Lucent Technologies
Bell Labs Innovations

PacketStar™
PSAX 20 Access Concentrator
User Guide

Issue 1, October 2000

System Software Release 6.3.0

Doc. No.: 255-700-019
COMCODE: 300303278

Copyright and Legal Notices

Copyright

This document was prepared by the Information Design and Development department of Lucent Technologies, InterNetworking Systems, Access Technology group. Offices are located in Landover, Maryland, U.S.A.

Trademarks

AQueView, *PacketStar*, *Lucent*, *Lucent Technologies*, and the Lucent Technologies logo are trademarks of Lucent Technologies. Other product and brand names mentioned in this guide are trademarks or registered trademarks of their respective owners.

Warranty Information

Software and Hardware Limited Warranties

Lucent Technologies provides a 90-day limited software warranty, and a one-year limited hardware warranty on this product. Refer to the *Software License and Limited Warranty Agreement* and the *Lucent Technologies InterNetworking Systems Global Warranty* that accompanied your package for more information.

Every effort has been made to ensure that this document is complete and accurate at the time of release, but information is subject to change. Lucent Technologies assumes no responsibility or liability for errors or inaccuracies that may appear in this guide.

Warranty Warnings

CAUTION:
Do not make electrical or mechanical modifications to any of the components in the PSAX system. Lucent Technologies is not responsible for the safety or the performance of a modified Lucent product. Do not attempt to repair any failed Power Supply module, Stratum 3–4 module, CPU module, I/O, or Server module.

CAUTION:
Do not make electrical or mechanical modifications to any of the components in the PSAX system. Lucent Technologies is not responsible for the safety or the performance of a modified Lucent product. Do not attempt to repair any failed removable I/O or server modules.

CAUTION:
Modifying or tampering with PSAX chassis components may void your warranty. Any modification to this equipment not expressly authorized by Lucent Technologies may void your granted authority to operate such equipment.

CAUTION:
Air vents in the PSAX chassis are provided to aid in ventilation and to protect from overheating. These vents must be regularly inspected by the user and cleared of dust and blockage. Equipment failure associated with improper maintenance or suspected failure to adhere to proper ventilation procedures as described above will void your warranty.

CAUTION:
You must replace an air filter having an accumulation of dust to ensure adequate airflow through the PSAX chassis. Reduced airflow could result in damaging heat buildup within the chassis.

- **Periodically inspect the air filter for accumulated dust and replace the filter as needed. At a minimum, monthly inspection is recommended. Equipment failure due to inadequate airflow voids your equipment warranty.**
- **Use only filters supplied by Lucent Technologies in your PSAX chassis. Use of other filters voids your equipment warranty.**

CAUTION:
You must maintain a minimum 5.08 cm (2 in.) of clearance around the chassis for adequate airflow. Failure to adhere to this space requirement may result in equipment failure due to overheating. Failure to provide a minimum of 5.08 cm (2 in.) of clearance between this unit and any other device/structure will void your warranty.

⚠ CAUTION:
If your system or location loses power or your current session ends abnormally while you are in the process of configuring the system, and you have not yet saved the values permanently, you will lose all unsaved values you have applied on the various windows.

⚠ CAUTION:
Shipping the chassis with removable modules installed may cause damage to the chassis and the modules. Damage to any of the components in the system resulting from shipping the chassis with removable modules installed could void your warranty. Only Lucent-authorized personnel should ship the PSAX 20 chassis with a module installed.

Regulatory Standards Compliance

The PSAX 20 Access Concentrator is fully compliant with the following environmental, safety, and emissions standards. Appropriate statements appear in the next subsection.

Safety Requirements

- Underwriter's Laboratory (UL) — Safety and Factory Compliance UL 1950
- CB-Scheme — IEC 60950:1991+A1:1992+A2:1993+A3:1995+A4:1996

Electromagnetic Compatibility (EMC) and Physical Requirements

- Federal Communications Commission (FCC) — EMC compliance (Part 15 Class A)
- EN 55022:1994 Class A (CISPR22:1993)

Regulatory Statements

United States Federal Communications Commission (FCC) Statements

Part 15. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with this guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference; in this case, you would be required to correct the interference at your own expense.

All cables used to connect to peripherals must be shielded and grounded. Operation with cables, connected to peripherals, that are not shielded and grounded may result in interference to radio and television reception.

The user is cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 68. This equipment complies with Part 68 of the FCC rules. On the back of the PSAX 20 chassis is a label that contains the FCC registration number, in addition to other information. You must provide this information to the telephone company, if they request it. The FCC requires Lucent Technologies, Inc., to provide you with the following information:

1. The PSAX 20 system has digital service interface capabilities using RJ-48C and RJ-48H connectors. The facility interface codes with which the PSAX 20 system complies for digital services are as follows: 04DU9-BN, 04DU9-DN, 04DU9-1KN, and 04DU9-1SN. The PSAX 20 system has loop start interface capabilities using an RJ-11C connector. The facility interface code with which the PSAX 20 system complies for service is 02LS2. The service order codes for the PSAX 20 system are 6.0F for the T-1 interface and 9.0Y for the loop start interface.
2. An FCC-compliant telephone network interface jack is built into this equipment and is compatible with interconnections that are Part 68 compliant.
3. The REN for the Voice 2-Wire Office module when used in the PSAX 20 system is 0.7B.
4. If the PSAX 20 system causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service might be required. But if advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe this is necessary.
5. The telephone company might make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice for you to make necessary modifications to maintain uninterrupted service.
6. If you experience trouble with the PSAX 20 system, or need repairs or warranty information, please refer to the Limited Hardware Warranty card that accompanied your PSAX 20 product shipment for instructions on obtaining technical support in your area.

If the PSAX 20 system is causing harm to the telephone network, the telephone company might request that you disconnect the equipment until the problem is resolved.

7. This equipment has no user-serviceable parts.

This equipment cannot be used on public coin telephone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact your state public utility commission, public service commission, or corporation commission for information.

Canadian Regulatory Statements

Industry Canada Information

Ringer Equivalence Number (REN) Notice. The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, the user should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed by using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations.

Repairs to some certified equipment should be made by an authorized maintenance facility designated by the supplier. Any repairs or alternations made by the user to this equipment or equipment malfunctions might give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the ground connections of the power utility, telephone lines, and internal metallic water pipe system are connected together. This precaution may be particularly important in rural areas.

▲ CAUTION:
Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority or electrician.

The Ringer Equivalence Number (REN) assigned to the Voice 2-Wire Office module denotes the percentage of the total load to be connected to a telephone loop, which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the REN of all devices does not exceed 5.

The REN for the Voice 2-Wire Office module when used in the PSAX 20 system is 0.7B.

Renseignements Industrie Canada

Avis de nombre équivalent de sonneries (REN). Le label Industrie Canada permet de reconnaître les équipements homologués. Cette homologation indique que l'équipement satisfait certaines règles de protection, d'exploitation et de sécurité des réseaux de télécommunications. Le ministère de l'Industrie ne garantit pas que l'équipement fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer cet équipement, l'utilisateur doit s'assurer qu'il est permis de le connecter aux installations de la compagnie de télécommunications locale. L'équipement doit également être connecté suivant une méthode convenable. Dans certains cas, il sera nécessaire de prolonger le câblage intérieur de la ligne d'abonné de la compagnie au moyen d'un connecteur homologué (rallonge de téléphone). L'abonné doit savoir que, dans certaines situations, la conformité aux dispositions ci-dessus ne prévient pas nécessairement la dégradation du service.

La réparation de certains équipements homologués doit être assurée par un atelier agréé désigné par le fournisseur. Toute réparation ou altération effectuée par l'utilisateur ou tout mauvais fonctionnement de cet équipement peut donner à la compagnie de téléphone des raisons de demander audit utilisateur de déconnecter celui-ci.

Pour leur propre sécurité, les utilisateurs doivent veiller à ce que les mises à la terre de l'alimentation secteur, des lignes téléphoniques et du système intérieur de conduites d'eau métalliques soient raccordés ensemble. Cette précaution peut s'avérer particulièrement importante dans les zones rurales.

▲ CAUTION:
Les utilisateurs ne doivent pas tenter d'effectuer eux-mêmes ces raccordements, mais doivent prendre contact avec un électricien ou organisme de vérification compétent.

Le nombre équivalent de sonnerie (REN) attribué au module central bifilaire (Voice 2-Wire Office) correspond au pourcentage de la charge totale à connecter à un circuit téléphonique bifilaire; il est utilisé par l'appareil pour prévenir la surcharge. Le circuit peut être terminé par n'importe quelle combinaison d'appareils, à la seule condition que le total des REN de ces derniers ne dépasse pas cinq.

Safety Warnings and Information

When installing and operating the PSAX 20 Access Concentrator, follow the safety guidelines provided below to help prevent serious injury and/or damage to the PSAX 20 equipment. Please read all warnings and instructions supplied before beginning installation or configuration of the PSAX 20 equipment. In addition to the general safety information provided below, you should also refer to the text in the user and installation guides for other important safety information and procedures.

⚠ DANGER:
Never push and/or place an object in or through any vent in the PSAX 20 chassis. Doing so may result in personal injury, equipment damage, or both. Touching exposed electrical components may cause injury.

⚠ DANGER:
Install only equipment identified in the installation guide for the PSAX 20 system. Using other equipment may result in improper connection of circuitry, which may lead to equipment fire, personal injury, or equipment damage.

⚠ DANGER:
Do not install or use the PSAX 20 unit in wet locations. In the event the unit becomes wet, turn it off, disconnect it from the facility power source, and allow the unit to dry thoroughly. If, after this procedure, you encounter problems with the performance of the unit, please contact your NetworkCare Service Center. (See the *Lucent Technologies InterNetworking Systems Global Warranty* that accompanied your shipment for the appropriate telephone number.)

⚠ DANGER:
When removing an alternating current (AC) power cord from an PSAX 20 chassis running on AC power, remove the power cord from the connector by grasping and pulling the plug, not the power cord.

⚠ DANGER:
Ensure that the voltage and frequency of the facility power source match the requirements of the PSAX 20 Power Supply unit. The PSAX 20 system should only be operated from the power source type indicated on the marking label. Failure to meet this requirement may cause personal injury, fire, and/or damage to the unit.

⚠ DANGER:
Shock hazard! Do not personally perform any maintenance on this equipment. This equipment does not contain any user serviceable parts. Maintenance is to be performed only by qualified personnel.

⚠ DANGER:
The OC-3c Single Mode (SM) and the STM-1 Single Mode (SM) modules contain a laser-generating device, which emits a laser light beam from the transmit port. This port is labeled TX on the module faceplate. When the module is inserted into an operational PSAX 20 chassis, personal injury may result from looking into, or near, either port. Personal injury may also result from looking into, or near, the far end of a connected fiber optic cable. For additional laser safety information, see Appendix B of the *OC-3c Multi-Mode and Single-Mode Module Guide*, the *OC-3c Multi-Mode and Single-Mode 1+1 APS Module Guide*, the *STM-1 Multi-Mode and Single-Mode Module Guide*, and the *STM-1 Multi-Mode and Single-Mode 1+1 MSP Module Guide*.

⚠ DANGER:
Read all installation instructions before connecting the system to a power source.

⚠ DANGER:
Do not work on the system, connect, or disconnect cables during periods of possible lightning activity.

⚠ DANGER:
Do not perform any action that could create a possible hazard to others or make the working environment and/or the equipment unsafe.

⚠ WARNING:
Be sure to cover all empty slots with blank faceplates to protect your equipment.

⚠ WARNING:
This product relies on the building's installation of short-circuit (over-current) protection. Ensure that a fuse or circuit breaker no larger than 120 V ac, 15 A U.S. (240 V ac, 10 A international) is used on the phase conductors (all current-carrying conductors).

⚠ WARNING:
Once the PSAX 20 chassis is operational (power is applied to the chassis) and the OC-3c SM or STM-1 SM module is fully inserted into the chassis backplane, use extreme caution during removal of the fiber optic cable from one or both ports. Keep the protective port caps supplied with these two types of modules nearby (for example, taped to the cable for the port), and place said cap on the port immediately after removing the cable from an operational module.

⚠ WARNING:
If you place the PSAX 20 chassis on or near the floor, dust or debris may accumulate faster inside the chassis than it would if placed on a table or standing structure. Therefore, if this unit is placed on or near the floor, accelerated routine vent and air filter inspection is necessary to avoid the risk of unit failure and/or injury to property or persons.

⚠ WARNING:
Be sure to use the ejector handles during installation and removal of I/O and server modules.

⚠ WARNING:
When inserting modules into the chassis, slide them gently, not forcefully. Excessive force may cause the modules to be seated improperly in the chassis, and result in possible damage to the module or the chassis.

⚠ WARNING:
Electrostatic discharge (ESD) can damage module and chassis components. All personnel should be grounded and follow proper ESD procedures before installing, removing, or handling PSAX 20 components.

⚠ WARNING:
The AC power cord is rated at 125 V ac. If you will be using this unit in an application above 125 V ac, you must source an appropriate Agency-approved cordset.

⚠ WARNING:
You must maintain the minimum 5.08 cm (2 in.) of clearance on both sides of the chassis for adequate airflow, or the equipment might fail due to overheating. If you place the unit on or near the floor, dust will accumulate faster inside the chassis.

⚠ CAUTION:
If your system or location loses power or your current session ends abnormally while you are in the process of configuring the system, and you have not yet saved the values permanently, you will lose all unsaved values you have applied on the various windows.

⚠ CAUTION:
Ultimate disposal of this product should be handled according to all laws and regulations in your specific geographic region.

⚠ CAUTION:
Install or remove modules one at a time. Doing this aids in preventing the PSAX 20 system from indicating any erroneous failure messages, and allows the PSAX 20 system to reinitialize and display the accurate configuration of the module that is inserted.

Contents

Copyright and Legal Notices iii
Copyright iii
Trademarks iii
Warranty Information iii
Software and Hardware Limited Warranties iii
Warranty Warnings iv
Regulatory Standards Compliance v
Safety Requirements v
Electromagnetic Compatibility (EMC) and Physical Requirements v
Regulatory Statements v
United States Federal Communications Commission (FCC) Statements v
Canadian Regulatory Statements vii
Industry Canada Information vii
Renseignements Industrie Canada viii

Safety Warnings and Information ix

1 Getting Started 1-1
Purpose of This Guide 1-1
Audience for This Guide 1-1
What You Should Know 1-1
Related Reading 1-1
Lucent Technologies Information Products 1-1
Product Information Library 1-1
Printed Documents 1-4
Other Publications 1-6
Technical Support 1-8
Text Conventions 1-8
Text Types Used in This Document 1-8
Icons and Symbols 1-9
Electrostatic Discharge Precautions 1-10
Grounding Wrist Straps 1-10
Floor Covering 1-10
Temperature and Humidity 1-10
Clothing 1-11

Handling PSAX 20 System Components 1-11
About Lucent Technologies 1-11
History 1-11
For More Information 1-11
Technical Support 1-11
Comments on This Guide 1-12
Before You Begin 1-12
About PacketStar™ PSAX Product Family 1-12

2 Hardware Description 2-1
Overview of This Chapter 2-1
PSAX 20 System Hardware Components 2-1
PSAX 20 Chassis 2-2
Central Processing Unit (CPU) Component 2-3
Stratum 3–4 Component 2-3
PSAX 20 Hardware Specifications 2-4
PSAX 20 Environmental Specifications 2-4
PSAX 20 CPU and Stratum Component Specifications 2-4
PSAX 20 Physical Interface Specifications 2-6

3 System Features 3-1
Overview of This Chapter 3-1
System Capabilities 3-1
Interface Architecture 3-3
User Interfaces 3-3
Circuit Emulation Service 3-4
Dynamic Bandwidth Circuit Emulation Service 3-5
DS1 Service 3-5
DS3 Service 3-5
HDLC Pass-through 3-6
The Interim Interswitch Signaling Protocol (IISP) Interface 3-6
Private Network-Network (PNNI) 1.0 Interface 3-6
PNNI Features Supported By the PSAX Systems 3-7
Peer Group Dynamics 3-7
Topology Information 3-8
PNNI Hierarchies 3-8
The ATM Terminal Emulation Interface 3-9
Network Management 3-9
In-band Management SVCs 3-11

AQueView™ Element Management System 3-11
PSAX 20 Software Features 3-12
Alternate Rerouting Using Dual-Homed PVCs. 3-12
Overview 3-12
Operation 3-13
Application 3-13
AQueMan™ Algorithm 3-14
Connection Gateway API 3-18
Console Help 3-18
Ethernet LAN Bridging 3-19
Firmware Release Control 3-20
Forward Error Correction 3-21
Frame Relay-to-ATM Interworking 3-22
FRF.5 Encapsulating Frames 3-23
FRF.8 Converting Frames 3-23
Frame Relay-to-Frame-Relay Interworking 3-23
Integrated Link Management Interface (ILMI) 3-23
Inverse Multiplexing over ATM (IMA) 3-24
LANET Protocol 3-24
Operations, Administration, and Maintenance (OAM) 3-26
Overview 3-26
OAM Functions 3-27
OAM Cell Characteristics 3-27
F4/F5 Flows 3-27
Fault Management Functions 3-28
Detection 3-28
Reporting 3-29
Localization 3-30
Activation/Deactivation 3-31
Characteristics of OAM Activation / Deactivation Cells 3-31
Module-Specific Alarm Functions 3-32
Loss of Signal (LOS) 3-32
Loss of Frame (LOF) 3-33
Alarm Indicator Signal (AIS) 3-33
Remote Defect Indications 3-34
Soft Permanent Virtual Circuits 3-34
Switched Virtual Circuits 3-35
Functional Description 3-36
Call States 3-36

Traffic Shaping 3-39
Voice Compression 3-41
Voice Processing 3-41
I/O, Optical, and Server Modules 3-42
I/O Modules 3-42
Optical-Type I/O Modules 3-43
Server Modules 3-43
Channelized DS3 Module 3-44
Software Features 3-44
Hardware Features 3-45
Channelized STS-1e (T1) Module 3-45
Software Features 3-46
Hardware Features 3-47
DS1 IMA Module 3-47
Software Features 3-47
Hardware Features 3-47
DS3 ATM Module 3-48
Software Features 3-48
Hardware Features 3-48
DS3 Frame Relay Module 3-48
Software Features 3-48
Hardware Features 3-49
DS3 IMA Module 3-50
Software Features 3-50
Hardware Features 3-50
DS3 ATM Module 3-51
Software Features 3-51
Hardware Features 3-51
DS3 Frame Relay Module 3-51
Software Features 3-51
Hardware Features 3-52
E1 IMA Module 3-52
Software Features 3-53
Hardware Features 3-53
E3 ATM Module 3-53
Software Features 3-53
Hardware Features 3-54
Enhanced DS1 Module 3-54
Software Features 3-55

Hardware Features 3-56
Enhanced E1 Module 3-56
Software Features 3-56
Hardware Features 3-57
Ethernet Module 3-57
Software Features 3-58
Hardware Features 3-58
High-Speed Module 3-58
Software Features 3-58
Hardware Features 3-59
Medium-Density DS1 Module 3-59
Software Features 3-60
Hardware Features 3-61
Multi-Serial Module 3-61
Bit Stuffing and CES Conversion 3-61
Interfaces 3-61
Software Features 3-62
Frame Relay 3-62
Circuit Emulation 3-63
Terminal Emulation 3-63
HDLC Pass-through 3-63
ATM 3-63
Hardware Features 3-63
Voice 2-Wire Office Module 3-64
Software Features 3-64
Voice 2-Wire Station Module 3-64
Software Features 3-65
Hardware Features 3-65
Optical-Type I/O Modules 3-65
OC-3c Multi-mode and Single-Mode Modules 3-65
Software Features 3-66
Hardware Features 3-66
STM-1 Multi-Mode and Single-Mode Modules 3-67
Software Features 3-67
Hardware Features 3-68
Server Modules 3-69
DSP2 Voice Server Module 3-69
Software Features 3-70
DSP2C Voice Server Features 3-71

Multiplexed or Nonmultiplexed AAL-2 3-71
Dynamic DSP Resource Allocation 3-72
Caller ID/Flash Hook Signalling 3-72
Hybrid A, B and C Mode Configurations 3-72
Previous Version Compatibility 3-72
Soft Permanent Virtual Circuit Support 3-72
Voice Processing 3-73
Silence Suppression Comfort Noise 3-73
DSP2A and DSP2B Single-Mode Voice Server Modules (System Release 6.2.0) 3-73
Hardware Features 3-74
Route Server Module 3-74
Hardware Features 3-76
Tones and Announcements Server Module 3-76
Hardware Features 3-76

