	77	0	Not Congested
	Prop Bw A	7	67	0	Not Congested
	Prop Bw B	7	58	0	Not Congested
	Prop Bw C	7	48	0	Not Congested
Hwy 2					

CAC Bandwidth Stats...

Cancel

Select to examine CAC Bandwidth Statistics.

Java Applet Window

Figure 6-12. Cell Highway/Priority Queue Stats Window

**Table 6-10. Cell Highway/Priority Queue Stats Fields and Buttons**

Field/Button	Type	Description
<b>Detail</b>		
Cell Highway(s)	read-only	Displays the selected cell highway (with the CPOD at the other end).
Slot#-POD#	read-only	Displays the location (slot and POD number) of the opposite end of the cell highway (the CPOD is at the other end).
<b>Cell Highway Statistics</b>		
Congestion Threshold (Hwy 1/Hwy 2)	read-only	Displays the congestion threshold of cell highways 1 and 2.
Total Empty Cell Buffers (Hwy 1/Hwy 2)	read-only	Displays the number of empty cell buffers on cell highways 1 and 2.
Buffer Congestion State (Hwy 1/Hwy 2)	read-only	Displays the status of buffer congestion on cell highways 1 and 2.
<b>Priority Queue</b>		
Queue Priority (Hwy 1/Hwy 2)	read-only	Displays the priority queue on cell highways 1 and 2.
Max Queue Size (Hwy 1/Hwy 2)	read-only	Displays the maximum queue size of the priority queue on cell highways 1 and 2.
Congestion Threshold (Hwy 1/Hwy 2)	read-only	Displays priority queue congestion threshold on cell highways 1 and 2.
Max Queue Depth (Hwy 1/Hwy 2)	read-only	Displays the maximum priority queue depth on cell highways 1 and 2.
Congestion State (Hwy 1/Hwy 2)	read-only	Displays the state of priority queue congestion on cell highways 1 and 2.
<b>(Other)</b>		
CAC Bandwidth Stats	window button	Opens a window displaying connection admission control (CAC) bandwidth statistics (see <a href="#">Figure 6-13</a> ). <a href="#">Table 6-11</a> describes the fields in the CAC Bandwidth Stats window.

## Viewing CAC Bandwidth Statistics

To display statistics concerning the Connection Admission Control bandwidth, choose the CAC Bandwidth Stats button in the Cell Highway/Priority Queue Stats window.

The CAC Bandwidth Statistics window appears (see [Figure 6-13](#)), displaying the relevant statistics.

	FBR	VBR
Hwy 1 Total:	420000	840000
Avail:	420000	840000
% Var. to Load:		10
B/W CAC Status:	Enable	
Hwy 2 Total:		
Avail:		
% Var. to Load:		
B/W CAC Status:		

Warning: Applet Window

**Figure 6-13. CAC Bandwidth Stats Window**

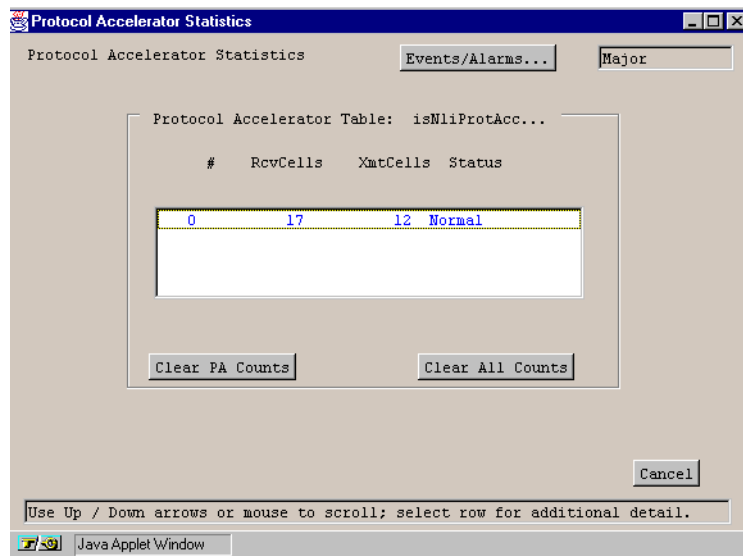
[Table 6-11](#) describes the fields and buttons in this window.

**Table 6-11. CAC Bandwidth Stats Fields**

Field (read-only)	Description
Total FBR	Displays the amount of fixed bandwidth (fixed bit rate, FBR) that has been allocated for connections.
Avail FBR	Displays the remaining fixed bandwidth (fixed bit rate, FBR) available for connections.
Total VBR	Displays the amount of variable bandwidth (variable bit rate, VBR) that has been allocated for connections.
Avail VBR	Displays the remaining variable bandwidth (variable bit rate, VBR) available for connections.
% Var. to Load	Displays the percentage of variable bandwidth that is treated as fixed bandwidth (for the purpose of subtracting fixed bandwidth allocated for connections from the remaining fixed bandwidth available for connections).
B/W CAC Status	Displays whether bandwidth CAC is enabled or disabled.

## Viewing Protocol Accelerator Statistics

To display statistics concerning a Protocol Accelerator, choose the Pro Accel Stats button in the Display Board Status window. The Protocol Accelerator Statistics window appears (see [Figure 6-14](#)), displaying the status of the Protocol Accelerator.



**Figure 6-14. Protocol Accelerator Statistics Window**

[Table 6-12](#) describes the fields and buttons in this window.

**Table 6-12. Protocol Accelerator Statistics Fields and Buttons**

Field/Button	Type	Description
#	read-only	Displays the slot number of the ICM where the Protocol Accelerator is located.
RcvCells	read-only	Displays the number of cells received by the Protocol Accelerator.
XmtCells	read-only	Displays the number of cells transmitted by the Protocol Accelerator.
Status	read-only	Displays the Protocol Accelerator operational status.
Clear PA Counts	command button	Enables you to reset the Protocol Accelerator counts to zero (0).
Clear All Counters	command button	Enables you to reset the RcvCells and XmtCells counters to zero (0).

## Viewing ATM File Check Information

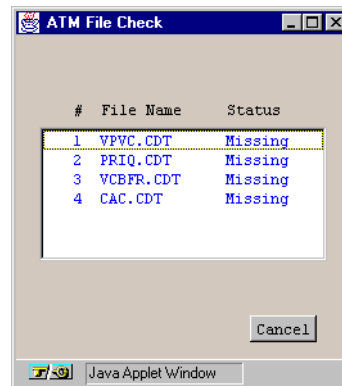


Note: The latest version of WebXtend (3.0) includes the ability to modify CAC parameters through the User Interface, and removes the need to customize CAC parameter files. The ATM File Check screen is no longer needed and may be ignored in favor of the parameters set in the various WebXtend CAC screens.

To display the status of ATM files, choose the ATM File Check button in the Display Board Status window. The ATM File Check window appears (see [Figure 6-15](#)), displaying the status of the ATM Files.



The default status is 'Missing,' meaning no modified file has been detected and default CAC values will be used for that file's parameters.



**Figure 6-15. ATM File Check Window**

[Table 6-13](#) describes the fields in the ATM File Check window.

**Table 6-13. ATM File Check Fields**

Field	Type	Description
#	read-only	Displays the number of the ATM file listed.
File Name	read-only	Displays the name of the ATM file listed. Four file names are listed: vpvc.cdt, priq.cdt, vcbfr.cdt, and cac.cdt.

**Table 6-13. ATM File Check Fields (Continued)**

Field	Type	Description
Status	read-only	Displays the status of the ATM file listed:  <i>Missing</i> (default) - No modified version of the indicated file is present. Default values will be used for this file's parameters.  <i>OK</i> - A modified version of the indicated file is present and the modified values for the parameters of this file will be used.  <i>Error</i> - An error was detected in the indicated CAC file. See Appendix E, "Customizing CAC Parameters" and repeat the steps to remodify, parse, and load the file to the SA unit.



## Monitoring PODs

This section describes how to monitor various Protocol Option Devices (PODs).

You can monitor POD status information:

- On the Monitor Status window by viewing the POD front-panel indicators
- On individual POD status windows

### POD Front Panel Indicators

The Monitor Status window mirrors the state of each front panel indicator of the PODs installed in the ICM(s). You can use these indicators to monitor the state of the SA unit. [Table 6-14](#) through [Table 6-20](#) describe the front panel indicators of the following POD types:

- 10/100 Ethernet POD
- DS1 POD
- E1 POD
- DS3 POD
- E3 POD
- OC3/STM-1 POD
- Universal Serial POD

For details on the various flavors of PODs available, see the [Hardware Installation Guide, Appendix A](#).

**Table 6-14. 10/100 Ethernet POD Front Panel Indicators**

Desig.	Name	Color	Description
ST	POD Status	green	ON when the POD is programmed and in service. OFF when the POD is not configured.
TX	Data Transmitted	green	ON when the POD is sending data.
RX	Data Received	green	ON when the POD is receiving data.

**Table 6-15. DS1 POD Front Panel Indicators**

<b>Desig.</b>	<b>Name</b>	<b>Color</b>	<b>Description</b>
ST	POD Status	green	ON when the POD is programmed and in service.  OFF when the POD is not configured.
TX	Cells Transmitted	green	ON when the POD sends ATM cells.
RX	Cells Received	green	ON when the POD receives ATM cells.
RED	Red Alarm	red	ON when the POD detects a red alarm condition in the received signal, perhaps due to loss of frame, delineation, or pointer.
YEL	Yellow Alarm	yellow	ON when the POD detects a yellow alarm condition in the received signal, i.e., a remote alarm indication exists in the incoming path, perhaps due to a remote defect condition (RDI) or yellow path layer indication on the incoming signal.
AIS	Alarm Indication Signal	yellow	ON when the POD detects an alarm indication signal (AIS) in the received signal, indicating a service interruption failure due to a loss of signal (LOS), out-of-frame (OOF) condition, or internal equipment failure.
(lower left corner of multiport POD connectors)		green	ON when the front panel indicators are reporting the status of that port (as chosen via the PORT SELECT push-button or by a single-click on the desired port).
(lower right corner of multiport POD connectors)		yellow	ON when the link is down for that port.

**Table 6-16. E1 POD Front Panel Indicators**

Desig.	Name	Color	Description
ST	POD Status	green	ON when the POD is programmed and in service.  OFF when the POD is not configured.
TX	Cells Transmitted	green	ON when the POD sends ATM cells.
RX	Cells Received	green	ON when the POD receives ATM cells.
SYN	Sync Alarm	red	ON when the POD detects a sync alarm condition, i.e., the POD is not receiving a signal, perhaps due to loss of frame or delineation.
REM	Remote Alarm Indication	yellow	ON when the POD detects a remote alarm indication in the received signal.
AIS	Alarm Indication Signal	yellow	ON when the POD detects an alarm indication signal (AIS) in the received signal, indicating a service interruption failure due to a loss of signal (LOS), out-of-frame (OOF) condition, or internal equipment failure.
(lower left corner of multiport POD connectors)		green	ON when the front panel indicators are reporting the status of that port (as chosen via the PORT SELECT push-button or by a single-click on the desired port).
(lower right corner of multiport POD connectors)		yellow	ON when the link is down for that port.

**Table 6-17. DS3 POD Front Panel Indicators**

Desig.	Name	Color	Description
ST	POD Status	green	ON when the POD is programmed and in service. OFF when the POD is not configured.
TX	Cells Transmitted	green	ON when the POD sends ATM cells.
RX	Cells Received	green	ON when the POD receives ATM cells.
RED	Red Alarm	red	ON when the POD detects a red alarm condition in the received signal, perhaps due to loss of frame, delineation, or pointer.
YEL	Yellow Alarm	yellow	ON when the POD detects a yellow alarm condition in the received signal, i.e., a remote alarm indication exists in the incoming path, perhaps due to a remote defect condition (RDI) or yellow path layer indication on the incoming signal.
AIS	Alarm Indication Signal	yellow	ON when the POD detects an alarm indication signal (AIS) in the received signal, which indicates a service interruption failure due to a loss of signal (LOS), out-of-frame (OOF) condition, or internal equipment failure.

**Table 6-18. E3 POD Front Panel Indicators**

<b>Desig.</b>	<b>Name</b>	<b>Color</b>	<b>Description</b>
ST	POD Status	green	ON when the POD is programmed and in service. OFF when the POD is not configured.
TX	Cells Transmitted	green	ON when the POD sends ATM cells.
RX	Cells Received	green	ON when the POD receives ATM cells.
SYN	Sync Alarm	red	ON when the POD detects a sync alarm condition, i.e., the POD is not receiving a signal, perhaps due to loss of frame or delineation.
REM	Remote Alarm Indication	yellow	ON when the POD detects a remote alarm indication in the received signal.
AIS	Alarm Indication Signal	yellow	ON when the POD detects an alarm indication signal (AIS) in the received signal, which indicates a service interruption failure due to a loss of signal (LOS), out-of-frame (OOF) condition, or internal equipment failure.

**Table 6-19. OC-3c/STM-1 POD Front Panel Indicators**

<b>Desig.</b>	<b>Name</b>	<b>Color</b>	<b>Description</b>
ST	POD Status	green	ON when the POD is programmed and in service. OFF when the POD is not configured.
TX	Cells Transmitted	green	ON when the POD sends ATM cells.
RX	Cells Received	green	ON when the POD receives ATM cells.
RED	Red Alarm	red	ON when the POD detects a red alarm condition in the received signal, i.e., the POD is receiving a signal that is not synchronized to the incoming SONET/SDH signal, perhaps due to loss of frame, delineation, or pointer.
YEL	Yellow Alarm	yellow	ON when the POD detects a yellow alarm condition in the received signal, i.e., a remote alarm indication exists in the incoming path, perhaps due to a remote defect condition (RDI) or yellow path layer indication on the incoming signal.
AIS	Alarm Indication Signal	yellow	ON when the POD detects an alarm indication signal (AIS) in the received signal, which indicates a service interruption failure due to a loss of signal (LOS), out-of-frame (OOF) condition, or internal equipment failure.

**Table 6-20. Universal Serial POD Front Panel Indicators**

<b>Desig.</b>	<b>Name</b>	<b>Color</b>	<b>Description</b>
ST	POD Status	green	On when the POD is programmed and in service.
TX	Cells Transmitted	green	On when the POD is transmitting data out the serial interface.
RX	Cells Received	green	On when the POD is receiving data from the serial interface.
LOS	Loss of Signal	red	On when the POD detects a loss of DTR and/or RTS if the port is DCE; or loss of DSR and/or CTS if the port is DTE .
LB	Loopback	yellow	On is control signal LL(141) is on or if line or local loopback is initiated by the user.

## Accessing POD Status Windows

To access the POD status windows, you first select the POD in one of three ways:

- Choose (double-click) the POD from the Monitor Status window (the callout displays *slot-POD*).
- Choose (double-click) the slot from the Monitor Status window (the callout displays *slot: #*).

When the Display Board Status window appears, select the POD from the Select POD list.

- Choose the system from the Monitor Status window (callout displays *system*).

In the Display System Status window, select the Slot from the Select Board list.

In the Display Board Status window, select the POD from the Select POD list.

After selecting a POD, the Display POD Status window appears ([Figure 6-16](#)), providing status information on the selected POD.

#	Type	Name	OPS Status	Alarm
1	ETHERNET	Ethernet Port	Up	None
2	ETHERNET	Ethernet Port	Up	None
3	ETHERNET	Ethernet Port	Up	None
4	ETHERNET	Ethernet Port	Up	None

**Figure 6-16. Display POD Status Window**

[Table 6-21](#) describes the fields and buttons in the Display POD Status window.

From the Display POD Status window, you can proceed to the next logical level (a port on this POD) by choosing a port from the Select Port list. This action opens the Display Port Status window for the selected port. See [“Monitoring Ports” on page 6-40](#) for details.

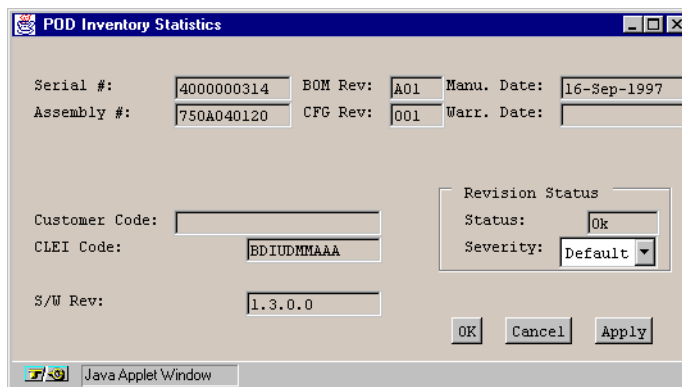


**Table 6-21. Display POD Status Fields and Buttons**

Field/Button	Type	Description
<b>POD Status</b>		
Slot#-POD#	read-only	Displays the location (slot and POD numbers) of the POD.
POD Type	read-only	Displays the type of the POD.
ADMIN Status	read-only	Displays the administrative state of the POD: Up or Down.
OPS Status	read-only	Displays the operational state of the POD: Up or Down.
Inventory	window button	Enables you to display inventory information about the POD. See <b>“Viewing POD Inventory Information”</b> on page 6-38.
<b>Select Port</b>		
#	read-only	Displays the port number of each POD port. Choosing a port from this list opens the Display Port Status window for the selected port.
Type	read-only	Displays the type of each port on this POD.
Name	read-only	Displays the user designation of each port.
OPS Status	read-only	Displays the operational state (up or down) of each port on this POD.
Alarm	read-only	Displays the current highest-level alarm, if any, associated with each port.
<b>(Other Buttons)</b>		
Cell Hwy Stats	window button	Enables you to display statistics about the POD cell highway. See <b>“Viewing POD Cell Highway Statistics”</b> on page 6-39.

## Viewing POD Inventory Information

To display POD “inventory” information, choose the Inventory button in the Display POD Status window. The POD Inventory Statistics window appears (see [Figure 6-17](#)), displaying POD inventory information.



**Figure 6-17. POD Inventory Statistics Window**

[Table 6-22](#) describes the fields in this window. (All fields in this window are read-only except Rev Status: Severity.)

**Table 6-22. POD Inventory Statistics Fields**

Field (read-only)	Description
Serial #	Displays serial number of the POD.
BOM Rev	Displays bill of material revision level of the POD.
Manu. Date	Displays date that the POD was manufactured.
Assembly #	Displays assembly part number of the POD.
CFG Rev	Displays software configuration revision level of the POD.
Warr. Date	Displays warranty date of the POD.
Customer Code	Displays customer code for the POD (not supported).
CLEI Code	Displays the POD’s Common-Language Equipment Identification code.
S/W Rev	Displays software revision level for the POD.
Revision Status: Status	Displays whether the POD’s revision level is valid for operation with the current software revision.

**Table 6-22. POD Inventory Statistics Fields (Continued)**

Field (read-only)	Description
Revision Status: Severity	<p>Selects the severity level of the alarm associated with an out-of-rev POD: default, info, minor, major, or critical.</p> <p>The default setting (recommended) compares the revision level of the POD against a database of component revision levels and reports an alarm based on the revision level of the POD in relation to the installed software. For example, a recent POD might elicit only an informational alarm, while a very old revision POD might elicit a critical alarm.</p>

## Viewing POD Cell Highway Statistics

To display statistics concerning the cell highway between the POD and the CPOD, choose the Cell Hwy Stats button in the Display POD Status window.

The Cell Highway/Priority Queue Stats window appears (see [Figure 6-12 on page 6-23](#)), enabling you to view statistics about the selected cell highway. [Table 6-10 on page 6-24](#) describes the fields and buttons in this window.



Cell Highways statistics are available for ATM Cell PODs only. PODs producing packet-based traffic which must be converted to cells by the Protocol Accelerator (Ethernet PODs for example) do not use the cell highways, and thus have no Cell Highway statistics to view.

## Monitoring Ports

To monitor a port, you first select the port in one of four ways:

- Choose the port from the Monitor Status window (the callout lists the slot, POD, and port).
- Choose the POD containing the port to monitor from the Monitor Status window (the callout lists the slot and POD).

When the Display POD Status window appears, select the port to monitor from the Select Port list box.

- Choose the slot from the Monitor Status window (the callout lists the slot).

When the Display Board Status window appears, select the POD containing the port to monitor from the Select POD list box.

When the Display POD Status window appears, select the port to monitor from the Select Port list box.

- Choose the system from the Monitor Status window (no callout appears).

When the Display System Status window appears, select the appropriate slot (ICM) from the Select Board list box.

When the Display Board Status window appears, select the POD containing the port from the Select POD list box.

When the Display POD Status window appears, select the port from the Select Port list box.

The Display Port Status window appears. The contents of this window varies depending on the type of port you are monitoring. The following sections describe each type of port status window:

- Ethernet Ports (see [page 6-41](#))
- DS1/E1 Ports (see [page 6-43](#))
- DS3/E3 Ports (see [page 6-55](#))
- OC-3/STM-1 Ports (see [page 6-66](#))
- Universal Serial Ports (see [page 6-78](#))

## Monitoring Ethernet Ports

To monitor an Ethernet port, select the port as described in “[Accessing Monitoring Functions](#)” on page 6-2. The Display Ethernet Port Status window appears (see [Figure 6-18](#)), enabling you to monitor the port.

Display Ethernet Port Status

Display Ethernet Port Status    Events/Alarms...    Major

Port Detail

Slot#-POD#-Port#: 1 1 1    Last Change: 0 days 02:25:30

ADMIN Status: Up    OPS Status: Up

Assigned to NLS Group: ☐    NLS Group Name: Management Group

Faults

Alarms: ☐ Link Fail    Defects: ☐ Link Fail

Performance Statistics

RX Packets: 38939    Overflow Count: 0

TX Packets: 22627    Missed Frames: 0

Clear Counters

Next Logical Layer...    Cancel

Select to Clear Counters.

Java Applet Window

**Figure 6-18. Display Ethernet Port Status Window**

[Table 6-23](#) describes the fields and buttons in the Display Ethernet Port Status window.

**Table 6-23. Display Ethernet Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Detail</b>		
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the port.
Last Change	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating since it became active.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
Assigned to NLS Group	read-only	Displays whether the port has been assigned to an NLS group.
NLS Group Name	read-only	Displays the NLS group name.
<b>Faults</b>		
Alarms: Link Fail	read-only	A check mark indicates that a link failure alarm has been detected.
Defects: Link Fail	read-only	A check mark indicates that a link failure defect has been detected.
<b>Performance Statistics</b>		
RX Packets	read-only	Displays the number of Ethernet packets received.
TX Packets	read-only	Displays the number of Ethernet packets transmitted.
Overflow Count	read-only	Displays the number of overflows that have occurred.
Missed Frames	read-only	Displays the number of Ethernet packet frames that have been missed.
Clear Counters	command button	Enables you to set all the counter (numeric) fields in the Performance Statistics frame to zero (0).
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Displays the available NLS groups for this POD. See <a href="#">“Viewing NLS Group Status Information” on page 6-116.</a>

## Monitoring DS1/E1 Ports

To monitor a DS1 port, select the port as described in “[Accessing Monitoring Functions](#)” on page 6-2. The Display DS1/E1 Port Status window appears (see [Figure 6-19](#)).

Display DS1 Port Status

Events/Alarms... Critical

Port Status

Last Change: 0 days 02:29:22

Slot#-POD#-Port#: 1 3 1 Faults... None

ADMIN Status: Up OPS Status: Up

Performance Statistics

LCVs:	0	PCVs:	0	SEFSs:	11
LESSs:	0	ESs:	11	UASs:	78
		BESSs:	0	CSSs:	0
		SESSs:	11		

Clear Counters Intervals...

Next Logical Layer... Cancel

Select to display DS1 Faults.

Java Applet Window

**Figure 6-19. Display DS1/E1 Port Status Window (DS1 shown)**

[Table 6-24](#) describes the fields and buttons in the Display DS1/E1 Port Status window.

**Table 6-24. Display DS1/E1 Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Status</b>		
Last Change	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating.
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the port.
Faults	window button	Enables you to view alarms and defects that have occurred.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
<b>Performance Statistics</b>		
LCVs	read-only	Displays the number of detected line coding violations (LCVs), i.e., the number of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
LESs	read-only	Displays the number of line errored seconds (LESs), i.e., the number of seconds in which one or more coding violations (CVs) were detected since the port came up or since the counters were reset to zero (0).
PCVs	read-only	Displays the number of detected path coding violations (PCVs) since the port came up or since the last reset to zero. In D4 and E1 non-CRC (cyclic redundancy check) formats, PCVs are frame synchronization bit errors. In extended superframe (ESF) and E1-CRC formats, PCVs are CRC errors.



**Table 6-24. Display DS1/E1 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
ESs	read-only	<p>Displays the number of errored seconds (ESs) since the port came up or since the counters were reset to zero, i.e. the number of one-second intervals with one or more:</p> <ul style="list-style-type: none"> <li>• path coding violations (PCVs)</li> <li>• out of frame (OOF) defects</li> <li>• controlled slip events</li> <li>• alarm indication signal (AIS) defect in extended superframe (ESF) and E1-CRC (cyclic redundancy check) formats, or</li> <li>• one or more line coding violations (LCVs) in D4 and E1 non-CRC formats</li> </ul>
BESs	read-only	<p>Displays the number of bursty errored seconds (BES or errored seconds type B) since the port came up or since the counters were reset to zero (0).</p> <p>BES is the number of one-second intervals with no less than two and not more than 319 path coding violation error events, no severely errored frame (SEF) defects, and no detected alarm indication signal (AIS) defects. Controlled slips are not included in this parameter.</p>
SEs	read-only	<p>Displays the number of severely errored seconds (SEs) since the port came up or since the counters were reset to zero (0).</p> <p>For extended superframe (ESF) signals, an SE is a second with 320 or more path coding violation (PCV) error events, one or more out of frame (OOF) defects or a detected Alarm Indication Signal (AIS) defect. For E1-CRC (cyclic redundancy check) signals, an SE is a second with 832 or more PCV error events or one or more OOF defects.</p> <p>For E1 non-CRC signals, an SE is 2048 LCVs or more. For D4 signals, an SE is a count of one-second intervals with framing error events, an OOF defect or 1544 or more LCVs.</p> <p>This parameter (1) does not include controlled slips and (2) is not incremented during unavailable seconds.</p>

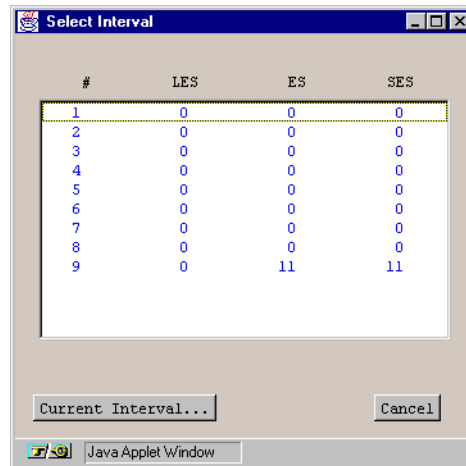
**Table 6-24. Display DS1/E1 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
SEFSs	read-only	Displays the number of severely errored framing seconds (SEFSs) since the port came up or since the counters were reset to zero (0), i.e., the number of seconds with one or more out-of-frame defects or a detected incoming alarm indication signal (AIS).
UASs	read-only	Displays the number of unavailable seconds (UASs) since the port came up or since the counters were reset to zero, i.e., the number of seconds the interface is unavailable due to 10 consecutive severely errored seconds (SESSs) or the onset of a condition leading to a failure.
CSSs	read-only	Displays the number of controlled slip seconds (CSSs) since the port came up or since the counters were reset to zero, i.e., the number of one-second intervals containing one or more controlled slips. Counts of controlled slips can be made accurately only in the path terminating network element of the DS1 signal where the controlled slip takes place.
Clear Counters	command button	Sets all the counter (numeric) fields in the Performance Statistics frame to zero (0).
Intervals	window button	Enables you to view port statistics for the current 15-minute interval or a previous 15-minute interval. (The number of viewable previous intervals depends on the setting of the Set Max Intervals parameter, which you can configure to display the previous 1 to 96 intervals [15 minutes to 24 hours].) See <a href="#">“Viewing Performance Statistics for an Interval”</a> on page 6-47 for details.
<b>(Other Buttons)</b>		
Next Logical Layer	window button	For ports on a DS1/E1 Cell POD, enables you to display statistics concerning the ATM UNI. See <a href="#">“Viewing ATM Status Information on DS1/E1 Cell Ports”</a> on page 6-81.  For ports on a DS1/E1 Circuit POD, enables you to display statistics for a selected CES-IWF. See <a href="#">“Configuring Circuit Emulation Services”</a> on page 5-83.  For ports on a DS1 Voice Compression POD, enables you to display statistics or configure VCS-IWFs. See

## Viewing Performance Statistics for an Interval

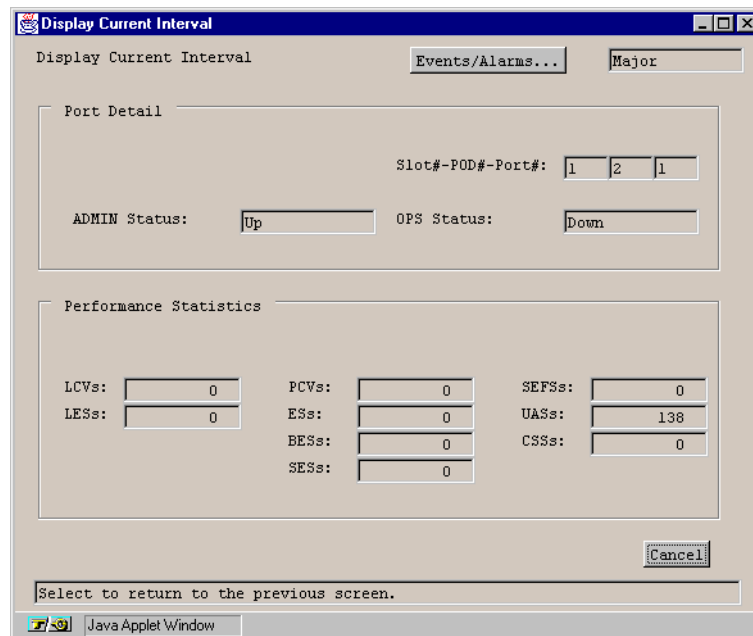
For the current 15-minute interval:

1. Choose the Intervals button in the Display DS1/E1 Port Status window. The Select Interval window appears (see [Figure 6-20](#)).



**Figure 6-20. Select Interval Window**

2. Choose the Current Interval button. The Display Current Interval window appears (see [Figure 6-21](#)), displaying statistics for the current 15-minute interval.



**Figure 6-21. Display Current Interval Window**

3. [Table 6-24 on page 6-44](#) describes the fields in the Display Current Interval window.

*For previous 15-minute intervals:*

To view performance statistics for a previous 15-minute interval:

1. Choose the Intervals button in the Display DS1/E1 Port Status window. The Select Interval window appears (Figure 6-20).
2. Choose the desired interval from the list, using the following criteria:

*To view a specific interval* - Use the # column in the list to calculate which interval you wish to view (interval 1 is the most recent interval). For example, to view an interval that occurred 90 minutes ago, select the interval numbered 6 (90 minutes / 15 minutes = 6 intervals).

*To view an interval containing a specific event* - Use the LES, ES and SES columns to find the interval in which the event occurred, then choose that interval to view.

The Display Intervals window appears (see Figure 6-22).

Display Interval

Display Interval Events/Alarms... Major

Port Detail

Slot#-POD#-Port#: 1 2 1 Interval: 9 10

ADMIN Status: Up OPS Status: Down

Performance Statistics

LCVs:	0	PCVs:	0	SEFSs:	11
LESs:	0	ESSs:	11	UASs:	358
		BESSs:	0	CSSs:	0
		SESSs:	11		

Cancel

Select to return to the previous screen.