4 Configuring the Basic System 4-1

Overview of This Chapter 4-1
Logging onto the System 4-1
Help Information 4-3
Selecting Options, Fields, and Commands 4-6
Changing the System Password and Other User Options 4-7
Console Interface Main Menu 4-9
Configuring the System for Your Site 4-9
System Identification Data 4-9
Rules for Configuring IP Addresses 4-11
Rules for Configuring IP Address Masks 4-12
Configuring System Identification 4-12
ATM Addresses and OAM Properties 4-12
Entering and Displaying ATM Addresses and OAM Properties 4-12
Configuring System Date and Time 4-15
System Date and Time Data 4-15
Configuring the TCP Client/Server for a Connection Gateway 4-17
Connection Gateway Application Programming Interface 4-18
Configuring the TCP Server 4-18
Configuring SNMP Trap Destinations 4-20
Configuring In-Band Management 4-21
Adding an In-Band Management ATM SVC Connection 4-22
Preparing for an In-Band Management SVC Connection 4-23
Creating an In-Band-Management SVC Connection 4-24

Viewing In-Band Statistics Data 4-30
Deleting an In-Band Management SVC Route 4-32
Deleting an In-Band Management SVC Route 4-32
Using the Equipment Configuration Window 4-32
Configuring the Stratum 3–4 Clock Timing 4-34
Setting the Stratum Configuration Values 4-34
Switching the Line Timing Source 4-37
Configuring I/O and Server Modules 4-38
Alarm Status Values 4-38
PNNI System-Wide Configuration 4-39
Configuring PNNI 4-39
Configuring PNNI Route Addresses 4-47
Configuring PNNI Metrics 4-51
Configuring Summary Addresses 4-55
Viewing the PNNI Map Link Table 4-58
Viewing the PNNI Link Table 4-62
Viewing the PNNI Neighbor Peer Table 4-68
Viewing PNNI System Statistics 4-71
Configuring Call Control Resource Allocation 4-75
Setting the Configuration Values 4-75
Configuration Guidelines 4-76
Saving the Configuration and Rebooting the System 4-80
Backing Up Your Configuration Data 4-81

5 Using System Diagnostics 5-1

Overview of This Chapter 5-1
Viewing System Status 5-1
Running Cell Test Diagnostics 5-5
Cell Test Diagnostics 5-5
Rebooting PSAX Hardware Components 5-9
Rebooting the PSAX System Hardware Components 5-9
Removing Configuration Files 5-11
Removing Configuration Files 5-12
Unlocking a Telnet Session 5-12
Unlocking a Telnet Session 5-12
Operations and Maintenance (OAM) 5-13
Creating OAM Connections 5-13
Monitoring OAM Functionality 5-23
Performing OAM Tests 5-26

OAM Tests 5-26
OAM Activation and Deactivation. 5-28
Activating and Deactivating OAM. 5-29

6 Configuring the VT100 Terminal Emulator 6-1
Overview of This Chapter 6-1
Setting Up The Windows 3.1 Terminal Emulator 6-1
Setting Up The Windows 95 HyperTerminal Emulator 6-3
Other Software for VT100 Terminal Emulation 6-3
Setting Up a U.S. Robotics-Compatible Modem 6-4

7 Upgrading and Backing Up System Software 7-1
Overview of This Chapter 7-1
Directory Structures 7-2
Installing a New Software Release 7-2
Setting Up a Windows FTP Server 7-3
Upgrading System Software Using FTP 7-4
Upgrading Using XModem/YModem File Transfer Method 7-9
Setting Up for the File Transfer Process 7-9
Transferring Software Upgrade Files 7-10
Field Descriptions 7-12
Upgrading Firmware 7-16
Firmware Drivers 7-16
Upgrading I/O and Server Module Firmware 7-18
Selecting Firmware Drivers 7-21
Falling Back to the Previous Software Release 7-22
Backing Up System Database Files. 7-24
Configuration and Connections Data Files 7-24
Backing Up Database Files Using FTP. 7-24
Backing Up Database Files Using FTP. 7-25
Backing Up Database Files Using XModem/YModem File Transfer. 7-26
Setting Up for the File Transfer Process 7-26
Copying the Database Files to a Storage Medium 7-27
Restoring System Database Files 7-30
Configuration and Connection Data Files 7-30
Restoring Database Files Using FTP 7-30
Restoring Database Files Using FTP 7-31
Rebooting the AC System. 7-32
Restoring Database Files Using XModem/YModem File Transfer 7-32

Setting Up for the File Transfer Process 7-33
Copying the Backup Files to the System 7-33
Rebooting the AC System 7-36

Appendix A: SNMP Trap Messages A-1
Viewing SNMP Trap Messages A-1
Definitions of MIB Objects Used for Traps A-43

Appendix B: Pin Configurations B-1
Overview of This Appendix B-1
Configuration for the Power Supply Connector B-1
AC Power Supply Connector B-1
Configuration for the CPU Connectors B-2
Console Serial Interface B-2
Ethernet 10Base-T Interface B-3
Configuration for the DS1/T1 Interface Cable Connector B-3

Appendix C: Configuring In-Band Management C-1
Setting Up In-Band Management Configuration C-1
Using the Direct Connection Configuration C-2
Using the Routed Connection Configuration C-4
Setting PVC Connections for Routed Connection Configuration C-7
Using the Hybrid Connection Configuration C-10
Setting PVC Connections for Hybrid Connection Configuration C-12

Appendix D: ATM Traffic Descriptors D-1
Overview of This Appendix D-1
Connections Supporting Traffic Descriptors D-1
Traffic Descriptors Supported D-1

Appendix E: Reference Tables E-1
Overview of This Appendix E-1
QoS Information Tables E-1
Compliance Matrix E-4
Alarm Status Table E-9
Connection Type by Interface Type Table E-10
Interface Type by Module Table E-12

Index Index-1

1 Getting Started

Purpose of This Guide

The *PacketStar™PSAX 20 Access Concentrator User Guide* provides information about the following:

- Understanding the PSAX 20 system functions and features
- Configuring basic system parameters and managing the PSAX 20 system

Note: If you are setting configuration values for a new, unconfigured PSAX device for the first time, you should read through this guide before beginning the configuration process.

Audience for This Guide

The information in this guide is intended for people who will configure and maintain the basic PSAX 20 system.

What You Should Know

Before you use this document or operate the PSAX 20 chassis you should already understand and have experience with the following:

- ATM Forum and Frame Relay Forum specifications
- Ethernet network capabilities
- Internet Protocol capabilities
- Data network design
- Telephony network design
- General network management practices

Only authorized personnel should use the Access Concentrator system.

Related Reading

Lucent Technologies Information Products

Product Information Library

To install and use your PSAX 20, you will need to read the following publications, which are provided on your Lucent Technologies PSAX 20 Product Information Library CD-ROM.

Table 1-1. PacketStar™ Release 6.3.0 Product Information Library (Adobe Acrobat Reader Files)

Menu Option	Document
PSAX 20 Access Concentrator	
	PSAX 20 Installation and Operation Guide
	PSAX 20 User Guide
Release Notes and Bulletins	
	Access Concentrator Family Release Notes R630 PDF, Issue 1
	New Features Bulletin for Release 6.3
	Safety Warnings Shipping Sheet, Issue 4
Connection Gateway API Documents	
	PacketStar Connection Gateway API Developers Guide
Application Notes	
	PacketStar ATM Access Concentrators and DEFINITY ECS Application Note R620
	Connecting a CBX or GX Switch to a PSAX Access Concentrator Via an ATM Port: Application Note, Issue 1
	PacketStar Access Concentrator Trunk Conditioning Application Note, Issue 1
	Using the PacketStar PSAX Access Concentrator Caller ID Feature Application Note, Issue 1

To configure the I/O and server modules, read the following publications that are provided on your Lucent Technologies Access Concentrator Modules Product Information Library CD-ROM.

Table 1-2. PacketStar™ Modules Product Information Library (Adobe Acrobat Reader Files) Release 6.3.0

Menu Option	Document
PacketStar PSAX Modules	
	Alarm Module Guide
	Channelized DS3 Module Guide
	Channelized STS-1e Module Guide
	DS1 IMA Module Guide
	DS3 ATM Module Guide
	DS3 Frame Relay Module Guide
	DS3 IMA Module Guide

Table 1-2. PacketStar™ Modules Product Information Library (Adobe Acrobat Reader Files) Release 6.3.0

Menu Option	Document
	DSP2A/ DSP2B/ DSP2C Voice Server Modules Guide
	E1 IMA Module Guide
	E3 ATM Module Guide
	Enhanced DS1 Module Guide
	Enhanced E1 Module Guide
	Ethernet Module Guide
	High-Density E1 (21-port) Module Guide
	High-Speed Module Guide
	Medium-Density DS1 Module Guide
	Multi-Serial Module Guide
	OC-3c Multi-Mode and Single-Mode 1+1 APS Module Guide
	OC-3c Multi-Mode and Single-Mode Modules Guide
	Route Server Module Guide
	STM-1 Multi-Mode and Single-Mode 1+1 MSP Module Guide
	STM-1 Multi-Mode and Single-Mode Modules Guide
	Tones and Announcements Server Module Guide
	Voice 2-Wire Station Module Guide
	Voice 2-Wire Office Module Guide
Release Notes and Bulletins	
	Access Concentrator Family Release Notes, Release 6.3, Issue 1
	New Features Bulletin for Release 6.3
	Voice 2-Wire Office Module Safety Bulletin, Issue 1
	Safety Warnings Shipping Sheet, Issue 4
Application Notes	
	PacketStar PSAX Access Concentrators Caller ID Application Note, R6.3
Declarations of Conformity	
	I/O Module 32 MB Memory Upgrade, Declaration of Conformity, EMC
	Route Server Module, EMC
	DSP2 Voice Server Module with Echo Cancellation, EMC

Table 1-2. PacketStar™ Modules Product Information Library (Adobe Acrobat Reader Files) Release 6.3.0

Menu Option	Document
	DSP2A Voice Server Module with Echo Cancellation, EMC
	DSP2B Voice Server Module with Echo Cancellation, EMC
	DSP2C Voice Server Module with Echo Cancellation, EMC
	High-Density E1 Module, EMC
	High-Density E1 Module, Telecom,
	High-Density E1 Module, Low Voltage,
Other Hardware Installation Guides	
	PacketStar PSAX CO Access Concentrators, Patch Panel and Cable Installation Guide, Issue 1

Printed Documents

For your convenience, the following documents from your Product Information Library CD-ROM are also available in printed form. For ordering information, contact your Lucent Technologies distributor or account representative.

Table 1-3. PacketStar™ Release 6.3.0 Product Information Library (Printed Documents)

Document	Issue	COMCODE	Document Number
PSAX 20 Installation and Operation Guide, Release 6.3	Issue 1	300303260	255-700-018
PSAX 20 User Guide, Release 6.3	Issue 1	300303286	255-700-020
PacketStar™ *Family of Access Concentrators, Release Note, System Software Release 6.3.0*	Issue 1	N/A	N/A
PacketStar™ *Connection Gateway API Developer's Guide, Release 6.3.0*	Issue 1	300314515	255-700-100
Using the PacketStar™ PSAX Access Concentrator Caller ID Feature Application Note	Issue 1	300284338	255-700-006
PacketStar™ ATM Access Concentrators and DEFINITY ECS Application Note	Issue 1	300306065	255-700-122

Table 1-3. PacketStar™ Release 6.3.0 Product Information Library (Printed Documents)

Document	Issue	COMCODE	Document Number
PacketStar™ ATM Access Concentrators Trunk Conditioning Application Note	Issue 1	300287018	255-700-072
Connecting a CBX or GC Switch to a PacketStar™ PSAX Access Concentrator Via an ATM Port Application Note	Issue 1	300287059	255-700-012

Table 1-4. *PacketStar*™ Modules Product Information Library (Printed Documents)

Document	Issue	COMCODE	Document Number
Channelized DS3 Module User Guide, Release 6.3	Issue 1	300303070	255-700-028
Channelized STS-1e T1 Module User Guide, Release 6.3	Issue 1	300303088	255-700-029
DS1 IMA Module User Guide, Release 6.3	Issue 1	300303096	255-700-032
DS3 ATM Module User Guide, Release 6.3	Issue 1	300303104	255-700-033
DS3 Frame Relay Module User Guide, Release 6.3	Issue 1	300303112	255-700-034
DSP2A, DSP2B and DSP2C Voice Server Modules User Guide, Release 6.3	Issue 1	300303120	255-700-035
Enhanced DS1 Module User Guide, Release 6.3	Issue 1	300303161	255-700-038
Ethernet Module User Guide, Release 6.3	Issue 1	300303179	255-700-040
High-Speed Module User Guide, Release 6.3	Issue 1	300303195	255-700-041
Medium-Density DS1 Module User Guide, Release 6.3	Issue 1	300298676	255-700-120
Multi-Serial Module User Guide, Release 6.3	Issue 1	300303203	255-700-042

Table 1-4. *PacketStar*™ Modules Product Information Library (Printed Documents)

Document	Issue	COMCODE	Document Number
OC-3c Multi-Mode and Single-Mode Modules User Guide, Release 6.3	Issue 1	300303229	255-700-044
Route Server Module User Guide, Release 6.3	Issue 2	300303328	255-700-052
STM-1 Multi-Mode and Single-Mode Modules User Guide, Release 6.3	Issue 1	300303344	255-700-045
Tones and Announcements Server Module User Guide, Release 6.3	Issue 1	300303427	255-700-121
Voice 2-Wire Office Module User Guide, Release 6.3	Issue 1	300303351	255-700-047
Voice 2-Wire Station Module User Guide, Release 6.3	Issue 1	300303377	255-700-048

Other Publications

Numerous books are currently available on the subject of basic telecommunications technology and specific protocols. In addition to such general reading, you should also be familiar with the specifications identified in the following documents:

- American National Standards Institute (ANSI) documents
  - T1.207, Operations, Administration, Maintenance, and Provisioning (OAM&P) Terminating Test Line Capabilities and Access Arrangements
  - *T1.403, af-phy-0016.000* and *af-test-0037.000*
  - *T1.646, Broadband ISDN-Physical Layer Specification for UNI Including DS1/ATM*
- ATM Forum Technical Committee Specifications:
  - *Circuit Emulation Service Interoperability Specification Version 2.0, af-vtoa-0078.000*
  - *Specifications of (DBCES) Dynamic Bandwidth Utilization, af-vtoa-0085.000*
  - *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*
  - *Interim Inter-switch Signaling Protocol (IISP) Specification Version 1.0, af-pnni-0026.000*
  - *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0, af-pnni-0055.000*
  - *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0 Addendum, af-pnni-0066.000*
  - *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0 Errata and PICS, af-pnni-0081.000*

  - *Traffic Management Specification Version 4.1*, af-tm-0121.000
  - *User to Network Interface (UNI) Specification Version 3.0*
  - *User to Network Interface (UNI) Specification Version 3.1*
  - *VTOA AAL1 Trunking Services*, af-vtoa-0098.000
- ATM Forum Implementation Agreements:
  - *Inverse Multiplexing over ATM Version 1.0, af-phy-0086.000*
  - *Inverse Multiplexing over ATM Version 1.1, af-phy-0086.1*
- Bellcore Documents:
  - *FR-796, Reliability and Quality Generic Requirements*
  - *GR-63-CORE, NEBS*
  - *GR-124-CORE (for OAM)*
  - GR-246-CORE (for Tones and Announcements Server Module test capability)
  - *GR-253-CORE, Issue 2, Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (for Channelized STS-1e module)*
  - *GR-499-CORE, Common Requirements for TSGR*
  - *GR-820-CORE, OTGR Section 5.1, Generic Transmission Surveillance*
  - *GR-1089-CORE, Emissions*
  - *GR-1248-CORE, Operations of ATM Network Elements*
- *CCITT Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Synchronous Operation of Public Data Networks, Recommendation X.21*
- CTR Documents
  - CTR 4
  - CTR 12
  - CTR 13
- ETSI 300-233, Access Digital Section for ISDN Primary Rates
- Frame Relay Forum (FRF) Implementation Agreements:
  - *FRF.1—User-to-Network Interface (UNI)*
  - *FRF.2—Network-to-Network Interface (NNI)*
  - *FRF.3—Multi-protocol Encapsulation Impementation Agreement*
  - *FRF.5—Frame Relay/ATM PVC Network Interworking*
  - *FRF.8—Frame Relay/ATM PVC Service Interworking*
- *IEEE 802.1D Specification*
- *International Telecommunication Union (ITU) Documents*
  - *G.703, Physical/Electrical Characteristics of Hierarchical Digital Interface*
  - *G.704, Synchronous Frame Structures Used at Primary and Secondary Hierarchical Levels*
  - *G.736, Characteristics of Synchronous Digital Multiplex Equipment Operating at 2048 Kb*
  - *G.775, Loss of Signal (LOS) and Alarm Indication Signal (AIS)*

  - *G.823, The Control of Jitter and Wander Within Digital Networks Which Are Based on the 2048 Kb/S Hierarchy*
  - *I.356, B-ISDN ATM Layer Cell Transfer Performance*
  - *I.361, B-ISDN ATM Layer Specification*
  - *I.363, B-ISDN ATM Adaptation Layer (AAL) Specification*
  - *I.371, B-ISDN Traffic Control and Congestion Control*
  - *I.431, ISDN, PRI User-Network Interface Layer 1 Specifications*
  - *I.610, ISDN Maintenance Principles, B-ISDN OAM*
  - *Q.2110, B-ISDN SAAL Service Specific Connection Oriented Protocol (SSCOP)*
  - *Q.2130, B-ISDN SAAL Service Specific Coordination Function (SSCF) for Support of Signaling at the User-Network Interface*
  - *Q.2931, B-ISDN DSS2 User-Network Interface (UNI) Layer 3 Specification*
- *TIA/EIA-464-B Requirements for Private Branch Exchange (PBX) Switching Equipment* (for caller ID/flash hook signaling)
- *Internet Engineering Task Force (IETF) Request for Comment (RFC) Documents*
  - *RFC 792, Internet Control Message Protocol (ICMP)*
  - *RFC 1406, Definitions of Managed Objects for the DS1 and E1 Interface Types*
  - *RFC 1407, Definitions of Managed Objects for the DS3 and E3 Interface Types*
  - *RFC 1595, Definitions of Managed Objects for the SONET/SDH Interface Types*
  - *RFC 1661, Point-to-Point Protocol*
  - *RFC 1662, PPP in HDLC-like Framing*
  - *RFC 2364, PPP Over AAL-5*

Technical Support

If you experience a problem with your PSAX 20 system, refer to the *Lucent Technologies InterNetworking Systems Global Warranty* card that accompanied your PSAX 20 product shipment for instructions on obtaining support in your area.

Text Conventions

Text Types Used in This Document

This book uses a different kind of type for each kind of text you will see on screens and equipment. In general, text you see in the book will closely resemble what you see on the screens and equipment. The following table shows how each typographical convention is used.

Appearance	How it is used
SERIF NORMAL, ALL CAPS	Text on module panels or other hardware
`Fixed-width normal`	Text you read on a screen
Sans serif bold	Menu commands followed by commands on pull-down menus (separated by commas) A menu item followed by a pull-down menu item
Serif bold	Text you type on a text-based screen or inside a field in a window Any key that you press on the keyboard
`Serif italics`	A variable name for which you will substitute your own information An argument or parameter on a command line

Icons and Symbols

Follow all safety guidelines in this document to help prevent personal injury to you and damage to the PSAX 20 Access Concentrator system equipment. Refer to the procedures within this user guide for important safety information and proper procedures.

Standard icons and symbols to alert you to dangers and cautions are listed below.

⚠ DANGER:
Warnings for a general personal injury hazard are identified by this format.

⚠ WARNING:
Warnings relating to risk of equipment damage or failure are identified by this format.

⚠ CAUTION:
Warnings relating to risk of data loss or other general precautionary notes are identified by this format.

Note: Identifies additional information pertinent to the text preceding this note.

Electrostatic Discharge Precautions

The room where the PSAX 20 system is located must have built-in precautions to provide protection from electrostatic discharge damage to electronic components. The following sections provide details on these necessary precautions.

Grounding Wrist Straps

Attach at least one grounding wrist strap to a common ground for each chassis/electronic rack to be handled. Follow these guidelines for wrist straps:

- Make sure the wrist straps or wrist strap cords have built-in 1-megaohm (minimum) resistance.
- Make sure the wrist straps and wrist strap cords are UL listed.
- Ensure the wrist strap cord is long enough so it can be worn while working either at the front or the back of the rack.
- Always discharge any static charge by touching your wrist strap before you touch the PSAX 20 chassis.

Floor Covering

Be sure the room has an antistatic floor covering (conductive mat, tiles, or carpeting) to minimize static charge buildup as you walk across the room. Follow these guidelines for installing and maintaining proper floor coverings:

- Using foot grounding straps (attached to the heels of your shoes) is recommended, even if you are walking in rooms with antistatic floor covering. These straps provide additional protection against electrostatic discharge. The straps should have built-in 1-megaohm (minimum) resistance.
- Wool carpet is not an acceptable floor covering.
- Other types of carpet must be sprayed daily with a topical antistatic chemical before you perform any work in the room. Paying constant attention to carpet maintenance is time-consuming but required.

Temperature and Humidity

Establishing the proper temperature and humidity in the room where the PSAX 20 system is located helps control many static discharge problems. Maintaining proper room climate is especially important when heat is turned on during the cold weather. To avoid damage to the PSAX 20 system, do not allow the humidity to increase to the level where water droplets appear on surfaces. The temperature and relative humidity must be kept within the specified tolerance limits as shown in the *PacketStar™PSAX 20 Access Concentrator Installation and Operation Guide*.

Clothing

When working with the PSAX 20 system, avoid wearing clothing made from wool or synthetic materials. Try to minimize contact between clothing and electronic components.

Handling PSAX 20 System Components

Follow these guidelines for proper handling of the PSAX 20 hardware to minimize electrostatic discharge damage:

- Do not remove the chassis, modules, and other items from their protective packaging until you are ready to install them.
- When installing modules and components, use a grounding wrist strap connected to a common electrical ground to prevent electrostatic discharge damage. (A common electrical ground is a complete circuit between a person or an electrical/electronic device and the earth.)
- Store components in electrostatic-discharge-protective bags when they are not in use.

About Lucent Technologies

History

Lucent Technologies is the communications systems and technology company formed through the restructuring of AT&T. We bring with us a tradition of more than 125 years of experience and a dedication to superior customer service.

Lucent Technologies manufactures, sells, and services a complete line of customer premises communications units, and commercial and multimedia communications and messaging systems designed and supported by our research and development unit, Bell Laboratories.

Our legacy and our spirit of innovation allow Lucent to provide our customers with the tools needed to communicate effectively, any time and anywhere, and to integrate the latest technologies into real-life solutions that help make business work.

For More Information

To learn more about the *PacketStar™* family of ATM Multiservice Access Concentrators and the complete line of Lucent Technologies products, visit our Web site at *www.lucent.com*.

Technical Support

If you experience a problem with your PSAX 20 system, refer to the *Lucent Technologies InterNetworking Systems Global Warranty* card that accompanied

your PSAX 20 product shipment for instructions on obtaining support in your area.

Comments on This Guide

To comment on the *PacketStar™PSAX 20 Access Concentrator User Guide*, please complete the comment card that accompanied your shipment and mail it to the following address:

Manager, Information Design and Development
InterNetworking Systems
Broadband Carrier Networks
Access Technology Group
Lucent Technologies
8301 Professional Place
Landover, MD 20785
U.S.A.

You may also fax the comment card to us at: 301-809-4540.

Before You Begin

Before you begin using your new PSAX 20 Access Concentrator system, be sure you accomplish the following:

- Install the PSAX 20 system according to directions in the installation guide accompanying this guide.
- Read carefully the safety cautions listed in the section"Safety Information," in the front matter of this guide.
- Work out and record your site-specific specifications such as IP addresses you will use, connections and interfaces you will need, user names and passwords you will assign, and so on.

About *PacketStar*™ PSAX Product Family

Lucent's PacketStar™ PSAX family provides a complete range of multiservice access concentrators, as described in Table 1-5.

This manual applies to the PSAX 20 only. For details on installing, operating, or managing other PSAX equipment, see the appropriate guides for those chassis.

Table 1-5. *PacketStar*™ PSAX Product Family

Target Market	Device Name	Application/Description
Small Customer Premises	AC 60	The *PacketStar* AC 60 is ideal for enterprise networks seeking to consolidate branch office voice, video, and data traffic onto a single ATM network. Supporting up to four user interfaces, this system offers high port-density in a small footprint for mid-to-large sized customer premises applications. It supports a full range of interfaces such as DS1/E1, DS3/E3, OC-3c and STM-1 in both Single- and Multi-mode, 10/100BaseT Ethernet, analog voice, or digital voice with processing capabilities.
	PSAX 15	The *PacketStar* PSAX 15 offers a low-speed T-1/E-1 integrated access option, especially for AAL-2 voice-focused applications. A scalable, multiservice access concentrator for enterprise applications, the *PacketStar* PSAX 15 optimizes wide area network (WAN) bandwidth with toll-quality voice compression, traffic optimization, and port scalability from T-1/E-1 to OC-3c connections.
	PSAX 20	The *PacketStar* PSAX 20 system is the most scalable and flexible multiservice access product in its class. This scalability enables service providers to meet the demands of a growing enterprise customer with a single-edge solution. The PSAX 20 optimizes wide area network bandwidth with toll-quality voice compression, traffic optimization, and port scalability from T1/E1 to OC-3c/STM-1 connections.
	PSAX 50	The *PacketStar* PSAX 50 provides a low-cost, entry-level platform for multiservice access onto a public or private asynchronous transfer mode (ATM) network at speeds up to T-1/E-1. The PSAX 50 unit accommodates up to 10 I/O interfaces, supporting a variety of voice, video, and data connections. It is upgradable to the more powerful PSAX 100 unit simply by upgrading the software. This low-speed T-1/E-1 integrated access solution is also appropriate for remote sites.
Customer Premises	PSAX 100	The *PacketStar* PSAX 100 unit offers high-speed (n X T-1/E-1 to OC-3c/STM-1) integrated access at the customer's premises. Designed to enable service providers to offer multiple applications and broadband services to corporate customers, the *PacketStar* PSAX 100 unit cost-effectively extends ATM services beyond the wide area network, into the customer premises. The PSAX 100 unit can accommodate up to 17 I/O interfaces that support a high mix of native applications and broadband services, including 10/100 Mbps Ethernet, frame relay, circuit-switched services for voice and video applications, and high-speed ATM connections for broadband services. The PSAX 100 also supports a wide range of ATM interfaces for network uplink access to a wide area network, including T-1/E-1, T-1/E-1 ATM IMA, T-3/E-3, and OC-3c/STM-1.

Table 1-5. *PacketStar*™ PSAX Product Family

Target Market	Device Name	Application/Description
	PSAX 600	The *PacketStar* PSAX 600 is a more sophisticated unit, ideal for low-end multiservice access concentration in the customer's premises or small central office. Designed to enable service providers to offer multiple applications and broadband services to multitenant and large enterprise customers, the *PacketStar* PSAX 600 furnishes a powerful, mid-level broadband service access solution and low-speed ATM access concentration. The PSAX 600 economically supports a high mix of applications and services enabling service providers to deliver advanced data, voice, and video services. The PSAX 600 unit can accommodate up to 57 I/O interfaces supporting 10/100 Mbps Ethernet ports, frame relay, circuit-switched services for voice and video applications, and high-speed ATM connections for broadcast-quality MPEG video over ATM, and high-throughput router and server connections, as well as advanced broadband services.
Carrier Class Office	PSAX 1250	The *PacketStar* PSAX 1250 is designed to provide a full range of central office-based multiservice access concentration. Ideal for the central office or a large enterprise's multiservice access concentration, the *PacketStar* PSAX 1250 provides highly reliable network access for TDM voice, frame relay, and ATM data applications. The PSAX 1250 I/O interfaces (that include 75 bps to 30 Mbps serial, T-1/E-1, DS3/E-3/STS-1e, OC-3c/STM-1, Ethernet and 2-wire station/office options) are supported by a sophisticated package of features. These features include a PNNI (Private Network-to-Network Interface), ILMI (Integrated Local Management Interface), 1+1 APS (Automatic Protection Switching), trunk alarming, and an SS7 signaling gateway interface. Featuring a 1.2 Gbps ATM cell bus architecture, carrier-class reliability, and full redundancy, the PSAX 1250 is a cost-effective access switch solution for bridging to legacy equipment.
	PSAX 2300	The *PacketStar* PSAX 2300 offers carrier-grade, high-density multiservice access concentration. Designed to provide multiservice access concentration in the central office or for a large enterprise customer, the *PacketStar* PSAX 2300 provides network access for TDM voice, frame relay, and ATM data applications. The PSAX 2300 I/O interfaces (that include 75 bps to 30 Mbps serial, T-1/E-1, DS3/E3/STS-1e, OC-3c/STM-1, Ethernet and 2-wire station/office) are supported by a sophisticated package of features, such as PNNI (Private Network-to-Network Interface), ILMI (Integrated Local Management Interface), 1+1 APS (Automatic Protection Switching), trunk alarming, and an SS7 signaling gateway interface. Featuring a 3.9 Gbps ATM cell bus architecture, carrier-class reliability, provisions for OC-12c interfaces, and N x T-1/E-1 module protection switching, the PSAX 2300 solves many demanding and diverse network design challenges with ease.

2 Hardware Description

Overview of This Chapter

This chapter presents an overview of the PSAX 20 Access Concentrator system hardware.The content is organized as follows:

- Overview of This Chapter
- PSAX 20 System Hardware Components
  - ~ PSAX 20 Chassis
  - ~ The Central Processing Unit (CPU) Component
  - ~ The 3–4 Stratum Component
- PSAX 20 Hardware Specifications
- PSAX 20 Environmental Specifications
- PSAX 20 Physical Interface Specifications

PSAX 20 System Hardware Components

The following hardware components make up the PSAX 20 system:

- Chassis—mounted in a standard 48.26-cm (19-inch) rack or a telco frame, or placed on a shelf or table
- Factory-installed components:
  - ~ Central Processing Unit (CPU) component
  - ~ Power Supply component
  - ~ Stratum 3–4 clock timing component
  - ~ T1/E1 component
  - ~ DSP2B component
- User-selected input/output (I/O) and server modules:
  - ~ Alarm module
  - ~ Channelized DS3 module
  - ~ DS1 IMA module
  - ~ DS3 module—three types available:
    - ATM
    - Frame Relay
    - IMA
  - ~ E3 ATM module
  - ~ Enhanced DS1 module

- Ethernet module
- High-Speed module
- Medium-Density DS1 module
- Multi-Serial module
- OC-3c Multi-Mode (MM) module—two types available:
  - AQueMan™ firmware (MMAQ)
  - Traffic-shaping firmware (MMTS)
- OC-3c Multi-Mode (MM) 1+1 APS module
- OC-3c Single-Mode (SM) module—two types available:
  - AQueMan™ firmware (SMAQ)
  - Traffic-shaping firmware (SMTS)
- OC-3c Single-Mode (SM) 1+1 APS module
- Route Server
- STM-1 Multi-Mode (MM) module—two types available:
  - AQueMan™ firmware (MMAQ)
  - Traffic-shaping firmware (MMTS)
- STM-1 Multi-Mode (MM) 1+1 MSP module
- STM-1 Single-Mode (SM) module—two types available:
  - AQueMan™ firmware (SMAQ)
  - Traffic-shaping firmware (SMTS)
- STM-1 Single-Mode (SM) 1+1 MSP module
- Tones and Announcements Server module
- Voice 2-Wire Office module
- Voice 2-Wire Station module

PSAX 20 Chassis

The PSAX 20 chassis consists of an enclosure with a backplane, two horizontal slots for user-selected I/O and server modules, and three cooling fans. The chassis fits in a standard 48.26-cm (19-inch) rack or telco frame. When mounted in a rack, the chassis requires at least 5.08 centimeters (two inches) of clearance at each side for cooling. The fan filter on the right side of the chassis draws air from the openings in the right side. The left side of the chassis faceplate has controls and indicators for the common equipment components (see Figure 2-1).

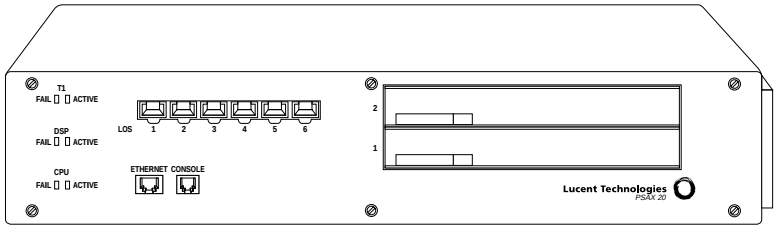

Figure 2-1. PSAX 20 System with Enclosed Chassis

The chassis backplane has a single bus, which supports 600 Mbps of ATM bandwidth, and live insertion and removal of the I/O and server modules. Power is distributed through the backplane to the cooling fans and the I/O and server modules.

Central Processing Unit (CPU) Component

The Central Processing Unit (CPU) component provides the processing, switching, and storage functions for the PSAX 20 system. The RISC-based microprocessor has the processing power to maintain data flow, perform numerical calculations, and manage the DMA interfaces. While the interface-specific physical and link layer protocol functions, in addition to the queuing and traffic management functions, are performed on each of the various I/O modules, the CPU module has 64 MB of memory for routing and signalling functions, forward error correction, processing of SVC connections, and network management capabilities.

Stratum 3–4 Component

The Stratum 3–4 component provides synchronization and monitoring for the PSAX 20 system. This component supports the backplane bus and furnishes 600 Mbps of ATM bandwidth. In addition, the PSAX 20 system can obtain network clock synchronization through the backplane from any of its I/O modules except for the DSP2A/B/C Voice Server, Ethernet, High-Speed, Tones and Announcements Server, Route Server, Voice 2-Wire Station, and Voice 2-Wire Office modules. The Multi-Serial module can be used for network timing, but it is not recommended. With the ability to accept a timing reference from any physical interface at low transmission rates, the system provides the network with a reliable transport and access infrastructure. The Stratum 3–4 clock timing is accurate to Stratum 3 requirements, allowing the PSAX 20 system to freely run even after losing external synchronization, for as long as 24 hours, without synchronization problems.

PSAX 20 Hardware Specifications

Table 2-1 describes the physical specifications for the hardware components that make up the PSAX 20 system.

Table 2-1. PSAX 20 Chassis Hardware Specifications

Slot configuration:	Two I/O and server modules
Height:	8.9 cm (3.5 in)
Width:	44.04 cm (17.34 in)
Depth:	33 cm (13 in)
Weight:	5.9 kg (13.1 lb)
Material:	Aluminum
Color:	Black
Cooling method:	Three fans and one filter kit on right side
Power source requirements:	Any power source input from 90 to 264 V ac power supply
Clock synchronization:	Built-in (factory-installed) Stratum 3–4 clocking

PSAX 20 Environmental Specifications

Table 2-2 describes the environmental specifications for the PSAX 20 system.

Table 2-2. Environmental Specifications for the PSAX 20 System

Specification	Range of Values
Operating temperature:	32° to 122° F 0° to 50° C
Storage temperature:	-40° to +158° F -40° to +70° C
Operating relative humidity:	40 to 60%, optimum; Up to 95°%, noncondensing

PSAX 20 CPU and Stratum Component Specifications

This section details the specifications for the installed CPU and Stratum components for the PSAX 20 system.

The hardware specifications for the PSAX 20 CPU component are given in Table 2-3.

Table 2-3. PSAX 20 CPU Component Specifications

Specification	Description
Units per system:	1 factory installed component
Power consumption	18 W, average
Processing:	RISC microprocessor
Memory:	128 MB flash drive 64 MB RAM
Connectors:	One RJ-45 connector labeled ETHERNET and one RJ-12 connector labeled CONSOLE on the faceplate
LED indicators:	Two indicators: • ACTIVE—green • FAIL—red

The hardware specifications for the PSAX 20 Stratum 3–4 component are given in Table 2-4.

Table 2-4. PSAX 20 Stratum 3–4 Component Specifications

Specification	Description
Operating temperature:	0° to 50° C
Operating humidity:	Up to 95%, noncondensing
Storage temperature:	-40° to +70° Celsius (-40° to 158° Fahrenheit)
Units per system:	1 factory installed component
Synchronization source:	Internal
Accuracy:	Stratum 3 or 4, selectable
LED indicators:	Two indicators: • ACTIVE—green • FAIL—red

PSAX 20 Physical Interface Specifications

Table 2-5 describes the interface specifications of the PSAX 20 system.

Table 2-5. Physical Interface Specifications

ATM Standards	ATM Forum User-network Interface (UNI) (Versions 3.0, 3.1) ATM Forum Inter-switch Signaling Protocol (IISP) (Version 1.0) ATM Forum Integrated Local Management Interface (ILMI) (Version 4.0) ATM Forum Inverse multiplexing over ATM (IMA) (Versions 1.0, 1.1) ATM Forum Private Network-Network Interface (PNNI) (Versions 1.0)
WAN Interfaces	DS1, E1, DS3, E3, OC-3c, STM-1, DS1 IMA, E1 IMA, DS3 IMA
Narrowband Interfaces	Voice 2-Wire Office (Sink), Voice 2-Wire Station (Source)
LAN Interfaces	T1, E1, OC-3c, Ethernet, Serial (RS-232, EIA-449, EIA-530), Parallel
Management Interfaces	Ethernet (RJ-45), EIA-232 (RJ-11), Inband (IP over ATM) (RFC 1483)

3 System Features

Overview of This Chapter

This chapter presents a software overview of the PSAX 20 Access Concentrator offered by Lucent Technologies. The following aspects of the PSAX 20 Access Concentrator system are discussed:

- Features and capabilities of the system
- Architecture, interfaces, and functions of the PSAX 20 Access Concentrator system
- Features that enable users to customize the PSAX 20 Access Concentrator system for specific requirements and applications

System Capabilities

The PSAX 20 system enables service providers, central offices or end users at customer premises to do the following:

- Consolidate voice, video, and data traffic on a single ATM network
- Extend the capabilities of embedded ATM-based equipment to voice and video traffic

The PSAX 20 Access Concentrator system offers a variety of user interfaces to support voice, video, and data applications (see Figure 3-1).

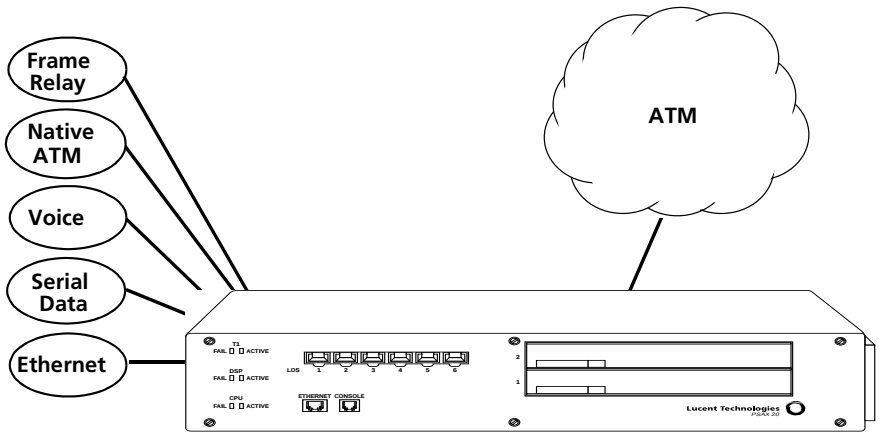

Figure 3-1. Interface Capabilities of the PSAX 20 System

While voice, video, and data traffic have traditionally been carried on separate overlay networks, the *PacketStar*™ Access Concentrator systems aggregate all traffic types into a common network infrastructure. Even though such consolidation means that traffic, in effect, competes for the same physical resources, the traffic management and bandwidth utilization capabilities of the Access Concentrator systems help to ensure that the required quality-of-service (QoS) levels are satisfied within the available constraints of the network. Unique features of the systems include:

- Variable-speed ATM access technology, implemented via the LANET (Limitless ATM Network Protocol), to support a wide range of interfaces
- An advanced queuing and cell-switching algorithm, provided by the *AQueMan*™ (adaptive queue management) firmware algorithm, a patented technology offered by Lucent Technologies to differentiate voice, video, and data requirements, thus helping to ensure QoS levels
- Cell-counting capability to allow ATM usage-based billing
- A connection gateway application programming interface (API) that provides an interface to the PSAX 20 by which an external workstation (gateway) can control the PSAX 20 ATM switching using non-native ATM networking protocols

  Through the use of the API, the gateway and the PSAX 20 can combine to perform powerful interworking of ATM, Integrated Services Digital Network (ISDN), SS7, channel associated signaling (CAS), and other protocols
- Inverse multiplexing over ATM (IMA) to create virtual access lines that are faster than E-1 lines, but not as expensive as T-3/E-3 lines
- Live insertion of hot-swappable modules
- An integrated local management interface (ILMI) feature that supports bidirectional exchange of ATM interface parameters between two connected ATM interface management entities (IMEs) using Simple Network Management Protocol (SNMP) and an ATM interface management information base (MIB)
- An alternate rerouting feature, known as dual-homed permanent virtual circuits (DHPVC), that improves reliability of PVC connections and supports redundancy options to deliver near-zero downtime using circuit emulation, terminal emulation, frame relay, Ethernet, and ATM interfaces
- A switched virtual circuit (SVC) feature, to provide dynamic allocation of connections through the use of interim interswitch signaling protocol (IISP) or private network-network interface (PNNI) for call setup and (automatic) rerouting
- A soft PVC (SPVC) feature, which is a semipermanent virtual connection used for call setup and (automatic) rerouting that has attributes of both a switched virtual connection and a permanent virtual connection

- PNNI, which computes paths through a network by defining a method for distributing topology information between switches and clusters of switches. PNNI also provides a method for signaling used to establish point-to-point and point-to-multipoint connections across ATM networks
- An operations, administration, and maintenance (OAM) feature that affects the system software and I/O module firmware associated with generating, receiving, and interpreting F4 and F5 OAM flows. The function types of the OAM cells include fault management, performance management, and system management
- A keep alive/heartbeat timer to confirm that connections are live
- Unidirectional connection and path modification
- A Remote Firmware Release feature that allows upgrading both CPU software and input/output (I/O) module firmware at a user site from either a CD-ROM or a downloaded FTP software file.