Java Applet Window

**Figure 6-22. Display Intervals Window**

The fields in this window are the same as those in the Display DS1/E1 Port Status window except:

- The fields represent statistics for the specified 15-minute interval.

- There is one additional field, the Interval field, which indicates the number of the interval you are viewing and the total number of intervals that are available for viewing (for example, 2 7 indicates that you are viewing the second interval out of a total of seven intervals).

Table 6-24 on page 6-44 describes the Performance Statistics fields.

Viewing Alarms and Defects on DS1/E1 Ports

With the Display DS1/E1 Port Status window open (Figure 6-19), you can view which alarm or defect conditions, if any, have been detected on the DS1/E1 port.

To view the alarms and defects, choose the Faults button. The DS1/E1 Faults window appears (see Figure 6-23 for the DS1 Faults window and Figure 6-24 for the E1 Faults window).

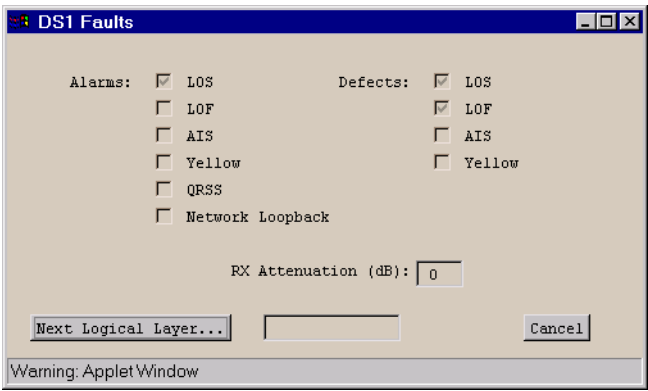


Figure 6-23. DS1 Faults Window

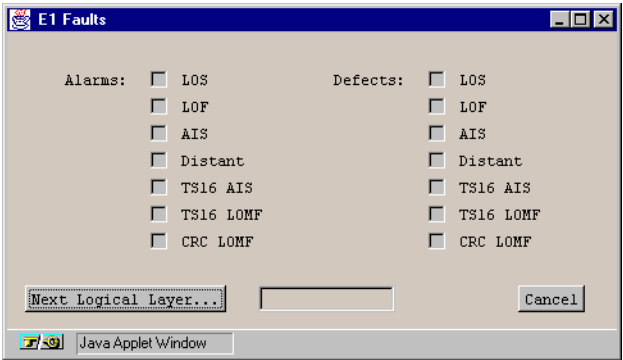


Figure 6-24. E1 Faults Window

Table 6-25 and Table 6-26 describe the fields and buttons in the DS1/E1 Faults windows, respectively.

**Table 6-25. DS1 Faults Fields and Buttons**

Field/Button	Type	Description
LOS Alarms/Defects	read-only	A check mark indicates that a loss of signal (LOS) alarm/defect has been detected.
LOF Alarms/Defects	read-only	A check mark indicates that a loss of frame (LOF) alarm/defect has been detected.
AIS Alarms/Defects	read-only	A check mark indicates that a alarm indication signal (AIS) alarm/defect has been detected.
Yellow Alarms/Defects	read-only	A check mark indicates that a yellow alarm/defect has been detected.
RX Attenuation (dB)	read-only	Displays the configured receive attenuation in decibels.
Next Logical Layer	window button	For ports on a DS1 cell POD, this button enables you to view the status of transmission convergence. See <a href="#">“Viewing the Status of Transmission Convergence on DS1/E1 Cell Ports”</a> on page 6-53.  For ports on a DS1 circuit POD, this button enables you to select a CES-IWF to monitor or configure. See <a href="#">“Configuring Circuit Emulation Services”</a> on page 5-83.
Next Logical Layer	read-only	Displays the current highest-level alarm detected, if any, on the next logical layer.

**Table 6-26. E1 Faults Fields and Buttons**

Field/Button	Type	Description
LOS Alarms/Defects	read-only	A check mark indicates that a loss of signal (LOS) alarm/defect has been detected.
LOF Alarms/Defects	read-only	A check mark indicates that a loss of frame (LOF) alarm/defect has been detected.
AIS Alarms/Defects	read-only	A check mark indicates that a alarm indication signal (AIS) alarm/defect has been detected.
Distant Alarms/Defects	read-only	A check mark indicates that a distant alarm/defect has been detected.
TS16 AIS Alarms/Defects	read-only	A check mark indicates that a time slot 16 alarm indication signal (TS16AIS) alarm/defect has been detected.
TS16 LOMF Alarms/Defects	read-only	A check mark indicates that a time slot 16 loss of multi-frame (TS16LOMF) alarm/defect has been detected.
CRC LOMF Alarms/Defects	read-only	A check mark indicates that a cyclic redundancy check loss of multi-frame (CRCLOMF) alarm/defect has been detected.
Next Logical Layer	window button	For ports on a E1 cell POD, this button enables you to view the status of transmission convergence. See <a href="#">“Viewing the Status of Transmission Convergence on DS1/E1 Cell Ports”</a> on page 6-53.  For ports on a E1 circuit POD, this button enables you to select a CES-IWF to monitor. See <a href="#">“Configuring Circuit Emulation Services”</a> on page 5-83 <a href="#">“Monitoring CES-IWF Connections”</a> on page 6-101.
Next Logical Layer	read-only	Displays the current highest-level alarm detected, if any, on the next logical layer.



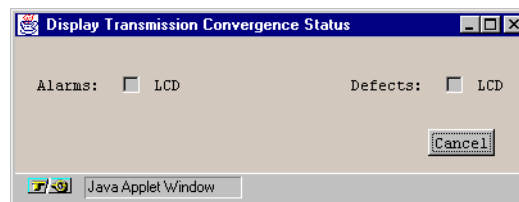
## Viewing the Status of Transmission Convergence on DS1/E1 Cell Ports

From the Display DS1/E1 Port Status window, you can view the state of the transmission convergence on a DS1/E1 cell POD port.

To access this information:

1. Choose the Faults button in the Display DS1/E1 Port Status window (see [Figure 6-19](#)).
2. Choose the Next Logical Layer button in the DS1/E1 Faults window. The Display Transmission Convergence Status window appears (see [Figure 6-25](#)).

Any detected loss of cell delineation alarms or defects is indicated by a check mark in the Alarms or Defects checkboxes.



**Figure 6-25. Display Transmission Convergence Status Window**

### **Viewing CES-IWF Statistics**

From the Display DS1/E1 Port Status window, you can access information about the interworking functions and all statistics on a DS1/E1 circuit POD port. See [“Monitoring CES-IWF Connections” on page 6-101](#) for more information.

## Monitoring DS3/E3 Ports

To monitor a DS3 or E3 port, select the port as described in “[Accessing Monitoring Functions](#)” on page 6-2. The Display DS3 Port Status window (see [Figure 6-26](#)) or Display E3 Port Status window (see [Figure 6-27](#)) appears.

**Display DS3 Port Status**

Events/Alarms... Critical

Port Status

Last Change: 0 days 00:02:04

Slot#-POD#-Port#: 1 2 1 Faults... None

ADMIN Status: Up OPS Status: Up

Performance Statistics

NEAR END					
PCVs:	35	LCVs:	65549	CCVs:	7
PESs:	4	LESs:	5	CESs:	4
PSESs:	0	SEFSs:	0	CSESs:	0
		UASs:	0		

Clear Counters Intervals...

Next Logical Layer... Cancel

Select to display DS3 Faults.

Java Applet Window

**Figure 6-26. Display DS3 Port Status Window**

Display E3 Port Status

Events/Alarms... Critical

Port Status

Last Change: 0 days 00:03:31

Slot#-POD#-Port#: 1 3 1

Faults... None

ADMIN Status: Up OPS Status: Up

Performance Statistics

LCVs:	43226	BIP8:	22
LESs:	3	FEBE:	13
SEFSs:	0		
UASs:	0		

Clear Counters Intervals...

Next Logical Layer... Cancel

Select to display E3 Faults.

Java Applet Window

**Figure 6-27. Display E3 Port Status Window**

Table 6-27 and Table 6-28 describe the fields and buttons in the Display DS3 Port Status and Display E3 Port Status windows, respectively.



The Performance Statistics fields represent a running total since the port came up or since the last reset to zero (0).

**Table 6-27. Display DS3 Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Status</b>		
Last Change	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating.
Slot#-POD#-Port#	read-only	Displays the ports' location (slot, POD, and port #'s).
Faults	window button	Opens a window indicating if any loss of signal, loss of frame, alarm indication signal or yellow alarms have occurred.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
<b>Performance Statistics</b>		
PCVs	read-only	Displays the number of detected P-bit coding violations (PCVs). PCVs occur when the received P-bit code on the DS3 M-frame does not match the locally calculated code.
PESs	read-only	Displays the number of detected near-end P-bit errored seconds (PESs), i.e., the number of seconds with one or more P-coding violations (PCVs), one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
PSESs	read-only	Displays the number of detected P-bit severely errored seconds (PSESs), i.e., the number of seconds with 44 or more P-code violations (PCVs), one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
LCVs	read-only	Displays the number of detected line coding violations (LCVs), i.e., the number of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
LESs	read-only	Displays the count of line errored seconds (LESs), i.e., the number of seconds in which one or more coding violations (CVs) or loss of signal (LOS) errors occurred.

**Table 6-27. Display DS3 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
SEFSs	read-only	Displays the number of detected severely errored framing seconds (SEFSs), i.e., the number of seconds with one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
UASs	read-only	Displays the number of detected unavailable seconds (UASs), i.e., the number of seconds the interface is unavailable (from the onset of 10 contiguous PSEs or the condition leading to a failure).
Near End CCVs	read-only	Displays the number of detected near-end C-bit coding violations (CCVs), i.e., the number of coding violations reported via the C-bits.
Near End CESs	read-only	Displays the number of detected near-end C-bit errored seconds (CESs), i.e., the number of seconds with one or more C-code violations (CCVs), one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
Near End CSEs	read-only	Displays the number of detected near-end C-bit severely errored seconds, i.e., the number of seconds with 44 or more C-code violations (CCVs), one or more out-of-frame (OOF) defects, or detected incoming alarm indication signal (AIS).
Far End CCVs	read-only	Displays the number of detected far-end C-bit coding violations (CCVs), i.e., the number of coding violations reported via the C-bits.
Far End CESs	read-only	Displays the number of detected far-end C-bit errored seconds (CESs), i.e., the number of seconds with one or more C-code violations (CCVs).
Far End CSEs	read-only	Displays the number of detected far-end C-bit severely errored seconds, i.e., the number of seconds with 44 or more C-code violations (CCVs).
Clear Counters	command button	Resets all the counter (numeric) fields in the Performance Statistics frame to zero (0).
Intervals	window button	Enables you to view port statistics for the current 15-minute interval or a previous 15-minute interval. (The number of previous intervals you can view depends on the value of the Set Max Intervals parameter.)  See <a href="#">“Viewing Performance Statistics for an Interval” on page 6-47</a> for instructions on viewing interval statistics.

**Table 6-27. Display DS3 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Enables you to view statistics concerning the ATM layer. See “ <b>Viewing ATM Layer Statistics on DS3/E3 Ports</b> ” on page 6-81.

**Table 6-28. Display E3 Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Status</b>		
Uptime	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating.
Slot#-POD#-Port#	read-only	Displays the ports' location (slot, POD, and port #'s).
Faults	window button	Enables you to see if any loss of signal, loss of frame, alarm indication signal or yellow alarms have occurred.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
<b>Performance Statistics</b>		
LCVs	read-only	Displays the number of detected line coding violations (LCVs), i.e., the number of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
LESs	read-only	Displays the number of line errored seconds (LESs), i.e., the number of seconds in which one or more coding violations (CVs) or one or more loss of signal (LOS) errors occurred.
SEFSs	read-only	Displays the number of detected severely errored framing seconds (SEFSs), i.e., the number of seconds with one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
UASs	read-only	Displays the number of detected unavailable seconds (UASs), i.e., the number of seconds the interface is unavailable (from the onset of 10 contiguous PSESs or the condition leading to a failure).
BIP8	read-only	Displays the number of detected bit interleaved parity 8 errors (BIP8), i.e., the number of detected bit errors in the payload.
FEBE	read-only	Displays the number of detected far end block errors (FEBE), i.e., the number of bit errors in the payload detected at the far end.
Clear Counters	command button	Allows you to set all the counter fields in the Performance Statistics frame to zero (0).



**Table 6-28. Display E3 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
Intervals	window button	Enables you to view port statistics for the current 15-minute interval or a previous 15-minute interval. (The number of previous intervals you can view depends on the setting of the Set Max Intervals parameter.)  See “ <a href="#">Viewing Performance Statistics for an Interval</a> ” on page 6-47 for instructions on viewing interval statistics.
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Enables you to view statistics concerning the ATM layer. See “ <a href="#">Viewing ATM Layer Statistics on DS3/E3 Ports</a> ” on page 6-81.

## Viewing Performance Statistics for an Interval on DS3/E3 Ports

See “Viewing Performance Statistics for an Interval” on page 6-47 for instructions on viewing interval statistics. See Table 6-27 on page 6-57 for DS3 field descriptions or Table 6-28 on page 6-60 for E3 field descriptions.

## Viewing Alarms and Defects on DS3/E3 Ports

From the Display DS3/E3 Port Status window, you can view any alarm or defect conditions that have been detected on the DS3 or E3 port.

To view the alarms and defects:

1. Choose the Faults button. The DS3 Faults or E3 Faults window appears (see Figure 6-28), displaying any faults detected on the port.

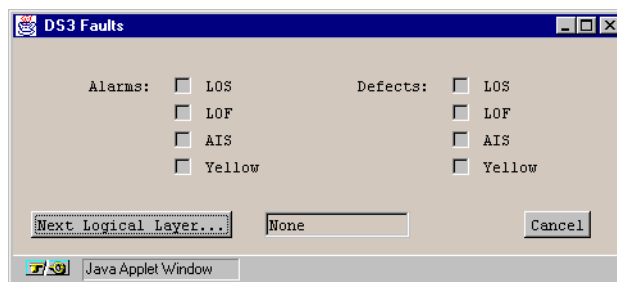


Figure 6-28. DS3/E3 Faults Window (DS3 shown)

Table 6-29 describes the buttons and fields in the DS3 Faults and E3 Faults windows.

Table 6-29. DS3/E3 Faults Fields and Buttons

Field/Button	Type	Description
LOS Alarms/Defects	read-only	A check mark indicates that a loss of signal (LOS) alarm/defect has been detected.
LOF Alarms/Defects	read-only	A check mark indicates that a loss of frame (LOF) alarm/defect has been detected.
AIS Alarms/Defects	read-only	A check mark indicates that an alarm indication signal (AIS) alarm/defect has been detected.
Yellow Alarms/Defects	read-only	A check mark indicates that a yellow alarm/defect has been detected.

**Table 6-29. DS3/E3 Faults Fields and Buttons (Continued)**

Field/Button	Type	Description
Next Logical Layer	window button	If PlcpFrame cell delineation is selected, enables you to view statistics concerning near and far-end phase layer convergence protocol (PLCP) faults. If HcsBased cell delineation is selected, enables you to view the status of transmission convergence. See <a href="#">“Viewing Alarms and Defects on DS3/E3 Ports” on page 6-62</a> for a description of the Display PLCP Status and the Display Transmission Convergence Status windows.
Next Logical Layer	read-only	Displays the current highest-level alarm detected, if any, on the next logical layer.

- Choose the Next Logical Layer button. The window that appears depends on whether PlcpFrame or HcsBased cell delineation is selected for the port in the Configure ATM Interface window.

*If PlcpFrame cell delineation is selected* - The Display PLCP Status window appears (see [Figure 6-29](#)) and you can view statistics concerning near and far-end phase layer convergence protocol (PLCP) faults. See [Table 6-30](#) for descriptions of the fields and buttons in the Display PLCP Status window.

*If HcsBased cell delineation is selected* - The Display Transmission Convergence Status window appears (see [Figure 6-30](#)) and you can see if any loss of cell delineation alarms or defects have been detected, indicated by check marks in the Alarms and Defects check boxes.

The screenshot shows a window titled "Display PLCP Status". It contains two columns of statistics: "NEAR END" and "FAR END".

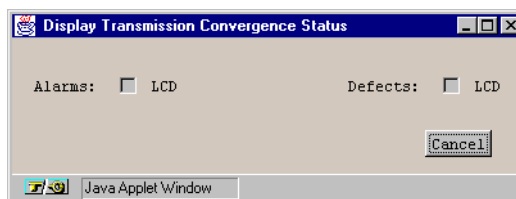
	NEAR END	FAR END
CVs:	58	49
ESs:	6	6
SESs:	3	2
SEFSs:	0	-----
UASs:	0	0
Frame Errors:	570	-----

On the right side, there are checkboxes for "Alarms" and "Defects", each with options for "LOF" and "Yellow".

At the bottom, there are two buttons: "Clear Counters" and "Cancel".

The window is identified as a "Java Applet Window" at the bottom.

**Figure 6-29. Display PLCP Status Window**



**Figure 6-30. Display Transmission Convergence Status Window**

**Table 6-30. Display PLCP Status Fields and Buttons**

Field/Button	Type	Description
Near End CVs	read-only	Displays the number of detected near-end code violations (CVs).
Near End ESs	read-only	Displays the number of detected near-end errored seconds (ESs), i.e., the number of one-second intervals with one or more bipolar violations (BPVs), or one or more excessive zeros (EXZs), or one or more loss of signal (LOS) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Near End SESs	read-only	Displays the number of detected near-end severely errored seconds (SESs), i.e., the number of one-second intervals with 1544 or more bipolar violations (BPVs) plus excessive zeros (EXZs), or one or more loss of signal (LOS) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Near End SEFSs	read-only	Displays the number of detected near-end severely errored framing seconds (SEFSs), i.e., the number of seconds with one or more out-of-frame (OOF) defects, or a detected incoming alarm indication signal (AIS).
Near End UASs	read-only	Displays the number of detected near-end unavailable seconds (UASs), i.e., the number of seconds the interface is unavailable.
Near End Frame Errors	read-only	Displays the number of detected near-end frame errors.
Far End CVs	read-only	Displays the number of detected far-end code violations (CVs).

**Table 6-30. Display PLCP Status Fields and Buttons (Continued)**

Field/Button	Type	Description
Far End ESs	read-only	Displays the number of detected far-end errored seconds (ESs), i.e., the number of one-second intervals with one or more bipolar violations (BPVs), excessive zeros (EXZs), or loss of signal (LOS) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Far End SESs	read-only	Displays the number of detected far-end severely errored seconds (SESs), i.e., the number of one-second intervals with 1544 or more bipolar violations (BPVs) plus excessive zeros (EXZs), or one or more loss of signal (LOS) defects. For a B8ZS-coded signal, BPVs that are part of the zero substitution code, as defined in ANSI T1.102, are excluded.
Far End UASs	read-only	Displays the number of detected far-end unavailable seconds (UASs), i.e., number of seconds the interface is unavailable.
LOF Alarms/Defects	read-only	A check mark indicates that a loss of frame (LOF) alarm/defect has been detected.
Yellow Alarms/Defects	read-only	A check mark indicates that a yellow alarm/defect has been detected.
Clear Counters	command button	Resets the near- and far-end counter fields to zero (0).

## Monitoring OC-3c/STM-1 Ports

To monitor a OC-3c/STM-1 port, select the port as described in “[Accessing Monitoring Functions](#)” on page 6-2. The Display OC-3/STM-1 Status window appears (see [Figure 6-31](#)).

Display OC-3 / STM-1 Port Status

Display OC-3 / STM-1 Port Status    Events/Alarms...    Major

Port Detail

Last Change: 0 days 00:18:45

Slot#-POD#-Port#: 1 3 1    Line Faults...    None

ADMIN Status: Up    OPS Status: Up

Performance Statistics

SECTION	LINE - NEAR END	LINE - FAR END
CVs: 42405	CVs: 20016800	CVs: 15
ESs: 4074	ESs: 12	ESs: 1
SEs: 4071	SEs: 4	SEs: 0
SEFs: 4068	UASs: 0	UASs: 0
	FCs: 0	FCs: 0

Clear Counters    Intervals...

Display Path Status...    Cancel

Select to display OC-3c / STM-1 Line Faults.

Java Applet Window

**Figure 6-31. Display OC-3/STM-1 Port Status Window**

[Table 6-31](#) describes the fields and buttons in the Display OC-3/STM-1 Port Status window.



The Performance Statistics fields represent a running total since the port came up or since last reset to zero (0).

**Table 6-31. Display OC-3/STM-1 Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Detail</b>		
Last Change	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating since it came up.
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the port.
Line Faults	window button	Enables you to view line alarms and defects which may have occurred: loss of signal (LOS), loss of frame (LOF), alarm indication signal line (AIS-L), or remote defect indication line (RDI-L). See <a href="#">“Viewing Alarms and Defects on OC-3c/STM-1 Ports” on page 6-70.</a>
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
<b>Performance Statistics</b>		
Section CVs	read-only	Displays the number of coding violations (CVs) detected in the section layer, i.e., the number of detected BIP-8 errors.
Section ESs	read-only	Displays the number errored seconds detected (ESs) in the section layer, i.e., the number of one-second intervals containing one or more bit interleaved parity (BIP) section errors, one or more loss of signal errors (LOS), or one or more severely errored frame (SEF) defects.
Section SESs	read-only	Displays the number severely errored seconds (SESs) detected in the section layer, i.e., the number of one-second intervals containing 2500 or more bit interleaved parity (BIP) section errors, one or more loss of signal (LOS), or one or more severely errored frame (SEF) defects.
Section SEFs	read-only	Displays the number of severely errored frame (SEFs) defects detected in the section layer, i.e., the number of one-second intervals containing one or more SEF defects.

**Table 6-31. Display OC-3/STM-1 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
Line Near CVs	read-only	Displays the number of near-end coding violations (CVs) detected in the line layer, i.e., the number of detected bit interleaved parity (BIP) errors.
Line Near ESs	read-only	Displays the number of near-end errored seconds (ESs) detected in the line layer, i.e., the number of one-second intervals containing one or more bit interleaved parity (BIP) line errors or one or more alarm indication signal (AIS) defects.
Line Near SESs	read-only	Displays the number of near-end severely errored seconds (SESs) detected in the line layer, i.e., the number of 1 second intervals containing 2500 or more bit interleaved parity (BIP) line errors or one or more alarm indication signal line (AIS-L) defects.
Line Near SEFs	read-only	Displays the number of near-end severely errored framing seconds (SEFs) defects detected in the line layer, i.e., the number of one-second intervals containing one or more SEF defects.
Line Near FCs	read-only	Displays the number of near-end failure counts (FCs) detected in the line layer, i.e., the number of alarm indication signal line (AIS-L) events.
Line Far CVs	read-only	Displays the number of far-end coding violations (CVs) detected in the line layer, i.e., the number of detected bit interleaved parity (BIP) errors.
Line Far ESs	read-only	Displays the number of far-end errored seconds (ESs) detected in the line layer, i.e., the number of one-second intervals containing one or more bit interleaved parity (BIP) line errors, one or more alarm indication signal (AIS) defects.
Line Far SESs	read-only	Displays the number of far-end severely errored seconds (SESs) detected in the line layer, i.e., the number of 1 second intervals containing 2500 or more bit interleaved parity (BIP) line errors, one or more alarm indication signal line (AIS-L) defects.
Line Far SEFs	read-only	Displays the number of far-end severely errored framing seconds (SEFs) defects detected in the line layer, i.e., the number of one-second intervals containing one or more SEF defects.



**Table 6-31. Display OC-3/STM-1 Port Status Fields and Buttons (Continued)**

Field/Button	Type	Description
Line Far FCs	read-only	Displays the number of far-end failure counts (FCs) detected in the line layer, i.e., the number of alarm indication signal line (AIS-L) events.
Clear Counters	command button	Resets all the counter (numeric) fields in the Performance Statistics frame to zero (0).
Intervals	window button	Enables you to view port statistics for the current 15-minute interval or a previous 15-minute interval. (The number of previous intervals you can view depends on the value of the Set Max Intervals parameter.)  See “ <a href="#">Viewing Performance Statistics for an Interval</a> ” on page 6-47 for instructions on viewing interval statistics.
<b>(Other Buttons)</b>		
Display Path Status	window button	Enables you to view statistics concerning the OC-3c/STM-1 path. See “ <a href="#">Viewing Path Statistics on OC-3c/STM-1 Ports</a> ” on page 6-73 for details.

## Viewing Interval Performance Statistics on OC-3c/STM-1 Ports

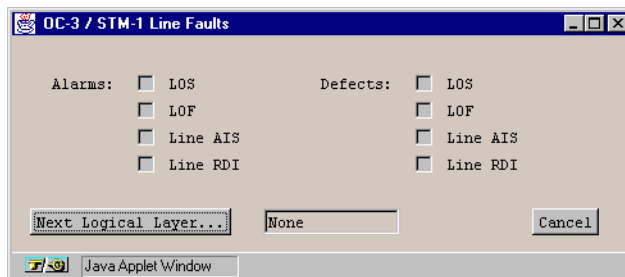
See “[Viewing Performance Statistics for an Interval](#)” on page 6-47 for instructions on viewing interval statistics. See [Table 6-31](#) on page 6-67 for field descriptions.

## Viewing Alarms and Defects on OC-3c/STM-1 Ports

From the Display OC-3/STM-1 Port Status window, you can view any line-level alarm or defect conditions that have been detected on the OC-3c/STM-1 port.

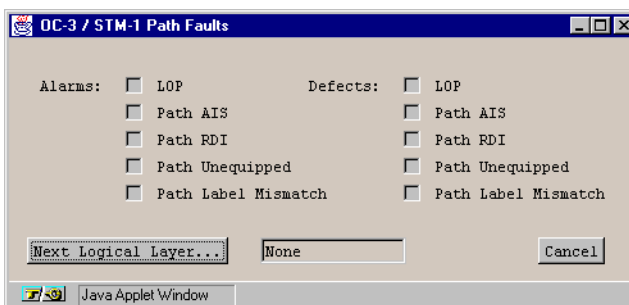
To view the alarms and defects:

1. Choose the Line Faults button. The OC-3c/STM-1 Line Faults window appears (see [Figure 6-32](#)), displaying any faults detected on the OC-3c/STM-1 line.



**Figure 6-32. OC-3/STM-1 Line Faults Window**

2. Choose the Next Logical Layer button. The OC-3/STM-1 Path Faults window appears (see [Figure 6-33](#)), displaying any faults detected on the OC-3c/STM-1 path.



**Figure 6-33. OC-3/STM-1 Path Faults Window**

[Table 6-32](#) and [Table 6-33](#) describe the fields and buttons in the OC-3/STM-1 Line Faults and OC-3/STM-1 Path Faults windows, respectively.

**Table 6-32. OC-3/STM-1 Line Faults Fields and Buttons**

Field/Button	Type	Description
LOS Alarms/Defects	read-only	A check mark indicates that a loss of signal (LOS) alarm/defect has been detected.
LOF Alarms/Defects	read-only	A check mark indicates that a loss of frame (LOF) alarm/defect has been detected.
Line AIS Alarms/Defects	read-only	A check mark indicates that an alarm indication signal line (AIS-L) alarm/defect has been detected.
Line RDI Alarms/Defects	read-only	A check mark indicates that a remote defect indication line (RDI-L) alarm/defect has been detected.
Next Logical Layer	window button	Opens the OC-3/STM-1 Path Faults window, enabling you to view OC-3c/STM-1 path alarms and defects.
Next Logical Layer	read-only	Displays the current highest-level alarm detected, if any, on the OC-3c/STM-1 path.

**Table 6-33. OC-3/STM-1 Path Faults Fields and Buttons**

Field/Button	Type	Description
LOP Alarms/Defects	read-only	A check mark indicates that a loss of pointer (LOP) alarm/defect has been detected.
Path AIS Alarms/Defects	read-only	A check mark indicates that an path alarm indication signal (AIS) alarm/defect has been detected.
Path RDI Alarms/Defects	read-only	A check mark indicates that a path remote defect indication (RDI) alarm/defect has been detected.
Path Unequipped Alarms/Defects	read-only	A check mark indicates that an path signal label unequipped alarm/defect has been detected.
Path Label Mismatch Alarms/Defects	read-only	A check mark indicates that an path signal label mismatch alarm/defect has been detected.
Next Logical Layer	window button	Enables you to view statistics concerning the ATM UNI layer. See <a href="#">“Viewing ATM Status Information on OC-3c/STM-1 Paths” on page 6-81</a> .

**Table 6-33. OC-3/STM-1 Path Faults Fields and Buttons (Continued)**

Field/Button	Type	Description
Next Logical Layer	read-only	Displays the current highest-level alarm detected, if any, on the OC-3c/STM-1 path.

## Viewing Path Statistics on OC-3c/STM-1 Ports

From the Display OC-3/STM-1 Port Status window, you can access status information related to the OC-3c/STM-1 path. To view this information, choose the Display Path Status button. The Display OC-3/STM-1 Path Status window appears (see [Figure 6-34](#)).

Display OC-3 / STM-1 Path Status

Events/Alarms... Major

Interface Detail

Slot#-POD#-Port#: 1 3 1 Path Faults... None

ADMIN Status: Up OPS Status: Up

Performance Statistics

PATH - NEAR END		PATH - FAR END	
CVs:	39721	CVs:	5530
ESs:	4070	ESs:	4071
SESSs:	4069	SESSs:	4069
UASs:	12	UASs:	0
FCs:	1	FCs:	1

Clear Counters Intervals...

Next Logical Layer... Cancel

Select to display OC-3c / STM-1 Path Faults.

Java Applet Window

**Figure 6-34. Display OC-3/STM-1 Path Status Window**

[Table 6-34](#) describes the fields and buttons in the Display OC-3/STM-1 Path Status window.



The Performance Statistics fields represent a running total that has been tallied since the path came up or since last reset to zero (0).

**Table 6-34. Display OC-3/STM-1 Path Status Fields and Buttons**

Field/Button	Type	Description
<b>Interface Detail</b>		
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the path.
Path Faults	window button	<p>Enables you to view any of the following alarms and defects that may have occurred:</p> <ul style="list-style-type: none"> <li>• Loss of pointer (LOP)</li> <li>• Path alarm indication signal (AIS)</li> <li>• Path remote defect indication (RDI)</li> <li>• Path signal label unequipped</li> <li>• Path signal label mismatch.</li> </ul> <p>See “<b>Viewing Alarms and Defects on OC-3c/STM-1 Ports</b>” on page 6-70 for a description of this window.</p>
ADMIN Status	read-only	Displays the administrative state of the path: Up or Down.
OPS Status	read-only	Displays the operational state of the path: Up or Down.
<b>Performance Statistics</b>		
Path - Near End CVs	read-only	Displays the number of coding violations (CVs) detected in the near-end path layer, i.e., the number of detected BIP-8 errors.
Path - Near End ESs	read-only	Displays the number errored seconds detected (ESs) in the near-end path layer, i.e., the number of one-second intervals containing one or more BIP-8 section errors, one or more loss of signal errors (LOS), or one or more severely errored frame (SEF) defects.
Path - Near End SESs	read-only	Displays the number severely errored seconds (SESs) detected in the near-end path layer, i.e., the number of one-second intervals containing 2400 or more BIP-8 section errors, one or more loss of signal (LOS), or one or more severely errored frame (SEF) defects.

**Table 6-34. Display OC-3/STM-1 Path Status Fields and Buttons  
(Continued)**

Field/Button	Type	Description
Path - Near End UASs	read-only	Displays the number unavailable seconds (UASs) detected in the near-end path layer, i.e., the number of seconds the path is unavailable.
Path - Near End FCs	read-only	Displays the number of near-end failure counts (FCs) detected in the path layer, i.e., the number of alarm indication signal line (AIS-L) events.
Path - Far End CVs	read-only	Displays the number of coding violations (CVs) detected in the far-end path layer, i.e., the number of detected BIP-8 errors.
Path - Far End ESs	read-only	Displays the number errored seconds detected (ESs) in the far-end path layer, i.e., the number of one-second intervals containing one or more BIP-8 section errors, one or more loss of signal errors (LOS), or one or more severely errored frame (SEF) defects.
Path - Far End SESs	read-only	Displays the number severely errored seconds (SESs) detected in the far-end path layer, i.e., the number of one-second intervals containing 2400 or more BIP-8 section errors, one or more loss of signal (LOS), or one or more severely errored frame (SEF) defects.
Path - Far End UASs	read-only	Displays the number unavailable seconds (UASs) detected in the far-end path layer, i.e., the number of seconds the path is unavailable.
Path - Far End FCs	read-only	Displays the number of far-end failure counts (FCs) detected in the path layer, i.e., the number of alarm indication signal line (AIS-L) events.
Clear Counters	command button	Resets all the counter (numeric) fields in the Performance Statistics frame to zero (0).
Intervals	window button	Enables you to view port statistics for the current 15-minute interval or a previous 15-minute interval. (The number of previous intervals you can view depends on the setting of the Set Max Intervals parameter.)  See <a href="#">“Viewing Performance Statistics for an Interval” on page 6-47</a> for instructions on viewing interval statistics.

**Table 6-34. Display OC-3/STM-1 Path Status Fields and Buttons  
(Continued)**

Field/Button	Type	Description
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Enables you to view ATM layer statistics. See “ <b>Viewing ATM Status Information on OC-3c/STM-1 Paths</b> ” on page 6-81.

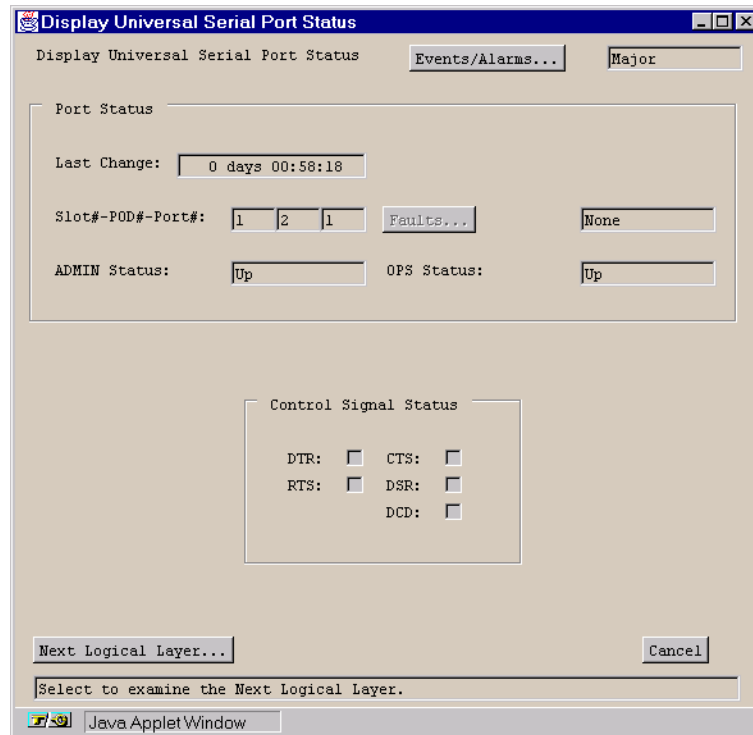


## **Viewing Interval Performance Statistics on OC-3c/STM-1 Paths**

See “[Viewing Performance Statistics for an Interval](#)” on [page 6-47](#) for instructions on viewing interval statistics. See [Table 6-34](#) on [page 6-74](#) for field descriptions.

## Monitoring Universal Serial Ports

To monitor a Universal Serial port, select the port as described in “[Accessing Monitoring Functions](#)” on page 6-2. The Display Universal Serial Port Status window appears (see [Figure 6-35](#)).



**Figure 6-35. Display Universal Serial Port Status Window**

[Table 6-35](#) describes the fields and buttons in the Display Universal Serial Port Status window.

**Table 6-35. Display Universal Serial Port Status Fields and Buttons**

Field/Button	Type	Description
<b>Port Detail</b>		
Last Change	read-only	Displays the amount of time (days, hours, minutes, seconds) that the port has been operating since it became active.
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the port.
ADMIN Status	read-only	Displays the administrative state of the port: up or down.
OPS Status	read-only	Displays the operational state of the port: up or down.
Faults	window button	Opens a window displaying any alarms and defects which have occurred.
Faults	read-only	Displays the highest-level fault currently detected on this port.
<b>Control Signal Status</b>		
DTR RTS CTS DSR DCD	read-only	These checkboxes indicate the presence (checked) or absence of various data control signals, as read at the port's physical interface.  The contents of these fields depends upon the type of cable connected to the port's physical interface.
<b>(Other Buttons)</b>		
Next Logical Layer	window button	Enables you to access status information concerning any interworking functions on this port. See <a href="#">“Configuring USF Interworking Functions” on page 5-106</a> for Serial Frame interworking functions or <a href="#">“Configuring CES Interworking Functions” on page 5-88</a> for Serial CES interworking functions.

## Monitoring the ATM Layer

For ATM UNI ports, the ATM Layer itself may be monitored. The Display ATM Status window (Figure 6-36) provides a variety of ATM performance statistics, depending on the type of ATM port selected. There are minor differences in the fields displayed for each type of ATM port; these are detailed in Table 6-36, which describes the fields and buttons in the Display ATM Status window.

The screenshot shows a Java Applet window titled "Display ATM Status". It contains several sections and controls:

- Top Bar:** Includes a "Display ATM Status" label, an "Events/Alarms..." button, and a "Critical" status indicator.
- Interface Detail Section:**
  - Slot#-POD#-Port#: 1 2 1
  - ADMIN Status: Up
  - OPS Status: Up
- Performance Statistics Section:**
  - TX Cell Count: 96
  - RX Cell Count: 96
  - Uncorrectable HCSs: 122
  - Idle Cell Count: 69409282
  - A "Clear Counters" button is located below these statistics.
- Bottom Bar:** Includes buttons for "Service Management...", "PLCP Status...", "TC Status...", and "Cancel". Below these is a text field labeled "Select to Clear Counters." and a "Java Applet Window" status bar.

Figure 6-36. Display ATM Status Window (DS3 ATM port shown)

### **Viewing ATM Status Information on DS1/E1 Cell Ports**

To view ATM Layer status information on a DS1/E1 Cell port:

At the Display DS1/E1 Port Status window ([Figure 6-19](#)), choose the Next Logical Layer button. The Display ATM Status window appears (see [Figure 6-36](#)), providing information on the status of the ATM UNI on the port.

### **Viewing ATM Layer Statistics on DS3/E3 Ports**

To view ATM Layer status information on a DS3/E3 Cell port:

At the Display DS3/E3 Port Status window, choose the Next Logical Layer button. The Display ATM Status window appears (see [Figure 6-36](#)), providing information on the status of the ATM UNI on the port.

### **Viewing ATM Status Information on OC-3c/STM-1 Paths**

To view ATM Layer status information on a OC-3/STM-1 Cell port:

At the Display OC-3/STM-1 Path Status window, choose the Next Logical Layer button. The Display ATM Status window appears (see [Figure 6-36](#)), providing information on the status of the ATM UNI on the port.

**Table 6-36. Display ATM Status Fields and Buttons**

Field/Button	Type	Description
<b>Interface Detail</b>		
Slot#-POD#-Port#	read-only	Displays the location (slot, POD, and port numbers) of the port.
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
<b>Performance Statistics</b>		
TX Cell Count	read-only	Displays number of ATM cells transmitted.
Correctable HCSs (OC3-c/STM-1 only)	read-only	Displays number of correctable header checksum sequences (HCSs), the number of errors detected and repaired in ATM cell headers.
Uncorrectable HCSs	read-only	Displays number of uncorrectable header checksum sequences (HCSs), that is, the number of uncorrectable errors detected in ATM cell headers.
RX Cell Count	read-only	Displays number of ATM cells received.
Idle Cell Count (DS1/E1 and DS3/E3 only)	read-only	Displays number of idle cells generated.
Clear Counters	command button	Resets all the counter (numeric) fields in the Performance Statistics frame to zero (0).
<b>Faults (OC3-c/STM-1 only)</b>		
Alarms LCD	read-only	A check mark indicates that a loss of cell delineation (LCD) alarm was detected.
Defects LCD	read-only	A check mark indicates that a loss of cell delineation (LCD) defect was detected.
<b>(Other Buttons)</b>		
Service Management	window button	Enables you to view status information concerning ATM connections. See <b>“Monitoring ATM-UNI Connections”</b> on page 6-87.

**Table 6-36. Display ATM Status Fields and Buttons (Continued)**

Field/Button	Type	Description
PLCP Status (DS3/E3 only)	window button	If PlcpFrame cell delineation is selected, enables you to view statistics concerning near-end and far-end phase layer convergence protocol (PLCP) faults. See “ <a href="#">Viewing Alarms and Defects on DS3/E3 Ports</a> ” on page 6-62 for a description of the Display PLCP Status window.
TC Status (DS1/E1 and DS3/E3 only)	window button	If HcsBased cell delineation is selected, enables you to view the status of transmission convergence. See “ <a href="#">Viewing the Status of Transmission Convergence on DS1/E1 Cell Ports</a> ” on page 6-53 or “ <a href="#">Viewing Alarms and Defects on DS3/E3 Ports</a> ” on page 6-62 for a description of the Display Transmission Convergence Status window.

## Monitoring Connections

Thus far, this chapter has approached monitoring from a system-, port- and interface-centric point of view. The next level beyond monitoring port-level and ATM Interface-level information is to view information on individual connections.

The connections made from interface to interface are monitored in similar manners across all connection types (ATM-UNI, NLS, CES, etc.) using the Connections window and Connection Options window. As discussed in the beginning of Chapter 5, the Connections window provides a single central tool for monitoring and configuring connections on a port.

The Connections window for each service type is similar in layout, with the top portion of the window displaying port-detail information (NLS group information for the Configure NLS Tunnel window) and the lower portion of the window listing configured connections and providing a button for adding a new connection. (Each service type is discussed independently in the following sections.)

The Connection Options window offers a variety of management and monitoring functions. The Modify, Delete, and Connect buttons enable you to change the connection's parameters, delete the connection, or set the connection's Administrative Status to Up or Down. The IWF Stats button and Cell Stats buttons enable you to view statistics regarding the non-ATM and ATM sides of a connection.

ATM UNI connections (from DS1/E1 Cell PODs, IMA PODs, DS3/E3 PODs, and OC-3/STM-1 PODs) are shown in the ATM UNI Connections window.

Adaptation services have corresponding Connections windows for configuring and monitoring connections. NLS connections (tunnels) are configured and monitored using the Native LAN Service Tunnels window. Universal Serial Frame connections are configured and monitored using the Configure USF Connections window. Circuit Emulation Service connections are configured and monitored using the Configure CES Connections window. Voice Compression Service connections are configured and monitored using the Configure VCS Connections window.

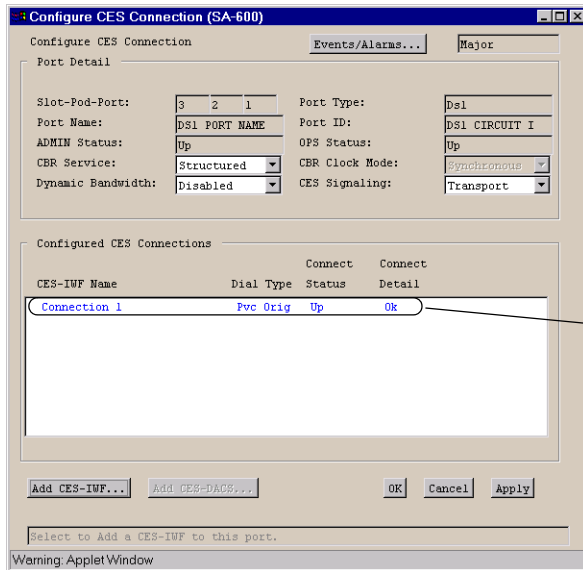
The Connections window may be accessed by selecting:

- the Service Management button from a Configure ATM Interface window,
- the Tunnels button from the NLS Group Options window, or
- the Next Logical Layer button from the Configure Port window of a non-ATM port.

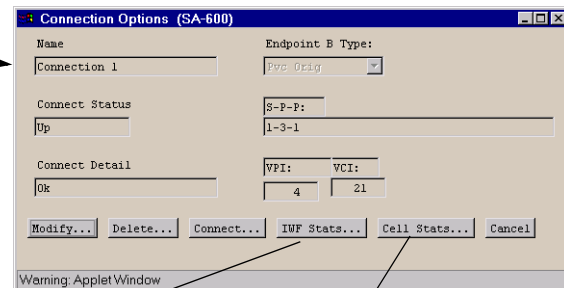
The general procedure for monitoring connections is shown in [Figure 6-37](#). The procedure is explained beginning at the Connections window (i.e., after selecting a service and an individual port). The details of each dialog box you may access are covered in complete detail throughout the rest of this chapter.



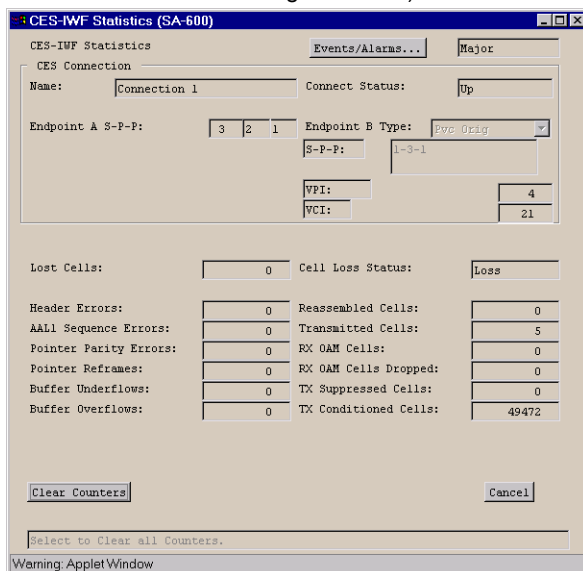
1. Beginning at the Connections window for the desired port, select the connection from the Configured Connections list.



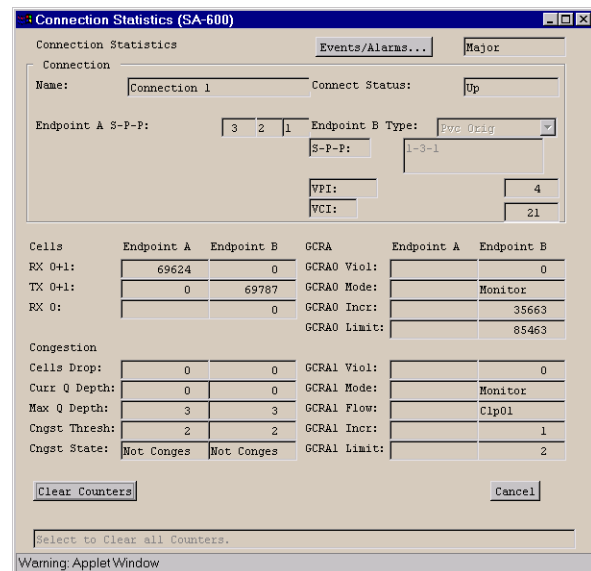
2. Selecting a connection displays its Connection Options dialog box.



3. Select the IWF Stats button to view statistics on the interworking function side of the connection. (Does not apply to ATM-to-ATM connections or NLS-to-ATM interworking functions.)



4. Select the Cell Stats button to view statistics on the ATM side of the connection.



**Figure 6-37. Connection Monitoring Example**

Selecting a connection from the Configured Connections list opens the Connection Options window for the selected connection. The Connection Options windows are similar among all service types. The Connection Options window displays Connection Name, Status, and Detail, along with Endpoint B information (Dialtype, S-P-P, etc).

For further details on monitoring each connection type, see:

[“Monitoring ATM-UNI Connections” on page 6-87](#)

[“Monitoring IMA Connections: Group and Link Statistics” on page 6-97](#)

[“Monitoring NLS Connections” on page 6-98](#)

[“Monitoring CES-IWF Connections” on page 6-101](#)

[“Monitoring Universal Serial Frame Connections” on page 6-103](#)

[“Monitoring Voice Compression Service Connections” on page 6-105](#)

## Monitoring ATM-UNI Connections

The ATM-UNI Connections window (see [Figure 6-38](#)) displays information on configured ATM-UNI connections. (The ATM-UNI Connections window is used for both configuring and monitoring connections. This window is the same one shown in [Figure 5-31](#). For convenience, it is repeated here.)

ATM UNI Connections (SA-600)

ATM UNI Connections Events/Alarms... Major

Port Detail

Slot-Pod-Port: 1 3 1

Port Name: SONET PORT NA

ADMIN Status: Up

Total Connections: 6

Port Type: SonetLinePlus

Port ID: SONET LINE CI

OPS Status: Up

Phy Port Stats... ATM Port Stats... CAC Port Stats...

Configured ATM UNI Connections

Name	Svc Dial Type	Connect Status	Connect Detail
ATM UNI Conn 1	UNI Pvc Orig	Up	Ok
NLS Tunnel 1	NLS Pvc Orig	Up	Ok
CES Conn 1	CES Pvc Orig	Up	Ok
CES Conn 2	CES Pvc Orig	Up	Ok
CES Conn 3	CES Pvc Orig	Up	Ok
CES Conn 4	CES Pvc Orig	Up	Ok

Add Connection... Connection Summary... Connection Stats... Cancel

Use Up/Down arrows or mouse to scroll; select row for more options.

Unsigned Java Applet Window

**Figure 6-38. ATM UNI Connections Window**

Unlike the CES, USF, and NLS Connections windows, which show only the CES, USF, or NLS end of a connection, the ATM-UNI Connections window enables you to see both ends of connections passing through the ATM port. This “mirroring” of connections makes this window a useful source of connection information.

**Table 6-37. ATM UNI Connections Fields and Buttons**

Field/Button	Type	Action/Description
<b>Port Detail</b>		
Total Connections	read-only	Displays the number of defined connections on the port.
Slot-POD-Port	read-only	Display the ports' slot, POD, and port numbers.
Port Type	read-only	Displays the type of port.
Port Name	read-only	Displays the port name (32 characters max).
Port ID	read-only	Displays the port ID (32 characters max).
ADMIN Status	read-only	Displays the administrative state of the port: Up or Down.
OPS Status	read-only	Displays the operational state of the port: Up or Down.
Phy Port Stats	window button	Enables you to view physical port statistics by opening the Display Port Status window corresponding to the specific port type. See the subsection on the specific port type earlier in this chapter.
ATM Port Stats	window button	Enables you to view ATM port statistics by opening the Display ATM Status window. See the subsection on the specific port type earlier in this chapter.
CAC Port Stats	window button	Enables you to view the Connection Admission Control port statistics by opening the CAC Port Statistics window. See <a href="#">“Viewing CAC Statistics” on page 6-90</a> .
<b>Configured ATM UNI Connections</b>		
Name	read-only	Displays the user designation of each configured connection on this port.
Svc	read-only	Displays the service type for Endpoint A of the connection: NLS, CES, FFS, UNI, or VCS.
Dial Type	read-only	Displays the dial type configured for each configured VCS interworking function on this port: PVC Orig, PVP, ASPVC Term, ASPVC Orig, or SPVC Orig.

**Table 6-37. ATM UNI Connections Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
Endpoint B	read-only	Displays the addressing details for Endpoint B based on the Dial Type. For PVC Orig and PVP dial types, the slot-POD-port, VPI, and VCI identifiers are displayed. For ASPVC Term and ASPVC Orig dial types, the AESA and Handle are displayed. For SPVC Orig dial type, the AESA and VPI/VCI are displayed.
Connect Status	read-only	Displays the connection state of each configured connection on this port: Up or Down.
<b>(Other Buttons)</b>		
Add Connection	window button	Enables you to add an ATM UNI connection. See <a href="#">“Adding a Connection” on page 5-38</a> .
Connection Summary	window button	Enables you to view a summary of the configuration data related to all the connections on this port. See <a href="#">“Viewing Connection Statistics via the Connections Summary Window” on page 6-95</a> .
Connection Stats	window button	Enables you to view connection statistics for all the connections on this port. See <a href="#">“Viewing Statistics on Individual ATM-UNI Connections” on page 6-93</a> .

## Viewing CAC Statistics

To view Connection Admission Control (CAC) statistics on the currently selected ATM-UNI port, select the CAC Port Stats button. The CAC Port Statistics window appears (see [Figure 6-39](#)):

**CAC Port Statistics**

Events/Alarms... Major

Port Detail

Slot-Pod-Port: 1 2 1 Port Name: DS1 PORT NAME

Port Bandwidth

	FBR	VBR
Forward Maximum:	3622	7244
Forward Available:	3622	7244
Reverse Maximum:	3622	7244
Reverse Available:	3622	7244

VPI/VCI Ranges

VPI Range VCI Range

PVP: 0 0 -----

PVC: 0 63 1 511

CAC Priority Queue Allocation

	rt	nrt	UBR/
Buffers	CBR1	VBR	ABR
Total:	97	101	485
Avail:	97	101	485

VC Buffer Allocation

	rt	nrt	UBR/
	CBR1	VBR	ABR
Shallow:	3	8	50
Medium:	6	15	500
High:	8	25	000

CAC Config Stats... Cancel

Warning: Applet Window

**Figure 6-39. CAC Port Statistics Window**

[Table 6-38 on page 6-91](#) describes the fields and buttons in the CAC Port Statistics window.

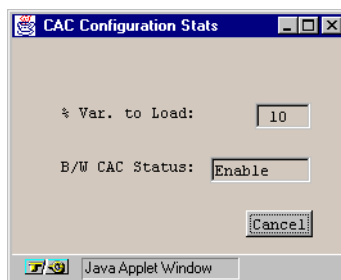
**Table 6-38. CAC Port Statistics Fields and Buttons**

Field/Button	Type	Description
<b>Port Detail</b>		
Slot-POD-Port	read-only	Displays the location (slot and POD number) of the currently selected port.
Port Name	read-only	Displays the port name (32 characters max).
<b>Port Bandwidth (Forward and Reverse)</b>		
Total FBR	read-only	Displays the amount of fixed bandwidth (fixed bit rate, FBR) that has been allocated for connections.
Avail FBR	read-only	Displays the remaining fixed bandwidth (fixed bit rate, FBR) available for connections.
Total VBR	read-only	Displays the amount of variable bandwidth (variable bit rate, VBR) that has been allocated for connections.
Avail VBR	read-only	Displays the remaining variable bandwidth (variable bit rate, VBR) available for connections.
<b>VPI/VCI Ranges</b>		
VPI Range: PVP	read-only	Displays the VPI Range for PVP.
VPI Range: PVC	read-only	Displays the VPI Range for PVC.
VCI Range: PVC:	read-only	Displays the VCI Range for PVC.
<b>CAC Priority Queue Allocation</b>		
CBR1 Total/Available	read-only	Displays total/available buffers for CBR1.
rt VBR Total/Available	read-only	Displays total/available buffers for rtVBR.
nrt VBR Total/Available	read-only	Displays total/available buffers for nrtVBR.
UBR/ABR Total/Available	read-only	Displays total/available buffers for UBR/ABR.

**Table 6-38. CAC Port Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
<b>VC Buffer Allocation</b>		
CBR1 Shallow/ Medium/High	read-only	Displays shallow/medium/high VC buffer allocations for CBR1.
rt VBR Shallow/ Medium/High	read-only	Displays shallow/medium/high VC buffer allocations for rt-VBR.
nrt VBR Shallow/ Medium/High	read-only	Displays shallow/medium/high VC buffer allocations for nrt-VBR.
UBR/ABR Shallow/ Medium/High	read-only	Displays shallow/medium/high VC buffer allocations for UBR/ABR.
<b>(Other Fields and Buttons)</b>		
CAC Config Stats	window button	Enables you to display CAC config statistics (see <a href="#">Figure 6-40</a> and <a href="#">Table 6-39</a> ).

The CAC Configuration Statistics window shows additional CAC parameters, described in [Table 6-39](#).



**Figure 6-40. CAC Configuration Stats Window**

**Table 6-39. CAC Configuration Statistics Fields**

Field (read-only)	Description
% Var to Load	Displays the percentage of variable bandwidth that is treated as fixed bandwidth (for the purpose of subtracting the fixed bandwidth that has been allocated for connections from the remaining fixed bandwidth available for connections).
B/W CAC Status	Displays whether bandwidth CAC is enabled or disabled.



## Viewing Statistics on Individual ATM-UNI Connections

From the ATM UNI Connections window, there are three ways to display ATM connection status information:

- Select the Connection from the Configured ATM UNI Connections list in the ATM UNI Connections window (see [page 6-87](#));
  - Select the Connection Summary button in the ATM UNI Connections window, then select the desired connection from the list in the Connections Summary window (see [page 6-95](#));
- or
- Select Connection Statistics button in the ATM UNI Connections window, then select the desired connection from the list in the Connections Statistics window (see [page 6-96](#)).

All three paths bring you to the Connection Options window (see [Figure 6-41](#)). Select the Statistics button in the Connection Options window to display the Connection Statistics window ([Figure 6-43 on page 6-96](#), described in [Table 6-41](#)).

**Figure 6-41. Connection Options Window (UNI)**

(The Connection Options window is described in [Table 5-1 on page 5-5](#).)

***Viewing Connection Statistics from the ATM UNI Connections Window***

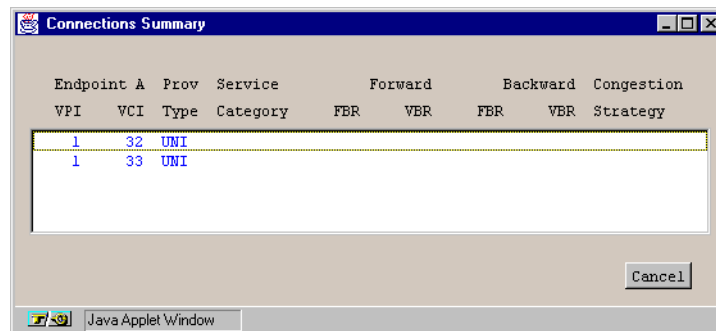
To view the Connection Statistics window from the ATM UNI Connections window:

1. Select a connection to view from the list of connections in the ATM UNI Connections window (Figure 6-38 on page 6-87).
2. When the Connection Options window appears, choose the Statistics button to open the Connection Statistics window (Figure 6-43 on page 6-96).

### Viewing Connection Statistics via the Connections Summary Window

To view the Connection Statistics window via the Connections Summary window:

1. Choose the Connection Summary button in the ATM UNI Connections window. The Connections Summary window appears (see [Figure 6-42](#) and [Table 6-40](#)):
2. From the list of connections in the Connections Summary window, select the desired connection.
3. When the Connection Options window appears, choose the Statistics button to display the Connection Statistics window ([Figure 6-43](#)).



**Figure 6-42. Connections Summary Window**

**Table 6-40. Connections Summary Fields**

Field (read-only)	Description
Endpoint A: VPI	Displays the virtual path identifier at endpoint A of each connection.
VCI	Displays the virtual channel identifier at endpoint A of each connection.
Prov Type	Displays the provisioning type used by each connection.
Service Category	Displays the ATM service category used by each connection.
Forward FBW	Displays the forward fixed bandwidth of each connection.
VBW	Displays the forward variable bandwidth of each connection.
Backward FBW	Displays the backward fixed bandwidth of each connection.
VBW	Displays the backward variable bandwidth of each connection.
Congestion Strategy	Displays the method of controlling connection congestion used by each connection.

### Viewing Connection Statistics via the Connections Statistics Window

To view the Connections Statistics window via the Connections Statistics window:

1. Choose the Connection Stats button in the ATM UNI Connections window. The Connections Statistics window appears (see [Figure 6-43](#) and [Table 6-41](#)).

Endpoint A			Endpoint B						
VPI	VCI	Cells In	Type	S	P	P	VPI	VCI	Cells In
1	32		UNI	1	3	1	1	32	
1	33		UNI	1	3	1	1	33	

**Figure 6-43. Connections Statistics Window**

2. Select the desired connection from the list in the Connections Statistics window.
3. When the Connection Options window appears, choose the Statistics button to display the Connection Statistics window ([Figure 6-43](#)).

**Table 6-41. Connections Statistics Fields**

Field (read-only)	Description
Endpoint A/B VPI	Displays the virtual path identifier (VPI) at endpoint A/B of each connection.
Endpoint A/B VCI	Displays the virtual channel identifier (VCI) at endpoint A/B of each connection.
Endpoint B Type	Displays the type of connection at the origin (endpoint B).
Endpoint B S-P-P	Displays the location (slot, POD, and port numbers) of the endpoint B port of each connection.
Endpoint A/B Cells In	Displays the number of incoming cells detected at endpoint A/B of each connection.

## **Monitoring IMA Connections: Group and Link Statistics**

IMA DS1/E1 Cell PODs provide multiple DS1/E1 ATM ports that may be “grouped” together to provide a virtual connection with the aggregate bandwidth of the grouped connections.

Monitoring functions separate from the Interface Management or Service Management functions have not yet been added to WebXtend. To view information specific to the IMA Group and the IMA Links which comprise the IMA group, you’ll need to use the Service Management or Interface Management procedures from the Main Menu as described in the following sections of the manual.

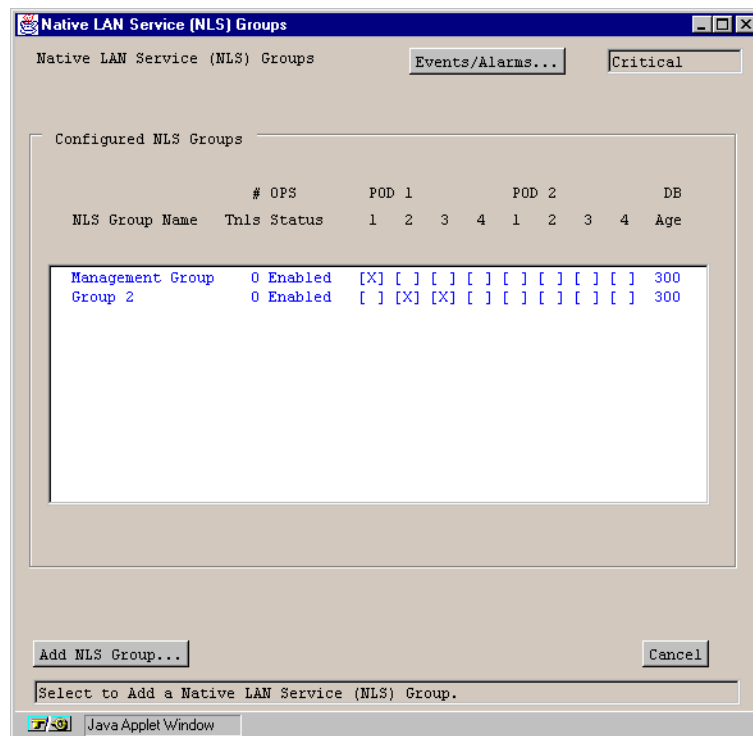
- **“Viewing IMA Group Statistics” on page 5-55**
- **“Viewing IMA Link Statistics” on page 5-60**

## Monitoring NLS Connections

Status information on NLS connections is available at the NLS groups level and the NLS Tunnels level.