Interface Architecture

The PSAX 20 interface architecture distinctly separates the ATM adaptation functions from the switching functions of the Access Concentrator system. The interface architecture has four distinct processes:

- Physical media access
- Service protocol translation
- ATM addressing
- Queuing

The physical media access layer handles functions specific to each physical interface, connecting each user port to other users or network elements.

The service protocol translation process performs segmentation and reassembly (SAR) to adapt non-native ATM services to ATM-based services and back again. It ensures that the data stream is mapped to standard ATM Adaptation Layer (AAL) protocols.

ATM addressing provides user-specified virtual path identifier/virtual channel identifier (VPI/VCI) coding, bandwidth allocation, and quality of service (QoS) information.

ATM cells are placed in input and output queues based on their QoS parameters. Employing the *AQueMan*™ adaptive queue management algorithm, the PSAX 20 access concentrator transports these cells from the ATM switching fabric to the I/O port.

User Interfaces

The PSAX 20 offers a variety of user interfaces to support voice, video, and data applications.

Circuit Emulation Service

Circuit emulation service transports traffic over a virtual channel-based connection. Circuit emulation service provides service to the end user that is indistinguishable from a real point-to-point, fixed-bandwith circuit. The PacketStar™ Access Concentrators support structured circuit emulation (individual DS0 circuit emulation) of traditional voice-based and data services on the DS1 module. Because voice services are essentially constant bit rate (CBR) data, ATM Forum ATM Adaptation Layer 1 (AAL-1) standards are used in circuit emulation. The circuit emulation service also provides signaling bit transport based on ATM Forum standards for channel-associated signaling (CAS).

The PacketStar™ Access Concentrators provide AAL-1 circuit emulation at the DS0 level. The individual DS0 modes of structured circuit emulation allows service providers to switch time-division multiplexing (TDM) traffic across the ATM network at individual subscriber levels; that is, each DS0 can be assigned a separate virtual path identifier (VPI) or virtual channel identifier (VCI). This service transports ABCD signaling bits based on the ATM Forum standard for G.704 CAS. M13 multiplexing capabilities are also supported, providing the ability to perform circuit emulation on a T-1 or E-1 link connected to a TDM network and convert it into ATM cells, in accordance with the ATM Forum CAS specification af-saa-0032.000. Each T-1 or E-1 carries all of the Extended Super Frame (ESF) information required for a full T-1 or E-1 in cases where the interfaces to the service access multiplexer (SAM) are a full T-1 or E-1. The Access Concentrators can convert superframe (SF) format to ESF format. Signaling from any input interface (including customer premisis equipment [CPE] interfaces) is converted to the appropriate signaling on the output interface. Framing information is converted and assignments are made on an individual DS0 basis.

Voice frames are converted into ATM cells based on the ATM Forum Circuit Emulation Service Interoperability Specification Version 2.0, af-vtm-0078.00. The DS0 mode of structured circuit emulation transparently supports voice applications in a network environment.

Users can now use DSP2C Voice Server processing options (including voice compression, silence detection, echo cancellation, tone detection, and PCM coding translation) for voice traffic on soft permanent virtual circuit (SPVC) connections between two or more *PacketStar*™ access concentrators. This completes Phase 1 of the planned augmentation of the DSP2C Server module introduced in Release 6.2.0.

Circuit emulation to ATM connections made through the Multi-Serial module now support 56 Kbps to 64 Kbps bit stuffing for SS7 link transport applications. Bit stuffing is selectable on a port basis by using the CPU software.

Dynamic Bandwidth Circuit Emulation Service

The dynamic bandwidth circuit emulation service (DBCES) feature is used with voice PVC connections to best utilize the available network bandwidth. This feature allows channels to be allocated dynamically as needed, based on ABCD signaling-bit information. The firmware supports 1x56 kbps time-slot trunking with channel-associated signaling (CAS) detection used, based on ATM Forum Specification af-vtoa-0085.000. Note that this feature is not fully compliant with the specification and does not interoperate with other devices that are fully compliant.

The DBCES feature, in essence, performs idle channel suppression for voice traffic. PBX voice traffic uses DBCES to save some of the available T-1 WAN bandwidth for LAN traffic. On average, only 8 DS0s are used for voice traffic, but at peak times, the number of DS0s used might approach the full 24 T-1 channels. When channels are not being used for voice traffic, the available bandwidth can be used for LAN UBR-class traffic.

DS1 Service

With the channelized DS1 interface, service providers can concentrate and adapt voice, video, and data traffic to an ATM network. The DS1 interface can adapt any number of DS0 channels on the service access interface to ATM virtual channels with individual virtual path identifiers (VPIs) and virtual channel identifiers (VCIs). Users can thus adapt traffic to ATM at the individual DS0 level; that is, using structured circuit emulation, frame relay, HDLC, and native ATM services. The PSAX 20 system also offers unstructured circuit emulation on the service interface of the DS1 interface.

With Release 6.3, the Channelized DS3 module supports activating and deactivating DS1 access network interface (ANI) in-line loopback codes embedded in the DS1 signal. These codes test transmissions between customer interface equipment and network interface equipment, such as between central office (CO) PSAX products and customer premises equipment (CPE) PSAX products at the edge of the ATM network. The system also generates alarm indication signals on all affected DS1 connections whenever a loop is activated.

DS3 Service

With the PSAX 20 system, service providers can also now concentrate the various ATM circuits onto an upstream interface to an ATM edge switch, typically at the DS3 rate. With the DS3 interface, service providers can concentrate various traffic types up to 45 Mbps. The ATM DS3, designed to meet the ATM Forum UNI 3.0 specifications, serves as an interface to the service provider's ATM edge switch. Each DS3 module supports two 45-Mbps DS3 ports.

HDLC Pass-through

The high-level data link control (HDLC) pass-through interface is a bit-oriented, ITU-TSS (Telecommunications Standard Section) link layer protocol standard for point-to-point and point-to-multipoint communication. In HDLC, control information is always placed in the same position. Specific bit patterns used for control are different from those used in representing data, so errors are unlikely to occur. The following Access Concentrator I/O modules support the HDLC Pass-through interface:

- Channelized DS3
- Channelized STS-1e
- Enhanced DS1 module
- Enhanced E1 module
- Multi-Serial module

High-level data link control (HDLC) uses an ITU-TSS link layer protocol standard for point-to-point and multipoint communication. Control information is always placed in the same position, using specified bit patterns dramatically different from data, reducing the likelihood of confusion. Providers are using this option primarily in wireless TDMA applications with ATM, finding that it is possible to save money by using ATM for backhauling information between central office equipment and edge devices instead of using time division multiplexing (TDM).

However, the process uses the new 5ESS switches that support a mixture of inverted and standard HDLC pass-through interfaces. The new HDLC Pass-through Bit Inversion option uses a software or firmware driver to reverse the polarity of every bit, and communications ensues, but only over ATM and only over this line.

Inversion will work for HDLC pass-through links at both 56 kbps and 64 kbps. Currently, bit inversion is available only with the Enhanced DS1 and STS-1e modules. It remains a configurable option or a special firmware load rather than a default.

The Interim Interswitch Signaling Protocol (IISP) Interface

Interim Interswitch Signaling Protocol, or IISP, was formerly known as PNNI Phase 0. Building on ATM UNI 3.0/3.1, it uses static routing tables established by the network administrator to route connections around link failures. IISP is meant to be used pending completion of the PNNI Phase 1.

Private Network-Network (PNNI) 1.0 Interface

The private network-network interface, known as PNNI, is a link-state routing information protocol that enables extremely scalable, full function, dynamic multivendor ATM switches to be integrated in the same network. It computes paths through a network by defining a method for distributing

topology information between switches and clusters of switches. This information is used to compute paths through the network, whether it is local or worldwide. The hierarchy mechanism of PNNI ensures that this protocol scales well for any size ATM network, and automatically configures itself in networks in which the address structure reflects the topology.

PNNI topology and routing is based on the link-state routing technique.

Another feature of PNNI is that it provides a method for signaling used to establish point-to-point and point-to-multipoint connections across ATM networks. PNNI is based on the ATM Forum UNI signaling, with mechanisms added to support source routing, crankback and alternate routing of all call setup requests in case of connection setup failure.

The path selections for specific calls are based on route options provided by PNNI messages. Load sharing between parallel paths is addressed by the route determination algorithm, which provides options for such factors as load sharing, cost, and override options.

PNNI Features Supported By the PSAX Systems

The following is a list of PNNI features supported for the PSAX systems:

- Alternate routing as a result of crankback

  Blocked calls will be "cranked back" with an indication of the cause. Alternate routes will be consistent with the higher-level designated transit lists in the original call request, and will avoid the blocked part of the network.
- CBR, rt-VBR, nrt-VBR, and UBR service
- Hello protocol
- Peer group leader election algorithm
- Point-to-point SVC and SPVC connections
- Point-to-multipoint SVC and SPVC connections
- Transfer of incoming extended Quality of Service (QoS)
- End-to-end transit delay parameters to outgoing PNNI interfaces
- Single peer group hierarchy
- Topology database synchronization
- PNNI topology state element (PTSE) aging within topology databases
- Summation and advertising of reachable addresses
- Source path selection and generic connection admission control (GCAC)

Peer Group Dynamics

PNNI simplifies the configuration of large networks because it allows ATM switches to automatically learn about their neighbors and to distribute call routing information dynamically.

PNNI allows switches to be arranged in a hierarchy, where each level represents one or more switches. A cluster of switches at the same level is called a peer group. Link-state topology updates circulate within a peer group.

PNNI allows hierarchies but does not require them. It is also possible to deploy PNNI with one peer group encompassing all switches within a network.

PNNI switches in the same peer group discover one another by sending hello packets across interswitch network-to-network interface (NNI) links. After a switch confirms that its neighbor at the other end of a link is a member of the same peer group, both exchange PNNI topology state packets (PTSPs) to advise and update their call routing information. PTSPs carry one or more PTSEs, describing the resources of the originating switch and the outbound resources of each of that switch's attached links.

PTSEs describe attributes, such as:

- Traffic types each link can support (any of the various ATM QoS levels)
- Maximum cell rate the link can sustain; cell delay variation (only for constant bit rate (CBR) and variable bit rate real-time circuits (VBRrt)
- Cell-loss ratio or cell-loss margin (CLM), a measure of the difference between effective bandwidth allocation and sustainable cell rate;
- Administrative weight (AW), a parameter that allows network architects to indicate relative link preference when deciding between alternative routes

Switches make use of this resource information to assess which of the available paths will best ensure QoS parameters are met.

Topology Information

After the initial exchange of topology information among switches in a peer group, regular broadcast topology updates are unnecessary. Each PTSE has a finite lifetime. Since individual elements age differently, their refresh updates occur at different times. This reduces the overhead associated with keeping the topology of the group updated. The only time a PTSE is rebroadcast is when there is a significant change in any of the key topology elements. For example, any change in cell-delay performance on a link will trigger a PTSE update from attached switches. Triggered updates further reduce network overhead.

Every switch in a peer group is aware of the topology state of the entire group. Thus it can build the entire call setup route from source to destination.

Of course, as peer groups grow and incorporate more nodes, the state information in each switch increases. PNNI supports hierarchies, which collapse the amount of state information shared by all switches.

PNNI Hierarchies

In networks that use a PNNI hierarchy, the switches at each level elect one switch as a peer group leader (PGL). This PGL concurrently belongs to its own level and to the next highest level, where it acts as a logical group node (LGN) that represents and summarizes topology information needed to reach any of the lower-level switches. The higher-level peer group can mirror this dual constituency, electing a PGL to represent it at the next highest level. This process may scale to over a hundred levels.

Each switch in a PNNI network has a unique 20-byte address that corresponds to the network service access point (NSAP) schema. Much like IP subnet addresses, NSAP identifiers have a network part and a user part.

The user part is the last seven bytes, and is reserved for end-system identification (insignificant to the PNNI). The network part is the first 13 bytes, and is used to identify peer groups.

Each level in the PNNI hierarchy also is assigned a scope number. Similar to an IP subnet mask, the scope specifies how much of the 13-byte network part is common to the switch addresses at a particular level in the hierarchy. For example, a scope of 72 (bits) masks the first 9 bytes of the network part as being common in all switches at that level. Higher levels have shorter scopes because they do not look as far into the NSAP; a level with a scope of 64 (masking the first 8 bytes) resides above a level with a scope of 72.

To make the best use of PNNI's capabilities, network architects must pay careful attention to the ATM addressing structure, allocating correct addresses to switches at each level of the hierarchy.

Load balancing allows communications trunks connecting access and edge switches to balance traffic between PNNI (dynamic source routing) and IISP (static hop-by-hop routing) links. In addition to the existing parameters of path and route selection, the PSAX devices can now consider the values of available bandwidth and available cell rate associated with the interfaces. Available bandwidth becomes the tiebreaker in calculating routes using default parameters for both IISP and PNNI routing. Load balancing between PNNI and IISP links, not available prior to this release, uses available bandwidth more efficiently while strengthening the routing function.

The ATM Terminal Emulation Interface

Terminal Emulation is an application that follows an intelligent computing device to mimic the operation of a dumb terminal for communications with a mainframe or minicomputer. This is made possible by inserting special printed circuit boards into its motherboard and/or special software. The Multi-Serial module is the only Access Concentrator module that supports this interface.

Network Management

The Access Concentrator system provides all the telecommunications management network (TMN) functions applicable to the system. The PSAX 20 system (which contains network elements) can be managed in several ways using a network element management system or network management system. The Access Concentrator system software features a Simple Network Management Protocol (SNMP)-compliant management information base (MIB) that gives external management systems access to the Access Concentrator system software.

The Access Concentrator system software supports the following options for network management:

- Serial port interface with a direct connection to a standard VT100 terminal emulator.

As the simplest option, the CPU module faceplate provides an EIA-232 serial port (RJ-11 connector labeled CONSOLE), to which a PC workstation or a console monitor, running a standard VT100 terminal emulator, is connected. The console interface provides access to the configuration, fault, network data-collection, and security-management features of the system software.The Access Concentrator system software lets users perform management tasks using a menu-based interface.

This port is typically used for local management (using a direct serial connection), but it can also be used for remote management. Remote management may be performed overa public switched telephone network (PSTN) with the use of an external modem, or over an ATM network with the use of a terminal emulation connection between Multi-Serial modules. The serial port is also used for the configuration of internet protocol (IP) parameters which are necessary for IP-based management.

- Ethernet interface connection on a local-area network (LAN).

  A 10BaseT Ethernet interface (RJ-45 connector labeled ETHERNET) on the PSAX 1250 and PSAX 2300 CPU module faceplates (and the Front Panel of the PSAX 20 and AC 60) allows the user to access the MIB, either using the *AQueView*™ application over a LAN or by telneting to the PSAX system. If a telnet session is used to manage a PSAX device, then the console interface is displayed (similar to that which is used for the serial interface, as explained above). Only one person can have access to the console interface at a time; therefore, direct access using the serial port precludes telnet access using the Ethernet port.

- In-band management by using a PVC connection over an ATM wide-area network (WAN).

  The in-band management feature on the CPU module allows a user to access and manage one or more PSAX 20 systems (managed targets) via a single PVC connection from a management workstation (management host) running an SNMP client over an ATM WAN. This allows for IP-based functions (e.g., telnet) and SNMP functions (e.g., element and network management software) to be performed remotely using ATM virtual circuits which terminate directly within the CPU of a managed node. The PVC connection is set up using an I/O module with an ATM cell bearing port (for example, the OC-3c, STM-1, DS1, DS3, E1, and E3 modules). Three basic types of configuration are possible:

  1. Direct connection from a management host over an ATM WAN to an I/O module port in a remote managed target.
  2. Routed connection from the management host over an ATM WAN to an I/O module port in a remote Access Concentrator chassis, which serves as a “router Access Concentrator,” with a connection to the managed target.

  This route connection allows you to flexibly manage any number of Access Concentrator systems.

3. Hybrid connection, which connects the main router Access Concentrator system directly to the end system Access Concentrator system through ATM PVC connections.

   These ATM PVC connections can be sent through several Access Concentrator systems to reach the end system Access Concentrator systems. The main router Access Concentrator system is connected to the NMS computer through an Ethernet LAN.

In-band Management SVCs

Release 6.2 added the option of in-band management with switched virtual circuits (SVC). Previously, a PSAX device or a network management system computer could only be set up to manage one or more access concentrator systems over an ATM wide area network with PVC connections. Using the host Access Concentrator system, you could find the IP addresses of remote PSAX systems and, with those addresses, create the SVC connections. This provides fault-tolerant in-band management, taking advantage of SVC's call setup and automatic rerouting functions.

Phase 2, available through Release 6.3, gives the complete PSAX product line ATM ARP Server functions. The OC-3c module is the module most often used to create switched virtual circuits.

The Access Concentrator system software features a standard SNMP agent that allows any standard SNMP network management system, including those based on systems such as HP OpenView and SunNet Manager, to perform all management functions.

In conjunction with the visual indicators displayed on the front panels of the individual modules, the system offers a full complement of SNMP trap messages that alert the user to faults in the PSAX 20 system. Usage-based messages collected on the CPU module allow a service provider to collect cell counts for traffic and performance monitoring, and for fault detection.

The SNMP MIB provides an extensive series of configuration management and provisioning features that allow the user to prepare the various components for supporting services.

AQueView™ Element Management System

The *AQueView*™ element management system (EMS) software is a graphic user interface (GUI)-based element management tool that is used to provision the *PacketStar*™ PSAX Access Concentrator systems; it enables a network of PSAX products to be managed and provisioned with easy-to-use windows from a single location. The *AQueView*™ EMS also provides centralized configuration, fault, performance, accounting, and security management of PSAX systems.

The *AQueView*™ element management system (EMS) software Release 4.4, supports the same software features supported in the PSAX system software Release 6.3. The new EMS release simplifies the use of both the *AQueView*™ system and managed PSAX devices. It offers significant new aids in troubleshooting problems encountered with the *AQueView*™ management system. It continues to be offered in two versions, the Client/Server application, for use within the HP OpenView Network Node Manager framework on Sun Solaris platforms, and Standalone, designed for use with either Windows NT or Solaris platforms. The *AQueView*™ R4.4 system

software supports Releases 6.1.0 through 6.3.0 software for the PSAX 2300, PSAX 1250, PSAX 20, AC 60 and AC 30, and Release 6.0 software for all models but the PSAX 2300 system. (The PSAX 2300 system was first introduced with PSAX Release 6.1.0 system software.)

Note: The AC 30 system is only supported for PSAX system software releases prior to Release 6.3.0.

PSAX 20 Software Features

The Access Concentrator system software uses permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) to provide end-to-end connectivity for transmission in a network. Because virtual connections are logical and not physical, multiple connections can be defined simultaneously across a single network facility, with each connection having flexible bandwidth.

Because PVCs establish end-to-end connectivity, a PVC eliminates the need for establishing a new route (call setup) each time a transmission is sent to a remote location. When establishing a connection with a PVC, the user simply selects a class of service for each connection.

The Access Concentrator system also features cell-counting capabilities that allow network data collection systems to generate usage-based billing reports. The *AQueMan*™ algorithm maximizes bandwidth efficiency while ensuring QoS on a congested network; and LANET, a physical layer protocol, efficiently adapts ATM to high-noise wireless and satellite environments.

Alternate Rerouting Using Dual-Homed PVCs

Overview

To protect ATM traffic from network outages, the Access Concentrator system can detect alarms or failures on an ATM backbone and reroute PVC traffic around the affected portions of the network. The system performs the rerouting function independently, without relying on operator intervention or rerouting capabilities within the network itself. This implementation allows for dual-homed PVCs (DHPVCs) to be established for ATM-to-ATM connections, circuit emulation-to-ATM connections, frame relay-to-ATM connections, bridge-to-ATM connections, and terminal emulation-to-ATM connections. DHPVCs for virtual paths can only be implemented on ATM-to-ATM connections. Alternate rerouting is a standard feature of the system software. The system sets up DHPVCs according to an industry-standard technique.

It is not necessary to designate an interface to perform solely as the "standby" for DHPVCs. Rather, ATM trunk interfaces can be used in a load-sharing design with the connection admission control (CAC) constraints automatically considered as the DHPVC is established. This allows particular links to be used as the primary link for certain DHPVCs, while they are used simultaneously as the standby for other DHPVCs.

Operation

As the DHPVC is established, both the primary and standby circuits are provisioned from the originating node to the terminating node, through the ATM network. When provisioning the primary circuit, the user enters the network parameters that are appropriate for the type of connection being established (e.g., ingress slot, ingress port, egress slot, egress port, QoS, AAL type, peak cell rate, VPI, VCI, and so on). When provisioning the standby circuit, the user is only required to enter the network parameters that are associated with the standby link (e.g., egress slot, egress port, VPI, VCI). The remaining parameters are taken from the primary circuit. Because DHPVCs make use of simple PVCs within the network, interoperability issues do not exist with intervening switches.