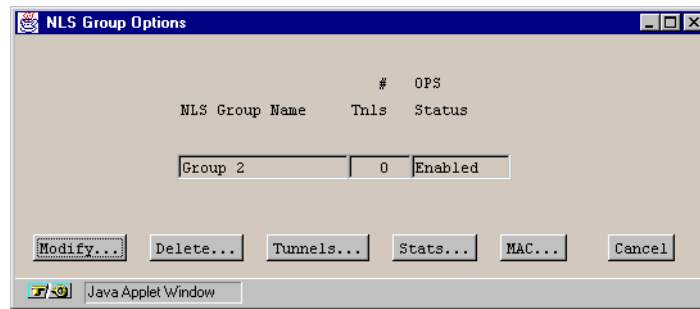
To access this information:

1. Choose the Next Logical Layer button in the Display Ethernet Port Status window. The Native LAN Service (NLS) Groups window appears (Figure 6-44), displaying information on the available Ethernet PODs and a list of currently configured NLS Groups, the number of tunnels attached, their present status, the ports assigned to each group, and the configured database age.



**Figure 6-44. Native LAN Service (NLS) Groups Window**

2. Select the NLS Group you wish to view from the Configured NLS Groups list. The NLS Group Options window appears (see Figure 6-45).



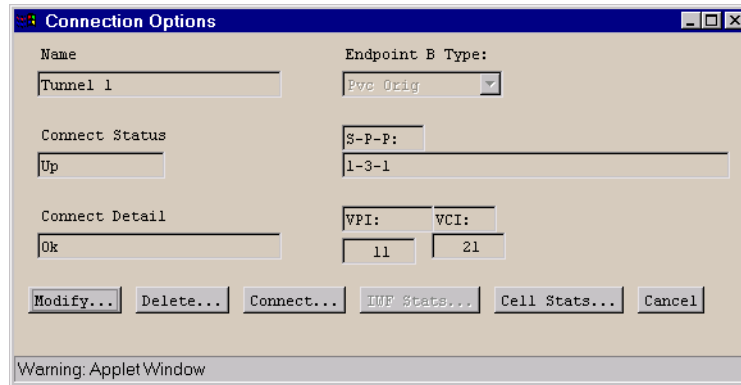
**Figure 6-45. NLS Group Options Window**

3. From the NLS Group Options window, you can view group-level statistics by choosing the Stats button. See “[Viewing NLS Group Status Information](#)” on page 6-116 for details.
4. You can view the MAC address table by selecting the MAC button. See “[Viewing MAC Address Cache Information](#)” on page 5-78 for details.
5. You can also view statistics on NLS Tunnels (the LAN equivalent of interworking functions) by selecting the Tunnels button to open the Configure NLS Tunnels window, displaying information on the selected NLS Group, its attached tunnels, status and associated ports ([Figure 6-46](#)).



**Figure 6-46. Native LAN Service (NLS) Tunnels Window**

6. Select the NLS Tunnel you wish to view from the Attached NLS Tunnels list. The Connection Options window appears (see [Figure 6-47](#)).



**Figure 6-47. NLS Tunnel Options Window**

7. From the Connection Options window, you can view statistics on the ATM side of the NLS tunnel by choosing the Cell Stats button. See [“Viewing Connection Statistics” on page 6-108](#) for details.



## Monitoring CES-IWF Connections

From the Display DS1/E1 Port Status window, you can access information about the interworking functions and all statistics on a DS1/E1 circuit POD port.

To access this information:

1. Choose the Next Logical Layer button in the Display DS1/E1 Port Status window or the DS1 Faults window. The Configure CES Connection window appears (Figure 6-48), displaying information on the selected port and a list of currently configured connections, their dial types and endpoints, and their present status.

**Configure CES Connection**

Events/Alarms... Major

**Port Detail**

Slot-Pod-Port: 3 1 2 Port Type: Dsl  
 Port Name: DS1 PORT NAME Port ID: DS1 CIRCUIT I  
 ADMIN Status: Up OPS Status: Up  
 CBR Service: Structured CBR Clock Mode: Synchronous  
 Dynamic Bandwidth: Enabled CES Signaling: Transport

**Configured CES Connections**

CES-IWF Name	Dial Type	Status	Detail

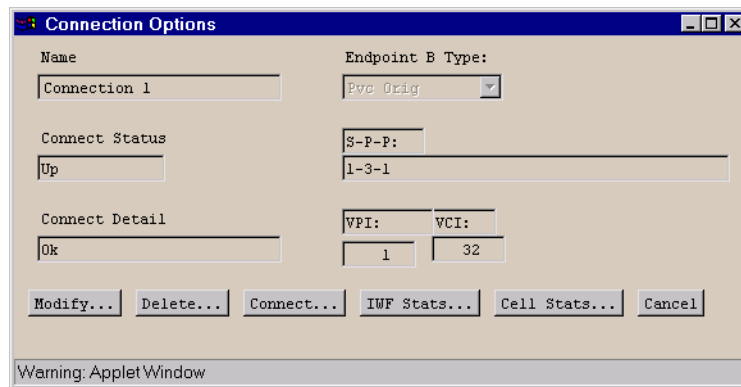
Add CES-IWF... Add CES-DACS... OK Cancel Apply

Select the type of CBR Service for this port.

Warning: AppletWindow

**Figure 6-48. Configure CES Connection Window**

2. Select the interworking function you wish to view from the Configured CES Connections list. The CES-IWF Options window appears (see Figure 6-49).



**Figure 6-49. Options Window (CES-IWF)**

3. From the Connection Options window, you can view statistics on the selected interworking function or on the ATM side of the connection. See [“Viewing Connection Statistics” on page 6-108](#) for details.

## Monitoring Universal Serial Frame Connections

You can view status information about connections by viewing the USF Connections window. You can access this window from the Main menu or from a Display USF Port Status window.

To access this information:

1. Choose the Next Logical Layer button in the Display USF Port Status window or the USF Faults window. The Configure USF Connection window appears (Figure 6-50 on page 6-103), displaying information on the selected port and a list of currently configured connections, their dial types and endpoints, and their present status.

Configure USF Connection

Events/Alarms... Major

Port Detail

Slot-Pod-Port: 1 2 1 Port Type: RvxPort

Port Name: Serial Frame Port ID: Serial Frame

ADMIN Status: Up OPS Status: Up

Configured USF Connections

Tunnel Name	Dial Type	Status	Detail

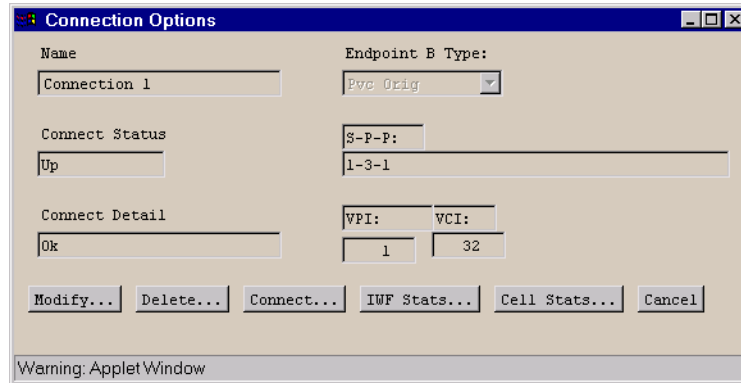
Add USF-IWF... Cancel

Use Up / Down arrows or mouse to scroll; select row for more options.

Warning: AppletWindow

**Figure 6-50. Configure USF Connection Window**

2. Select the tunnel (interworking function) you wish to view from the Configured USF Connections list. The Connection Options window appears (see Figure 6-51).



**Figure 6-51. Connection Options Window**

3. From the Connection Options window, you can view statistics on the selected interworking function or on the ATM side of the connection. See [“Viewing Connection Statistics”](#) on page 6-108 for details.

## Monitoring Voice Compression Service Connections

You can view status information about VCS connections by viewing the VCS Connections window. You can access this window from the Main menu or from the Display DS1 Port Status window of a DS1 Voice Compression POD.

To access this information:

1. Choose the Next Logical Layer button in the Display DS1 Port Status window. The Configure VCS Connection window appears (Figure 6-52), displaying information on the selected port and a list of currently configured connections, their dial types and endpoints, and their present status.

**Configure VCS Connection**

Port Detail

Slot-Pod-Port: 1 2 1 Port Type: DS1

Port Name: DS1 PORT NAME Port ID: DS1 CIRCUIT I

ADMIN Status: Up OPS Status: Up

PCM Coding Scheme: U Law

VCS Port Stats...

Configured VCS Connections

VCS-IWF Name	Dial Type	Connect Status	Connect Detail
1	Pvc Orig	Up	Ok

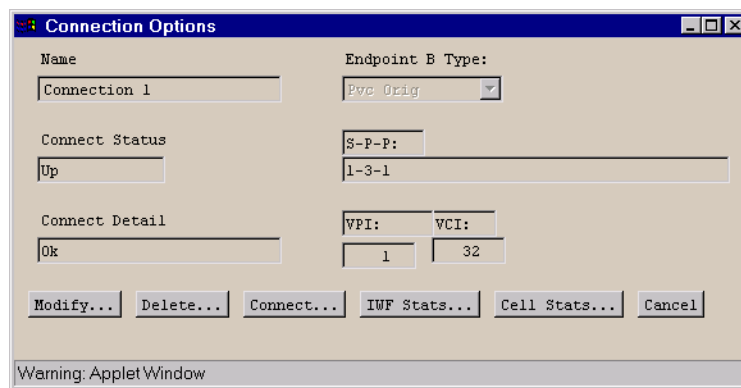
Add VCS-IWF... OK Cancel Apply

Select to specify the operating status of this connection.

Warning: AppletWindow

**Figure 6-52. Configure VCS Connection Window**

2. To view port-level statistics, select the VCS Port Stats button.
3. To view statistics on an individual VCS interworking function, select it from the Configured VCS Connections list. The Connection Options window appears (see Figure 6-53).

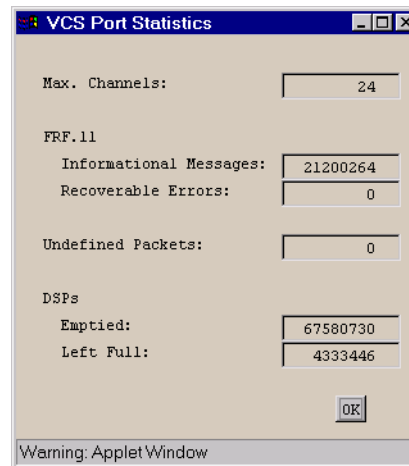


**Figure 6-53. Connection Options Window (VCS-IWF)**

4. From the Connection Options window, you can view statistics on the selected interworking function or on the ATM side of the connection. See [“Viewing Connection Statistics” on page 6-108](#) for details.

## Viewing VCS Port Statistics

From the Configured VCS Connections window, you can view port-level statistics regarding the VCS port by selecting the VCS Port Statistics button. The VCS Port Statistics window is displayed (Figure 6-54):



**Figure 6-54. VCS Port Statistics Window**

Table 6-42 describes the fields and buttons in the VCS Port Statistics window.

**Table 6-42. VCS Port Statistics Fields and Buttons**

Field/Button	Type	Description
Max Channels	read-only	Displays the maximum number of channels available based on the installed hardware configuration (POD type and number of DSP mezzanine cards).
FRF.11 Informational Messages	read-only	Displays the number of informational messages received from the FRF.11 stack.
FRF.11 Recoverable Errors	read-only	Displays the number of recoverable errors reported by the FRF.11 stack.
Undefined Packets	read-only	Displays the number of packets received from the WAN bound for unconfigured channels.
DSPs Emptied	read-only	Displays the number of tiems the DSPs were processed until all were empty. If this count is not rolling, the hardware is abnormally busy.
DSPs Left Full	read-only	Displays the number of times the DSPs still had information to process when background processing was started. This count should be rolling.

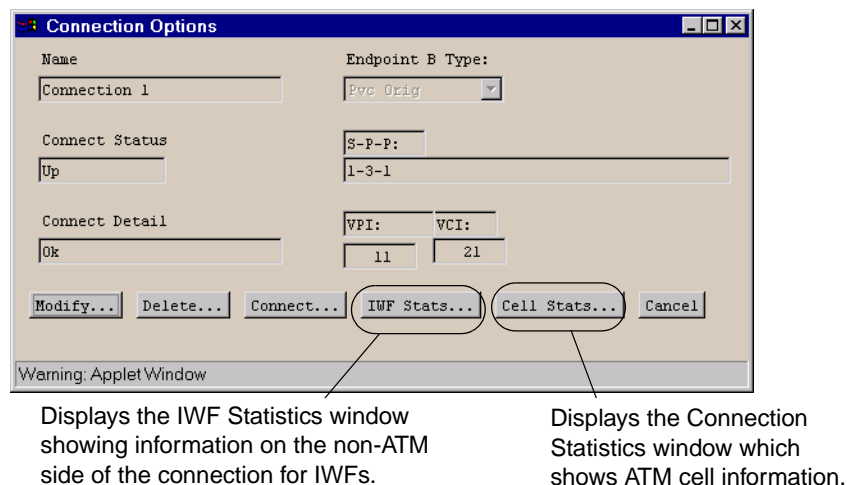
## Viewing Connection Statistics

Connections are either interworking functions or straight ATM UNI connections. Interworking functions (such as NLS tunnels, Universal Serial Frame IWFs, Circuit Emulation Service IWFs, or Voice Compression Service IWFs) are connections which have one non-ATM side and one ATM side. Straight ATM UNI connections are ATM at both ends.

Interworking functions have separate screens for viewing IWF statistics and ATM connection statistics. ATM connections by nature require only the ATM connection information screen.

Both IWF statistics windows and ATM connection statistics windows are accessed from the connection's Options window.

Figure 6-55 shows an example of the Connections Options window for a CES-IWF. The format of the Connection Options window is similar for all types of IWFs and ATM connections.



**Figure 6-55. Connection Options Window Example**

The Cell Stats button is available for both IWFs and ATM UNI connections. The IWF Stats button is not available for ATM UNI connections since there are only Cell statistics to view.



IWF Stats are not available for NLS Tunnels.

Selecting the Cell Stats button enables you to monitor ATM cell statistics on the selected connection or interworking function. See [“Viewing ATM Connection Statistics” on page 6-110](#).



Selecting the IWF Stats button enables you to monitor statistics on the selected Interworking Function. See [“Viewing Interworking Function Statistics” on page 6-115](#).

## Viewing ATM Connection Statistics

To view ATM connection statistics for an interworking function or ATM connection:

*From the Main menu:*

1. Choose the Service Management button from the Main Menu.
2. When the Select Service window appears ([Figure 5-1 on page 5-2](#)), choose the button for the desired service.
3. When the Select Port window appears, select the desired port to view. The Connections window appears. From the Configured Connections or Configured IWFs field, select the desired interworking function to open its Connection Options window.
4. At the Connection Options window, select the Cell Stats button to display the Connection Statistics window.

*From a Display Port or Path Status window on an ATM Cell POD:*

1. From a Display Port Status window, choose the Next Logical Layer button to open the Display ATM Status window or choose the Display Path Status button to open the Display Path Status window.
2. From a Display Path window, choose the Next Logical Layer button to open the Display ATM Status window.
3. From the Display ATM Status window, choose the Service Management button. The ATM UNI Connections window appears ([Figure 6-38 on page 6-87](#)). From the Configured Connections field, select the desired interworking function to open its Connection Options window.
4. At the Connection Options window, select the Cell Stats button to display the Connection Statistics window.

*From a Display Port window on an Ethernet POD:*

1. From a Display Port Status window, choose the Next Logical Layer button to open the NLS Groups window.
2. Select an NLS Group from the Configured NLS Groups list to open the NLS Group Options window. Choose the Tunnels button to open the NLS Tunnels window.
3. Select an NLS Tunnel from the Attached NLS Tunnels list to open the Connection Options window for that NLS Tunnel. At the Connection Options window, select the Cell Stats button to display the Connection Statistics window.

**Connection Statistics**

Events/Alarms... Major

Connection  
Name: CES Connection 1 Connect Status: Down

Endpoint A S-P-P: 3 1 2 Endpoint B Type: Aspvic Term

AESA: Handle: 1

Cells	Endpoint A	Endpoint B	GCRA	Endpoint A	Endpoint B
RX 0+1:	0	0	GCRA0 Viol:		0
TX 0+1:	0	0	GCRA0 Mode:	0	
RX 0:		0	GCRA0 Incr:		0
			GCRA0 Limit:		0

Congestion

	Endpoint A	Endpoint B	GCRA1	Endpoint A	Endpoint B
Cells Drop:	0	0	GCRA1 Viol:		0
Curr Q Depth:	0	0	GCRA1 Mode:	0	
Max Q Depth:	0	0	GCRA1 Flow:	Clp0	
Cngst Thresh:	0	0	GCRA1 Incr:		0
Cngst State:	Not Conges	Not Conges	GCRA1 Limit:		0

Clear Counters Cancel

Select to Clear all Counters.

Warning: AppletWindow

**Figure 6-56. Connection Statistics Window**

Table 6-41 on page 6-96 describes the fields and buttons in the Connection Statistics and NLS Group Statistics windows.



For NLS Tunnels, the Connection Statistics window is called the NLS Tunnel Statistics window, and the Connection field is replaced by the Associated NLS Group and NLS Tunnel Detail fields, displaying information regarding the NLS group rather than the Connection Name and Endpoint information seen at other Connection Statistics windows. The ATM cell data fields in the lower portion of the window remain identical to the other Connection Statistics windows.

**Table 6-43. Connection Statistics/NLS Group Statistics Fields and Buttons**

Field/Button	Type	Description
<b>Connection (all PODs except Ethernet)</b>		
Name	read-only	Displays the user designation of the connection.
Connect Status	read-only	Displays the state of the ATM side of the connection: Up or Down.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the IWF.
Endpoint B Type	read-only	Displays the dial type for this connection: <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI. <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI. <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle. <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle. <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read-only	Displays Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
<b>Ethernet PODs only: Associated NLS Group</b>		
NLS Group Name	read-only	Display NLS group name.
# Tnls	read-only	Displays the number of tunnels established for this NLS group.
OPS Status	read-only	Displays the operational state of the group: Up or Down.
POD 1 Port 1—4	read-only	Displays a check mark next to the POD 1 ports that are part of this NLS group.
POD 2 Port 1—4	read-only	Displays a check mark next to the POD 2 ports that are part of this NLS group.

**Table 6-43. Connection Statistics/NLS Group Statistics Fields and Buttons**

Field/Button	Type	Description
DB Age	read-only	Displays the age of the database.
<b>Ethernet PODs only: NLS Tunnel Detail</b>		
NLS Tunnel Name	read-only	Displays the name of the NLS tunnel.
Connect Status	read-only	Displays the connection status of the NLS tunnel.
<b>(Other Fields and Buttons)</b>		
Cells Endpoint A/B RX 0+1	read-only	Displays the number of cells with a cell loss priority of 0+1 received at endpoint A/B.
Cells Endpoint A/B TX 0+1	read-only	Displays the number of cells with a cell loss priority of 0+1 transmitted at endpoint A/B.
Cells Endpoint A/B RX 0	read-only	Displays the number of cells with a cell loss priority of 0 received at endpoint A/B.
Congestion Endpoint A/B Cells Drop	read-only	Displays the number of cells dropped at endpoint A/B in order to control congestion.
Congestion Endpoint A/B Curr Q Depth	read-only	Displays the present number of cells in the congestion buffer at endpoint A/B.
Congestion Endpoint A/B Max Q Depth	read-only	Displays the maximum number of cells that can be contained by the congestion buffer at endpoint A/B.
Congestion Endpoint A/B Cngst Thresh	read-only	Displays the congestion threshold at endpoint A/B, that is, the number of cells in the congestion buffer that triggers the implementation of the congestion strategy, if any.
Congestion Endpoint A/B Cngst State	read-only	Displays the state of the ATM connection relative to congestion at endpoint A/B.
GCRA Endpoint A/B GCRA0 Viol	read-only	Displays the number of generic cell rate algorithm 0 (GCRA 0) violations at endpoint A/B.

**Table 6-43. Connection Statistics/NLS Group Statistics Fields and Buttons**

Field/Button	Type	Description
GCRA Endpoint A/B GCRA0 Mode	read-only	Displays the generic cell rate algorithm 0 (GCRA 0) mode of operation at endpoint A/B.
GCRA Endpoint A/B GCRA0 Incr	read-only	Displays the generic cell rate algorithm 0 (GCRA 0) increment at endpoint A/B.
GCRA Endpoint A/B GCRA0 Limit	read-only	Displays the generic cell rate algorithm 0 (GCRA 0) limit at endpoint A/B.
GCRA Endpoint A/B GCRA1 Viol	read-only	Displays the number of generic cell rate algorithm 1 (GCRA 1) violations at endpoint A/B.
GCRA Endpoint A/B GCRA1 Mode	read-only	Displays the generic cell rate algorithm 1 (GCRA 1) mode of operation at endpoint A/B.
GCRA Endpoint A/B GCRA1 Flow	read-only	Displays the generic cell rate algorithm 1 (GCRA 1) flow type at endpoint A/B.
GCRA Endpoint A/B GCRA1 Incr	read-only	Displays the generic cell rate algorithm 0 (GCRA 0) increment at endpoint A/B.
GCRA Endpoint A/B GCRA1 Limit	read-only	Displays the generic cell rate algorithm 0 (GCRA 0) limit at endpoint A/B.
Clear Counters	command button	Resets all the counter (numeric) fields in the Connection Status window to zero (0).

## Viewing Interworking Function Statistics

To view statistics for an interworking function:

1. Choose the Service Management button from the Main Menu.
2. When the Select Service window appears ([Figure 5-1 on page 5-2](#)), choose the button for the desired service.
3. When the Select Port window appears, select the desired port to view.
4. The Connections window appears. From the Configured Connections or Configured IWFs field, select the desired interworking function to open its Connection Options window.
5. At the Connection Options window, select the IWF Stats button to display the IWF Statistics window.

## Viewing NLS Group Status Information

To view NLS group status information:

1. Select Service Management from the Main menu.
2. Select an NLS group from the Configured NLS Groups list to open the NLS Group Options window (Figure 6-45 on page 6-99).
3. Choose the Stats button. The NLS Group Statistics window appears (see Figure 6-57):

NLS Group Name	#	OPS	POD 1	POD 2	DB						
			1	2	3	4	1	2	3	4	Age
Management Group	0	Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	300

Total TX Packets: 3002      Total RX Packets: 3151

Clear Group Counts    Clear All Counts    Cancel

Select to Clear Counters for this Group.

**Figure 6-57. NLS Group Statistics Window**

Table 6-44 describes the fields and buttons in the NLS Group Statistics window.



**Table 6-44. NLS Group Statistics Fields and Buttons**

Field/Button	Type	Action/Description
<b>NLS Group Detail</b>		
NLS Group Name	read-only	Displays NLS group name.
# Tnls	read-only	Displays the number of tunnels established for this NLS group.
OPS Status	read-only	Displays the operational state of the group: Up or Down.
POD 1 Port 1—4	read-only	Displays a check mark next to the POD 1 ports that are part of this NLS group.
POD 2 Port 1—4	read-only	Displays a check mark next to the POD 2 ports that are part of this NLS group.
DB Age	read-only	Displays the age of the database.
Total TX Packets	read-only	Displays the total number of packets transmitted by this NLS group.
Total RX Packets	read-only	Displays the total number of packets received by this NLS group.
Clear Group Counts	command button	Resets the group count (numeric) fields in the NLS Group Statistics window to zero (0).
Clear All Counts	command button	Resets all the counter (numeric) fields in the NLS Group Statistics window to zero (0).

## Viewing CES-IWF Statistics

To view CES-IWF statistics:

1. Open the Connection Options window (Figure 6-49 on page 6-102).
2. Choose the IWF Stats button. The CES-IWF Statistics window appears (see Figure 6-58):

**Figure 6-58. CES-IWF Statistics Window**

Table 6-45 describes the fields and buttons in the CES-IWF Statistics window.

**Table 6-45. CES-IWF Statistics Fields and Buttons**

Field/Button	Type	Description
<b>CES Connection</b>		
Name	read-only	Displays the name of the CES-IWF.
Connect Status	read-only	Displays the status of the CES-IWF connection: Up or Down.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the CES-IWF.

**Table 6-45. CES-IWF Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
Endpoint B Type	read-only	Displays the dial type for this connection:  <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.  <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI.  <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.  <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.  <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read-only	Displays Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).  For ASPVC Orig dial type, displays the handle being called (read/write).
<b>Statistics</b> (fields marked with an asterisk represent the number of 250ms intervals in which one or more of the indicated events occurred)		
Lost Cells*	read-only	Displays the number of intervals in which cells have been lost on the CES-IWF.

**Table 6-45. CES-IWF Statistics Fields and Buttons (Continued)**

Field/Button	Type	Description
Header Errors*	read-only	Displays the number of intervals in which header errors have been detected on the CES-IWF, i.e., a discrepancy between what the port expected in the header and what was received.
AAL1 Sequence Errors*	read-only	Displays the number of intervals in which ATM adaptation layer type 1 (AAL1) errors have been detected on the CES-IWF.
Pointer Parity Errors*	read-only	Displays the number of intervals in which cells have been received with pointer parity errors.
Pointer Reframes*	read-only	Displays the number of intervals in which loss of pointer (LOP) defects have been corrected (reframed) on the CES-IWF.
Buffer Underflows*	read-only	Displays the number of intervals in which cell underflow in the CES-IWF's reassembly buffer have been detected.
Buffer Overflows*	read-only	Displays the number of intervals in which reassembly-buffer cell overflow has been detected.
Cell Loss Status	read-only	Displays whether any cell loss has occurred ("loss" or "no loss") on the CES-IWF.
Reassembled Cells	read-only	Displays the number of cells that have been reassembled on the CES-IWF.
Transmitted Cells	read-only	Displays the number of cells that have been transmitted on the CES-IWF.
RX OAM Cells	read-only	Displays the number of operations administration and maintenance (OAM) cells that have been received on the CES-IWF.
RX OAM Cells Dropped	read-only	Displays the number of OAM cells that have been dropped on the CES-IWF.
TX Suppressed Cells	read-only	Displays the number of transmitted cells that were suppressed on the CES-IWF.
TX Conditioned Cells	read-only	Displays the number of conditioned cells that were transmitted on the CES-IWF.
<b>(Other Button)</b>		
Clear Counters	command button	Resets all the counter (numeric) fields in the Statistics frame to zero (0).

## Viewing USF-IWF statistics

To view USF-IWF statistics:

1. Open the USF-IWF Options window (Figure 6-51 on page 6-104).
2. Choose the IWF Stats button. The USF-IWF Statistics window appears (see Figure 6-59):

**USF-IWF Statistics**

USF-IWF Statistics    Events/Alarms...    Major

USF Connection

Name: USF to IMA IP0D    Connect Status: Up

Endpoint A S-P-P: 11 1 1    Endpoint B Type: Pvc Orig

S-P-P: 11-2-1

VPI: 1

VCI: 34

**Statistics**

Input:		Output:	
Frames:	5320873	Frames:	2868266
Bytes:	1351501742	Bytes:	728539564
Discarded Frames:	0	Discarded Frames:	0
Overrun Errors:	0	Underrun Errors:	0
CRC Errors:	0		

Clear Counters    Cancel

Select to Clear all Counters.

Warning: Applet Window

**Figure 6-59. USF-IWF Statistics Window**

Table 6-46 describes the fields and buttons in the USF-IWF Statistics window.

**Table 6-46. USF-IWF Statistics Fields and Buttons**

Field/Button	Type	Action/Description
<b>USF Connection</b>		
Name	read-only	Display USF-IWF Connection name.
Connect Status	read-only	Displays the current connection status: Up or Down.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the USF-IWF.
Endpoint B Type	read-only	Displays the dial type for this connection:  <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI. <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI. <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle. <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle. <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read-only	Displays Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).  For ASPVC Orig dial type, displays the handle being called (read/write).

**Table 6-46. USF-IWF Statistics Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Statistics (Input/Output)</b>		
Frames	read-only	Displays the number of frames received and transmitted on this USF-IWF.
Bytes	read-only	Displays the number of bytes received and transmitted on this USF-IWF.
Discarded Frames	read-only	Displays the number of input and output frames discarded on this USF-IWF.
Overflow Errors	read-only	Displays the number of input and output overflow errors on this USF-IWF.
Underrun Errors	read-only	Displays the number of input and output underrun errors on this USF-IWF.
CRC Errors	read-only	Displays the number of frames received with CRC errors.
<b>(Other Fields and Buttons)</b>		
Clear Counters	command button	Clears all counters in this window.

## Viewing VCS-IWF statistics

To view VCS-IWF statistics:

1. Open the Connection Options window (Figure 6-51 on page 6-104).
2. Choose the IWF Stats button. The VCS-IWF Statistics window appears (see Figure 6-60):

VCS-IWF Statistics

VCS Connection

Name: Connection 1 Connect Status: Up

Endpoint A S-P-P: 1 2 1 Endpoint B Type: Pvc Orig

S-P-P: 1-3-1

VPI: 1

VCI: 46

Statistics

AAL5 Packets Transmitted: 3567757 Octets Transmitted: 264028226

AAL5 Packets Received: 3567552 Octets Received: 264013104

Packet Transmit Errs: 0

Timeslot	Defects	Key Count	Dial Ends	FAX Starts	FAX Ends
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	0	0
24	0	0	0	0	0

Clear Counters Cancel

Warning: Applet Window

Figure 6-60. VCS-IWF Statistics Window

Table 6-47 describes the fields and buttons in the VCS-IWF Statistics window.



**Table 6-47. VCS-IWF Statistics Fields and Buttons**

Field/Button	Type	Action/Description
<b>USF Connection</b>		
Name	read-only	Display VCS-IWF Connection name.
Connect Status	read-only	Displays the current connection status: Up or Down.
Endpoint A S-P-P	read-only	Displays the location (slot, POD, port numbers) of endpoint A of the VCS-IWF.
Endpoint B Type	read-only	Displays the dial type for this connection:  <i>PVC Orig</i> – Permanent Virtual Connection, addressed by Slot-POD-Port, VPI, VCI.  <i>PVP</i> – Permanent Virtual Path, addressed by Slot-POD-Port, VPI.  <i>ASPVC Orig</i> – Adaptation Service Permanent Virtual Connection, Originating side. Addressed by AESA and Handle.  <i>ASPVC Term</i> – Adaptation Service Permanent Virtual Connection, Terminating side. Addressed by AESA and Handle.  <i>SPVC Orig</i> – Soft Permanent Virtual Connection, addressed by AESA and VPI/VCI.
(Address field) S-P-P or AESA	read-only	Displays Endpoint B as either a S-P-P (PVC Orig and PVP dial types) or as an AESA (SPVC Orig and ASPVC Orig dial types).
VPI (applies to PVP, PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual path identifier of endpoint B for this connection.
VCI (applies to PVC Orig, and SPVC Orig dial types only)	read-only	Displays the virtual channel identifier of endpoint B for this connection.
Handle (ASPVC Term and ASPVC Orig dial types only)	read-only	For ASPVC Term dial type, displays the handle number assigned for this IWF (read-only).  For ASPVC Orig dial type, displays the handle being called (read/write).

**Table 6-47. VCS-IWF Statistics Fields and Buttons (Continued)**

Field/Button	Type	Action/Description
<b>Statistics</b>		
AAL5 Packets Transmitted	read-only	Displays the number of AAL5 packets transmitted on this VCS-IWF.
AAL5 Packets Received	read-only	Displays the number of AAL5 packets received on this VCS-IWF.
Octets Transmitted	read-only	Displays the number of octets transmitted on this VCS-IWF.
Octets Received	read-only	Displays the number of octets received on this VCS-IWF.
Packet Transmit Errors	read-only	Displays the number of Packet Transmit Errors logged on this VCS-IWF.
Timeslot	read-only	Displays the number of each configured timeslot.
Defects	read-only	Displays the number of bitfield defects presently observed on each timeslot (DS0).
Key Count	read-only	Displays the number of touch-tone key presses detected.
Dial Ends	read-only	Displays the number of dial-sequence ends detected.
Fax Starts	read-only	Displays the number of fax call starts detected.
Fax Ends	read-only	Displays the number of fax call ends detected.
<b>(Other Fields and Buttons)</b>		
Clear Counters	command button	Clears all counters in this window.

## What's Next?

After you understand the monitoring functions of WebXtend, you may want to customize event and alarm functions, or generate event log files. These functions are described in [Chapter 7, “Managing Events.”](#)

# Managing Events

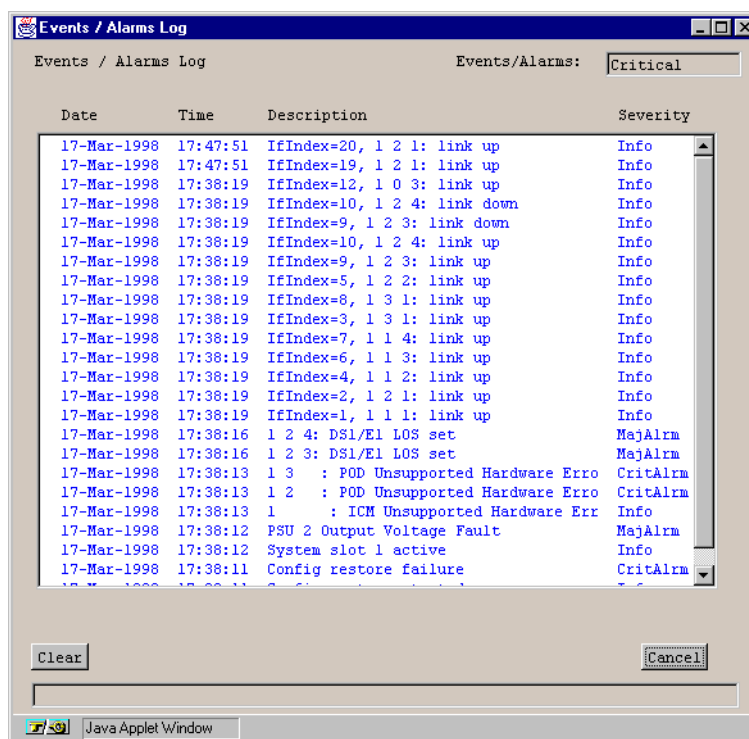
This chapter describes how to:

- Display events and alarms (see [page 7-2](#))
- Manage events and traps (see [page 7-5](#))

## Displaying the Events/Alarms Log

The Events/Alarms button (located in the upper-right corner of most WebXtend windows) enables you to view a summary of any current events and alarms.

To view current events and alarms, choose the Events/Alarms button. The Events/Alarms Log window appears (see [Figure 7-1](#)).



**Figure 7-1. Events/Alarms Log Window**

The Events/Alarms Log window displays four fields of information about each event and alarm detected by the SA unit. [Table 7-1](#) describes each field in the window.

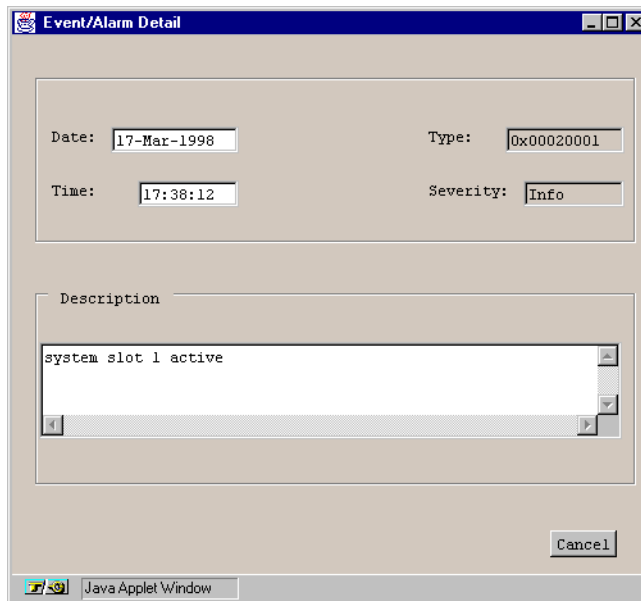
The newest event or alarm appears at the end of the log. When the log becomes full, the oldest event or alarm is deleted from the log (the log capacity is approximately 200 events/alarms).

**Table 7-1. Events/Alarms Log Fields**

<b>Designation</b>	<b>Description</b>
Date	Displays the date in European format (day-month-year) when the SA unit detected the event or alarm.
Time	Displays the time in 24-hour format when the SA unit detected the event or alarm.
Description	Displays a short statement about the type of alarm.
Severity	Displays the importance of the event or alarm that the SA unit detected: <ul style="list-style-type: none"><li>• CritAlrm for critical alarm</li><li>• MajAlrm for major alarm</li><li>• MinAlrm for minor alarm</li><li>• Info for informational purposes (applies to events, rather than alarms)</li><li>• Debug for software debugging purposes.</li></ul>

## Viewing Details of Individual Events/Alarms

To view additional details on an individual event or alarm, select it from the log. The Event/Alarm Detail window appears:



**Figure 7-2. Event/Alarm Detail Window**

Table 7-2 describes each field in the window.

**Table 7-2. Event/Alarm Detail Fields**

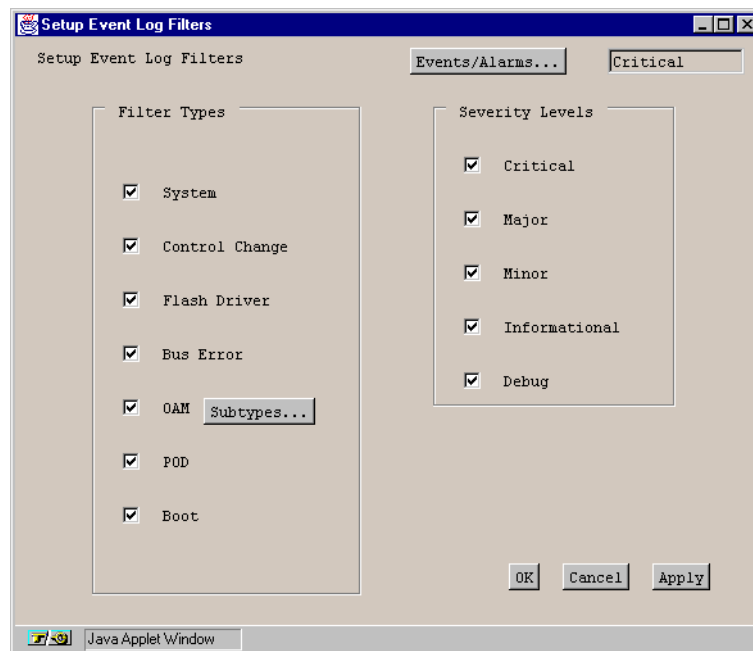
Field	Description
Date	Displays the date in European format (day-month-year) when the SA unit detected the event or alarm.
Type	Displays the type code for the selected error or alarm.
Time	Displays the time (24-hour format) when the SA unit detected the event or alarm.
Severity	Displays the importance of the event or alarm that the SA unit detected: <ul style="list-style-type: none"><li>• CritAlrm for critical alarm</li><li>• MajAlrm for major alarm</li><li>• MinAlrm for minor alarm</li><li>• Info for informational purposes (applies to events, rather than alarms)</li><li>• Debug for software debugging purposes.</li></ul>
Description	Displays a short statement about the type of alarm.

## Managing Events and Traps

WebXtend provides several functions for handling alarms and events detected by the SA unit. You can use the Event Management window to:

- Create a file containing the current contents of the Events/Alarms log
- Filter the types of events and alarms that appear in the Events/Alarms log
- Filter the types of events and alarms that generate a trap

To access the Event Management window, choose the Event Management button from the Main menu. The Event Management window appears (Figure 7-3).



**Figure 7-3. Event Management Window**

Table 7-3 briefly describes the fields and buttons in the Event Management window.



**Table 7-3. Event Management Buttons and Fields**

Button/Field	Type	Description
System Name	read-only	Displays the name of the SA unit.
System Date _Time	read-only	Displays the current date in European format (day-month-year) and the current time in 24-hour format as measured by the SA unit clock.
<b>File Management</b>		
Gen Event File	window button	Enables you to save the current contents of the Events/Alarms log to a file (not supported).
<b>Filter Management</b>		
Set Event Filters	window button	Enables you to select or filter the types of events and alarms that appear in the Events/Alarms log. See <a href="#">“Filtering Events and Alarms” on page 7-8.</a>
Set Trap Filters	window button	Enables you to select or filter the types of events and alarms that cause a trap to be transmitted. See <a href="#">“Filtering Traps” on page 7-10.</a>

## Generating Event Files (not supported)

To save the Events/Alarms log to a file:

1. Choose the Gen Event File button from the File Management frame of the Event Management window. The Generate Event File window appears.
2. Enter a name for the event file in the “Enter a File Name” field. You may enter a maximum of eight characters in this field.
3. Select the Now box.
4. When you are finished, choose OK.

If you choose the OK or Apply button, the SA unit creates the event file and stores it in flash memory.

To retrieve the event file, you use the Zmodem file transfer protocol to transfer the event file from the SA unit’s flash memory to your computer. (See [“Transferring Files with Zmodem” on page A-9](#) for instructions on how to use Zmodem.)

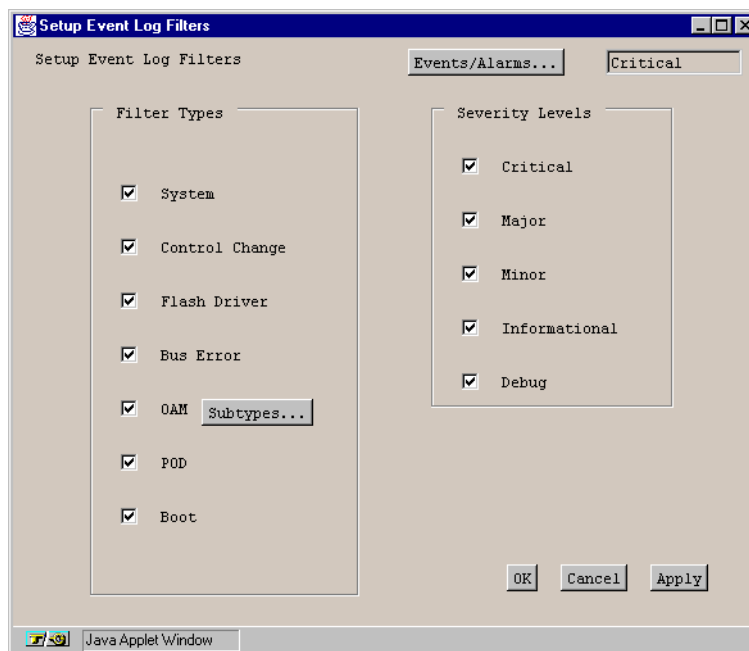
After the file is stored on your computer, you may view, format, and print it with a text editor, word processor, or spreadsheet program.

## Filtering Events and Alarms

By default, the Events/Alarms log contains each type of event and alarm at every level of severity detected by the SA unit. When diagnosing SA unit or network problems, it is convenient to filter this information so that you see only the alarms and events you are specifically concerned with. For instance, you can filter the log to display only alarms and events of a particular type and/or severity level.

To use the event and alarm filtering function:

1. Choose the Set Event Filters button from the Event Management window. The Setup Event Log Filters window appears (Figure 7-4).



**Figure 7-4. Setup Event Log Filters Window**

2. Select the types of events and alarms to include in the Events/Alarms log.
3. Select the event and alarm severity levels to include in the Events/Alarms log. (Table 7-4 describes the fields in the Setup Event Filters window.) For example, to include system related events and alarms and informational severity-level events and alarms from the Events/Alarms log, select the System field (in the Filter Types frame) and the Informational field (in the Severity Levels frame) of the Setup Event Log Filters window. Leave the other check boxes blank.



The Filter Types: OAM field has an associated button (Subtypes) that enables you to filter specific types of OAM events and alarms, versus selecting the OAM field itself, which enables you to filter all types of OAM events and alarms.

4. When you are finished, choose OK.

**Table 7-4. Setup Event Log Filters Fields and Buttons**

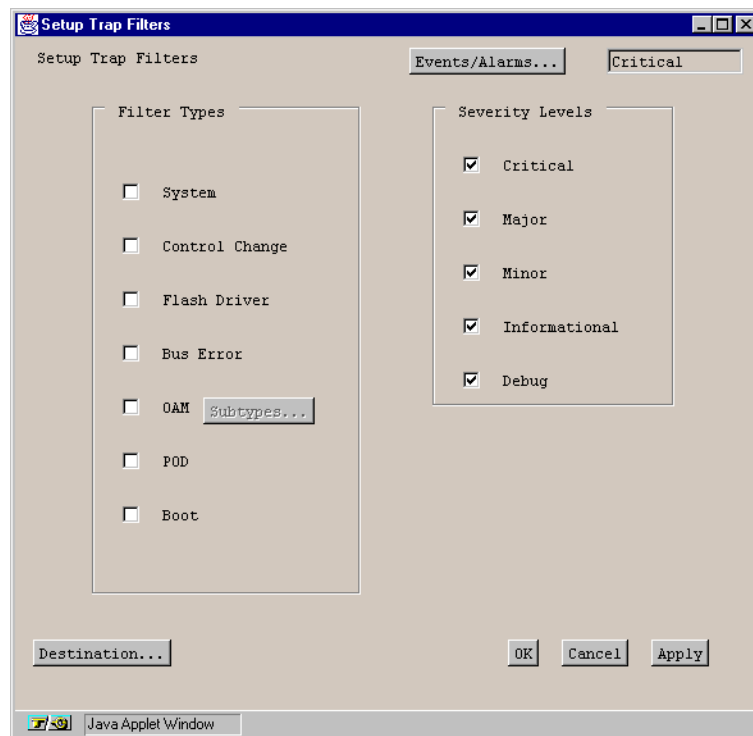
Field/Button	Type	Description
<b>Filter Types</b>		
System	read/write	A check mark indicates that system events and alarms are included in the Events/Alarms log.
Control Change	read/write	A check mark indicates that control change events and alarms are included in the Events/Alarms log.
Flash Driver	read/write	A check mark indicates that flash driver events and alarms are included in the Events/Alarms log.
Bus Error	read/write	A check mark indicates that bus error events and alarms are included in the Events/Alarms log.
OAM	read/write	A check mark indicates that operations administration and maintenance (OAM) events and alarms are included in the Events/Alarms log.
Subtypes	window button	Enables you to select specific OAM events and alarms to include in the Events/Alarms log.
POD	read/write	A check mark indicates that protocol option device (POD) events and alarms are included in the Events/Alarms log.
Boot	read/write	A check mark indicates that boot events and alarms are included in the Events/Alarms log.
<b>Severity Levels</b>		
Critical	read/write	A check mark indicates that critical events and alarms are included in the Events/Alarms log.
Major	read/write	A check mark indicates that major events and alarms are included in the Events/Alarms log.
Minor	read/write	A check mark indicates that minor events and alarms are included in the Events/Alarms log.
Informational	read/write	A check mark indicates that informational events and alarms are included in the Events/Alarms log.
Debug	read/write	A check mark indicates that debug events and alarms are included in the Events/Alarms log.

## Filtering Traps

By default, the SA unit generates a trap for every event and alarm it detects. To reduce the transmission of extraneous information to receiving management stations, you can set the SA unit to generate traps only in response to certain types of events and alarms and to events and alarms of certain severity-levels.

To use the trap filtering function:

1. Choose the Set Trap Filters button from the Filter Management frame of the Event Management window. The Setup Trap Filters window appears (see [Figure 7-5](#)).



**Figure 7-5. Setup Trap Filters Window**

2. Select the types of events and alarms that you want to generate a trap.
3. Select the event and alarm severity levels that you want to include. [Table 7-5](#) briefly describes the fields in the Setup Trap Filters window.

For example, to generate a trap on POD-related events and alarms and debug severity-level events and alarms, select the POD field in the Filter Types frame and the Debug field in the Severity Levels frame.

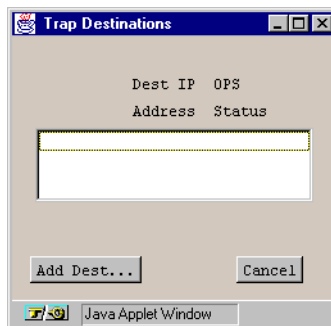


The OAM field in the Filter Types frame has an associated button (Subtypes) that enables you to select specific types of OAM events and alarms to generate traps. This is in contrast to selecting the OAM field itself, which enables you to select all types of OAM events and alarms to generate traps.

**Table 7-5. Setup Trap Filters Fields and Buttons**

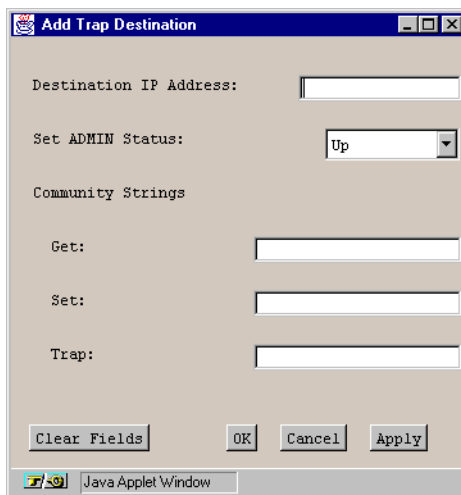
Field/Button	Type	Description
<b>Filter Types</b>		
System	read/write	A check mark indicates that system events and alarms will generate traps.
Control Change	read/write	A check mark indicates that control change events and alarms will generate traps.
Flash Driver	read/write	A check mark indicates that flash driver events and alarms will generate traps.
Bus Error	read/write	A check mark indicates that bus error events and alarms will generate traps.
OAM	read/write	A check mark indicates that operations administration and maintenance (OAM) events and alarms will generate traps.
Subtypes	window button	Enables you to select specific OAM events and alarms that will generate traps.
POD	read/write	A check mark indicates that protocol option device (POD) events and alarms will generate traps.
Boot	read/write	A check mark indicates that boot events and alarms will generate traps.
<b>Severity Levels</b>		
Critical	read/write	A check mark indicates that critical events and alarms will generate traps.
Major	read/write	A check mark indicates that major events and alarms will generate traps.
Minor	read/write	A check mark indicates that minor events and alarms will generate traps.
Informational	read/write	A check mark indicates that informational events and alarms will generate traps.
Debug	read/write	A check mark indicates that debug events and alarms will generate traps.
<b>Other Buttons</b>		
Destinations	window button	Enables you to specify which nodes will receive traps generated by the SA unit.

4. When you are finished selecting which events, alarms, and severity levels will generate traps, choose the Destinations button. The Trap Destinations window appears, listing any current trap destination addresses and their op status (Figure 7-6):



**Figure 7-6. Trap Destinations Window**

5. Choose the Add Dest(ination) button. The Add Trap Destination window appears (Figure 7-7):



**Figure 7-7. Add Trap Destination Window**

In the Destination IP Address field, enter the IP address of the management station you want to receive the traps generated by the SA unit. Set the ADMIN Status to up or down, and complete any community strings you wish in the Get, Set, and/or Trap fields, then click OK to return to the Trap Destinations window.

6. In the Trap Destinations window, you can double-click on a destination address in the Trap Destinations list to display the Trap Destination Options screen for the selected destination. The Trap Destination Options screen enables you to modify or delete a destination, or enable or disable the sending of traps to this IP address, using the connect button.
7. When you are finished assigning trap destinations, choose OK in the Trap Destinations window and the Setup Trap Filters window.

## What's Next?

After you understand how to manage events, alarms and traps, you are ready to perform diagnostic tests on the SA unit, as described in **Chapter 8, “Testing an SA Unit”**.



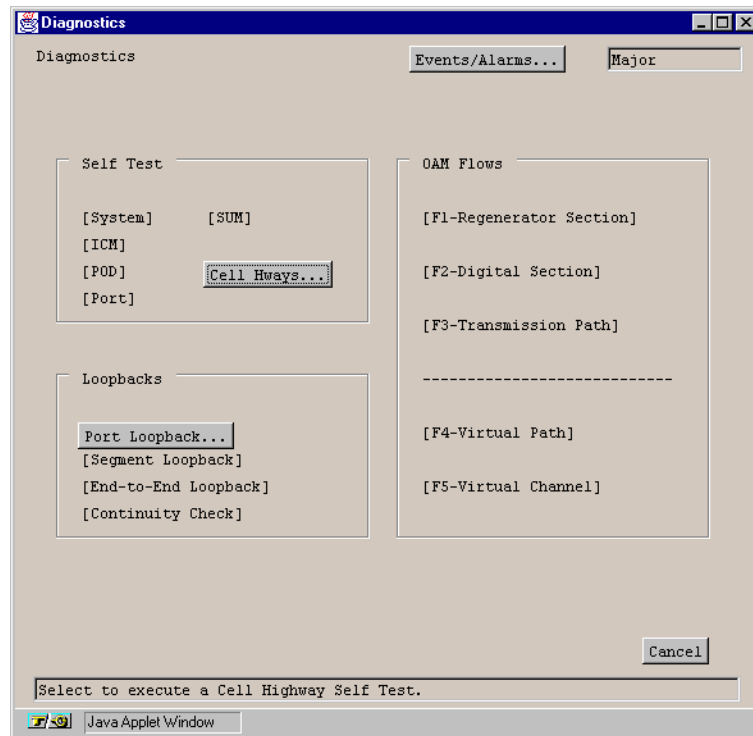
## Testing an SA Unit

This chapter describes how to test SA unit's operation using built-in diagnostics including:

- Cell highway diagnostics (refer to [page 8-3](#))
- Port loopback diagnostics (refer to [page 8-7](#))
- Intentional error insertion (refer to [page 8-15](#))

## Accessing Diagnostics Functions

To access diagnostic functions, choose the Diagnostics button from the Main menu. The Diagnostics window appears (see [Figure 8-1](#)).



**Figure 8-1. Diagnostics Window**

Choose one of the following buttons:

**Cell Hways** – Cell highways diagnostic. See [“Testing Cell Highways” on page 8-3](#) for instructions.

**Port Loopbacks** - Port loopback diagnostics test a port by creating paths within the port circuitry that enable you to route test data back to its source for validation. See [“Testing with Port Loopbacks” on page 8-7](#) for instructions.



You can also access Port Loopbacks by selecting ports in the Interface Management window.

## Testing Cell Highways

To run diagnostics testing on an ICM's Cell Highways:

1. Select Cell Hways from the Diagnostics menu. The Select Slot (ICM) window appears: (Figure 8-2):

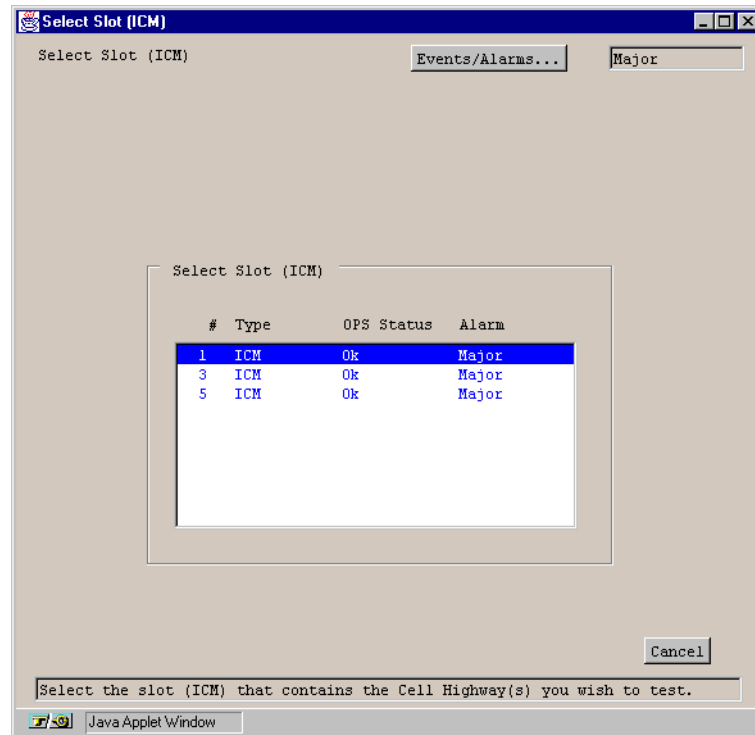


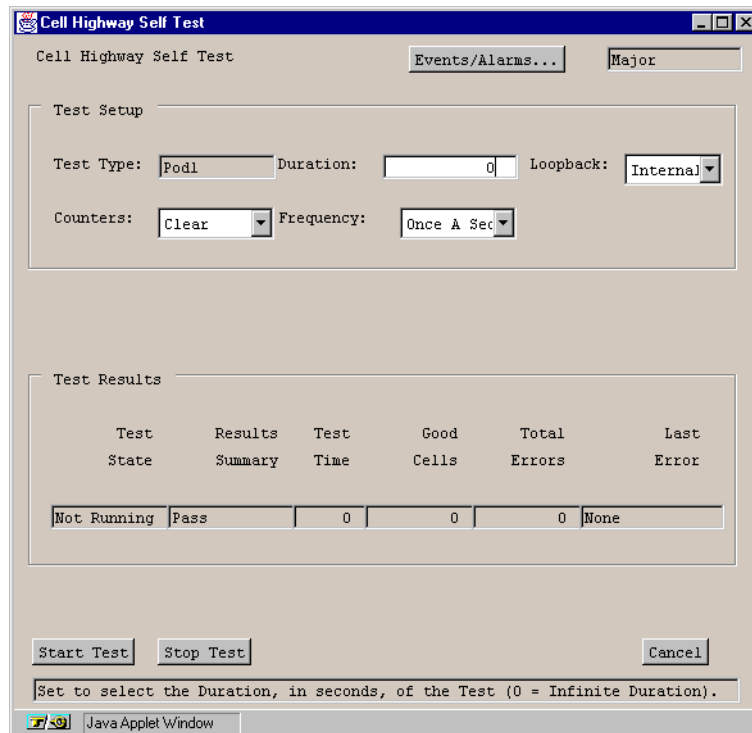
Figure 8-2. Select Slot (ICM) Window

- From the Select Slot (ICM) list, choose the ICM whose cell highways you wish to test. The Select Cell Highways Self Test window appears (Figure 8-3):

Test Type	Test State	Results Summary	Test Time	Good Cells	Total Errors	Last Error
Pod1 Not Running		Pass	0	0	0	None
Pod2 Not Running		Pass	0	16	0	None
Xpod Not Running		Pass	0	16	0	None
Proto Acc Not Running		Pass	0	6	0	None
System Not Running		Pass	0	32	0	None

**Figure 8-3. Select Cell Highways Self Test Window**

3. Choose the cell highway you want to test from the Select Cell Highway Self Test list. The Cell Highway Self Test Window appears (Figure 8-4):



The screenshot shows a Java Applet Window titled "Cell Highway Self Test". At the top, there are buttons for "Events/Alarms..." and a dropdown menu set to "Major". Below this is a "Test Setup" section with fields for "Test Type" (set to "Pod1"), "Duration" (set to "0"), "Loopback" (set to "Internal"), "Counters" (set to "Clear"), and "Frequency" (set to "Once A Sec"). Below the setup section is a "Test Results" section containing a table with columns: Test State, Results Summary, Test Time, Good Cells, Total Errors, and Last Error. The table has one row with the following values: "Not Running", "Pass", "0", "0", "0", and "None". At the bottom of the window are three buttons: "Start Test", "Stop Test", and "Cancel". A text box at the very bottom says "Set to select the Duration, in seconds, of the Test (0 = Infinite Duration)."

Test State	Results Summary	Test Time	Good Cells	Total Errors	Last Error
Not Running	Pass	0	0	0	None

**Figure 8-4. Cell Highways Self Test Window**

4. Complete the fields described in Table 8-1 and choose Start Test to begin running a self test on the cell highway according to the parameters you have selected.

**Table 8-1. Cell Highway Self Test Fields and Buttons**

Field/Button	Type	Description
<b>(Test Setup)</b>		
Test Type	read-only	Displays the type of test selected.
Duration	read/write	Specify the duration of the self test in seconds. (0 = infinite duration; runs until cancelled.)
Loopback	read/write	Specify the loopback method for the test: Internal or External.
Counters	read/write	Specify whether to clear or accumulate test counters when the test begins.
Frequency	read/write	Specify how often the test is to be run.
<b>(Test Results)</b>		
Test State	read-only	Displays the current testing state: Not Running or the name of the component being tested.
Results Summary	read-only	Displays a brief description of the test results: Pass or Fail.
Test Time	read-only	Displays the total run-time of the test.
Good Cells	read-only	Displays the total number of good cells passed during the test.
Total Errors	read-only	Displays the total number of errors recorded during the test.
Last Error	read-only	Displays the last error recorded before the test was halted.
<b>(Other Buttons)</b>		
Start Test	command button	Start the cell highway self test according to the parameters selected in the Test Setup frame.
Stop Test	command button	Stop the test and display the results in the Test Results frame.

## Testing with Port Loopbacks

To perform port loopback tests:

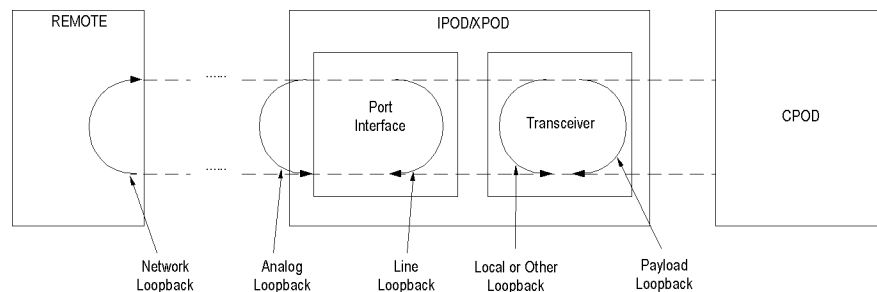
1. From the Main menu, choose either the Diagnostics or Interface Management button. If you choose Interface Management, skip Step 2.
2. If you chose the Diagnostics button in Step 1, the Diagnostics window appears. Choose the Port Loopbacks button.
3. When the Interface Management window appears, select the port you wish to test using the same procedure you use for selecting a port to configure, i.e., by double-clicking the desired port in the window (refer to [“Selecting a Port” on page 4-7](#)).
4. When the configuration window for the selected port appears, select the desired port loopback from the Set Port Loopback field in the Fault Management frame, and click Apply or OK to begin the test. The test will continue until you return the Set Port Loopback field to (port type)NoLoop and choose OK or Apply.

You can select various port loopbacks depending on the port type you select for testing: DS1/E1, DS3/E3, or OC-3c/STM-1. The following sections describe the port loopbacks available for each type port.

## Testing DS1/E1 Ports

Six port loopbacks are available with DS1/E1 ports, shown in **Figure 8-5**.

- **Payload** – Payload loopback tests the internal circuitry of a DS1/E1 port by routing received data through the port receiver and transmitter circuitry and back out of the port.
- **Line** – Line loopback tests the port interface by routing received data back out of the port.
- **Local** – loops data back towards the CPOD. On an IMA POD, the data gets looped back toward the IMA chip.
- **Analog** – enables a metallic loopback at the port.
- **Network** – generates an inband ‘loop activate’ code to instruct the remote end to perform a line loopback test.
- **OtherLoop** – presently provides the same function as local loopback.