During normal operation, the primary PVC carries all the data associated with the DHPVC. During this time, user data is not transmitted over the standby PVC. The DHPVC implementation makes use of ATM Forum OAM F5 flows to automatically initiate rerouting.

When connections are provisioned, active and backup PVC routes are defined. If a link failure is detected on the primary PVC (on either the transmit path or the receive path), the associated network element that detects the failure generates an OAM F5 alarm indication signal (AIS) to the downstream node, which in turn sends the AIS to the destination edge node. At that point the edge node converts the AIS to remote defect indication (RDI) messages, which are transmitted to the originating node. Intermediary nodes relay the RDI messages upstream, ultimately to the originating or terminating nodes. Affected nodes that implement DHPVCs automatically switch over to standby PVCs upon detecting an RDI or AIS. In addition, this switchover will occur upon detecting a hardware failure associated with the ports used for the circuit. In such instances, the CPU will recognize the failure and initiate the DHPVC reroute.

Application

A pair of PSAX 20 systems, acting as the originating node and terminating node, cooperatively accomplish the network-wide rerouting regardless of the number of connections affected by the network outage. The systems can switch the PVCs to the backup link within 1 second, avoiding service interruptions under reasonably likely conditions of network congestion. Figure 3-2 illustrates how the alternate rerouting is accomplished.

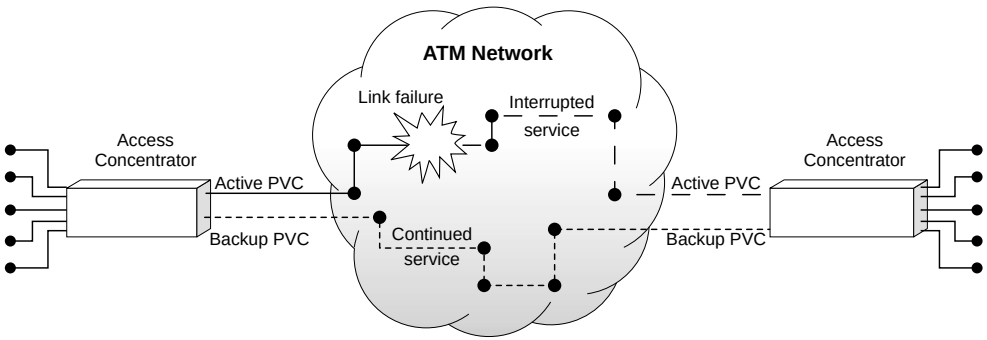

Figure 3-2. Automatic Rerouting With Dual-Homed PVCs

If zero errors are detected by the PSAX 20 system for a user-selectable interval of 10 seconds, 30 seconds, 1 minute, or 5 minutes (or not allowed), the system restores the primary link.

AQueMan™ Algorithm

With ATM, predictable QoS is achieved for all applications by the transmission of voice, video, and data using short, fixed-length cells interleaved at guaranteed bit rates. The guaranteed bit rates are implemented by assigning ATM Forum-established QoS classes for each type of data to be transferred. The following attributes are considered in assigning an ATM service class:

- Cell transfer delay characteristics
- Cell loss ratio
- Type of connection required
- Timing or synchronization of the source and destination

AQueMan™ manages traffic while supporting ATM Forum classes of service. This adaptive algorithm allocates bandwidth by statistically multiplexing traffic within two sets of queues according to weighted priorities. One set of queues addresses avoidance of cell loss, which is normally a concern for data traffic, while the other manages cell transfer delay, which is critical to voice and some video traffic. Within each set of queues, *AQueMan*™ assigns internal priorities even more specialized than the ATM Forum class definitions. Generally, the lower the assigned priority number, the greater the access to bandwidth and the less likelihood of loss.

Table 3-1 details the Access Concentrator system support of defined ATM quality of service (QoS) classes.

Table 3-1. Access Concentrator System-Supported Service Classes

ATM Service Class	Description
Constant Bit Rate (CBR)	Service that operates on a connection basis and offers consistent delay predictability; used for applications such as circuit emulation, voice, and video.
Variable Bit Rate—Real Time (VBR-RT)	Service that operates on a connection basis and offers very low delay variance but requires access to a variable amount of network bandwidth; used for such applications as packet video and voice.
Variable Bit Rate—Nonreal Time (VBR-NRT)	Service that operates on both a connection and connectionless basis and allows delay variance between the delivery of cells; used for data applications that have potentially bursty traffic characteristics, including LAN interconnect, CAD/CAM, and multimedia. This class can be used to support SMDS (switched multimegabit data service).
Unspecified Bit Rate (UBR)	Service that operates on a connection basis and allows for raw cell or best-effort transport by the network. In this service, cells are transported by the network whenever bandwidth is available and traffic is presented by the user. Data using UBR service is more apt to be discarded during peak traffic times in deference to data using other classes of service.

Table 3-2 illustrates the attributes of the classes of service supported by the Access Concentrator system software.

Table 3-2. Class of Service Descriptions

	Constant Bit Rate (CBR)	Real Time (VBR-RT)	Nonreal Time (VBR-NRT)	Unspecified Bit Rate (UBR)
QoS Class	Class 1	Class 2	Classes 3, 4	Class 5
Applications	Voice and video	Packet video and voice	Data	
Bit Rate	Constant	Variable		
Timing Required Source/ Destination	Required		Not required	

Table 3-2. Class of Service Descriptions

	Constant Bit Rate (CBR)	Real Time (VBR-RT)	Nonreal Time (VBR-NRT)	Unspecified Bit Rate (UBR)
Service Examples	Private line	Com-pressed voice	Frame relay, Switched multimedia data service	Raw cell, Ethernet
AAL	1	2	3/4 and 5	3/4 and 5

The following two tables illustrate how ATM classes of service map to internal priority levels to structure the *AQueMan*™ algorithm. Table 3-3 identifies the cell-loss and cell-delay tolerance of each service class. Table 3-4 on page 3-17 lists the class-of-service choices available when configuring PVC connections on an Access Concentrator system and shows service level examples for each PVC connection type.

The examples are intended simply as illustrations and will need fine tuning based on the network applications supported by the Access Concentrator system. The flexibility of the Access Concentrator systems allows the user to tailor the system based on the required service applications and the selection of the appropriate priority levels.

Table 3-3. Cell-Loss and Cell-Delay Characteristics of ATM Service Classes

ATM Classes of Service	QoS Class Sup-ported by AC Systems	Cell Loss Tolerance	Cell Delay Tolerance	Internal Priority
Constant Bit Rate (CBR)	Class 1	High	Very Low	CBR-1
	Class 1	High	Very Low	CBR-2
	Class 1	High	Low	CBR-3
	Class 1	High	Low	CBR-4
Variable Bit Rate (VBR)	Class 2	Very Low	Very Low	VBR-1
	Class 2	Low	Low	VBR-2
Variable Bit Rate, Real Time (VBR-RT)	Class 2	Low	Low	VBR-3
Variable Bit Rate, Nonreal Time (VBR-NRT)	Classes 3, 4	Low	Medium	VBR-4
	Classes 3, 4	Low	High	VBR-5
Unspecified Bit Rate (UBR)	Class 5	Very High	Very High	VBR-6

Table 3-4. Mapping ATM Service Classes to Access Concentrator Systems Priority Levels

ATM Classes of Service	Internal Priority	PVC Connection Configuration Selections	Service Examples
Constant Bit Rate (CBR)	CBR-1	CBR1	911 calls
	CBR-2	CBR2	Preferred customers
	CBR-3	CBR3	Standard
	CBR-4	CBR4	Cellular
Variable Bit Rate (VBR)	VBR-1	VBR-express	Network management
Variable Bit Rate Real Time (VBR-RT)	VBR-2	VBR-RT1	Real-time videos
	VBR-3	VBR-RT2	MPEG1-2/JPEG
Variable Bit Rate Nonreal Time (VBR-NRT)	VBR-4	VBR-NRT1	FR data
	VBR-5	VBR-NRT2	FTP/e-mail transfer
Unspecified Bit Rate (UBR)	VBR-6	UBR	IP data

AQueMan™ classifies traffic based on service-level priorities and limits congestion by addressing three dimensions of traffic management:

- Cell loss versus cell delay for cell discard

  As Table 3-5 indicates, there are VBR traffic types (for example, network management data traffic) that are, in fact, higher in priority than some CBR traffic (for example, off-peak cellular voice calls). The *AQueMan*™ algorithm accounts for the service-level priorities of the traffic when determining which cells to discard during traffic congestion. Thus, CBR does not necessarily imply a higher priority.

  Table 3-5. CBR and VBR Service-level Priorities

Priority	CBR	VBR
High	911 voice call	Network management data
Low	Off-peak cellular voice	IP data

- Weighted priorities using queue depth ratios

  To alleviate congestion in the network caused by lower-priority VBR traffic, *AQueMan*™ provides a weighted priority mechanism. This mechanism allows lower-priority VBR data to be sent ahead of higher-priority VBR data in cases where there are too many cells in lower-priority VBR buffers and relatively few cells in higher-priority VBR

buffers. The execution of this algorithm is based on the priority levels the user selects.

- Cell aging

This capability prevents the lowest-priority data (for example, IP data) from being buffered in the Access Concentrator systems indefinitely. *AQueMan*™ keeps track of how long each cell stays in the buffer. The lower the priority of the traffic, the longer its cell-aging time; that is, UBR traffic has a longer cell-aging period than VBR-RT traffic. This capability allows the Access Concentrator systems to periodically send low-priority cells through the network. Doing so prevents retransmission of IP data traffic while increasing the time-out window for the TCP/IP sessions. The cell-aging mechanism allows for orderly decongestion of the network without resorting to traffic rerouting and other complicated protocols and procedures.

Connection Gateway API

The Connection Gateway Application Programming Interface (API) provides an interface to the PSAX 20 by which an external workstation (gateway) can control PSAX 20 ATM switching using nonnative ATM networking protocols. The Connection Gateway Application Programming Interface (API) was initially used only in custom releases, to work with *PacketStar*™ central office products, such as the PSAX 1250 and the PSAX 2300. Software Release 5.1 fully integrated the Connection Gateway API with the *PacketStar*™ line. Using this interface, an external workstation can control ATM switching in a PSAX 1250 or PSAX 2300 using non-native ATM networking protocols. The connection gateway allows powerful interworking of ATM, ISDN, SS7, CAS, and other protocols.

In Release 6.3.0, these capabilities have been improved to support such new features as Type 102, Type 105, and Type 108 milliwatt termination tests on the Tones and Announcements Server module, CAS signaling, and extending existing Connection Gateway API functionality to new PSAX hardware and software components such as the Medium-Density DS1 and DSP2C Voice Server modules.

See the *PacketStar*™ *Connection Gateway Application Programming Interface Developer's Guide* for detailed information about implementing a connection gateway API.

Console Help

As new features have been added to enhance the *PacketStar*™ line of Access Concentrators, the console help files have been updated. They now offer meaningful, helpful advice to users who need assistance in implementing both the new and existing features. Advice offered for many other fields has been totally rewritten, often in response to advice from customers. Where possible, our guidelines point to the information base in the appropriate *PacketStar*™ *Installation and Operation Guide, User Guide, and Module User Guide*.

Ethernet LAN Bridging

The Ethernet LAN bridging feature is provided on the Ethernet module. The various functions and interfaces associated with Ethernet LANs are governed by standards published by the Institute of Electrical and Electronics Engineers (IEEE). The relationships of the various IEEE standards that affect LAN bridging are shown in Figure 3-3.

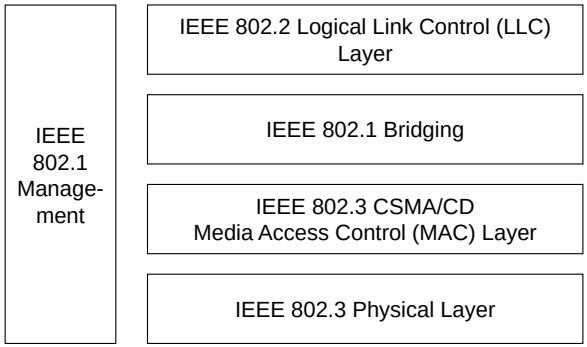

Figure 3-3. IEEE Protocols for Ethernet LANs (IEEE 802.1)

Bridging is accomplished by relaying data from the MAC layer of one LAN to the MAC layer of another LAN (see Figure 3-4).

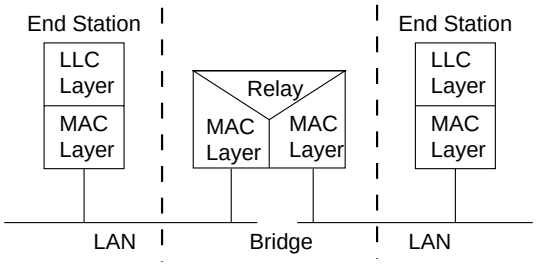

Figure 3-4. Ethernet Bridging via the MAC Layer (IEEE 802.1)

Ethernet bridging over the ATM network is accomplished using ATM Forum standards; that is, document RFC 1483, which specifies multiprotocol encapsulation within ATM. Ethernet MAC data is encapsulated using ATM Adaptation Layer 5 (AAL-5) and transported over the ATM network (see Figure 3-5).

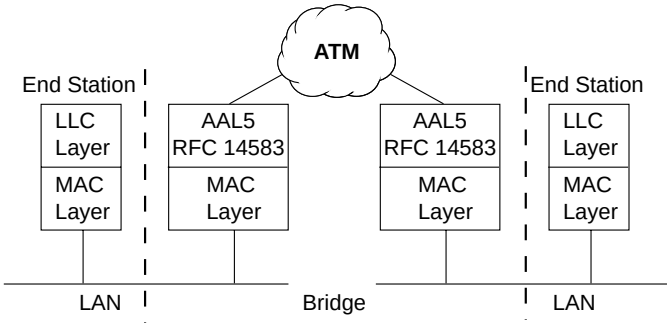

Figure 3-5. Ethernet Bridging over an ATM Network (RFC 1483, AAL-5)

The Ethernet LAN bridging feature incorporates the following functions:

- Bridging

  Ethernet MAC layer data is encapsulated by using standards in the ATM Forum document RFC 1483.

- Filtering

  Certain Ethernet frames are filtered out and not relayed, according to a filtering database. This frame filtering prevents frames from being transmitted unnecessarily across the ATM network. The Spanning Tree Algorithm and Protocol is the mechanism used to populate the filter database dynamically.

- Bridge management

  This function enables end users to manage configuration and performance, and collect cell records and billing information. Standard Ethernet MIBs, as defined in ATM Forum document RFC 1643, support SNMP management.

- Performance

  The Ethernet module provides simultaneous operation on all ports.

Firmware Release Control

Note: The Firmware Version Control window as described in the procedure in the "Upgrading and Backing Up System Software and Firmware" chapter should be used only on the advice of Lucent Technologies NetworkCare (see the "Technical Support" section in Chapter 1, "Getting Started.").

The Access Concentrator CPU has access to the firmware binaries of all modules present in the access concentrator mainframe. The firmware is downloaded into the RAM, into the secondary FLASH of each module, through a dedicated communication channel.

The firmware download is performed under the control of two Interworking Functions (IWFs) resident in the Access Concentrator CPU, and in the I/O or server module, respectively. Once the binaries are downloaded, the modules execute the downloaded code that controls the module.

A user does not need to take the initiative to download an I/O or server module's firmware separately from the Access Concentrator CPU software upgrade. When the Access Concentrator software is upgraded using the SRD Download Configuration window (see Chapter 7, "Upgrading and Backing Up the AC System Software"), the system reboots and all firmware of the I/O and server modules (in the rebooted chassis) is also upgraded.

You can use the following procedure to revert to an older firmware release if a module is not working properly with its current firmware.

Access Concentrator I/O modules released with Access Concentrator 6.0.0 software release are supported by the Firmware Release Control feature. The I/O modules that were released before the Access Concentrator 6.0.0 software release will work in the Access Concentrator chassis, but are not supported by the Firmware Release Control feature.

Forward Error Correction

The forward error correction (FEC) feature is a combination of functions designed to protect data transmission in a noisy communications environment, such as traffic transmitted across satellite and line-of-sight radio-frequency circuits. Most of these types of circuits transmit at the rate of 2.048 Mbps or slower. The three stages of FEC are multiple redundancy addressing, cell encoding, and cell scrambling. Since these FEC functions are applied in conjunction with LANET, which helps maintain cell-delineation capability up to random 10^{-2} bit error rate (BER) with 0.625 percent bandwidth overhead, maximum protection is obtained.

Multiple redundancy addressing sets up multiple virtual circuits to the same destination. The addresses for the circuits are within the error space of the principal one used for actual transmission. Thus, the most probable error patterns occurring in the address field cause the address to be changed to another valid one. To tolerate 2-bit random errors or 5-bit burst errors, 526 addresses are required for each channel. This is not a serious constraint because high-noise, low-speed links are normally used by only a small number of users. The more constraining situation, however, is that the signaling channel VPI value 0 and VCI value 5 is within 2 bit-errors of the null cell address (0,0). Thus, in high-error conditions, signaling is inhibited. The PTI and GFC fields need to be separately protected with the payload. The user needs only to set up a single connection using a VPI value 0 and a VCI value in the range from 32 to 92. This provides for 60 simultaneous, noise-tolerant base connections. Each connection (ATM-to-ATM, VCC, PVC) is created between an ATM-enabled port on a Multi-Serial module and another ATM port (such as the OC-3c and the STM-1 modules). Internally within the Access Concentrator chassis, the connection is routed through the CPU module for the cell-encoding stage.

Cell encoding is executed by the CPU module on cell payload data destined for noisy interfaces. Based on a user-selected encoding rate for the connection, source-data cell payloads are divided into six blocks and fed into a Reed Solomon encoder. The encoded data, now approximately 48 bytes larger, is loaded into new cell payloads and forwarded to the Multi-Serial module for the cell-scrambling stage. The user selects a Reed Solomon encoding rate with a specific error-correction capability, as follows:

- 1/2 rate

  For each data cell, the encoder loads one redundant cell. This rate provides correction of payload cells with 10^{-3} BER to 10^{-6} BER.

- 1/4 rate

  For each set of three data cells, the encoder loads one redundant cell. This rate provides correction of payload cells with 10^{-4} BER to 0 BER.

- 1/8 rate

  For each set of seven data cells, the encoder loads one redundant cell. This rate provides correction of payload cells with 10^{-5} BER to 0 BER.

- Dynamically changing rate options (see Table 3-6):

Table 3-6. Rate Option

Cell Encoding Rate / Bit Error Rate	10^{-3} Threshold	10^{-4} Threshold	10^{-5} Threshold
Automatic—low quality	1/2 rate	1/4 rate	1/8 rate
Automatic	1/2 rate	1/2 rate	1/8 rate
Automatic—high quality	1/2 rate	1/2 rate	1/4 rate

When the user selects the 1/2, the 1/4, or the 1/8 rate, the encoder maintains that selected rate of encoding regardless of actual error conditions. When the user selects one of the dynamically changing rate options, the encoder employs the 1/2, 1/4, or 1/8 rate, dynamically adjusting the rate as needed, depending on the number of errors encountered on the decoding side of the circuit.

Cell scrambling is a function performed on the Multi-Serial module. This function moves the first three bytes of the cell header (GFC, VPI, and VCI fields) into the payload and spreads them out to protect against burst errors. This action increases the burst error tolerance of the header from 5 bits to 54 bits with no cell loss.

Frame Relay-to-ATM Interworking

Any port on the Channelized DS3, Channelized STS-1e, Enhanced E1, DS3 Frame Relay, and Multi-Serial modules, and the Enhanced DS1 component can be used to connect to a frame relay device. Frame relay-to-

ATM interworking is performed at the network level Frame Relay Forum FRF.5 and at the service level FRF.8. This allows the *PacketStar*™ Access Concentrator to adapt and concentrate traffic from one frame relay network, and transmit it to other frame relay or ATM networks. In this way, the Access Concentrator acts as a gateway between routers, remote dial access servers, IBM SNA equipment, and other devices configured for frame relay operation.

FRF.5 Encapsulating Frames

With FRF.5 network level interworking, frames are encapsulated within ATM cells at the network ingress point and "tunneled" through the ATM network. At the network egress point, the ATM cell headers are removed and the frames are reassembled for delivery to a frame relay device.

FRF.8 Converting Frames

With FRF.8 service level interworking, frames are converted into one or more ATM cells at the network ingress point. At the network egress point, the ATM cells are delivered to an ATM device. This conversion is compliant with both the FRF.8 implementation agreement and the IETF multiprotocol encapsulation specifications (RFC1490, RFC1483). FRF.8 interworking is performed at the end of the ATM network that connects to the frame relay device.

Note: FRF.5 and FRF.8 are not interoperable and cannot be used at both sides of a network. You may wish to use an FRF.8 approach for applications involving interconnectivity between two frame relay devices because the capabilities of FRF.8 include those which are available with FRF.5.

Frame Relay-to-Frame-Relay Interworking

In addition to frame relay-to-ATM interworking, it is possible to configure an Access Concentrator for strictly frame relay operation. A frame relay-to-frame-relay connection can be made between two ports of an Access Concentrator if both ports have frame relay capacity. In this case, frame relay data received by one of the ports is converted to ATM cells for transmission across the backplane of the Access Concentrator, and then converted back into frame relay for transmission out of another port.

Integrated Link Management Interface (ILMI)

The integrated link management interface (ILMI) is network management function that supports bidirectional exchange of ATM interface parameters between two connected ATM Interface Management Entities (IMEs).

ILMI provides status information and statistics using Simple Network Management Protocol (SNMP) and a MIB to provide any ATM device with status and configuration information concerning the virtual path connections (VPCs), virtual channel connections (VCCs), registered ATM network prefixes, registered ATM addresses, and registered services and capabilities available at its ATM interfaces. It also determines the operational status of the logical port. ILMI is supported for all ATM UNI 3.0 and ATM UNI 3.1 interfaces.

Inverse Multiplexing over ATM (IMA)

Inverse multiplexing over ATM (IMA) creates virtual access pipes that are faster than E-1, but not nearly as expensive as a T-3/E-3 line. This allows for ATM capabilities without the costs associated with broadband access. The DS1 IMA and E1 IMA I/O modules support the ATM IMA interface.

LANET Protocol

The LANET (Limitless ATM Network) protocol, coupled with a simple error-tolerant addressing scheme, addresses the fundamental problem of noise in adapting ATM to low-speed environments. LANET permits application-dependent payload protection, allowing selective implementation of bandwidth-costly, forward-error-correction techniques. It is designed to identify and extract ATM cells at bit error rates as high as 10^{-2}. A simple, robust addressing scheme facilitates reliable delivery of ATM cells in a noisy environment. By maintaining the cell extraction capabilities and strengthening the cell-header error protection, LANET brings the advantages of the ATM protocol to noisy, low-speed links.

The main features of LANET include the following:

- Regular framing-bit patterns that enhance cell delineation in high-noise environments
- Compatibility with traditional link enhancement schemes such as forward error correction (FEC) and bit interleaving
- Consistent interface to the higher layer of the protocol stack (that is, the ATM layer)
- Transmission rate and media independence
- Natural synchronization with a standard 8-kHz telecommunication clock

The LANET solution permits both application-dependent payload protection and link-quality-dependent header protection, while maintaining maximum compatibility with ATM standards. Figure 3-6 shows the relationship between LANET and the Open Systems Interconnection (OSI) model.

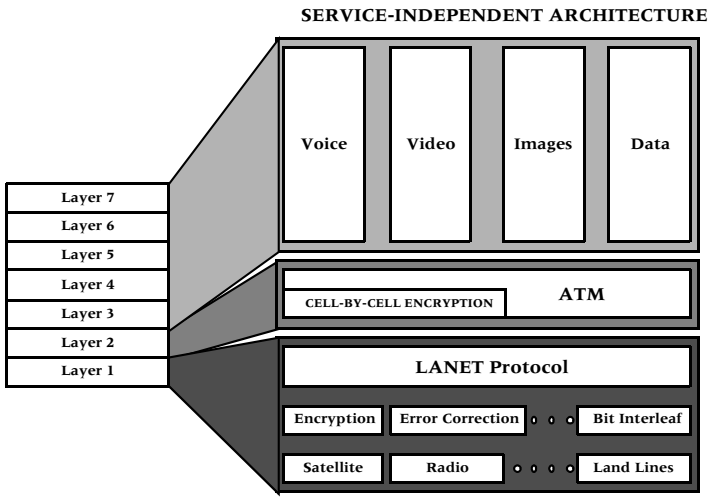

Figure 3-6. The Relationship Between LANET and the OSI Model

The LANET protocol is designed to be active in the upper end of the physical layer of the OSI seven-layer model. Within a byte-oriented serial data stream, LANET provides a framing structure around ATM cells for transmission purposes and thus regular frame-marker bit patterns for cell extraction. Each LANET frame (2400 bytes) is subdivided into 45 ATM cells (totaling 2385 bytes) with a 15-byte overhead. This structure permits a transmission rate scalable according to the physical medium. The 15-byte overhead, accounting for 0.63 percent of the bandwidth, includes the LANET frame and subframe headers, which are used in conjunction with traditional cell-header error-detection methods, such as header error correction (HEC), to enhance cell delineation for noisy environments. The protocol thus becomes independent of the transmission rate while still naturally synchronizing with an 8-kHz transmission clock via the 2400 bytes-per-frame structure.

Traditionally, block-error correction schemes, such as Reed Solomon (RS) coding, have been used to protect the header. As a simple alternative, the Access Concentrator system software uses an error-tolerant addressing scheme (multiple redundancy addressing) that establishes multiple virtual circuits to the same destination, thus requiring no special hardware and no modification to the current standard. The addresses for the circuits are within the error space of the principal address used for actual transmission. Thus, the most probable error patterns occurring in the address field will simply change the address to another valid one. This approach maintains independence from the application layer because it encodes the header

address within the same 10-nibble header space of standard ATM cells. In addition, it avoids the extra delay (detrimental to CBR traffic) required of multiple header-encoding schemes. In practice, to tolerate 2-bit random errors or 5-bit burst errors will require setting up 526 addresses per each channel. This is not a serious constraint because high-noise and low-speed links will likely be used to support only a small number of users.

Finally, given the ability to deliver cells, the payload can now be FEC-protected on a per-virtual-circuit basis depending on the error tolerance of the application at the service-specific convergence sublayer (SSCS). Figure 3-7 shows the LANET frame structure.

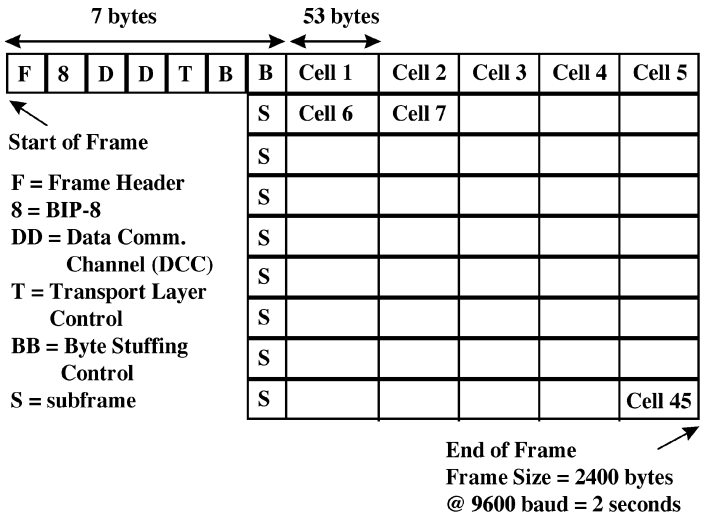

Figure 3-7. LANET Frame Structure

The LANET subframe functions in the following ways:

- The timely arrival of the header patterns is used as a confidence check, confirming that the system is properly synchronized.
- In the event of synchronization loss, a state machine can easily seek and resynchronize to the regular appearance of the simple header patterns.

Operations, Administration, and Maintenance (OAM)

Overview

The Operations, Administration, and Maintenance (OAM) feature on the PSAX 2300 and PSAX 1250 chassis detects and reports on abnormal behavior in virtual path connections (VPC) and virtual channel connections (VCC) in the ATM and physical layers associated with an ATM network. OAM affects the system software and I/O module firmware associated with generating,

receiving, and intrepreting F4/F5 OAM flows. This feature requires the user to run *AQueWin*™ and the *AQueView*™ system.

OAM Functions

The OAM functions (and their cell types) are:

- Fault management
  - ~ detection (continuity check): periodically verifiy connection integrity
  - ~ reporting (alarm indication signals [AISs]) and remote defect indications [RDIs]: periodically notify connection faults in upstream and downstream directions
  - ~ localization (loopback): isolate failed entities if defect information is insufficient
- Activation/deactivation: remote activation/deactivation of continuity check functions

OAM Cell Characteristics

OAM cells are bidirectional and follow the same physical and logical route as user payload cells. There are two variants for each flow: one that checks a particular segment, and the other, an end-to-end flow. A segment is indicated by a virtual channel identifier (VCI) of three for F4 flows, or a payload type (PT) of 4 for F5 flows. End-to-end flows are indicated by a VCI of 4 for F4 flows, or a PT of 5 for F5 flows.

OAM cells are ATM cells with the fields shown in Figure 3-8:

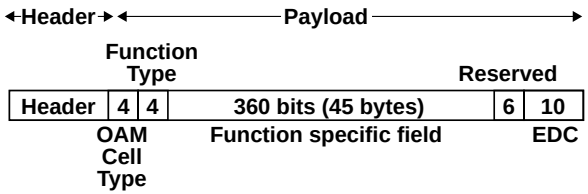

Figure 3-8. OAM Cell Fields

- Header: this is the same as the ATM cell header
- OAM Cell Type: the management type (fault, activation/deactivation)
- OAM Function Type: the specific function (AIS, RDI, continuity check, loopback, forward monitoring, backward reporting, and so on)
- Function-specific field: data required for the specific function
- Reserved: reserved for further specification
- EDC: CRC-10 error detection code computed over the cell payload (except the CRC-10 field) and used to check for data corruption

F4/F5 Flows

OAM has two flows of management information: F4 and F5. F4/F5 in-band maintenance flows are defined at the ATM layer for the VPC and VCC level, respectively. F4 is used for path level connections, where the virtual path (VP) flows are identified by reserved values within the path. F5 is used for

circuit level connections, where the circuit virtual channel (VC) flows are identified by the payload type (PT) values.

Characteristics of OAM F4 Cells

- Bidirectional
- Have the same VPI value as user cells for VPC
- Identified by one or more preassigned VCIs for both directions
- In the same physical route for fault correlation and performance information

Characteristics of OAM F5 Cells

- Bidirectional
- Have the same VPI/VCI values as the user cells for the VCC
- Adentified by one or more preassigned VCIs for both directions
- In the same physical route for fault correlation and performance information

Fault Management Functions

Alarm surveillance functions are designed to aid in physical layer detection and notification of network faults. Alarm surveillance measures are performed on a continuous basis by features within network elements and management systems. They monitor network elements for anomalies, defects, and failures.

The three major aspects of the fault management functions are:

- Detecting
- Reporting
- Localizing

Detection

Detection (continuity checks): periodically verifies connection integrity.

The activation/deactivation OAM mechanism is used to remotely start and stop the generation of cells that perpetually monitor performance and continuity. These mechanisms can indicate to the far end a connection is alive, even if no user data traffic has been recently transmitted. When a connection activates the continuity mechanism, continuity check cells are inserted by the originating end point, either at predefined time intervals (for example, a few seconds apart), or when the connection has been idle for a given time interval (for example, a second to two seconds).

Continuity Checks at Connection or Segment End Points

End points, either connection or segment, use activation procedures to request continuity checking with the opposite end point. The requesting end point specifies the direction of the continuity checking (from the requesting end point, to the requesting end point, or both directions). If the far end

accepts the request, the specified source point(s) starts sending continuity checks periodically to the receiving point.

A source may send continuity check cells independently of the user's cells sent. Source continuity check cells are sent at predefined intervals of one per second when no user cells have been sent within one second.

If a point along the continuity check route does not receive a user cell or continuity cell within 3.5+/- 0.5 seconds, it assumes a loss of continuity (LOC) fault and sends AIS cells downstream. The continiuty check receiving point declares an AIS state and sends remote defect indication (RDI) cells upstream to the source, indicating the interruption of cell transfers in the downstream direction. When the connection is re-established and user or continuity check cells are received again, the affected points remove the LOC fault condition and stop sending AIS/RDI cells.

Continuity Checks at VPC or VCC End or Connecting Points

A VPC or VCC end or connecting point (the source) sends an activation or deactivation request to the receiving point. The receiving point responds by either confirming or denying the request. On receiving an activation confirmation, the source or receiving point (depending on the direction of the action) periodically generates performance management or continuity check cells.

Reporting

Reporting AIS and RDI: periodic notification when connection faults in the upstream and/or downstream direction among various network elements are affected by a defect.

Alarm Indication Signals

A network element (NE) transmits an AIS alarm downstream when it receives a major alarm condition such as a loss of frame. This prevents the generation of unnecessary alarms, and maintains communications.

A VPC or VCC connecting point receives an F4/F5 AIS alarm and sends AIS cells periodically (usually one per second) downstream, notifying all intermediate points in the connection of a fault.

F4/F5 AIS alarms are generated when a network element receives one of the following failure indications from the physical layer:

- LOS (Loss of Signal) alarm

  The LOS alarm indicates there are no transitions occurring in the NE received signal. For optical interfaces, an all ones pattern results after receiving no light pulses for a prescribed period. For electrical interfaces, a consecutive zero pattern results after receiving no signal transitions.

  You can simulate a LOS with an optical interface by turning the laser off.

- LOF (Loss of Frame) alarm

  The LOF alarm indicates the receiving equipment has lost frame delineation.

You can stimulate a LOF alarm by injecting a frame word error by using the Generate Frame Error dialog box.

- LOP (Loss of Pointer) alarm

  The LOP alarm indicates the receiving equipment has lost the pointer to the start cell in the payload.

- P-AIS (Path Alarm Indication Signal)

  The P-AIS alarm can occur on a SONET interface.

- LOCS (Loss of Cell Synchronization) alarm

  A LOCS alarm is generated by a NE at the convergence layer. It enters a LOCS state when it receives seven successive bad cell headers, and exits the LOCS state when it correctly receives six valid cell headers.

  LOCS is not used when PLCP framing is present.

  LOCS is only displayed in seconds.

Remote Defect Indications

The VPC/VCC end point sends RDI cells in the backward direction to the far end point, in order to indicate the interuption of cell transfers in the forward direction.

F4/F5 RDI alarms are generated when a network element receives one of the following failure indications from the physical layer: The failure indications are exactly the same as those listed for AIS.

Note: The F4 RDI alarm was formerly called the F4 FREF alarm. The F5 RDI alarm was formerly called the F5 FERF alarm.

Localization

Localization (loopback): isolation of failed entities if defect information is insufficient.

Loopback check: The detection of faults in the physical and ATM layers, and the detection of defects and declaration of failures within the network elements. A VPC or VCC end or connecting point sends a loopback cell to a destination end or connecting point. If the source receives a looped cell back within five seconds, the loopback is considered successful. If the source does not receive a successful loopback, it declares a time out.

Loopback check supports the following applications:

- End-to-end loopback: An end-to-end loopback cell is inserted by an end point, and looped back by the corresponding far-end end point.
- Access line loopback: A segment loopback cell is inserted by the customer or the network, and looped back by the first ATM node (at the VP/VC level) in the network or customer equipment respectively. For this application, the segment is defined by mutual agreement.
- Interdomain loopback: A segment loopback cell is inserted by one network operator and looped back by the first ATM node (at the VP/VC level) in an adjacent network operator domain. For this application, the segment is defined by mutual agreement.

- ~ Network-to-endpoint loopback: An end-to-end loopback cell is inserted by one network operator, and looped back by the end point in another domain.
- ~ Intradomain loopback: A segment loopback is inserted by a connection/segment end point or a connecting point, and looped back by a segment or a connecting point. For this application, the use of the loopback location identifier is a network operator option.

Activation/Deactivation

Activation/deactivation is an in-service OAM mechanism used to remotely start and stop the generation of cells that perpetually monitor performance and continuity.

A VPC or VCC end or connecting point (the source) sends an activation or deactivation request to the receiving point. The receiving point responds by either confirming or denying the request. On receiving an activation confirmation, the source or receiver (depending on the direction of the action) periodically generates performance management or continuity check cells.

Characteristics of OAM Activation / Deactivation Cells

The activation/deactivation cells are OAM cells with the function-specific fields shown in Figure 3-9.

Message ID	Directions of Action	Correlation Tag	PM Block Size A-B	PM Block Size B-A	Unused
6	2	8	4	4	336 bits (42 bytes)

Figure 3-9. OAM Activation/Deactivation Cells

- Message ID: indicates whether to request, confirm, or deny the activation or deactivation of cells
- Directions of Action: direction (s) in which to start/stop generating performance management or continuity cells
  - ~ A-B (ingress): away from the activator/deactivator
  - ~ B-A (egress): toward the activator/deactivator
  - ~ both: bidirectional
- Correlation Tag: number used to correlate transmitted activation/deactivation requests with their responses
- PM Block Size (A-B, B-A): This feature works with activation requests only. It monitors the size of user cell blocks used to monitor the performance in the forward or backward direction (default is 1,024 cells).

Module-Specific Alarm Functions

Loss of Signal (LOS)

Module: DS1 IMA

A network element (NE) will transmit an AIS alarm when it enters the LOS state for 2.5 +/- 0.5 seconds. This occurs when the NE has detected 175 +/- 75 consecutive pulse positions with no positive or negative pulses.

- The AIS alarm is stopped by the NE when it detects an average pulse density of at least 12.5% with no more than 15 consecutive zeros over a perioid of 175 +/- 75 pulse positions, starting with receiving a pulse.
- The AIS alarm continues if, at the end of the pulse position interval, any subintervals of 100 pulse positions containing no pulses of either polarity are observed.
- The AIS alarm is cleared when the LOS state is absent for 20 seconds.

Modules: Channelized DS3, DS3 IMA, DS3 ATM, DS3 Frame Relay

A network element (NE) will transmit an AIS alarm downstream when a LOS state persists for 2.5 +/- 0.5 seconds. This occurs when the NE has detected 175 +/- 75 consecutive zeros, or no pulses on an incoming signal.

- The AIS alarm is stopped by the NE when it receives an average pulse density of at least 33% over a period of 175 +/- 75 consecutive pulse positions, starting with receiving a pulse.
- The AIS alarm continues if, at the end of the pulse-position interval, any subintervals of 100 pulse positions containing no pulses of either polarity are observed.
- The AIS alarm is cleared when the LOS state is absent for 10.0 +/- 0.5 seconds.

Modules: E1 IMA, High-Density E1

A network element (NE) enters the LOS state when there is an absence of signal transitions on the incoming signal for a period of 5 milliseconds to 1 microsecond.

- The AIS alarm is cleared when the LOS state is absent for 3 seconds.

Module: E3 ATM

A network element (NE) will transmit an AIS alarm when it enters a Loss of Signal (LOS) state after not detecting input for 32 clock cycles.

- The AIS alarm is stopped by the NE as soon as it receives an input signal.

Modules: OC-3 MM APS, OC-3 MMAQ, OC-3 MMTS, Oc-3 SM APS, OC-3 SMAQ, OC-3 SMTS

A network element (NE) will transmit an L-AIS (line AIS in SONET) alarm downstream within 100 milliseconds of the onset of all zeros. This occurs when the receiver declares a Loss of Signal (LOS) after a violating period (20 +/- 3 milliseconds) of consecutive all zero bytes, or zero optical power, is detected in the received signal.

- The L-AIS alarm is cleared after the receiver removes an LOS. This occurs when two valid framing patterns (A1, A2) are received and no violations have been detected.

Modules: STM-1 MM MSP, STM-1 MMAQ, STM-1 MMTS, STM-1 SM MSP, STM-1 SMAQ, STM-1 SMTS

A network element (NE) will transmit an MS-AIS alarm downstream within 100 microseconds of the onset of all zeros. This occurs when the receiver declares a Loss of Signal (LOS) after a violating period (20 +/- 3 microseconds) of consecutive all zero bytes, or zero optical power, is detected in the received signal.

- The MS-AIS alarm is cleared after the receiver removes an LOS. This occurs when two valid framing patterns (A1, A2) are received and no violations have been detected.

Loss of Frame (LOF)

Modules: Channelized DS3, DS1 IMA

A network element (NE) will transmit a Loss of Frame (LOF) alarm when an Out of Frame (OOF) condition persists for 2.5 seconds +/- 0.5 seconds (except when the AIS defect or failure is present.)

- The LOF alarm stops when the NE detects valid framing for 20 seconds or when the AIS defect is detected.

Modules: DS3 IMA, DS3 ATM, DS3 Frame Relay

A network element (NE) will transmit a Loss of Frame (LOF) alarm when an Out of Frame (OOF) condition persists for 2.5 seconds +/- 0.5 seconds.

- The LOF alarm stops when the NE detects valid framing for 10.0 seconds +/- 0.5 seconds.

Modules: E3 ATM, OC-3 MM APS, OC-3 MMAQ, OC-3 MMTS, OC-3 SM APS, OC-3 SMAQ, OC-3 SMTS, STM-1 MM MSP, STM-1 MMAQ, STM-1 SM MSP, STM-1 SMAQ, STM-1 SMTS

A network element (NE) will transmit a Loss of Frame (LOF) alarm when an Out of Frame (OOF) condition persists for 3 milliseconds or longer.

- The LOF alarm stops when the NE receives a valid signal for 3 milliseconds.

Note: In order to account for intermittent out-of-frame conditions, the 3 milliseconds time is not reset to zero until an in-frame condition persists for more than 3 milliseconds.