**Figure 8-5. DS1/E1 POD Port Loopbacks**

**To perform a port loopback test** — Select the desired test from the Set Port Loopback field and choose OK or Apply to begin the test. Use the Monitor Status function to check the progress of the test.

**To stop a port loopback test** — Select None from the Set Port Loopback field and choose OK or Apply.

**To insert intentional errors into the loopback** — Select the desired error from the Set Error Insertion field:

- *TxYellow* – This enables the insertion of yellow alarms in the transmit path.
- *TxAIS* – This enables the insertion of alarm indication signal (AIS) alarms in the transmit path.
- *TxEIFasError* – (E1 only) This enables the insertion of frame alignment errors in the transmit path.



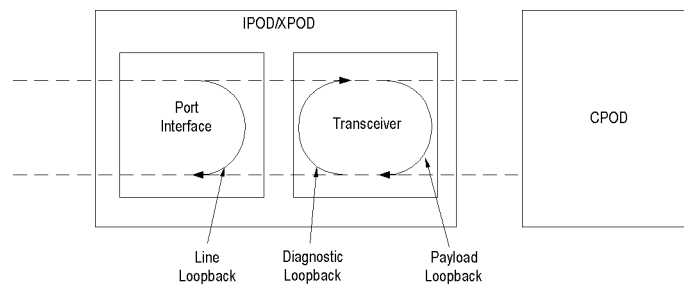
- *TxEITS16AIS* – (E1 only) This enables the insertion of time-slot 16 alarm indication signal (AIS) alarms in the transmit path.
- *TxEIMASerror* – (E1 only) This enables the insertion of multiframe alignment errors in the transmit path.

**To stop intentional error insertion** — Select None from the Set Error Insertion field and choose OK or Apply.

## Testing DS3/E3 Ports

Three port loopbacks are available with DS3/E3 ports, shown in **Figure 8-6**:

- **Line** – Line loopback tests a DS3/E3 port interface by routing received data back out of the port.
- **Diagnostic** – Diagnostic loopback tests the internal circuitry of a DS3/E3 port by routing transmit data back through the port receiver.
- **Payload** – Payload loopback tests the internal circuitry of a DS3/E3 port by routing received data to through the port receiver and transmitter circuitry and back out of the port.



**Figure 8-6. DS3/E3 POD Loopbacks**

**To perform a port loopback test** — Select the desired test from the Set Port Loopback field and choose OK or Apply to begin the test. Use the Monitor Status function to check the progress of the test.

**To stop a port loopback test** — Select None from the Set Port Loopback field and choose OK or Apply.

**To insert intentional errors into the loopback** — Select the desired error from those that are available in the Set Error Insertion field:

- *TxLOS* – This enables the insertion of loss of signal alarms in the transmit path.
- *TxAIS* – This enables the insertion of alarm indication signal (AIS) alarms in the transmit path.
- *TxFERF* – This enables the insertion of far end receive failure (FERF) or yellow alarms in the transmit path.
- *TxIdle* – (DS3 only) This enables the insertion of idle maintenance signals in the transmit path.
- *TxLCV* – This enables the insertion of line code violations (LCV) in the transmit path.

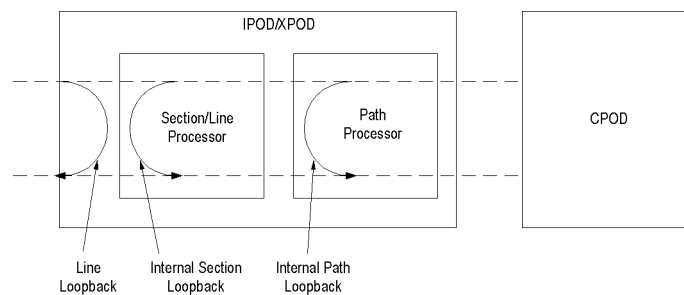
- *TxPbitErrs* – (DS3 only) This enables the insertion of P-bit errors in the DS3 stream.
- *TxCbitErrs* – (DS3 using C-bit framing only) This enables the insertion of C-bit parity errors in the DS3 stream.

**To stop intentional error insertion** — Select None from the Set Error Insertion field and choose OK or Apply.

## Testing OC-3c/STM-1 Ports

Three port loopbacks are available with OC-3c/STM-1 ports, shown in **Figure 8-7**:

- **Line** – Line loopback tests an OC-3c/STM-1 port interface by routing received data back out of the port.
- **Internal Section** – Internal section loopback tests the internal circuitry of a OC-3c/STM-1 port by routing received data through the port receiver and transmitter circuitry and back out of the port.
- **Internal Path** – Internal path loopback tests a OC-3c/STM-1 port interface by routing received data back out of the port.



**Figure 8-7. OC-3c/STM-1 POD Loopbacks**

**To perform a port loopback test** — Select the desired test from the Set Port Loopback field and choose OK or Apply to begin the test. Use the Monitor Status function to check the progress of the test.

**To stop a port loopback test** — Select None from the Set Port Loopback field and choose OK or Apply.

**To insert intentional errors into the loopback** — Select the desired error from the Set Error Insertion field:

- *TxDigitalLOS* – This enables the insertion of digital loss of signal (LOS) alarms in the transmit path.
- *TxLineAIS* – This enables the insertion of line alarm indication signal (AIS) alarms in the transmit path.
- *TxLineRDI* – This enables the insertion of line remote defect indication (RDI) or line yellow alarms in the transmit path.
- *TxFrameBitErr* – This enables the insertion of frame bit errors in the transmit path.
- *TxSectBipErr* – This enables the insertion of section BIP errors in the transmit path.

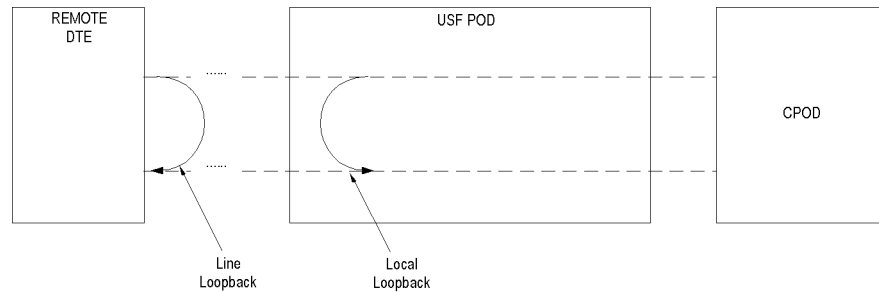
- *TxLineBipErr* – This enables the insertion of line BIP errors in the transmit path.

**To stop intentional error insertion** — Select None from the Set Error Insertion field and choose OK or Apply.

## Testing Universal Serial Ports

Three port loopbacks are available with USF ports, shown in **Figure 8-8**:

- **Line** – Line loopback tests a USF port interface by routing received data back out of the port.
- **Local** – Local loopback tests the internal circuitry of a USF port by looping data back towards the CPOD.



**Figure 8-8. Universal Serial Frame POD Loopbacks**

**To perform a port loopback test** — Select the desired test from the Set Port Loopback field and choose OK or Apply to begin the test. Use the Monitor Status function to check the progress of the test.

**To stop a port loopback test** — Select None from the Set Port Loopback field and choose OK or Apply.

**Insertion of intentional errors into the loopback** — not currently supported.

## Inserting Intentional Errors

The error insertion feature is available on DS1, E1, DS3, E3, and OC-3c/STM-1 ports and OC-3c/STM-1 paths. In addition to using this feature in conjunction with port loopback tests (as already described), you may use this feature as a self-contained diagnostic to test a port or OC-3c/STM-1 path.

### Inserting Errors to Test a Port

To intentionally insert errors on a DS1, E1, DS3, E3 or OC-3c/STM-1 port:

1. In the Fault Management frame of the Configure window for the port you wish to test, select the desired error from the Set Error Insertion field and choose OK or Apply.
2. Use the Monitor Status function of WebXtend to check the progress of the test.
3. To stop intentional error insertion, select None from the Set Error Insertion field and choose OK or Apply.

### Inserting Errors to Test an OC-3c/STM-1 Path

To intentionally insert errors in an OC-3c/STM-1 path:

1. In the Fault Management frame of the Configure OC-3/STM-1 Path window, select the desired error from the Error Insertion field and choose OK or Apply.
2. Use the Monitor Status function to check the progress of the test.
3. To stop intentional error insertion, select None from the Error Insertion field and choose OK or Apply.

## **What's Next?**

After you have learned to test the SA unit, refer to Chapter 9, “Using System Utilities”, for information on functions such as saving configurations and shutting down the SA unit.



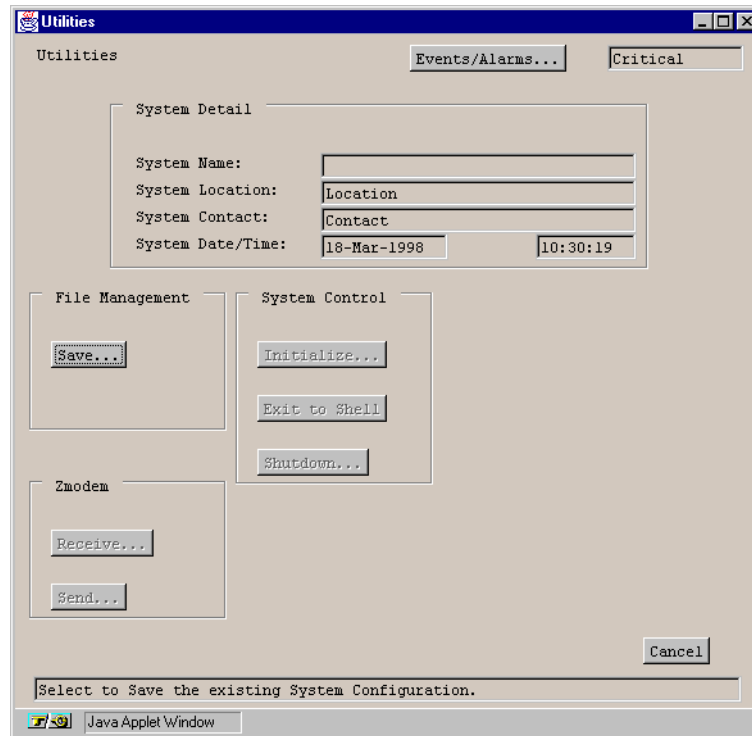
## Using Utilities

This chapter describes how to:

- Save an SA unit's configuration (refer to [page 9-4](#))
- Initialize an SA system (refer to [page 9-5](#))
- Shut down the SA system (refer to [page 9-5](#))
- Exit to the shell operating system (refer to [page 9-5](#))
- Send and receive files using the Zmodem file transfer protocol (refer to [page 9-5](#))

## Accessing SA Utilities

To use the SA utilities, choose the Utilities button from the Main menu. The Utilities window (see [Figure 9-1](#)) appears.



**Figure 9-1. Utilities Window**

In addition to buttons that provide access to utility tasks, the Utilities window contains fields that provide information about the SA system. [Table 9-1](#) describes the fields and buttons in the Utilities window.

**Table 9-1. Utilities Fields and Buttons**

Field/Button	Type	Description
<b>System Detail</b>		
System Name	read-only	Displays the name of the SA unit.
System Location	read-only	Displays the name of the site where the SA unit is located.
System Contact	read-only	Displays contact information for the SA unit.
System Date/Time	read-only	Displays the SA unit date and time.
<b>File Management</b>		
Save	window button	Enables you to save current configuration file.
<b>System Control</b>		
Initialize	n/a	This function is not available through the WebXtend browser interface. Use the Craft interface for this function. See Appendix A for details.
Exit to Shell	n/a	This function is not available through the WebXtend browser interface. Use the Craft interface for this function. See Appendix A for details.
Shutdown	n/a	This function is not available through the WebXtend browser interface. Use the Craft interface for this function. See Appendix A for details.
<b>Zmodem</b>		
Receive	n/a	This function is not available through the WebXtend browser interface. Use the Craft interface for this function. See Appendix A for details.
Send	n/a	This function is not available through the WebXtend browser interface. Use the Craft interface for this function. See Appendix A for details.

## Saving Configurations

You can save the current configuration of the SA unit when you log off or at any time using the Utilities function.



**IMPORTANT:** SA units do not save configurations automatically. You must click in the Save Configuration box of the Logoff window to save a configuration. After clicking the Save Configuration box, select Yes. The dialog box reads “Saving...” and shows a progress indicator. When the dialog box vanishes, it is safe to turn off the unit.

**WARNING:** Turning off an SA unit before it has finished saving configuration data can cause corruption of the configuration file and result in improper operation of the unit the next time it is booted up.

To save configuration at logoff:

- Select the Save Configuration radio button in the Log Off window.

To save the configuration at any other time, choose the Save button in the File Management frame of the Utilities window. The Save Configuration File window appears, enabling you to save the configuration immediately or at a future specified date and time (not yet supported).

- To save the configuration immediately, click in the box labeled Now, then choose OK.
- In a future software release, you will also have the ability to schedule a Save Configuration to occur at a specified date and time.



It is a good idea to back up your SA unit’s configuration file periodically, so that it may be quickly restored if necessary. This procedure is described in **“Using FTP to Back Up Configuration Data” on page C-2.**

## Initializing the System

Initializing the SA unit is not supported in the WebXtend browser interface. To initialize the SA system, use the Craft interface as described in [Appendix A, “Using the Craft Interface”](#).

## Shutting Down the System

Shutting down the SA unit is not supported in the WebXtend browser interface. To shut down the SA system, use the Craft interface as described in [Appendix A, “Using the Craft Interface”](#).

## Exiting to the Shell

Exiting to the Shell is not supported in the WebXtend browser interface. To exit to the shell operating system of the SA unit, use the Craft interface as described in [Appendix A](#).

## Transferring Files with Zmodem

File transfers are not supported in the WebXtend browser interface. To transfer files to and from the SA system using Zmodem, use the Craft interface as described in [Appendix A, “Using the Craft Interface”](#). To transfer files to and from the SA unit using FTP, see [Appendix C, “Using FTP to Transfer Files”](#).

## **What's Next?**

You've now completed the general instructions for configuring, operating, managing, and testing the SA unit. For troubleshooting information, refer to Chapter 10. For additional information on using the SA unit, refer to the Appendices of this manual.

# Resolving Problems

This chapter describes how to troubleshoot an SA unit and provides Customer Support information.

## Technical Support Checklist

Before placing a call to the Ascend Technical Assistance Center, review the following checklist to make sure you have gathered all the information you need:

- The SA unit's serial number
- A list of the PODs installed in the ICMs
- Type of management interface (craft or ethernet)
- The SA unit's IP address and subnet mask

Please have access to your SA unit when calling the Ascend Technical Assistance Center.

## Contacting the Technical Assistance Center

Ascend provides a full range of support to ensure that maximum network uptime is achieved with low equipment cost. Ascend's Technical Assistance Center can assist you with any problems you may encounter when using an SA unit. You can contact the Technical Assistance Center by phone, electronic mail (email), or fax.

### Phone

Ascend offers support 24 hours a day, 7 days a week. To contact Ascend's Technical Assistance Center by phone, call:

1-800-DIAL-WAN or 1-978-692-2600 (in the U.S. and Canada)

0-800-96-2229 (in the United Kingdom)

1-978-952-7299 (all other areas)

### E-mail and Fax

Include the following information when requesting assistance electronically (by email or fax):

- Your name, your company name, and your telephone number
- Name of contact person and their telephone number (if different from above)
- Brief description of the problem
- List of identifiable symptoms



To contact Ascend's Technical Assistance Center by email, address your email to:

`cs@casc.com`

To contact Ascend's Technical Assistance Center by fax, call:

1-978-392-9768

# Using the Craft Interface

This appendix describes:

- Setting up the VT100 Terminal to access an SA unit (see [page A-2](#))
- The SA unit's boot sequence (see [page A-3](#))
- The functions and features of the craft interface (see [page A-4](#))
- How to access the craft interface (see [page A-6](#))
- Craft interface conventions (see [page A-7](#))
- How to perform functions unique to the craft interface (see [page A-9](#))

## Setting up the VT100 Terminal

Before you access the craft interface:

1. Make the necessary connections to the craft interface, as described in the SA unit's *Hardware Installation Guide*.
2. Set your VT100 terminal or your computer terminal emulator software to the following parameters (if you are accessing the craft interface remotely, set your modem to the same parameters):
  - 38,400 bps data rate
  - 8 data bits, no parity, 2 stop bits
  - software flow control (XON/XOFF) enabled
  - hardware flow control (RTS/CTS, DSR/DTR) disabled
  - VT100 terminal emulation display selected

## About the SA Unit's Boot Sequence

When an SA unit is powered up, it follows a defined boot sequence. [Table A-1](#) shows the sequence of events, what is shown on the screen during each segment of the boot sequence, and what access is available during each period.

Procedure Name	Screen Shows:	What you may access...
Initial boot sequence	Press SPACEBAR if you want to send a new boot file...  2... 1...	For Ascend technical service personnel only.
Boot service terminal	Booting...  Hit the enter key to begin the boot service terminal.  Counting down to SA-600 system boot...  0  Booting SA-600...	For use only when upgrading SA software. See <a href="#">Appendix D, "Upgrading the SA Unit's Software"</a> for details.  Please use the Exit to Shell command from the Utilities menu (see <a href="#">"Accessing the SA Unit's Operating System Shell"</a> on <a href="#">page A-11</a> ) to access OASOS commands.
Login prompt	Login:  Password:	Enter your user name and password to access the craft interface main menu, described in <a href="#">"Accessing the Craft Interface"</a> on <a href="#">page A-6</a> .

**Table A-1. Boot Sequence**

## About the Craft Interface

The craft interface enables you to configure, monitor, and control the SA unit locally or remotely using a series of menu-driven screens on a VT100 terminal or on a computer running VT100 terminal-emulation software.

All the functions and windows available in WebXtend are also available through the craft interface. Since the craft interface consists of text-based windows versus the graphic user interface (GUI) of WebXtend, its windows look different but provide exactly the same functions as their WebXtend counterparts. For a comparison, see [Figure A-1](#) and [Figure A-2](#), which illustrate the craft interface and WebXtend versions of the System Administration window.

In addition to supporting all the functions accessible with WebXtend, the craft interface also provides two additional functions that are not supported by WebXtend:

- Zmodem file transfer
- SA operating system (OASOS) access

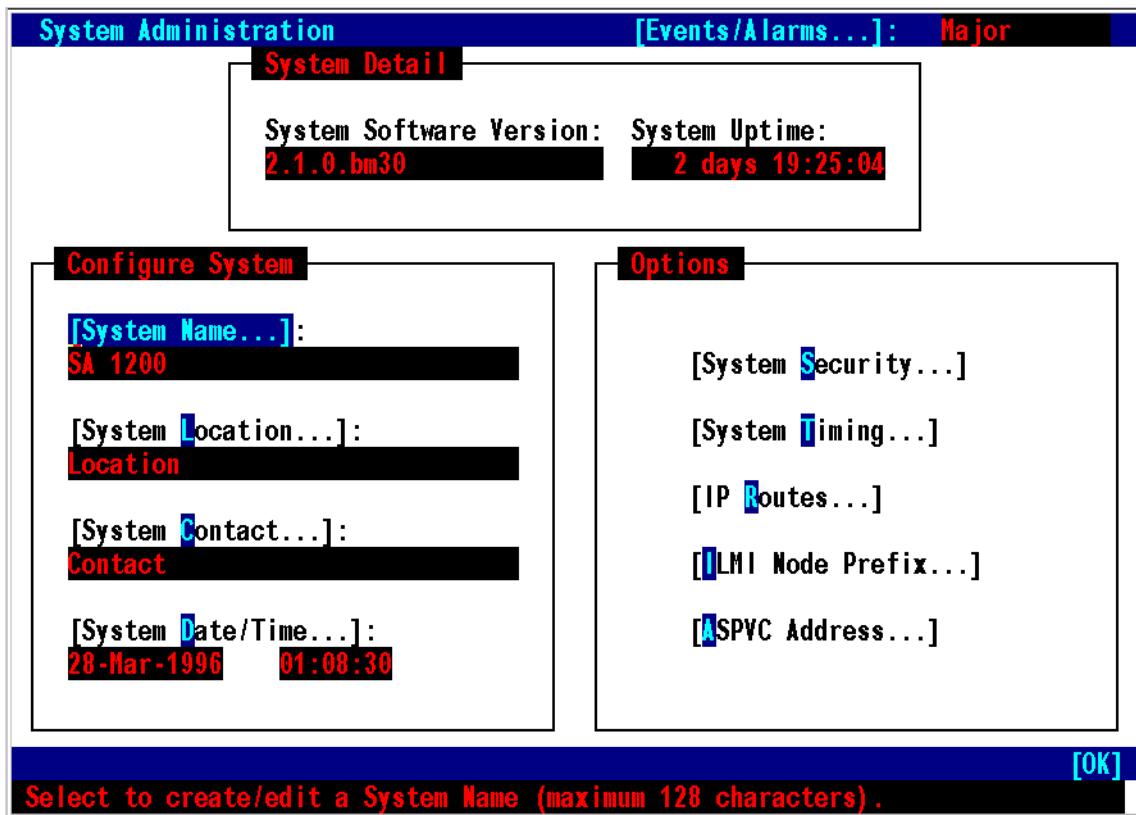


Figure A-1. System Administration Window — Craft Interface Version

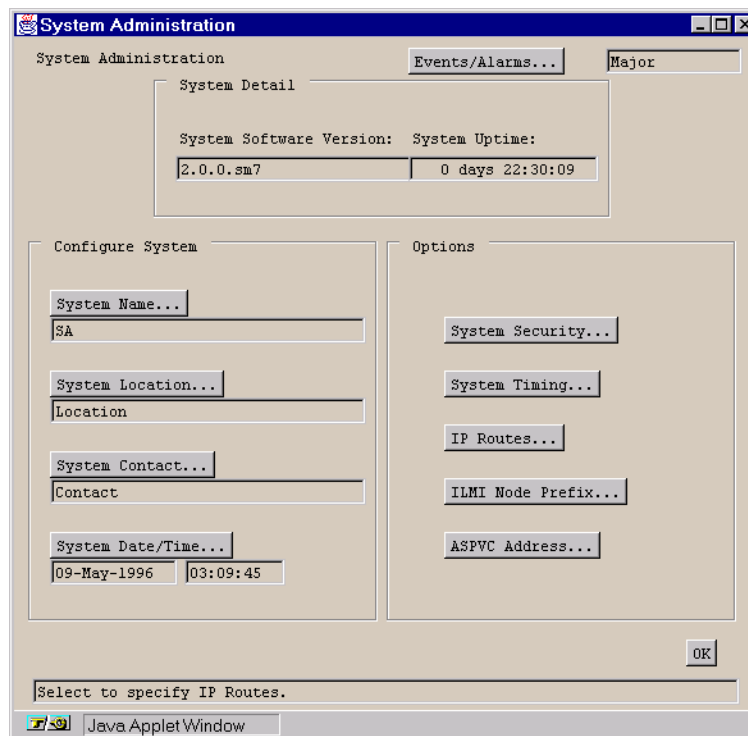


Figure A-2. System Administration Window — WebXtend Version

## Accessing the Craft Interface

To access the craft interface:

1. Power up the SA unit by toggling on the power switch(es) located on the front panel of the unit.
2. Upon power-up, the SA unit displays a number of messages in your terminal window as the system boots. After approximately one minute, the system prompts you for login.
3. Type your user name at the Login prompt (“root” is the default user name) and press Enter.
4. Type your password at the Password prompt (“ascend” is the default password) and press Enter.

After accepting your password, the SA unit displays the Main menu of the craft interface.



Upon logging in to the SA unit for the first time, you should use the System Administration>System Security menu item to establish a new user name and password and disable the default user name and password, to prevent unauthorized access to the unit. See “**Setting System Security**” on page 3-5 for instructions on establishing a new user and assigning a password.

## Craft Interface Conventions

In order to use the craft interface efficiently, you should be familiar with its conventions.

### Navigating Buttons and Fields

There are two ways to navigate the buttons and user-selectable fields that appear in each craft interface window.

- You can use the Tab, Arrow, Enter, and Space Bar control keys.
  - To move between buttons and user-selectable fields, use the Tab and Arrow key.
  - To choose a highlighted button or highlighted option in a user-selectable field, use the Enter key.



Highlighted buttons and fields contain reversed text, i.e., black text on a light background.

- To place or remove an X in a user-selectable field, use the Tab and/or Arrow key to move the cursor to the field, then press the Space Bar to place or remove the X in that field.
- You can use alphanumeric keys.

The names of some buttons and user-selectable fields contain an alphanumeric character displayed in reverse text. Typing that highlighted character and the Enter key causes the cursor to move to that button or field.



You can select OK, Cancel and Apply buttons at any time by typing O, C and A, respectively, followed by the Enter key.

### Activating Pull-down Menus

To use pull-down menus in the craft interface, select the menu by using the arrow keys as described above, then press F2 to display the pull-down menu options. Use the arrow keys to make your selection, then press the Enter key.



## OK vs. Cancel vs. Apply Buttons

OK, Cancel and Apply buttons appear in various craft interface windows. These buttons serve the following functions:

- **OK** — confirms all previous actions you have performed in a window and then closes that window. It also saves all configuration work you performed in that window.
- **Apply** — confirms all previous actions you have performed, but it keeps the window opened for further work. It also saves all configuration work you performed in that window.
- **Cancel** — performs the opposite function of the OK button. It negates all previous actions you have performed in a window and then closes that window. All configuration work you performed in that window is lost.

## Events/Alarms Button/Field

In the upper-right corner of each craft interface full-size window is an Events/Alarms field and button, which serves the following functions:

- Events/Alarms field displays the current highest level alarm (Critical, Major, or Minor), if any, detected by the SA unit.
- Events/Alarms button permits you to obtain a summary of any the current events and alarms.

## Help Field

Near the bottom of each craft interface window is a Help field. This field provides a brief, one-line description of whatever button or selectable field is currently highlighted in that window.

## Using the Craft-Only Functions

The following sections describe how to use the craft interface to perform those functions that are not accessible with WebXtend. (For those functions that are accessible with the craft interface *and* WebXtend, see Chapters 2 through 10.)

### Transferring Files with Zmodem

The SA unit supports the Zmodem file transfer protocol, which enables you to upload configuration files and new software from your computer to an SA unit, or to download configuration files from the SA unit to your computer for backup.



Your computer must have a terminal emulator or data communications program that supports the Zmodem file transfer protocol in order to use this function.

There are two ways of accessing the Zmodem function from the craft interface:

- From the Utilities window of the interface
- During the SA unit's power-up sequence. *This option is for Ascend Technical Service personnel only.*



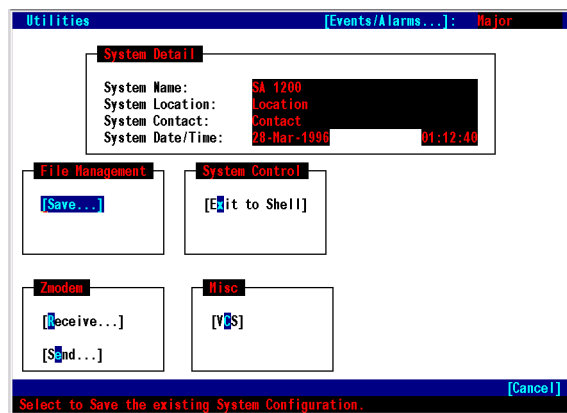
When you access the Zmodem function during the SA unit's power-up sequence, its functionality is limited to receiving new a boot file only. Only Ascend Technical Service personnel should access the boot-sequence Zmodem utility.

## Accessing Zmodem from the Utilities Window

To access the Zmodem function from the Utilities window:

1. Choose the Utilities button from the Main menu of the craft interface.
2. When the Utilities window appears (see [Figure A-3](#)), choose the Send or Receive button in the Zmodem frame of that window.

► The Send and Receive directions are from the perspective of the SA unit. Send transfers a file *from* the SA unit to a Zmodem client over the craft port. Receive sets the SA unit to *receive* an incoming Zmodem file transfer over the craft port.



**Figure A-3. Craft Interface Utilities Window**

After selecting the Send button, you are prompted for a file name to transmit.

After selecting the Receive button, the “You may start the ZModem transfer now” message appears. Send the desired file(s) to the SA unit using the Zmodem file transfer protocol. (See the documentation that accompanies the terminal emulator or data communications software for information on how to use its Zmodem functions.)

► To cancel a Zmodem file transfer, enter CTRL-Xs until the file transfer stops.

3. After completing the file transfer, log off, shut down, and power up the SA unit.

## Accessing the SA Unit's Operating System Shell

The SA unit has an internal operating system called “OASOS” that enables you to perform several functions that are not accessible with WebXtend. However, the typical user only needs OASOS to perform one task: setting the IP address of the SA unit. This function is described in “[Changing the IP address](#)” on page 2-6.

The procedure below describes how to access OASOS. The commands available at the OASOS> prompt are described in [Appendix B, “Operating System \(OASOS\) Command Set”](#).

### Accessing OASOS

To access the SA operating system (OASOS), after logging in to the craft interface:

1. Choose the Utilities button from the Main menu of the craft interface. The Utilities window appears (see [Figure A-3](#)).
2. Choose the Exit to Shell button in the System Control frame of the Utilities window.

When the OASOS prompt appears (OASOS>), you have access to the SA operating system.

# Operating System (OASOS) Command Set

This appendix describes:

- The SA unit's built-in operating system commands

## OASOS Commands

Figure B-1 shows the commands available at the OASOS> prompt.

```
Type "Exit" and press the [Enter] key to return to the user interface.
OASOS> help
cat      clear  cp      echo    help    ls      mv      pwd      rmdir
cd        cmp     date    head    kill    mkdir  ping    rm      sync    touch
sa_cfg    sa_exec sa_flog reboot  rz      telnet sa_wanip sa_trctl
upgrade  sa_rlog sa_flash dump    sz      sa_iplog sa_corip
OASOS>
```

Figure B-1. OASOS Commands

# CAT

## **NAME**

**cat** - concatenate and display

## **SYNOPSIS**

**cat** [ -benstv ] filename

## **DESCRIPTION**

cat reads each filename in sequence and displays it on the standard output. Thus:

```
OASOS>cat goodies
```

displays the contents of goodies on the standard output.

## **OPTIONS**

- b Number the lines, as -n, but omit the line numbers from blank lines.
- e Display non-printing characters, as -v, and in addition display a \$ character at the end of each line.
- n Precede each line output with its line number.
- s Substitute a single blank line for multiple adjacent blank lines.
- t Display non-printing characters, as -v, and in addition display TAB characters as ^I (CTRL-I).
- v Display non-printing characters (with the exception of TAB and NEWLINE characters) so that they are visible. Control characters print like ^X for CTRL-X; the DEL character (octal 0177) print as '^?'. Non-ASCII characters (with the high bit set) are displayed as M-x where M- stands for 'meta' and x is the character specified by the seven low order bits.

## **NOTES**

Using cat to redirect output of a file to the same file, such as cat filename1 > filename1 or cat filename1 >> filename1, does not work. This type of operation should be avoided since it may cause the system to go into an indeterminate state.

## CD

### ***NAME***

**cd** - change working directory

### ***SYNOPSIS***

cd [ directory ]

### ***DESCRIPTION***

*directory* becomes the new working directory.



## CLEAR

### *NAME*

**clear** - clears the terminal screen

## CMP

### ***NAME***

**cmp** - perform a byte-by-byte comparison of two files

### ***SYNOPSIS***

**cmp** [ -ls ] filename1 filename2 [ skip1 ] [ skip2 ]

### ***DESCRIPTION***

cmp compares filename1 and filename2. With no options, cmp makes no comment if the files are the same; if they differ, it reports the byte and line number at which the difference occurred, or, that one file is an initial subsequence of the other. skip1 and skip2 are initial byte offsets into filename1 and filename2 respectively, and may be either octal or decimal; a leading 0 denotes octal.