Alarm Indicator Signal (AIS)

Module: DS1 IMA

A network element (NE) will transmit an AIS alarm when it detects a defect on the unframed, all ones AIS signal for 2.5 seconds +/- 0.5 seconds, or when it detects a Loss of Frame (LOF). In this situation, the NE will also transmit a RAI upstream.

- The AIS alarm stops when the NE receives a valid signal for 20 seconds.

Modules: Channelized DS3, DS3 IMA, DS3 ATM, DS3 Frame Relay

A network element (NE) will transmit an AIS alarm when it detects an AIS defect that persists for 2.5 +/- 0.5 seconds. In this situation, the NE will also transmit RDI upstream.

- The AIS alarm stops when the NE receives a valid signal for 10.0 seconds +/- 0.5 seconds.

Modules: E1 IMA, Enhanced E1, High-Density E1

A network element (NE) will transmit an AIS alarm when the defect of two or fewer zeros in each of two consecutive double frame periods (a total of 512 bits) is detected.

- The AIS alarm stops when the NE receives either of the following:
  - ~ two consecutive double frame periods (a total of 512 bits) containing three or more zeros
  - ~ A frame alignment signal error

Module: E3 ATM

A network element (NE) will transmit an all ones AIS downstream when it detects a loss of signal (LOS) or loss of frame (LOF). In this situation, the NE also transmits a far-end remote failure (FERF) alarm upstream.

Remote Defect Indications

Modules: Channelized DS3, DS3 IMA, DS3 ATM, DS3 Frame Relay

A network element (NE) will transmit an RDI when it detects a severely errored frame (SEF) or AIS (if implemented) for 2.5 seconds +/- 0.5 seconds.

- The RDI alarm stops when the NE's received failure stops for 10.0 seconds +/- 0.5 seconds.

E1 IMA, Enhanced E1, High-Density E1

A NE will transmit a RDI alarm upstream when a "1" in bit 3 in Non-Facility-Associated Signaling (NFAS) frames is detected.

- The RDI alarm stops .6 seconds after the condition has been removed.

Soft Permanent Virtual Circuits

The soft permanent virtual circuit (SPVC) feature is a semi-permanent virtual circuit enabled by management action. It is a PVC-type circuit in which SVCs are used for call setup and (automatic) rerouting. Once either a PVC or a permanent virtual path connection has been configured, an SPVC can be established between the two network interfaces serving the PVC by using signaling procedures. Consequently, this type of connection has attributes of both a switched virtual connection and a permanent virtual connection.

Specifically, an SPVC is established and released between the two network interfaces (NIs) serving the PVC. The user assigns unique ATM addresses, including the SEL octet in the case of a private ATM address (see Section 3.1 of UNI 4.0 signaling specification), to the corresponding NIs, thus identifying the startpoint and endpoint of the SPVC.

Using the *PacketStar*™ Access Concentrators, you can make a maximum of 30,000 connections per node, and a maximum of 5,000 SPVC connections per node.

Release 6.3 implements Phase 2 of a multiphase development program to eventually improve ATM traffic management on all modules except DS3 and E3. Over several development phases, Lucent will add new service classes and expand feature coverage on ATM interface modules. Phase 1 added traffic management to the OC-3c APS and the STIM-1 MSP modules. Phase 2 gives this capability to the Channelized DS3, DS1 and E1 modules.

One of the main improvements is upgraded usage parameter control (UPC). This feature allows the end system to check the validity of the ATM connection and protect it from malicious or unintentional misbehavior that could affect the quality of service (QoS) of established connections. After a set of service categories is specified, UPC is given a set of parameters for each, describing the traffic presented to the network and the quality of service the network requires. A number of traffic control mechanisms are defined, which the network may use to meet the QoS objectives.

Switched Virtual Circuits

Switched virtual circuit (SVC) connections are used for voice traffic over a public ATM WAN or private line network. SVCs are supported on all the ATM cell-bearing interfaces, including the DS3, E3, OC-3c, STM-1, Multi-Serial, and High Speed modules. The Access Concentrator system software supports the following features:

- Each ATM port on a single module can be individually configured for ATM UNI 3.0, UNI 3.1, IISP user, IISP network, or PNNI interfaces.
- SVCs can be allocated on UNI (public and private), IISP, and PNNI interfaces.
- Point-to-point and point-to-multipoint VCC connections are supported.
- VCC connections support both symmetric and asymmetric bandwidth requirements.
- The Access Concentrator system can process 60 calls per second, 100 maximum UNIs per system, 5,000 maximum simultaneous point-to-point SVC call originations, and 2,000 maximum point-to-multipoint call originations.
- The Access Concentrator system (equipped with 64 MB of memory on the CPU module) can process 20,000 maximum simultaneous SVC calls in progress.
- The individual call setup time is 16 milliseconds (ms) maximum, while the minimum call setup time for SVCs is approximately 10 ms from the time the call setup message enters the CPU module, and the acknowledgment leaves the CPU module.

Using the *PacketStar*™ Access Concentrator, you can make a maximum of 30,000 PVC connections per node, a maximum of 10,000 SVC point-to-point connections per node, and a maximum of 6,000 SVC point-to-multipoint connections per node.

Functional Description

SVC signalling, per ATM Forum UNI 3.0 and UNI 3.1, is selectable on a per-port basis. Call control is performed on the CPU module, including management of the call-state transitions for each of the calls. This process allows on-demand allocation of bandwidth and connection resources. The signaling protocol supports the following basic functions at the UNI interface:

Feature	Description
Connection/Call Setup	Origination/establishment of a call.
Connection/Call Request	Request of resources for connectivity to a certain destination. The Information Element (IE) field contains resource information, that is, PCR, SCR, MBS, QoS class, and so on.
Connection/Call Answer	Allows the destination party to respond to a request with VPI/VCI and other information related to the connection/call.
Connection/Call Clearing	Provides the information associated for removing the call/connection request. This includes: 1) calls removed because there weren't enough resources to meet the call request, or 2) connections removed due to call disconnect requests from either party, or 3) calls removed due to link and other network failures.
Reason for Clearing	Allows the clearing party to indicate the cause for initiating its removal from a connection/call.

Call States

Call states exist on both the user side and the network side of the transaction. Call states define which messages can be accepted by the user or the network entity, and how they are expected to react to those messages. As the user or network entity moves from call state to call state, the call switching process is accomplished.

In cases where the calling party is the user, and the called party is across the network, the UNI at the Access Concentrator port presents a user-side interface (UNI) to the user. The Access Concentrator port receives these user-side messages from the user and based on resource availability, route determination, and other network factors, presents a network-side (NNI or IISP) interface to the called party or the network-side Access Concentrator

port. Both user-side and network-side interfaces undergo similar state transitions. Transition messages trigger these call-state changes as follows:

Call States	Description
#0—Null	No call exists.
#1—Call initiated	• User—Outgoing call when the user requests call establishment from the network. • Network—Received the call establishment request, but has not responded yet to the outgoing call.
#3—Outgoing call proceeding	• User—Outgoing call when the user receives an acknowledgment that all call information required for call establishment has been received from the network. • Network—Network has sent an acknowledgment to the user that all call information has been received.
#6—Call present	• User—For incoming calls, the user has received the call establishment request, but has not responded yet. • Network—For incoming calls, the user has sent the call establishment request, but has not received a satisfactory response.
#8—Connect request	• User—For incoming calls, when the user has answered the call and is waiting to be awarded the call. • Network—For incoming calls, when the network has received an answer but the network has not yet awarded the call.
#9—Incoming call proceeding	• User—For incoming calls, when the user has sent acknowledgment that the user has received all call information necessary to establish a call. • Network—For incoming calls, when the network has received acknowledgment that the user has received all call information necessary to affect call establishment.

Call States	Description
#10—Active	• User—For incoming calls, when the user has been awarded the call. For outgoing calls, when the user has received an indication that the remote user has answered the call. • Network—For incoming calls, when the network has awarded the call to the called user. For outgoing calls, when the network shows that the remote user has answered the call.
#11—Release request	• User—The user has requested that the network clear the end-to-end connection and is waiting for a response. • Network—The network has requested a request from the user to clear the end-to-end connection.
#12—Release indication	• User—The user has received an indication to disconnect because the network has disconnected the end-to-end connection. • Network—The network has disconnected the end-to-end connection and has sent an indication to disconnect the user-to-network connection.

The following state transition messages are used for ATM point-to-point call and connection control:

Call establishment messages:	• Call proceeding • Connect • Connect acknowledgment • Setup
Call clearing messages:	• Release • Release complete
Miscellaneous messages:	• Status • Status inquiry

- The information elements used in the Call Establishment-Setup message allow the user to request the called party number, specific PCR, SCR, MBS, QoS class, forward and backward direction rates, performance, congestion control parameters, and so on, from the Access Concentrator UNI. The Call Establishment-Connect message allows the called party to respond with available traffic parameters, such as PCR, SCR, MBS, QoS class, forward and backward direction rates, performance, congestion control parameters, and so on. Usually this message also indicates the available VPI/VCI allocated for the connection. The other state-transition messages are specified by the ATM Forum UNI 3.0 and UNI 3.1 specifications and are transparent to the user.

Traffic Shaping

The traffic shaping feature is a method for controlling the flow of data traffic. It is implemented in firmware on modules that are offered with traffic-shaping variations. Those modules are the OC-3c Multi-Mode, OC-3c Single-Mode, STM-1 Multi-Mode, and STM-1 Single-Mode modules.

Traffic shaping ensures that variable bit-rate (VBR) traffic entering the Access Concentrator system (via the OC-3c and the STM-1 modules) complies with the parameters of established service contracts. If bursty VBR traffic exceeds the parameters of the output connection, the rate of the traffic flow is controlled to comply with the specified output rate by means of an input cell-selection algorithm before the traffic flow reaches the Access Concentrator backplane. If traffic exceeds the buffer capacity of the OC-3c or the STM-1 module (that is, rises above the maximum-capacity level), cells are discarded. Traffic shaping allows the network side of the Access Concentrator system to multiplex more efficiently the traffic-shaped virtual channel connections (VCCs) with other customer premises equipment (CPE) traffic (voice, video, and so on) for transport across the ATM network link. Constant bit-rate (CBR) traffic is unaffected by traffic shaping.

The only application of the traffic-shaping module is shown in Figure 3-10.

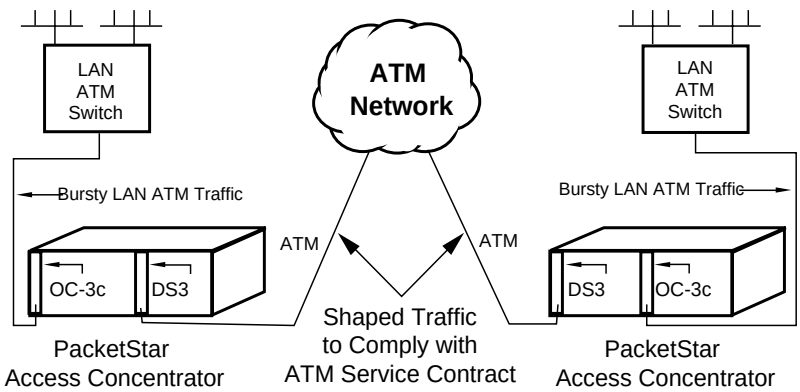

Figure 3-10. Traffic-Shaping Application

An end user has an ATM DS3 network connection and has subscribed to a VBR VCC connection contract from a carrier (service provider) with the following traffic parameters: 1) sustained cell rate (SCR) is 40,000 cells/second; 2) peak cell rate (PCR) is 80,000 cells/second; and 3) maximum burst size (MBS) is 250 cells. Even though LAN switches usually maintain a sustained cell-transport rate of 40,000 cells/second, they allow LAN traffic to burst in violation of carrier traffic contracts, causing clusters of cells to exceed the MBS parameter. Because carriers monitor traffic at the edge of a network and enforce adherence to traffic contracts by discarding cells that exceed the

MBS parameter, end users whose traffic violates their contractual MBS parameter experience high cell loss (and hence high packet loss). With the traffic-shaping feature of the OC-3c and the STM-1 modules, the Access Concentrator system effectively smooths bursty input LAN traffic to comply with the carrier traffic contract.

The input cell-selection buffering scheme is shown in Figure 3-11.

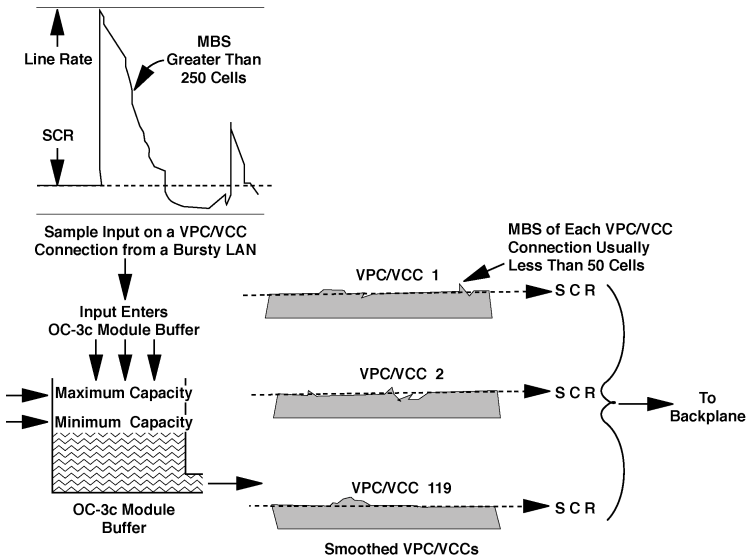

Figure 3-11. Traffic Shaping Using the Input Cell-Selection Algorithm

Connected to the LAN ATM switch via an ATM OC-3c or STM-1 link, the OC-3c and the STM-1 modules with traffic shaping support a total of 119 VCCs and VPCs. All inbound traffic is processed by the input cell selection algorithm, dynamically shared by all VCCs and VPCs, which smooths the traffic. The module buffer of the OC-3c or the STM-1 module is always 4 MB smaller than the total amount of memory installed on the module. For example, if 8 MB of memory are installed, 4 MB are available for queuing; if 32 MB of memory are installed, 28 MB are available for queuing. This dynamically shared buffer allows inbound VBR traffic to burst up to the line rate.

The module buffer of the OC-3c or the STM-1 module is set up with a maximum-capacity level (defined as 31/32 of the buffer size), and a minimum-capacity level (defined as 3/4 of the buffer size). When the incoming cells exceed the maximum-capacity level, the input cell-selection algorithm starts discarding cells to maintain a smooth traffic flow. The algorithm discards traffic on the connection with the longest queue first, then traffic on the connection with the second longest queue, and continues on until the module buffer of the OC-3c or the STM-1 module reaches the minimum-capacity level.

The algorithm processes traffic moving out of the input cell selection buffer according to the SCR of the particular VPC/VCC. The MBSs of traffic-shaped output are set as follows:

Sustained Cell Rate (SCR) of VPC/VCC	Maximum Burst Size (MBS) of Traffic-Shaped Output
0–20 Mbits/sec.	< 4 cells
20–30 Mbits/sec.	< 5 cells
30–40 Mbits/sec.	< 6 cells
75–120 Mbits/sec.	approximately 20–50 cells

The OC-3c and the STM-1 modules can perform traffic shaping on multiple high-rate connections (such as three 40-Mbps connections). Assigning a SCR to a connection above 75 Mbps, however, is not recommended in sensitive, bursty traffic environments. Assigning a SCR above 120 Mbps will essentially eliminate any traffic shaping, and thus is strongly discouraged.

- The OC-3c and the STM-1 modules perform only limited traffic management on the output side. The output buffer is limited to 2 Mbps for VBR traffic and 128 cells for CBR traffic, with only three priority levels supported: CBR, VBR1, and VBR2. The maximum-capacity level for congestion control is 32,000 cells, and the minimum-capacity level is 24,576 cells, with VBR traffic being shut off first from the backplane.

Voice Compression

A noncompressed voice channel uses 64 Kbps of bandwidth. Voice compression reduces the 64 Kbps bandwidth to a lower value, based on the algorithm chosen. Compressed voice messages can be carried over ATM Adaptation Layer 2 (AAL-2) only. The software on the CPU module assumes a 30 percent bandwidth savings.

Voice compression over AAL-2 will only work for a voice channel that is connected to an Access Concentrator through an ISDN PRI line. This is because AAL-2 does not transfer the voice channel signaling bits. If silence detection is enabled for a voice compression channel and no voice is detected, no ATM cell will be sent.

Voice Processing

With the DSP2C module, the Access Concentrator system can process voice traffic on selected DS0 circuits within the DS1 connections of the system. This module, a significant improvement over the earlier DSP2A and DSP2B server modules, processes ciruit emulation voice messages and can apply voice compression, echo cancellation, silence suppression, and comfort noise. Used with the channelized circuit emulation service modules, the DSP2C offers superior voice processing capability through the *PacketStar*™ line for the Lucent voice traffic over ATM (VToA) solution.

The DSP2C module supports ATM Adaptation Layer 2 (AAL-2) SVC connections and PVC multiplexing for reduced call latency.

To protect facsimile transmissions, the DSP2C module automatically turns off voice processing and echo cancellation on any channel when it detects a modem tone.

Figure 3-12 illustrates how an Access Concentrator system using voice processing might be deployed in a combined voice/data network.

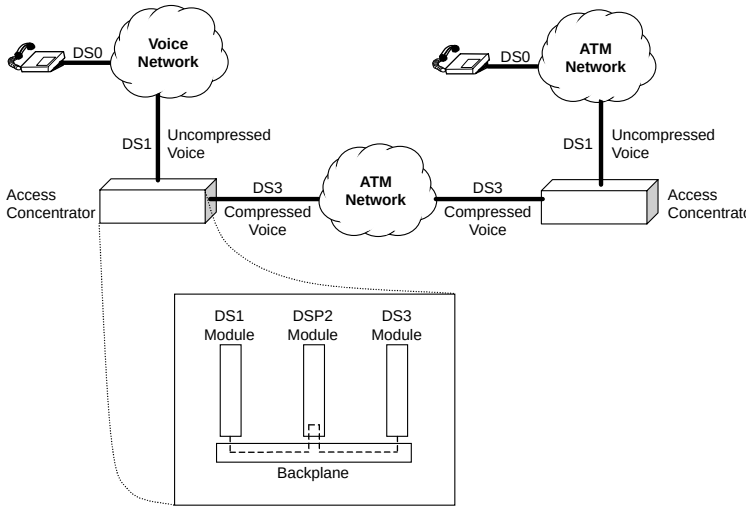

Figure 3-12. Voice Processing on the DSP2C Voice Server Module

I/O, Optical, and Server Modules

This section describes the functions and features for each type of I/O and server module, including the following:

I/O Modules

- Channelized DS3 module
- Channelized STS-1e T1 module
- DS1 IMA module
- DS3 ATM module
- DS3 Frame Relay module
- DS3 IMA module

- E1 IMA module
- E3 ATM module
- Enhanced E1 module
- Ethernet module
- High-Density E1 module
- High-Speed module
- Medium-Density DS1 module
- Multi-Serial module
- Voice 2-Wire Office module
- Voice 2-Wire Station module

Optical-Type I/O Modules

- OC-3c Multi-Mode (MM) module—three types available:
  - *AQueMan*™ firmware
  - Traffic-shaping firmware
  - 1+1 APS with AQueMan/VPC
- OC-3c Single-Mode (SM) module—three types available:
  - *AQueMan*™ firmware
  - Traffic-shaping firmware
  - 1+1 APS with AQueMan/VPC
- STM-1 Multi-Mode (MM) module—three types available:
  - *AQueMan*™ firmware
  - Traffic-shaping firmware with AQueMan/VPC
  - 1+1 MSP
- STM-1 Single-Mode (SM) module—three types available:
  - *AQueMan*™ firmware
  - Traffic-shaping firmware
  - 1+1 MSP with AQueMan™/VPC

Server Modules

- DSP2A Voice Server module
- DSP2B Voice Server module
- DSP2C Voice Server module
- Route Server module
- Tones and Announcements Server module

Channelized DS3 Module

The Channelized DS3 module provides one port with a line rate of 44.736 Mbps. The user can configure this module to provide N x 64 Kbps (fractional DS1) structured circuit emulation service. When configured for DS1 circuit-emulation service, the module interfaces with TDM channelized DS1 circuits. It converts the channelized digital signals (usually voice data) to ATM virtual channels. By using structured (channelized) circuit emulation, the Channelized DS3 module can adapt a maximum of 28 DS1 channels per port to ATM virtual channels with individual VPIs and VCIs. Signaling bit transport is also provided, using ATM Forum standards for channel-associated signaling (CAS). This module can connect to a device using 56 Kbps or 64 Kbps for service transport, with 8 Kbps for robbed-bit signaling per DS0. With the 64 Kbps "clear channel" capability, this module can connect to a device using ISDN primary rate interface (PRI) service. Because this structured circuit-emulation service can be configured to use only a fraction of the time slots, the user can configure several independent emulated circuits to share one service interface.