### ***OPTIONS***

-l    Print the byte number (in decimal) and the differing bytes (in octal) for all differences between the two files.

-s    Silent. Print nothing for differing files.

## CP

### **NAME**

**cp** - copy files

### **SYNOPSIS**

`cp [-i] filename1 filename2 cp -rR [-i] directory1 directory2 cp [-irR] filename... directory`

### **DESCRIPTION**

cp copies the contents of *filename1* onto *filename2*. If *filename1* is a symbolic link, or a duplicate hard link, the contents of the file that the link refers to are copied; links are not preserved.

In the second form, cp recursively copies *directory1*, along with its contents and subdirectories, to *directory2*. If *directory2* does not exist, cp creates it and duplicates the files and subdirectories of *directory1* within it. If *directory2* does exist, cp makes a copy of the *directory1* directory within *directory2* (as a subdirectory), along with its files and subdirectories.

In the third form, each filename is copied to the indicated directory; the base name of the copy corresponds to that of the original. The destination directory must already exist for the copy to succeed.

cp refuses to copy a file onto itself.

### **OPTIONS**

**-i** Interactive. Prompt for confirmation whenever the copy would overwrite an existing file. A y in answer confirms that the copy should proceed. Any other answer prevents cp from overwriting the file.

**-r**

**-R** Recursive. If any of the source files are directories, copy the directory along with its files (including any subdirectories and their files); the destination must be a directory.

### **EXAMPLES**

To copy a file:

```
OASOS> cp goodies goodies.old
```

```
OASOS> ls
```

```
goodies goodies.old
```

To copy a directory, first to a new, and then to an existing destination directory.

```
OASOS> cp -r src bkup
```

```
OASOS> ls -R bkup
```

```
x.c yx z.sh
```

```
OASOS> cp -r src bkup
```

```
OASOS> ls -R bkup
```

```
src xx yx z.sh
```

```
src:
```

```
xx y.c z.sh
```

## DATE

### ***NAME***

**date** - display or set the date

### ***SYNOPSIS***

date [ yyyyymmddhhmm [ ss ] ]

### ***DESCRIPTION***

If no argument is given, date displays the current date and time. Otherwise, the current date is set.

yyyy is the four digits of the year; the first mm is the month number; dd is the day number in the month; hh is the hour number (24 hour system); the second mm is the minute number; ss (optional) specifies seconds. The year may be omitted; the current year is supplied as default.

### ***EXAMPLES***

**date 10080045**

sets the date to Oct 8, 12:45 A.M. of the current year.

## ECHO

### ***NAME***

**echo** - echo arguments to the standard output

### ***SYNOPSIS***

echo [ -n ] [ argument ... ]

### ***DESCRIPTION***

echo writes its arguments on the standard output. Arguments must be separated by SPACE characters or TAB characters, and terminated by a NEWLINE.

### ***OPTIONS***

-n Do not add the NEWLINE to the output.

## HEAD

### ***NAME***

**head** - display first few lines of specified files

### ***SYNOPSIS***

head [ -n ] filename...

### ***DESCRIPTION***

head copies the first n lines of each filename to the standard output. The default value of n is 10 lines.

When more than one file is specified, the start of each file looks like:

```
==>filename<==
```

### ***EXAMPLE***

The following example:

```
OASOS> head -4 junk1 junk2
```

produces:

```
=> junk1 <==
```

```
This is junk file one
```

```
=> junk2 -
```

```
This is junk file two
```

## HELP

### **NAME**

**help** - get help about shell commands

### **SYNOPSIS**

help [ command-name ]

### **DESCRIPTION**

help prints to the console information about shell commands. If no command name is given, help prints out a list of shell commands. If a valid command name is given, help prints out information about that command.

### **OPTIONS**

NONE

### **EXAMPLE**

```
OASOS> help
```

cat	MP	echo	help	mkfs	pcmount
cd	Cp	getid	kill	mount	ping
clear	date	getpri	Ls	MV	popd
console	du	head	mkdir	pcmkfs	pushd

```
OASOS> help cat
```

```
cat - concatenate and display (reentrant, not locked)
```



## KILL

### ***NAME***

**kill** - terminate a task

### ***SYNOPSIS***

kill tname|-tid

### ***DESCRIPTION***

kill will terminate a task named tname or a task with a tid. It does this by calling t\_restart with a second argument of -1. The task must be designed to read this second argument and do its own resource clean up then terminate.

### ***OPTIONS***

NONE

### ***EXAMPLE***

```
OASOS> kill tftd
```

## LS

### **NAME**

**ls** - list the contents of a directory

### **SYNOPSIS**

**ls** [ -aACdfFgilqrRsl ] filename ...

### **DESCRIPTION**

For each filename which is a directory, **ls** lists the contents of the directory; for each filename which is a file, **ls** repeats its name and any other information requested. By default, the output is sorted alphabetically. When no argument is given, the current directory is listed. When several arguments are given, the arguments are first sorted appropriately, but file arguments are processed before directories and their contents.

### **OPTIONS**

- a List all entries.
- A (**ls** only) Same as -a, except that '.' and '..' are not listed.
- C Force multi-column output, with entries sorted down the columns; for **ls**, this is the default when output is to a terminal.
- d If argument is a directory, list only its name (not its contents); often used with -l to get the status of a directory.
- f Force each argument to be interpreted as a directory and list the name found in each slot. This option turns off -l, -s, and -r, and turns on -a; the order is the order in which entries appear in the directory.
- F Mark directories with a trailing slash ('/'), executable files with a trailing asterisk ('\*').
- g For **ls**, show the group ownership of the file in a long output.
- i For each file, print the i-number in the first column of the report.
- l List in long format, giving mode, number of links, owner, size in bytes, and time of last modification for each file. If the time of last modification is greater than six months ago, it is shown in the format 'month date year'; files modified within six months show 'month date time'.
- q Display non-graphic characters in filenames as the character '?'; for **ls**, this is the default when output is to a terminal.
- r Reverse the order of sort to get reverse alphabetic or oldest first as appropriate.

- R Recursively list subdirectories encountered.
- s Give size of each file, including any indirect blocks used to map the file, in kilobytes.
- l Force single-column output.

## **MKDIR**

This command reserved for Ascend technician use only.

## MV

### ***NAME***

**mv** - move or rename files

### ***SYNOPSIS***

**mv** [-if] filename1 filename2

**mv** [-if] directory1 directory2

**mv** [-if] filename... directory

### ***DESCRIPTION***

mv moves files and directories around in the file system. A side effect of mv is to rename a file or directory. The three major forms of mv are shown in the synopsis above.

The first form of mv moves (changes the name of) filename1 to filename2. If filename2 already exists, it is removed before filename1 is moved.

The second form of mv moves (changes the name of) directory1 to directory2, only if directory2 does not already exist - if it does, the third form applies.

The third form of mv moves one or more filenames (may also be directories) with their original names, into the last directory in the list.

mv refuses to move a file or directory onto itself.

### ***OPTIONS***

**-i** Interactive mode. mv displays the name of the file followed by a question mark whenever a move would replace an existing file. If you type a line starting with y, mv moves the specified file, otherwise mv does nothing with that file.

**-f** Force. Override any mode restrictions and the -i option.

## PING

### ***NAME***

**ping** - send ICMP ECHO\_REQUEST packets to network hosts

### ***SYNOPSIS***

ping [ -s ] host\_address [ timeout ]

### ***DESCRIPTION***

ping utilizes the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from the specified host, or network gateway. ECHO\_REQUEST datagrams, or "pings," have an IP and ICMP header, followed by a struct timeval, and then an arbitrary number of bytes to pad out the packet. If host responds, ping will print host is alive on the standard output and exit. Otherwise after timeout seconds, it will write no answer from host. The default value of timeout is 10 seconds.

When the -s flag is specified, ping sends one datagram per second, and prints one line of output for every ECHO\_RESPONSE that it receives. No output is produced if there is no response. The default datagram packet size is 64 bytes.

When using ping for fault isolation, first 'ping' the local host to verify that the local network interface is running.

### ***EXAMPLE***

```
OASOS> ping 192.103.54.190
PING (192.103.54.190): 56 data bytes
192.103.54.190 is alive
```

## PWD

### ***NAME***

**pwd** - display the pathname of the current working directory

### ***SYNOPSIS***

pwd

### ***DESCRIPTION***

pwd prints the pathname of the working (current) directory.

### ***OPTIONS***

NONE

### ***EXAMPLE***

```
OASOS> cd 5.5/usr
```

```
OASOS> pwd
```

```
5.5/usr
```

## REBOOT

### ***NAME***

**reboot** - reboots the SA unit

### ***SYNOPSIS***

reboot [#]

### ***DESCRIPTION***

Reboots the SA unit after prompting you for confirmation.

### ***OPTIONS***

# enter a slot number (3 or 5) to reboot an individual ICM. Entering slot 1 reboots the entire system.

### ***EXAMPLE***

```
OASOS> reboot
```

```
OASOS> reboot 3
```



## **RMDIR**

This command reserved for Ascend technician use only.

## RZ

### ***NAME***

**rz** - receive Zmodem

### ***SYNOPSIS***

**rz**

### ***DESCRIPTION***

Sets the SA unit to receive mode, awaiting a Z-modem file transfer.

### ***OPTIONS***

None

### ***EXAMPLE***

```
OASOS> rz
```

### ***NOTES***

While in shell mode, any incoming Z-modem file transfers are auto-detected. There is no need to issue an additional rz command to receive an incoming Z-modem file transfer.

## SA\_CFG

### **NAME**

**sa\_cfg** - configure SA unit IP address, subnet mask and serial port baud rate, enable/disable WAN IP access (see SA\_WANIP for details), enable/disable Core IP access (see SA\_CORIP for details).

### **SYNOPSIS**

sa\_cfg

### **DESCRIPTION**

sa\_cfg enables you to configure the SA unit's management IP address, management IP subnet mask, and the baud rate for the console serial port. Enter each item when prompted, pressing ENTER after each one. Baud rates up to 38.4kbps are supported.

You are also prompted to enable/disable WAN IP access. If you select Y (enable), you are also prompted to complete the WAN IP information (see [page B-33](#)).

You are also prompted to enable/disable Core IP access. If you select Y (enable), you are also prompted to complete the Core IP information (see [page B-24](#)).

### **OPTIONS**

None

### **EXAMPLE**

```
OASOS> sa_cfg
```

## SA\_CORIP

### **NAME**

**sa\_corip** - enables you to establish a single IP management tunnel between an SA unit and an Ascend CBX 500 or GX 550 ATM switch for use managing the SA unit across an ATM WAN.

### **SYNOPSIS**

sa\_corip

### **DESCRIPTION**

Suppose that you have an SA unit connected via an ATM connection to an Ascend CBX 500 or GX 550 ATM switch. You want to manage the SA unit remotely via WebXtend (TCP/IP) across the ATM cloud. The sa\_corip command enables you to define a single IP management tunnel for this application.

The Core IP management parameters may be collected during sa\_cfg command (see sa\_cfg command) or separately using the sa\_corip command.

The core IP parameters are stored in the SA unit's flash memory separately from the file system. This ensures that the parameters for a core IP management interface are preserved across software upgrades or flash file system formatting.



The Core IP command differs from the WAN IP command in that the core IP management interface, once configured, will be created regardless of the presence of an nv\_db.dat file.

### **EXAMPLES**

```
OASOS> sa_corip
```

Enter each of the following items when prompted, pressing ENTER after each one. Default values are shown in **bold**.

Parameter	Value	Notes
Enable Core IP	Y, N	Defines whether or not the Core IP restore feature is enabled.
Enter Core IP addr	<b>11.22.33.1</b>	Enter the SA unit's IP address.
Enter Core IP remote addr	<b>11.22.33.2</b>	Enter the CBX 500 or GX 550 ATM switch's IP address.

Parameter	Value	Notes
Enter Core IP subnet mask	<b>255.255.255.0</b>	Enter the subnet mask used by the SA unit and the CBX 500 or GX 550.
Core IP Service Rate Selections	64 Kbps, 128 Kbps, <b>256 Kbps,</b> 512 Kbps, 1544 Kbps, 2048 Kbps	Select a service rate for the IP tunnel.
slot / pod / port	<b>1 / 3 / 1</b>	Enter the Slot/POD/Port of the SA unit's ATM connection to the CBX 500 or GX 550.
VPI / VCI	<b>0 / 32</b>	Enter the VPI/VCI to use for the connection between the SA unit and the ATM switch.

## **SA\_EXEC**

This command reserved for Ascend technician use only.

## SA\_FLASH

### ***NAME***

**sa\_flash** - provides information on the flash file system's available space

### ***SYNOPSIS***

sa\_flash [-v]

### ***DESCRIPTION***

sa\_flash displays a summary of the space used and space available to the SA unit's flash file system.

### ***OPTIONS***

-v turns on verbose diagnostic output, displaying additional information

### ***EXAMPLE***

```
OASOS> sa_flash
```

## SA\_FLOG

### **NAME**

**sa\_flog** - displays the last three fatal error logs

### **SYNOPSIS**

sa\_flog [#]

sa\_flog [c]

### **DESCRIPTION**

sa\_flog displays the last three fatal error logs for diagnostic purposes.

### **OPTIONS**

c    the c option clears the fatal error logs for all slots

#    enter a slot number (3 or 5) to display the fatal error log for an individual ICM.  
Entering slot 1 displays the log for the entire system.

### **EXAMPLES**

```
OASOS> sa_flog
```

```
OASOS> sa_flog 3
```

```
OASOS> sa_flog c
```



## SA\_IPLOG

This command reserved for Ascend technician use only.

## SA\_LNBS

This command is reserved for Ascend technician use only.

### ***NAME***

**sa\_lnbs** - load new boot application into flash memory

### ***SYNOPSIS***

sa\_lnbs filename...

### ***DESCRIPTION***

sa\_lnbs loads the filename into flash memory. This file is usually named lzrom.bin.

### ***OPTIONS***

None

### ***EXAMPLE***

```
OASOS> sa_lnbs
```

## SA\_RLOG

### **NAME**

**sa\_rlog** - displays non-volatile event log.

### **SYNOPSIS**

sa\_rlog X

### **DESCRIPTION**

sa\_rlog displays the X most recent event logs.

### **OPTIONS**

X The integer x represents the number of event logs to display.

### **EXAMPLE**

```
OASOS> sa_rlog 3
```

The example shown would display the three most recent event logs.

### **NOTES**

The format of the event logs display may seem cryptic; this command is intended for Ascend technician use. You should access event log information using the craft interface or WebXtend.

## SA\_ROUTE

### **NAME**

**sa\_route** - enables you to configure a predefined IP default route for an SA node. Once configured, the IP default route is re-established on power up, even in the absence of a saved configuration (nv\_db.dat). This allows IP connectivity to an SA node to be maintained across software upgrades / flash file system reformatting.

### **SYNOPSIS**

sa\_route

### **DESCRIPTION**

The sa\_route command is available in boot mode only.

Establishing an IP route defines a gateway (i.e., an IP router or switch) for the SA unit to use when passing TCP/IP traffic between network segments connected by the gateway.

sa\_route creates a default IP route which will be re-established whenever the unit is powered up, allowing you to manage the SA unit via TCP/IP even after a software upgrade or flash-file format has deleted the SA unit's configuration file (nv\_db.dat).

The function of the sa\_route command is identical to establishing an IP route using WebXtend.

### **EXAMPLES**

```
OASOS> sa_route
```

```
Enable IP Default Route (y/n) [n] ?
```

```
Enter gateway IP addr [152.148.123.254]:
```

```
Enter route admin status 1=down, 2=up [up]:
```

The system will prompt you to confirm your selections before the ICM Configuration is updated:

```
You have entered ...
```

```
Default Route Enable:  y
```

```
Gateway IP address:    152.148.123.254
```

```
Route Admin Status:   up
```

```
Is this correct (y/n) [n] ?
```

## SA\_WANIP

### NAME

**sa\_wanip** - configure SA unit WAN IP address, WAN IP subnet mask, service rate, service category, dial type (must be PVC or ASPVC-Orig) and enable/disable WAN IP access.

### SYNOPSIS

sa\_wanip

### DESCRIPTION

sa\_wanip enables you to configure a WAN-accessible management connection which is used if the nvdb.dat file is not present or fails to load. This WAN-accessible connection enables you to connect to a remote SA unit or an SA unit without an Ethernet POD, via a PVC or by dialing out to another SA unit equipped with an NLS adaption service.

Enter each of the following items when prompted, pressing ENTER after each one. Default values are shown in **bold**.

Parameter	Value	Notes
Enable	Y, N	Defines whether or not the WAN IP restore feature is enabled. If not enabled, no attempt is made to restore the management channel, even when nv_db.dat restore fails.
WAN IP addr	<b>10.25.252.15</b>	
WAN IP subnet mask	<b>255.255.0.0</b>	
dialType	PVC, <b>ASPVC-Orig</b>	Selects whether WAN IP management channel is established via PVC or dialed out (aspcv-orig)
AESA	20 octet string (all 0's)	20-octet ATM Address of SA node on which remote NLS service resides (Applies to ASPVC-Orig dial type only).
RemoteHandle	0, 1, ..., 16777215	Identifies NLS service instance on remote node through which management channel connects.
SigProtVariant	<b>UNI 3.0</b> , UNI 3.1, UNI 4.0, IISP 3.0, IISP 3.1, IISP 4.0	Specifies signalling protocol variant to be used for ASPVC_Orig dial type connections.

Parameter	Value	Notes
slot / pod / port	<b>1 / 3 / 1</b>	For PVC dial type, these parameters select an ATM interface for the trunk-side VCL. For ASPVC-Orig dial type, these parameters select the ATM interface to be configured for the signalling protocol type specified by the SigProtVariant parameter. There is only one instance of these parameters in the ICM Configuration, shared by both dial types.
VPI / VCI	<b>7 / 255</b>	Selects trunk-side ATM VCL (applies to PVC dial type only)
Service Rate	100M, 45M, 34M, <b>10M</b> , 2M, 1544K, 512K, 384K, 256K, 128K, 64K, 56K, user_defined	Selections are same as those defined by saNliTunnelSvcRate
User Rate	<b>10000000</b>	Applies only when Service Rate is 'user-defined'.
Service Category	<b>CBR1</b> , rt_VBR1, rt_VBR2, rt_VBR3, nrt_VBR1, nrt_VBR2, nrt_VBR3, UBR1, UBR2	Selections are same as those defined by saAspvcServiceCategory.

## EXAMPLE

```
OASOS> sa_wanip
```

The example shown displays the Enable WAN IP (y/n) [n]? prompt.

## NOTES

The management connection configured by SA\_WANIP is active **ONLY** if no nvdb.dat file loads on the SA unit and the WAN IP Enable parameter has been set to Yes. If the WAN IP Enable parameter is set to No, the WAN management connection is *never* available, even if the nvdb.dat file fails to load.

The WAN IP parameters are stored in the ICM configuration structure, which is placed in a flash sector separate from the file system. This ensures that the parameters needed to configure a node for a WAN-based management channel are preserved across software upgrades or formatting the flash file system, unlike the nvdb.dat file, which is overwritten during software upgrades or flash file system formats.

## SYNC

### ***NAME***

**sync** - force changed blocks to disk

### ***SYNOPSIS***

sync

### ***DESCRIPTION***

sync brings a mounted volume up to date, by writing to the volume all modified file information for open files, and cache buffers containing physical blocks that have been modified.

This call is superfluous under immediate write synchronization mode and is not allowed on a NFS volume.

### ***OPTIONS***

None

### ***EXAMPLE***

```
OASOS> sync
```

## SZ

### ***NAME***

**sz** - send Zmodem

### ***SYNOPSIS***

**sz** filename

### ***DESCRIPTION***

Initiates a Z-modem transfer of the indicated file. This function enables you to back up SA unit's configuration files prior to performing an **sa\_format** command.

### ***OPTIONS***

None

### ***EXAMPLE***

```
OASOS> sz nv_db.dat
```



## TELNET

This command reserved for Ascend technician use only.

## TOUCH

### ***NAME***

**touch** - update the access and modification times of a file

### ***SYNOPSIS***

touch [ -cf ] filename ...

### ***DESCRIPTION***

touch sets the access and modification times of each argument to the current time. A file is created if it does not already exist.

### ***OPTIONS***

- c Do not create filename if it does not exist.
- f Attempt to force the touch in spite of read and write permissions on filename.

## UPGRADE

### ***NAME***

**upgrade** - performs an automatic update of an SA unit's two boot files.

### ***SYNOPSIS***

upgrade

### ***DESCRIPTION***

Upgrading the SA unit's software involves upgrading the unit's two boot files, factory.bin and lzrom.bin. The upgrade command checks to see if these two files have been copied to the SA unit's RAM disk. If the two files are present, the upgrade command automatically upgrades the factory boot and lzrom boot files.

### ***EXAMPLES***

```
OASOS> upgrade
```



**IMPORTANT:** Do not use the UPGRADE command without referring to the SA Release Notes which accompanied the software build you are attempting to load.

# Using FTP to Transfer Files

This appendix describes:

- How to use File Transfer Protocol (FTP) to transfer files to and from an SA unit.
- How to use FTP to back up configuration information
- How to use FTP to restore a backup configuration to an SA unit

## Using FTP to Transfer Files

All SA units are equipped with a built-in FTP server for easy file transfers and software upgrades.

To transfer files to and from an SA unit via FTP:

1. Launch FTP client software on your PC or workstation.
2. FTP to the TCP/IP address of the SA unit.  
(A TCP/IP route between the PC or workstation and the SA unit must exist, either directly to an Ethernet POD installed in the SA unit (see [“Making the Ethernet Management Connection”](#) on page 4-31 of the *Hardware Installation Guide*) or via a remote management connection, as described in [Appendix G, “Managing SA Units Remotely.”](#))
3. Log in with your user name and password (default are “root” and “ascend”).
4. Make sure binary transfer mode is selected at your FTP client software.
5. Initiate an FTP transfer of one or more files to or from the SA unit.

## Using FTP to Back Up Configuration Data

The most common application of FTP is to back up the SA unit’s configuration data to your local workstation for archival purposes. The configuration data file is named `nv_db.dat`. It is a good idea to back up this file whenever major changes are made to the SA unit’s configuration.

Using FTP client software as described above, transfer the `nv_db.dat` file from the SA unit to your terminal. Save the file in an appropriate location and make note of the configuration setup and the time and date the backup file represents.

## Using FTP to Restore Configuration Data

To restore a previously saved `nv_db.dat` file to the SA unit, use an FTP client as described above, but transfer the `nv_db.dat` file *to* the SA unit instead of *from* the SA unit. After transferring the file, however, one additional step is required to force the SA unit to begin using the fresh file instead of the `nv_db.dat` file it booted up with.

The procedure is:

1. Log out of any WebXtend or craft interface session currently running.
2. FTP your `nv_db.dat` backup *to* the SA unit.
3. Log in to WebXtend.
4. Reboot the system using the Reset button in the Configure ICM window.  
(Main Menu>Interface Management>Configure ICM>Reset Slot)

Background: When a file is transferred *to* an SA unit, it is stored in a temporary buffer until a command to synchronize with the file currently in use is issued. This happens when you issue a Reset command from WebXtend or from the craft interface, or use the Reboot or Sync commands from the OASOS command prompt.

# Upgrading the SA Unit's Software

This appendix describes software upgrade procedures for an SA unit.

## About the Release Notes

Each SA unit is accompanied by a set of Release Notes containing the software upgrade procedure required for a given release. Refer to the Release Notes for details on obtaining current software, upgrading an SA unit's boot files, and upgrading the SA unit's software. The Release Notes also contain any caveats or anomalies which may impact the upgrade process.



Newer versions of the SA software may not be compatible with older revision hardware. For compatibility details, refer to the Release Notes accompanying any new release software **PRIOR** to installing the upgrade. All hardware must meet minimum compatibility requirements for the new software to function properly.

## Backing Up and Restoring Configuration Data

Prior to upgrading the SA unit's software, you should back up your configuration settings. All configuration data is stored in a file named `nv_db.dat`, which can easily be backed up and then restored after the software upgrade is complete.

See **“Using FTP to Back Up Configuration Data” on page C-2** for instructions on backing up the `nv_db.dat` file.

After upgrading the SA unit's software, restore the `nv_db.dat` file by using your FTP client to transfer the file back to the SA unit. See **“Using FTP to Restore Configuration Data” on page C-2** for details.



## Downloading the Enterprise MIB

This appendix describes:

- The procedure to download the Ascend Broadband Access Enterprise MIB from the Ascend FTP site

## Accessing the Ascend FTP Site

The Ascend Broadband Access Enterprise MIB can be found at the Ascend Broadband Access FTP site. The URL is:

ftp.casc.com

For a username and password to access the site, please contact your local Ascend Sales Engineer or Ascend Technical Support.

The Ascend Broadband Access Enterprise MIB is available in either Windows 95/NT or UNIX form:

Windows 95/NT:        Sahara.exe

UNIX:                   Sahara.tar

A subdirectory exists for each release version of the SA product family. Navigate the directory structure to locate the desired MIB.

Download the file appropriate to your system needs. The Windows version is a self-extracting archive. Simply execute in the directory where you store your enterprise MIBs.

For the UNIX version, use the UNIX .tar utility to extract the files from the archive to the desired directory.

In either case, take a moment to review the README file.

Finally, follow the instructions of the SNMP manager you are using to load and compile the MIB.



If you are unsure of which release version of the MIB file is appropriate for your hardware, or experience any difficulties with the above procedure, contact the Ascend Technical Assistance Center, as described in **Chapter 10, “Resolving Problems.”**

# NavisCore Integration

This appendix describes:

- Downloading the required Java Runtime Environment files from Javasoft (see [page F-2](#))
- Downloading the required .tar files from Ascend (see [page F-3](#))
- Unpacking and installing the SA files (see [page F-4](#))
- Integrating the SA unit into NavisCore

## Downloading the Java Runtime Environment

To download the Java Runtime Environment for Solaris from the Ascend FTP site:

1. Access the FTP site as described in “[Accessing the Ascend FTP Site](#)” on [page E-2](#).
2. Locate the Java Runtime Environment archive in the “NMS INTEGRATION” directory. The archive is a self-extracting binary file named `jre115_solaris2_sparc.bin`.
3. FTP the file to your machine.  
`get jre115_solaris2_sparc.bin`
4. Copy the file to the `opt/nms/` directory:  
`mv jre115_solaris2_sparc.bin ./opt/nms/jre115_solaris2_sparc.bin`
5. Make the file executable:  
`chmod a+x jre115_solaris2_sparc.bin`
6. Execute the binary file to extract its contents.  
(Note: you must be logged in as “root”.)  
`./jre115_solaris2_sparc.bin`

## Downloading the Sahara.tar File

To integrate an SA unit into a NavisCore map, you must first download the SA configuration file (Sahara.tar.Z) from the Ascend FTP site (ftp.casc.com/sauser/nms integration/Sahara.tar.Z). Access the FTP site as described in **“Accessing the Ascend FTP Site” on page E-2**. Open the “NMS INTEGRATION” directory. Download the Sahara.tar.Z file to your local hard drive following the instructions of your FTP software.

## Sahara.tar Contents

The sahara.tar archive is approximately 700K in size (compressed), and contains the following files:

- cesv2.mib — a MIB file.
- sahara.mib — a MIB file.
- identitydb.obj — this file is the security database for the applet viewer, enabling secured viewing of WebXtend applets.
- sa.arf — HPOV application registration file.
- sa.frf — HPOV file registration file.
- sa.srf — HPOV system registration file.
- sa100\*.\* — these files are NavisCore SA 100 icon files.
- sa600\*.\* — these files are NavisCore SA 600 icon files.
- sa\_app — this file provides support for adding, deleting, or modifying SA 100 and SA 600 icons to a map.
- sa\_install — this file contains the installation script.
- sa\_uninstall — the Navis WebXtend uninstallation script
- satrapd.conf — HPOV trap configuration file.
- java.security
- applet.viewer.properties

## Unpacking the Sahara.tar File

To unpack the Sahara.tar archive:

1. Open a terminal session.
2. At the \$ prompt, type:  

```
mkdir sa_install
```
3. At the \$ prompt, type:  

```
mv Sahara.tar.z ./sa_install/Sahara.tar.Z
```
4. Change to the newly-created sa\_install directory.
5. From the sa\_install directory, unpack the WebXtend archive by typing:  

```
uncompress Sahara.tar.Z
```
6. The result is a file **Sahara.tar**.
7. Unpack this file by entering the following command:  

```
tar -xvf Sahara.tar
```

In the next step, you'll integrate these files into your NavisCore installation.

## Installing the Navis WebXtend Files

To install the WebXtend files, you must be logged in as root.

1. At the # prompt, type:

```
chmod +x sa_install
```

2. Install one of the three Java clients by following the appropriate step below:

- To install the files necessary to use the Java Runtime Environment (the recommended Java client), type:

```
./sa_install jre
```

- To install the files necessary to use the Java Developer's Kit as your Java client, type:

```
./sa_install jdk
```

- To install the files necessary to use Netscape Navigator as your Java client, type:

```
./sa_install Netscape
```

3. If an error message reading **Error: Duplicate "atmFormumdbreport"** appears, ignore it.
4. Allow a minute or two for files to install.
5. When the # prompt reappears, you may restart your NavisCore sessions.

## Verifying the Navis WebXtend Installation

You can verify the installation's success by adding an object to your NavisCore map.

1. From NavisCore's Edit menu, select Add Object.
2. At the Add Object Palette, select the Ascend Objects class to display the symbol subclasses for Ascend objects.
3. Use the middle mouse button to select and drag an SA unit symbol to the submap. This will cause the Add Object window to open.
4. Complete the Add Object window for the new SA unit object:

Fill in a label for the object.

In Object Attributes, select Ascend SA Node, and click Set Object Attributes. Enter the node's IP address and click Verify, then OK, to return to the Add Object window.

Click OK to close the Add Object window and place the object on the submap.

## Uninstalling the Navis WebXtend Files

To uninstall the Navis WebXtend files from your NavisCore installation:

1. Log in as root.
2. Exit any active NavisCore sessions.
3. Execute the sa\_uninstall script located in the sa\_install directory.



## Managing SA Units Remotely

This appendix describes:

- How to manage SA units not equipped with an Ethernet port or remote SA units to which an Ethernet connection cannot be made.



The remote management connection established using the procedures in this chapter is saved as part of the nvdb.dat configuration file. If the nvdb.dat file is renamed, deleted or becomes corrupted, the remote management connection parameters will be lost.

The sa\_wanip OASOS command enables you to configure a backup management connection which is available only if the nvdb.dat file is not present or fails to load. The WANIP configuration is stored in the ICM's configuration structure, separate from the file system and the nvdb.dat file. This ensures that the management connection parameters needed to configure a node for WAN-based management are preserved across software upgrades and formatting of the flash file system.

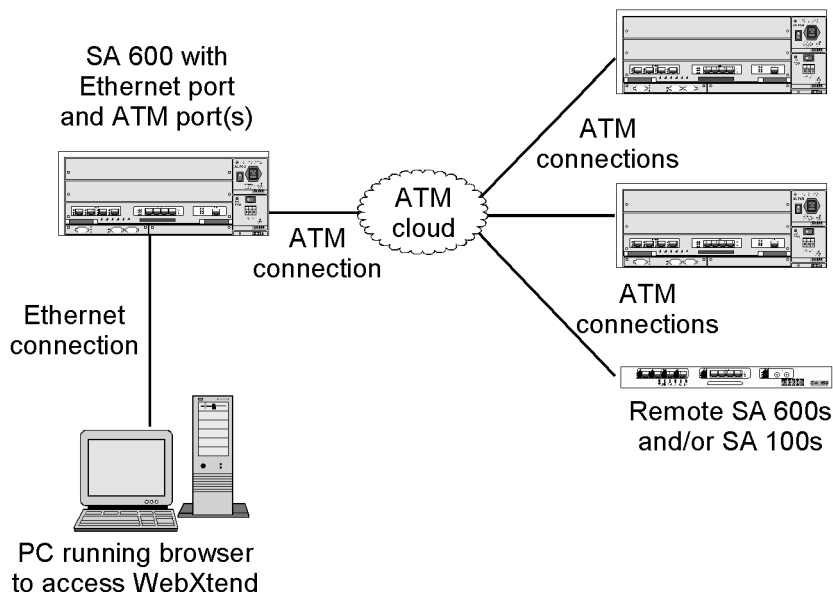
The sa\_corip OASOS command enables you to establish a single IP management tunnel between an SA unit and an Ascend CBX 500 or GX 550 ATM switch for use managing the SA unit across an ATM WAN. The core IP parameters are stored in the SA unit's flash memory separately from the file system. This ensures that the parameters for a core IP management interface are preserved across software upgrades or flash file system formatting.

The sa\_route OASOS command enables you to configure a predefined IP default route for an SA node. Once configured, the IP default route is re-established on power up, even in the absence of a saved configuration file. This allows IP connectivity to an SA node to be maintained across software upgrades / flash file system reformatting.

For details on using the sa\_wanip or sa\_route commands, see [Appendix B, "Operating System \(OASOS\) Command Set."](#)

## Setting up a Connection to a Remote SA Unit

It is not necessary to have a direct PC-to-SA unit physical connection or even an Ethernet connection to manage an SA unit. WebXtend makes it possible to remotely manage SA units over ATM connections, as shown in **Figure G-1**.



**Figure G-1. Remote Management of SA Units without Ethernet Ports**

The following instructions make several assumptions:

- All SA units have been properly configured with IP addresses as described in the Hardware Installation Guide.
- The Ethernet connection between your PC and the local SA unit has been made as described in “**Making the Ethernet Management Connection**” on page 4-31 of the Hardware Installation Guide.
- The ATM network connections between the local and remote SA unit have been made, including any intermediate switching connections (in the ATM cloud).

Follow the instructions below to prepare an SA unit for remote management, then configure your local SA device to connect to the remote unit, as described on **page G-4**.

## Preparing an SA unit for remote management

To prepare an SA unit for use as a remote unit:

1. Log in to the SA unit using the craft interface as described in **“Accessing the Craft Interface”** on page A-6.
2. Select Service Management at the Main menu.
3. From the Service Management window, select Native LAN Service.
4. From the Native LAN Service Groups window, select Add NLS Group.
5. Complete the Add NLS Group window as described in **“Adding an NLS Group”** on page 5-65. In the IP Management frame, set the Select IP Access to IP, and enter the unit’s IP Address and Subnet Mask. Choose OK to add the new group and return to the Native LAN Service Groups window.
6. From the Configured NLS Groups window, select the group created in step 5 to open its NLS Group Options window.
7. From the NLS Group Options window, select the Tunnels button.
8. From the NLS Tunnels window, select Add Tunnel.
9. Complete the Add Tunnel window as described in **“Creating Tunnels for an NLS Group”** on page 5-69. In the VPI and VCI fields, define a VPI and VCI for this connection. Choose OK to close the window and confirm the new tunnel.

The SA unit is now ready to serve as a remote unit, able to receive management connections from your local SA unit and web browser.

## Creating the connection from local to remote

To set up a management connection to a remote SA unit:

1. Log in to the local SA unit using your browser as described in **“Accessing WebXtend” on page 2-8**.
2. Select Service Management at the Main menu.
3. From the Service Management window, select Native LAN Service.
4. From the Native LAN Service Groups window, select Add NLS Group.
5. Complete the Add NLS Group window as described in **“Adding an NLS Group” on page 5-65**. Choose OK to add the new group and return to the Native LAN Service Groups window.
6. From the Configured NLS Groups window, select the group created in step 5 to open its NLS Group Options window.
7. From the NLS Group Options window, select the Tunnels button.
8. From the NLS Tunnels window, select Add Tunnel.
9. Complete the Add Tunnel window as described in **“Creating Tunnels for an NLS Group” on page 5-69**. In the VPI and VCI fields, enter a VPI and VCI for this ATM connection. If the ATM connection you are creating is a point-to-point connection directly from the local to the remote unit, the VPI/VCI should match the VPI/VCI assigned to the remote unit. Otherwise, enter the VPI/VCI of the next device within the ATM cloud. Choose OK to close the window and confirm the new tunnel.

You have now established a connection from your PC over Ethernet through the local SA unit and from the local SA unit over the ATM network to the remote SA unit.

To manage the remote SA unit, enter its IP address into your browser. The connection will be made to the remote SA unit and you will be prompted to log in.

# Acronyms

<b>AAL1</b>	ATM adaptation layer type 1
<b>AIS</b>	alarm indication signal
<b>AIS-L</b>	alarm indication signal line
<b>AMI</b>	alternate mark inversion
<b>ANSI</b>	American National Standards Institute
<b>ATM</b>	asynchronous transfer mode
<b>B8ZS</b>	bipolar with 8 zero substitutions
<b>BES</b>	bursty errored seconds
<b>BIP</b>	bit interleaved parity
<b>BOM</b>	bill of material
<b>BPV</b>	bipolar violation
<b>BSU</b>	broadband service unit
<b>CAC</b>	connection admission control
<b>CAS</b>	channel associated signaling
<b>CBR</b>	constant bit rate
<b>CCS</b>	common channel signaling
<b>CCV</b>	C-bit coding violation

<b>CDV</b>	cell delay variation
<b>CDVT</b>	cell delay variation tolerance
<b>CES</b>	C-bit errored seconds or circuit emulation service
<b>CLEI</b>	common-language equipment identification
<b>CLP</b>	cell loss priority
<b>CPE</b>	customer provisioned equipment
<b>CPOD</b>	cell protocol option device
<b>CRC</b>	cyclic redundancy check
<b>CRCLOMF</b>	cyclic redundancy check loss of multiframe
<b>CSES</b>	C-bit severely errored seconds
<b>CSS</b>	controlled slip seconds
<b>DS1</b>	digital service type 1
<b>DS3</b>	digital service type 3
<b>EFCI</b>	explicit forward congestion indicator
<b>ES</b>	errored seconds
<b>ESB</b>	errored seconds type B
<b>ESF</b>	extended superframe format
<b>ETSI</b>	European Telecommunications Standards Institute
<b>EXZ</b>	excessive zeros
<b>FBR</b>	fixed bit rate
<b>FBW</b>	fixed bandwidth
<b>FC</b>	failure count
<b>FCS</b>	frame check sequence
<b>FEBE</b>	far end block errors

<b>FERF</b>	far end receive failure
<b>FTP</b>	file transfer protocol
<b>GCRA</b>	generic cell rate algorithm
<b>HCS</b>	header checksum sequence
<b>HP</b>	Hewlett-Packard
<b>ICM</b>	interface control module
<b>IEC</b>	International Electrotechnical Commission
<b>IEEE</b>	Institute of Electrical and Electronic Engineers
<b>IP</b>	internet protocol
<b>IPOD</b>	interface protocol option device
<b>ITU-T</b>	International Telecommunication Union Telecommunication Standard Sector
<b>IWF</b>	interworking function
<b>LAN</b>	local area network
<b>LCD</b>	loss of cell delineation
<b>LCV</b>	line code violation or line coding violation
<b>LES</b>	line errored seconds
<b>LOF</b>	loss of frame
<b>LOS</b>	loss of signal
<b>MAP</b>	management access path
<b>Mbps</b>	Megabits per second
<b>MBS</b>	maximum burst size
<b>MCR</b>	minimum cell rate
<b>MIB</b>	management interface base

<b>NLS</b>	native LAN service
<b>NNI</b>	network-to-network interface
<b>NRT-VBR</b>	non-real time variable bit rate
<b>OAM</b>	operations administration and maintenance
<b>OC</b>	optical carrier
<b>OOF</b>	out of frame
<b>PCMCIA</b>	Personal Computer Memory Card International Association
<b>PCR</b>	peak cell rate
<b>PCV</b>	path code violation, path coding violation, or P-bit coding violation
<b>PES</b>	P-bit errored seconds
<b>PID</b>	protocol identification
<b>PLCP</b>	phase layer convergence protocol
<b>POD</b>	protocol option device
<b>PSES</b>	P-bit severely errored seconds
<b>RDI</b>	remote defect indication
<b>RDI-L</b>	remote defect indication line
<b>RFC</b>	request for comment
<b>RISC</b>	reduced instruction set computer
<b>RT-VBR</b>	real time variable bit rate
<b>RX</b>	receive or received
<b>SCM</b>	system control module
<b>SCR</b>	sustainable cell rate
<b>SDH</b>	synchronous digital hierarchy
<b>SEF</b>	severely errored frame



<b>SEFS</b>	severely errored framing seconds
<b>SES</b>	severely errored seconds
<b>SF</b>	superframe format
<b>SNMP</b>	simple network management protocol
<b>SNP</b>	sequence number protection
<b>SONET</b>	synchronous optical network
<b>STM</b>	synchronous transfer mode
<b>TS16AIS</b>	time slot 16 alarm indication signal
<b>TS16LOMF</b>	time slot 16 loss of multiframe
<b>TX</b>	transmit or transmitted
<b>UAS</b>	unavailable seconds
<b>UBR</b>	unspecified bit rate
<b>UNI</b>	user-to-network interface
<b>UPC</b>	usage parameter control
<b>VBR</b>	variable bit rate
<b>VBW</b>	variable bandwidth
<b>VCI</b>	virtual channel identifier
<b>VPI</b>	virtual path identifier
<b>WAN</b>	wide area network
<b>XPOD</b>	expansion protocol option device

# Glossary

## A

### **address**

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

### **alarm**

A message notifying an operator or administrator of a network problem.

### **Alarm Indication Signal (AIS)**

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

### **Alterable Mark Inversion (AMI)**

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

### **American National Standards Institute (ANSI)**

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

### **applet**

A small software module that runs on a Java virtual machine inside a Web browser.

### **Asynchronous Transfer Mode (ATM)**

A method used for transmitting voice, video, and data over high-speed LAN and WAN networks.

**attenuation**

The decrease in power of a signal over distance. Attenuation is measured in decibels.

**B****backbone**

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

**backplane**

A circuit board assembly that provides a means of transferring signals between other circuit board assemblies that are connected to it.

**bandwidth**

The transmission capacity of a computer or a communications channel.

**Bipolar with 8 Zero Substitution (B8ZS)**

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

**bit**

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

**bits per second (bps)**

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

**broadband network**

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

**broadband service unit (BSU)**

A broadband Wide Area Network device that consolidates wide-area ATM access for a combination of video, voice, and LAN-based data traffic.

**browser**

A software program for navigating and viewing the World Wide Web.

**burst**

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

**C****cell**

Any fixed-length data packet. For example, ATM uses fixed-length, 53-byte cells.

**cell highway**

Circuits in an SA unit that are used to relay packets between the CPOD and the IPOD(s), XPOD, and ICM.

**Cell Loss Priority (CLP)**

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

**Cell Protocol Option Device (CPOD)**

An ICM subsystem that provides cell switching.

**cell switching**

An operational feature of cellular networks that enables callers to move from one location to another without losing the call connection. The cellular system is designed to switch calls to a new cell with no noticeable drop in the conversation. Cell switching is sometimes called "handing off." While not noticeable in voice communications, the approximate 300 milliseconds this switching requires can be a problem in data transmission.

**channel**

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

**circuit**

A communications channel or path between two devices.

**circuit switching**

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

**client**

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

**congestion**

The point at which devices in the network are operating at their highest capacity. Congestion is handled by employing a congestion avoidance mechanism.

**connection admission control (CAC)**

Tasks performed by the network to determine whether to accept or reject a request for a connection or requests for reallocation of bandwidth

**Constant Bit Rate (CBR)**

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

**craft interface**

An interface that allows the user to locally or remotely configure, monitor, and control an SA unit using a series of menu-driven screens on a VT100 terminal or on a computer running VT100 terminal emulation software.

**CRC error**

A condition that occurs when the Cyclic Redundancy Check (CRC) in a frame does not agree with the CRC frame received from the network.

**CSU (Channel Service Unit)**

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

**Cyclic Redundancy Check (CRC)**

A calculation method used to check the accuracy of digital transmission over a communications link.

**D****D4-format**

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

**DCE (Data Communications Equipment)**

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

**Digital Signal (Digital Service) (DS)**

A classification of digital circuits. The DS defines the level of common carrier digital transmission service. DS-0 = 64 kbps (Fractional T1), DS-1 = 1.544 Mbps (T1), DS-2 = 6.312 Mbps (T2), DS-3 = 44.736 Mbps (T3), and DS-4 = 274.176 Mbps (T4).

**DS1**

A standard digital transmission facility, operating at 1.544 Mbps.

**DTE (Data Terminal Equipment)**

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

**E****E1**

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

**error rate**

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

**ethernet**

A popular LAN protocol and cabling scheme with a transfer rate of 10 or 100 Mbps.

**Expansion Protocol Option Device (XPOD)**

An ICM subsystem that provides expansion capabilities, including an additional ATM wide-area connection.

**Extended Superframe Format (ESF)**

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

### F

#### **fail count**

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

#### **File Transfer Protocol (FTP)**

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

#### **Frame Check Sequence (FCS)**

In a frame, a field that contains the standard 16-bit cyclic redundancy check used to detect errors in HDLC and LAPD frames.

### G

#### **Gbps**

Abbreviation for gigabits (1 billion bits) per second. See also *bps*.

### H

#### **header**

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

#### **HP OpenView**

The UNIX-based network management application used with CascadeView/UX on an NMS to manage a Ascend-switch network.

### I

#### **Institute of Electrical and Electronic Engineers (IEEE)**

A professional organization that defines network standards.

#### **Interface Control Module (ICM)**

An SA-unit subsystem with a cell subsystem and a packet subsystem that switches cells and packets simultaneously.

#### **Interface Protocol Option Device (IPOD)**

An ICM subsystem that supports service interfaces including Ethernet, circuit switching, and ATM UNI/NNI.

**Interim Local Management Interface (ILMI)**

A management information base (MIB) that provides status and communication information to ATM UNI devices and provides for a port keep alive protocol. ILMI provides status information and statistics about virtual paths, connections, and address registration. It also determines the operational status of the logical port.

**internal clocking**

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

**International Telecommunication Union Telecommunication Standard Sector (ITU-T)**

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

**Internet Protocol (IP)**

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

**Internet Protocol address**

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

**IP address**

See *Internet Protocol address*.

**J****Java**

An object-oriented programming language that creates distributed, executable applications.

**jitter**

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

**K****kbps**

Abbreviation for kilobits (1000 bits) per second. See *bps*.



### **keepalive message**

This message is used in the Link Management Interface of a frame relay port to verify link integrity.

## **L**

### **Local Area Network (LAN)**

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

### **loopback**

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

### **loss of frame (LOF)**

A T1 error condition when an out-of-frame condition exists for a normal period of 2 1/2 seconds.

### **loss of signal (LOS)**

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

## **M**

### **Management Information Base (MIB)**

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

### **Mbps**

Abbreviation for megabits (1 million bits) per second. See *bps*.

### **multiplexer (mux)**

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

### **multiplexing**

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

## N

### **Network-to-Network Interface (NNI)**

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

### **node**

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

## O

### **OASOS**

The internal operating system of an SA unit.

### **out of frame (OOF)**

A T1 error condition where two or three framing bits of any five consecutive frames are in error.

## P

### **packet**

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

### **packet-switched network**

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

### **packet switching**

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

### **payload**

The portion of a frame that contains the actual data.

### **PDN**

see *Public Data Network*.

### **Peak Cell Rate (PCR)**

In ATM transmission, the maximum cell transmission rate. PCR defines the shortest time period between two cells.

### **Permanent Virtual Circuit**

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

### **Permanent Virtual Path**

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

### **protocol**

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

### **Protocol Accelerator™**

A subsystem on each ICM (Interface Control Module) that translates between flows at multiple levels at up to 200,000 packets per second.

### **Public Data Network**

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

### **PVC**

See *Permanent Virtual Circuit*.

### **PVP**

See *Permanent Virtual Path*.

## **R**

### **red alarm**

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

**Request For Comment (RFC)**

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

**router**

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

**S****server**

A device or software application that provides information or services based on requests from client devices or programs.

**Simple Network Management Protocol (SNMP)**

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

**Sustainable Cell Rate (SCR)**

The average cell transmission rate in ATM transmission. Equivalent to CIR for Frame Relay, SCR is measured in cells per second and converted internally to bits per second. Usually, SCR is a fraction of the peak cell rate. Cells are sent at this rate if there is no credit.

**T****T1**

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

**T3**

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

**telnet**

The Internet standard protocol for remote terminal-connection services.

**throughput**

The actual speed of the network.

### **transceiver**

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

## **U**

### **User-to-Network Interface (UNI)**

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

## **V**

### **Virtual Channel**

A connection between two communicating ATM networks.

### **Virtual Circuit**

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

### **Virtual Circuit Identifier (VCI)**

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

### **Virtual Path**

A group of VCs carried between two points. VP provides a way to bundle traffic headed in the same direction.

### **Virtual Path Identifier (VPI)**

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

## **W**

### **WebXtend™**

The Web browser user interface built into Ascend broadband access products.

### **Wide Area Network (WAN)**

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

## Y

### **yellow alarm**

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

# Index

## A

- About Connections [5-10](#)
- accessing the craft interface [A-6](#)
- Add ATM UNI Connection window [5-38](#) to [5-43](#)
- Add USF IWF Connection window [5-107](#) to [5-112](#)
- Add VCS IWF Connection window [5-122](#)
- Add/Modify Structured DS1 CES-IWF window [5-89](#), [5-99](#)
- Add/Modify Unstructured DS1 CES-IWF window [5-89](#), [5-99](#)
- Adding an Operator [3-5](#) to [3-7](#)
- alarms
  - DS1 port [6-50](#) to [6-53](#)
  - DS3 ports [6-62](#) to [6-65](#)
  - E1 port [6-50](#) to [6-53](#)
  - E3 ports [6-62](#) to [6-65](#)
  - filtering [7-8](#) to [7-9](#)
  - OC-3C/STM-1 [6-70](#) to [6-71](#)
- Alarms and Defects on DS1/E1 Ports, Viewing [6-50](#)
- Apply button [2-12](#), [A-8](#)
- Arrow key [2-11](#), [A-7](#)
- ATM File Check [6-27](#)
- ATM interface
  - cell delineation [4-47](#)
- ATM Statistics on OC-3c/STM-1 Paths [6-81](#)
- ATM UNI connection
  - congestion control strategy [5-42](#) to [5-43](#)
  - constant bit rate service [5-40](#), [5-72](#), [5-109](#)
  - deleting [5-45](#)
  - disabling [5-44](#)
  - drop CLP1 [5-42](#), [5-74](#)
  - early packet discard [5-42](#), [5-74](#)
  - enabling [5-44](#)
  - explicit forward congestion indicator [5-42](#), [5-74](#)
  - non-real time variable bit rate [5-40](#), [5-72](#), [5-109](#)

- real time variable bit rate service [5-40](#), [5-72](#), [5-109](#)
- service definition [5-40](#), [5-109](#)
- service rate [5-41](#), [5-73](#), [5-110](#)
- unspecified bit rate service [5-40](#), [5-72](#), [5-109](#), [5-124](#)
- ATM UNI connections
  - adding [5-38](#) to [5-43](#)
  - modifying [5-44](#)
- ATM UNI service
  - configuration [5-33](#) to [5-45](#)
- ATM UNI statistics
  - OC-3C/STM-1 path [6-66](#)
- ATM UNI Statistics on DS1/E1 Cell POD Ports [6-81](#)

## B

- board
  - inventory [6-19](#) to [6-20](#)
- Board Inventory Statistics window [6-19](#) to [6-20](#)
- Boot Sequence [A-3](#)

## C

- CAC Bandwidth Stats window [6-25](#)
- Cancel button [2-12](#), [A-8](#)
- Cell Highway Statistics [6-22](#)
- cell highway statistics [6-22](#) to [6-25](#), [6-39](#)
- Cell Highway/Priority Queue Stats window [6-22](#) to [6-25](#), [6-39](#)
- CES interworking function
  - adding [5-89](#) to [5-92](#)
  - conditioning [5-94](#)
  - statistics [6-54](#) to [6-120](#)

- CES-IWF
  - disabling 5-100
  - enabling 5-100
- CES-IWF connection
  - modifying 5-99
- CES-IWF Statistics window 6-54 to 6-120
- Circuit Emulation Service
  - configuration 5-83 to 5-95
  - structured constant bit rate service 5-85
  - unstructured constant bit rate service 5-85
- configuration of an SA unit 1-7
- Configure DS1 Port window 4-11 to 4-12
- Configure DS3/E3 Port window 4-21 to 4-29
- Configure Ethernet Port window 4-9 to 4-10
- Configure OC-3/STM-1 Path window 4-38, 4-41 to 4-42
- Configure OC-3/STM-1 Port window 4-30 to 4-35
- Connect Detail 5-105
- Connection Statistics Window 6-111 to 6-114
- Connection Summary window 6-95
- connections
  - monitoring 6-84
- Connections Statistics window 6-96
- constant bit rate service 5-124
- conventions 2-11 to 2-13
- conventions, text xxix
- craft interface
  - accessing A-6
  - conventions A-7 to A-8
  - description A-4
  - using 2-6, A-9 to A-11
  - Utilities Window A-10
- Display Interval window 6-48 to 6-49
- Display OC-3/STM-1 Path Status window 6-66, 6-73
- Display PLCP Status window 6-62 to 6-65
- Display POD Status window 6-36
- Display System Status window 6-6 to 6-12
- Display Transmission Convergence Status window 6-63 to 6-64
- DS1 Faults window 6-50 to 6-52
- DS1 POD
  - indicators 6-30
- DS1 port
  - alarms 6-50 to 6-53
  - configuration 4-11 to 4-12
  - D4 framing 4-14
  - error insertion 4-17
  - extended superframe 4-14
  - jammed bit line coding 4-15
  - monitoring 6-43 to 6-120
  - port loopback 8-8 to 8-9
- DS3 Faults window 6-62 to 6-65
- DS3 POD
  - indicators 6-32
- DS3 port
  - alarms 6-62 to 6-65
  - ATM UNI statistics 6-80 to 6-83
  - C-bit framing 4-24
  - configuration 4-21 to 4-29
  - M.23 framing 4-24
  - monitoring 6-55 to 6-59, 6-80 to 6-83
  - port loopback 4-25, 8-10 to 8-11
- Dynamic Bandwidth Allocation 5-96 to 5-98

## D

- Delete UNI Connection window 5-45
- Display Board Status window 6-13 to 6-16
- Display Current Interval window 6-47
- Display DS1 Status window 6-43 to 6-120
- Display DS3 Port Status window 6-55 to 6-59, 6-80 to 6-83
- Display E3 Port Status window 6-55 to 6-59, 6-80 to 6-83
- Display Ethernet Port Status window 6-41, 6-78

## E

- E1 Faults window 6-50 to 6-52
- E1 POD
  - indicators 6-31, 6-35
- E1 port
  - alarms 6-50 to 6-53
  - configuration 4-11 to 4-12
  - E1 framing 4-14
  - E1-CRC framing 4-14
  - E1-CRC-MF framing 4-14



E1-MF framing 4-14  
error insertion 4-17  
ITU-T Recommendation G.704 framing 4-14  
jammed bit line coding 4-15  
monitoring 6-43 to 6-120  
port loopback 8-8 to 8-9  
E3 POD  
  indicators 6-33  
E3 port  
  alarms 6-62 to 6-65  
  ATM UNI statistics 6-80 to 6-83  
  configuration 4-21 to 4-29  
  G.751 framing 4-24  
  G.832 framing 4-24  
  monitoring 6-55 to 6-59, 6-80 to 6-83  
  port loopback 4-25, 8-10 to 8-11  
Enter key 2-11, A-7  
ethernet POD  
  indicators 6-29  
ethernet port  
  configuration 4-9 to 4-10  
  monitoring 6-41, 6-78  
Event Management window 7-5 to 7-6  
event/alarm log 7-2 to 7-4  
event/alarm log files  
  generating 7-7  
Event/Alarm Log window 7-2 to 7-4  
events  
  filtering 7-8 to 7-9  
Events/Alarms... button 2-12, A-8  
Events/Alarms... field 2-12, A-8  
exit to shell 9-5

## F

Far End Alarm and Control 4-28  
file  
  transferring A-9 to A-10  
file transfer 9-5, A-9 to A-10  
filtering alarms 7-8 to 7-9  
filtering events 7-8 to 7-9  
filtering traps 7-10 to 7-11  
Frame Service  
  configuration 5-102 to 5-116

front panel 2-2, 2-3, 2-4

## G

gray buttons 2-11  
gray fields 2-11

## H

help 2-13, A-8

## I

I/P Routes 3-11  
ICM  
  inventory 6-19 to 6-20  
IMA Group Statistics 5-55 to 5-59  
IMA Groups  
  configuring 5-46 to 5-52  
IMA Link Statistics 5-60 to 5-63  
IMA Links  
  configuring 5-53  
Indicators  
  E3 POD 6-33  
indicators  
  chassis 6-4  
  DS1 POD 6-30  
  DS3 POD 6-32  
  E1 POD 6-31, 6-35  
  ethernet POD 6-29  
  OC-3C/STM-1 POD 6-34  
  power-up sequence 2-2, 2-3, 2-4  
  sum 6-5  
initialization  
  system 9-5  
Interface Control Module 1-6  
Interface Management window 4-2  
inventory statistics 6-11  
IP address 2-6, 2-8

### L

logging off [2-18](#)  
Logoff window [2-18](#)

### M

MAC Address Cache Information [5-78](#)  
Main Menu [2-9](#) to [2-10](#)  
Management Interformation Base statistics [6-12](#)  
managing events and traps [7-5](#) to [7-11](#)  
MIB statistics [6-12](#)  
microprocessor  
    monitoring [6-17](#) to [6-18](#)  
Modify ATM UNI Connection window [5-44](#)  
Modify USF IWF Connection window [5-114](#),  
    [5-127](#)  
Modifying or Deleting ILMI Node Prefixes [3-18](#),  
    [4-54](#)  
Modifying or Deleting IP Routes [3-13](#)  
Monitor Status window [6-2](#) to [6-4](#)  
mouse [2-11](#)  
    clicking [2-12](#)  
    double-clicking [2-12](#), [6-3](#)

### N

Native LAN Service (NLS) Groups window [5-64](#),  
    [5-65](#)  
Navigating WebXtend Buttons and Fields [2-11](#)  
NLS Group, adding [5-65](#)  
NLS service  
    configuration [5-64](#)  
non-real time variable bit rate [5-124](#)

### O

OASOS  
    accessing [2-6](#), [A-11](#)  
OC-3/STM-1 Line Faults window [6-70](#) to [6-71](#)  
OC-3/STM-1 Path Faults window [6-70](#) to [6-71](#)  
OC-3/STM-1 port  
    configuration [4-30](#) to [4-35](#)

OC-3C/STM-1  
    alarms [6-70](#) to [6-71](#)  
OC-3C/STM-1 path  
    ATM UNI statistics [6-66](#)  
OC-3C/STM-1 POD  
    indicators [6-34](#)  
OC-3C/STM-1 port  
    monitoring [6-66](#)  
    path configuration [4-38](#), [4-41](#) to [4-42](#)  
    path statistics [6-66](#), [6-73](#) to [6-74](#)  
    port loopback [4-34](#), [8-12](#) to [8-13](#)  
OK button [2-12](#), [A-8](#)  
operating system  
    accessing [2-6](#), [A-11](#)  
Operators  
    adding [3-5](#) to [3-7](#)

### P

password [2-8](#), [3-5](#)  
Path Statistics on OC-3c/STM-1 Ports [6-73](#)  
Performance Statistics for an Interval [6-47](#)  
POD [1-6](#)  
    indicators [6-29](#) to [6-34](#)  
    inventory [6-38](#)  
    monitoring [6-29](#)  
POD Inventory Statistics window [6-38](#)  
POD Status Windows [6-36](#)  
port  
    monitoring [6-40](#), [6-66](#)  
    selection [4-7](#)  
port loopback [8-2](#), [8-7](#) to [8-13](#)  
    DS1 port [8-8](#) to [8-9](#)  
    DS3 port [8-10](#) to [8-11](#)  
    E1 port [8-8](#) to [8-9](#)  
    E3 port [8-10](#) to [8-11](#)  
    OC-3C/STM-1 port [8-12](#) to [8-13](#)  
    USF port [8-14](#)  
power switch [2-3](#), [2-4](#)  
powering up [2-2](#), [2-3](#), [2-4](#)  
problems  
    resolving [10-1](#) to [10-3](#)  
Processor Utilization window [6-17](#) to [6-18](#)  
Protocol Accelerator Statistics [6-26](#)

protocol option device 1-6  
provisioning information, saving 2-18  
Pull-down Menus (craft interface) A-7

## R

read-only fields 2-11  
real time variable bit rate service 5-124  
rear panel 2-2

## S

SA 100  
    description 1-3  
SA 1200  
    description 1-5  
SA 600  
    description 1-4  
save configuration 2-18  
security 3-5  
Select CES Port window 5-83  
Select Service window 5-2  
Select USF Port window 5-102  
Select VCS Port window 5-117  
Selecting a Network Service 5-2  
Setting up the VT-100 Terminal A-2  
Setup Event Log Filters window 7-8 to 7-9  
Setup Trap Filters window 7-10 to 7-11  
shut down system 9-5  
shutting down 2-18  
slot  
    inventory 6-19 to 6-20  
Space Bar A-7  
SUM Status Information 6-11  
system  
    monitoring 6-6 to 6-12  
    shut down 9-5  
System Administration window 3-2 to 3-3  
system initialization 9-5  
System Inventory Statistics window 6-11  
system security 3-5  
system timing 3-8 to 3-10  
System Timing window 3-8 to 3-10

System Utility Module, Status Information 6-11

## T

Tab key 2-11, A-7  
text conventions xxix  
Trail Trace window 4-27  
transferring files 9-5  
transmission convergence status 6-53  
traps  
    filtering 7-10 to 7-11  
troubleshooting 10-1 to 10-3

## U

Universal Serial Frame  
    clock rate 4-57  
Universal Serial Frame service  
    configuration 5-102 to 5-116  
user name 2-8  
USF IWF connections  
    adding 5-107 to 5-112  
    modifying 5-114, 5-127  
USF port  
    port loopback 8-14  
USF-IWF  
    disabling 5-115  
    enabling 5-115  
    explicit forward congestion indicator 5-112  
USF-IWF connection  
    drop CLP1 5-112  
    early packet discard 5-112  
    SetEFCIandCLP1 5-112  
    SetEFCIandEPD 5-112  
Utilities Window A-10  
Utilities window 9-2 to 9-3

## V

VCS  
    configuration 5-117 to 5-133  
VCS IWF connections

## Index

---

- adding 5-122 to 5-126
- VCS-IWF
  - disabling 5-128
  - enabling 5-128
- Viewing ATM UNI Statistics on DS1/E1 Cell POD Ports 6-81
- Viewing ATM-UNI Connection Information 6-87
- Viewing Cell Highway Statistics 6-22
- Viewing NLS Tunnel Status Information 6-116
- Viewing System Utility Module (SUM) Status Information 6-11
- Voice Compression IWF
  - service definition 5-124
- Voice Compression Service
  - configuration 5-117 to 5-133

## W

- WebXtend
  - accessing 2-8
  - description 1-7
- WebXtend Buttons and Fields
  - Navigating 2-11

## Z

- Zmodem 9-5, A-9 to A-10