The Channelized DS3 module uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allow any DS1 port to act as a user network interface (UNI), or an interim inter-switch protocol (IISP) user or IISP network interface to an ATM network.

With Release 6.3, the Channelized DS3 module supports activating and deactivating DS1 access network interface (ANI) in-line loopback codes embedded in the DS1 signal. These codes test transmissions between customer interface equipment and network interface equipment, such as between central office PSAX products and PSAX products at the edge of the ATM network. The system also generates alarm indication signals on all affected DS1 connections whenever a loop is activated.

Software Features

The following Frame Relay Forum (FRF) Implementation Agreements are supported by the software:

- FRF.1—User-to-Network Interface (UNI)
- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking

The following ATM Forum Technical Committee Specifications are supported by the software:

- *Circuit Emulation Service Interoperability Specification Version 2.0* af-vtoa-0078.00
- *User-to-Network Interface Specification Version 3.0*, af-uni.0010.001
- *User-to-Network Interface Specification Version 3.1*, af-uni.0010.002

- *Private Network-Network Interface (PNNI), Specification Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface (ILMI) Specification Version 4.0, af-ilmi-0065.000*

The following services and functions are available:

- ATM services (channelized and unchannelized) with ATM traffic policing (UPC support) capability:
  - ATM UNI 3.0 and 3.1, with integrated link management interface (ILMI) capability
  - Interim inter-switch signaling protocol (IISP) user and IISP network
  - ATM private network-node interface (PNNI)
- Circuit emulation service (CES):
  - Unstructured and structured DS1 signal transport
  - Nx64 Kbps circuit emulation (where 1=N=24)
  - Dynamic bandwidth circuit emulation service (DBCES)—proprietary version
  - Channel-associated signalling (CAS)
- Integrated services digital network with primary rate interface service (PRI ISDN) with 64 Kbps clear channel capability and HDLC passthrough mode for the D-channel
- Frame relay UNI and NNI with frame relay policing (ITU-T I.370) capability
- High-level data link link control (HDLC) passthrough mode (Nx64)
- AAL2 cell formatting is provided for interworking with the DSP2A, DSP2B, and DSP2C Voice Server modules.
- Mixed circuit emulation, ATM, and frame relay channels can be configured within a virtual DS1 port.

Hardware Features

- Number of ports: one
- Connector type: two BNC connectors, one to receive data and one to transmit data
- Line rate: 44.736 Mbps

Channelized STS-1e (T1) Module

The Channelized STS-1e T1 module provides one port with a line rate of 51.84 Mbps. The user can configure this module to provide n X 64 Kbps (fractional DS-1) structured circuit-emulation service. When configured for DS-1 circuit-emulation service, the module interfaces with TDM channelized DS-1 circuits. It converts the channelized digital signals (usually voice data) to ATM virtual channels. By using structured (channelized) circuit

emulation, the Channelized STS-1e T1 module can adapt a maximum of 28 DS-1 channels per port to ATM virtual channels with individual VPIs and VCIs. Signalling bit transport is also provided, using ATM Forum standards for channel-associated signaling (CAS). This module can connect to a device using 56 Kbps or 64 Kbps for service transport, with 8 Kbps for robbed-bit signalling per DS-0. With the 64 Kbps "clear channel" capability, this module can connect to a device using ISDN primary rate interface (PRI) service. Because this structured circuit-emulation service can be configured to use only a fraction of the time slots, the user can configure several independent emulated circuits to share one service interface.

The Channelized STS-1e T1 module uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allow any DS-1 port to act as a user network interface (UNI), or an interim inter-switch protocol (IISP) user or IISP network interface to an ATM network.

Software Features

The following services are supported:

- Circuit emulation service (CES) with unstructured and structured DS1 signal transport
- N X 64 kbps circuit emulation service (1 = N = 24)
- Primary ISDN service with optional HDLC pass-through mode for the D-channel
- Channel-associated signalling (CAS)

The PacketStar™ Access Concentrator system software supports the following specifications, agreements, and protocols:

- Frame Relay Forum (FRF) Implementation Agreements:
  - FRF.1—User-to-Network Interface (UNI)
  - FRF.2—Network-to-Network Interface (NNI)
  - FRF.5—Frame Relay/ATM PVC Network Interworking
  - FRF.8—Frame Relay/ATM PVC Service Interworking
- ATM Forum Technical Committee Specifications:
  - *Circuit Emulation Service Interoperability Specification Version 2.0,* af-vtoa-0078.00
  - *User-to-Network Interface Specification Version 3.0,* af-uni.0010.001
  - *User-to-Network Interface Specification Version 3.1, af-uni.0010.002*
  - *Integrated Local Management Interface (ILMI) Specification Version 4.0, af-ilmi-0065.000*
  - *Private Network-Network Interface (PNNI), Version 1.0,* af-pnni-0055.000
- Multiservices:
  - ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network, ILMI, PNNI
  - CE: Circuit emulation service (CES) with ISDN PRI using 64 Kbps clear channel; 1 X 56 Kbps structured CAS; unstructured CES

- ~ Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
- ~ ITU-T I.370 (frame relay policing)
- ~ Congestion management
- ~ Traffic policing

Hardware Features

- Number of ports: one
- Connector type: two BNC connectors, one to receive data and the other to transmit data
- Line rate: 51.84 Mbps

DS1 IMA Module

The DS1 IMA module has six physical RJ-45 ports. Inverse multiplexing over ATM permits a user to strap two to six of the physical ports together to create ATM interfaces that support 3–9 Mbps of bandwidth. A maximum of three IMA groups may be configured per module.

Source data enters the module from the backplane and is divided between the ports within the IMA group specified in the virtual circuit connection. The data leaves the front of the module and is transported across individual T-1 lines. At the destination IMA module, the T-1 streams are merged back together in correct order and passed on to other modules as directed by virtual circuit connections. IMA dynamically handles conditions when T-1s within an IMA group become unavailable: the IMA "pipe" shrinks in bandwidth to the remaining T1s and continues to pass traffic. When a problem T-1 comes back on line, the IMA "pipe" will enlarge to take full advantage of the restored bandwidth.

Software Features

The firmware supports the following ATM Forum Implementation Agreements:

- ~ *Inverse Multiplexing over ATM Version 1.0*, af-phy-0086.000
- ~ *Inverse Multiplexing over ATM Version 1.1*, af-phy-0086.*1*
- Protocols: ATM, IMA (inverse multiplexing over ATM)

Hardware Features

- Number of ports: six
- Connector type: RJ-45
- Line rate: 1.544 Mbps

DS3 ATM Module

The DS3 ATM module provides a network interface at Digital Signal Level 3 (DS-3), with a line rate of 44.736 Mbps. This module accommodates ATM cell-bearing traffic. Typically, this module is used to connect the Access Concentrator system to an ATM edge switch. The DS3 ATM module has three types of LED indicators: FAIL, ACTIVE, and LOS (loss of signal).

Software Features

The DS3 ATM module uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allows either DS-3 port to act as a user network interface (UNI), an interim inter-switch protocol (IISP) user or IISP network interface, or as a PNNI network interface to an ATM network.

The software supports the following ATM Forum Technical Committee Specifications:

- *User-to-Network Interface Specification Version 3.0*, af-uni.0010.001
- *User-to-Network Interface Specification Version 3.1*, af-uni.0010.002
- *Interim Inter-switch Signaling Protocol, Version 1.0,* af-pnni-0026.000
- *Private Network-Network Interface (PNNI), Version 1.0,* af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Hardware Features

- Number of ports: two
- Connector type: four BNC connectors for the two ports (each port has one receive connector and one transmit connector)
- Line rate: 44.736 Mbps (typical)

DS3 Frame Relay Module

The DS3 Frame Relay module provides an unchannelized, high-speed frame relay network interface at Digital Signal Level 3 (DS3), with a line rate of 44.736 Mbps. Typically, the DS3 module is used to connect the Access Concentrator system to an ATM edge switch. The module has three types of light-emitting diode (LED) indicators: FAIL, ACTIVE, and LOS (loss of signal).

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)

- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking
- Multiservices:
  - ~ Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
  - ~ ITU-T I.370 (frame relay policing)
  - ~ Congestion management
  - ~ Traffic policing
  - ~ HDLC pass-through

Frame Relay

The DS3 Frame Relay module has interfaces for frame-relay network-level interworking (FRF.5) and service-level interworking (FRF.8). A maximum of 350 permanent virtual circuits (PVCs) can be assigned on each frame relay user-network interface (UNI) port. These features enable the Access Concentrator system to act as a gateway between routers, remote dial-access servers, IBM SNA equipment, and other devices configured for frame-relay operation.

Frame relay policing, and user-selected point-to-point SVCs are supported on the DS3 Frame Relay module. Frame relay policing enables the user to manage traffic at the user-network interface (UNI) or network-network interface (NNI) by setting performance parameters such as the Committed Information Rate (CIR), Excess Burst size (Be), and Committed Burst size (Bc).

HDLC Pass-through

Each port on the DS3 Frame Relay module can be configured to perform adaptation for high-level data link control (HDLC) pass-through. Without this feature, AAL-1 adaptation would be required for data from HDLC devices connected to a port on the DS3 Frame Relay module. With this feature, AAL-5 adaptation can be used to allow HDLC data to be handled as if it were VBR rather than CBR. Since ATM cells are only generated when HDLC is present, optimal bandwidth is used.

Hardware Features

- Number of ports: one
- Connector type: two BNC connectors for the single port which has one receive connector and one transmit connector
- Line rate: 44.736 Mbps (typical)

DS3 IMA Module

The DS3 IMA (Inverse Multiplexing over ATM) module combines the features of the Channelized DS3 module (see the *PacketStar™ Channelized DS3 Module User Guide*) and the DS1 IMA module (see the *PacketStar™ DS1 IMA Module User Guide*). It allows you to configure up to 28 virtual T1 ports for native DS1 ATM services or for as many as 14 independent groups. This gives you point-to-point bandwidth options between that of a single T1 line and that of a T3 line.

Software Features

The following services and functions are available:

- Protocols: ATM, IMA (inverse multiplexing over ATM)
- ATM channelized services over IMA groups:
  - ATM UNI 3.0 and 3.1, with integrated link management interface (ILMI) capability
  - Interim inter-switch signaling protocol (IISP) user and IISP network
  - ATM private network-network interface (PNNI)

The following ATM Forum Technical Committee Specifications are supported by the software:

- *User-to-Network Interface Specification Version 3.0*, af-uni.0010.001
- *User-to-Network Interface Specification Version 3.1*, af-uni.0010.002
- *Private Network-Network Interface (PNNI), Specification Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface (ILMI) Specification Version 4.0, af-ilmi-0065.000*
- *Inverse Multiplexing over ATM Version 1.0*, af-phy-0086.000
- *Inverse Multiplexing over ATM Version 1.1*, af-phy-0086.001

Hardware Features

- Front-End: DMA interface with one physical port
- Number of ports: one; port density: 28 virtual channels
- Connector type: two BNC connectors, one to receive data and one to transmit data
- Line rate: 44.736 Mbps
- Bandwidth: 1.544 to 44.736 Mbps

DS3 ATM Module

The DS3 ATM module provides a network interface at Digital Signal Level 3 (DS-3), with a line rate of 44.736 Mbps. This module accommodates ATM cell-bearing traffic. Typically, this module is used to connect the Access Concentrator system to an ATM edge switch. The DS3 ATM module has three types of LED indicators: FAIL, ACTIVE, and LOS (loss of signal).

Software Features

The DS3 ATM module uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allows either DS-3 port to act as a user network interface (UNI), an interim inter-switch protocol (IISP) user or IISP network interface, or as a PNNI network interface to an ATM network.

The software supports the following ATM Forum Technical Committee Specifications:

- *User-to-Network Interface Specification Version 3.0*, af-uni.0010.001
- *User-to-Network Interface Specification Version 3.1*, af-uni.0010.002
- *Interim Inter-switch Signaling Protocol, Version 1.0,* af-pnni-0026.000
- *Private Network-Network Interface (PNNI), Version 1.0,* af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Hardware Features

- Number of ports: two
- Connector type: four BNC connectors for the two ports (each port has one receive connector and one transmit connector)
- Line rate: 44.736 Mbps (typical)

DS3 Frame Relay Module

The DS3 Frame Relay module provides an unchannelized, high-speed frame relay network interface at Digital Signal Level 3 (DS3), with a line rate of 44.736 Mbps. Typically, the DS3 module is used to connect the Access Concentrator system to an ATM edge switch. The module has three types of light-emitting diode (LED) indicators: FAIL, ACTIVE, and LOS (loss of signal).

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)

- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking
- Multiservices:
  - Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
  - ITU-T I.370 (frame relay policing)
  - Congestion management
  - Traffic policing
  - HDLC pass-through

Frame Relay

The DS3 Frame Relay module has interfaces for frame-relay network-level interworking (FRF.5) and service-level interworking (FRF.8). A maximum of 350 permanent virtual circuits (PVCs) can be assigned on each frame relay user-network interface (UNI) port. These features enable the Access Concentrator system to act as a gateway between routers, remote dial-access servers, IBM SNA equipment, and other devices configured for frame-relay operation.

Frame relay policing, and user-selected point-to-point SVCs are supported on the DS3 Frame Relay module. Frame relay policing enables the user to manage traffic at the user-network interface (UNI) or network-network interface (NNI) by setting performance parameters such as the Committed Information Rate (CIR), Excess Burst size (Be), and Committed Burst size (Bc).

HDLC Pass-through

Each port on the DS3 Frame Relay module can be configured to perform adaptation for high-level data link control (HDLC) pass-through. Without this feature, AAL-1 adaptation would be required for data from HDLC devices connected to a port on the DS3 Frame Relay module. With this feature, AAL-5 adaptation can be used to allow HDLC data to be handled as if it were VBR rather than CBR. Since ATM cells are only generated when HDLC is present, optimal bandwidth is used.

Hardware Features

- Number of ports: one
- Connector type: two BNC connectors for the single port which has one receive connector and one transmit connector
- Line rate: 44.736 Mbps (typical)

E1 IMA Module

The E1 IMA module has six physical RJ-45 ports. Inverse multiplexing over ATM permits a user to strap two to six of the physical ports together to create

ATM interfaces that support 4 to 12 Mbps of bandwidth. A maximum of three IMA groups may be configured per module.

Source data enters the module from the backplane and is divided between the ports within the IMA group specified in the virtual circuit connection. The data leaves the front of the module and is transported across individual E-1 lines. At the destination IMA module, the E-1 streams are merged back together in correct order and passed on to other modules as directed by virtual circuit connections. IMA dynamically handles conditions when E-1s within an IMA group become unavailable: the IMA "pipe" shrinks in bandwidth to the remaining E-1s and continues to pass traffic. When a problem E-1 comes back online, the IMA "pipe" will enlarge to take full advantage of the restored bandwidth.

Software Features

The firmware supports the following ATM Forum Implementation Agreements:

- *Inverse Multiplexing over ATM Version 1.0*, af-phy-0086.000
- *Inverse Multiplexing over ATM Version 1.1*, af-phy-0086.1

Hardware Features

- Number of ports: six
- Connector type: RJ-45 (120-Ohm symmetrical pair [4 wire] interface)
- Line rate: 2.048 Mbps
- Framing mode: cyclic redundancy mode multifrequency (CRC-mf)
- Line encoding mode: HDB3
- Protocols: ATM, IMA (inverse multiplexing over ATM)

E3 ATM Module

The E3 ATM module provides a network interface with a line rate of 34.368 Mbps. Typically, the E3 module is used to connect the Access Concentrator system to an ATM edge switch. This module has three types of light-emitting diode (LED) indicators: ACTIVE, FAIL, and LOS (loss of signal).

Software Features

The E3 ATM module uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allow either E-3 port to act as a user network interface (UNI), an interim inter-switch protocol (IISP) user or network interface, or as a PNNI network interface to an ATM network.

The software supports the following ATM Forum Technical Committee Specifications:

- *User-to-Network Interface Specification Version 3.0*, af-uni-0010.001

- *User-to-Network Interface Specification Version 3.1*, af-uni-0010.002
- *Interim Inter-switch Signaling Protocol, Version 1.0*, af-pnni-0026.000
- *Private Network-Network Interface (PNNI), Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Hardware Features

Hardware Features

- Number of ports: two
- Connector type: four BNC connectors for the two ports (each port has one receive connector and one transmit connector)
- Line rate: 34.368 Mbps (typical)

Enhanced DS1 Module

The DS1/T1 component provides six ports, each with a line rate of 1.544 Mbps. The interfaces support *American National Standards Institute (ANSI) T1.403*, af-phy-0016.000 and af-test-0037.000. Each port can be independently configured to provide services for channelized and unchannelized frame relay configurations, circuit emulation service, dynamic bandwidth circuit emulation service, and ATM service. This component has three types of light-emitting diode (LED) indicators: FAIL, ACTIVE, and LOS (loss of signal).

The component has built-in channel service unit (CSU) capability which allows it to interface directly to a DS1/T1 line with multiple repeaters. This feature allows the component to interface with a time-division multiplex (TDM) channelized DS1/T1 circuit. Configured for channelized T1 service, the DS1/T1 component maps up to 24 individual high-level data link control (HDLC) data links on a single T1 connection (144 HDLC data links per component). This component also provides a data service unit/channel service unit (DSU/CSU) for each port in order to configure individual DS-0s.

The user can configure this component to provide n X 64 Kbps (fractional DS1) structured circuit-emulation service. When configured for DS1 circuit-emulation service, the DS1/T1 component interfaces with TDM channelized DS1 circuits. It converts channelized digital signals (usually voice data) to ATM virtual channels. This component can adapt a maximum of 24 DS-0 channels per port to ATM virtual channels with individual VPIs and VCIs using structured (channelized) circuit emulation. Signaling bit transport is also provided, based on ATM Forum standards for channel-associated signalling (CAS). This component can connect to a device using 56 Kbps with 8 Kbps for robbed-bit signaling per DS-0. With the 64 Kbps "clear channel" capability, the DS1/T1 component can connect to a device using a ISDN primary rate interface (PRI) service. Because this structured circuit-emulation service can be configured to use only a fraction of the time slots,

the user can configure several independent emulated circuits to share one service interface.

The DS1/T1 component uses ATM Forum specifications UNI 3.0 or UNI 3.1, which allows any DS1 port to act as a user network interface (UNI), or an interim inter-switch protocol (IISP) user or network interface to an ATM network.

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)
- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking

ATM Forum Technical Committee Specifications:

- *Circuit Emulation Service Interoperability Specification Version 2.0,* af-vtoa-*0078.00*
- *User-to-Network Interface Specification Version 3.0, af-uni.0010.001*
- *User-to-Network Interface Specification Version 3.1, af-uni.0010.002*
- *Private Network-Network Interface (PNNI), Specification Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0,*

  af-ilmi-0065.000

Multiservices:

- ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network
- CE: Circuit emulation service (CES) with ISDN PRI using 64 Kbps clear channel; dynamic bandwidth circuit emulation service (DBCES—proprietary version); 1 X 56 Kbps structured CAS; unstructured CES
- HDLC Passthrough
- Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
- PRI ISDN
- ITU-T I.370 (Frame relay policing)
- Congestion management
- Traffic policing

Hardware Features

- Number of ports: six
- Connector type: RJ-45
- Line rate: 1.544 Mbps

Enhanced E1 Module

The Enhanced E1 module provides six ports, each with a line rate of 2.048 Mbps. The interfaces support ITU-T G.703 and ITU G.704. Each port can be independently configured to provide services for channelized and unchannelized frame relay configurations, circuit emulation service, and ATM service. This module has three types of light-emitting diode (LED) indicators: FAIL, ACTIVE, and LOS (loss of signal).

Configured for channelized E-1 service, the Enhanced E1 module maps up to 31 individual high-level data links (HDLCs) on a single E-1 connection (180 HDLCs per module). This module provides a data service unit (DSU)/channel service unit (CSU) for each port in order to configure individual DS-0s. The module has a built-in CSU capability that allows it to interface directly to an E-1 line with multiple repeaters. This feature allows the module to interface with a time-division multiplex (TDM) channelized E-1 circuit.

The user can configure the Enhanced E1 module to provide n X 64 Kbps (fractional E-1) structured circuit emulation service. When configured for E-1 circuit emulation service, the module interfaces with TDM channelized E-1 circuits. It converts channelized data (usually voice data) to ATM virtual channels. This module can adapt a maximum of 31channels per port to ATM virtual channels with individual virtual path identifiers (VPIs) and virtual channel identifiers (VCIs), using structured (channelized) circuit emulation. Signaling bit transport from time slot 16 is also provided, based on ATM Forum standards for channel-associated signaling (CAS). With the 64 Kbps "clear channel" capability, this module can connect to a device using a integrated services digital network with a primary rate interface (ISDN PRI) service. Because this structured circuit emulation service can be configured to use only a fraction of the time slots, the user can configure several independent emulated circuits to share one service interface. The Enhanced E1 module uses ATM Forum Specification UNI 3.0 or UNI 3.1, which allows any E-1 port to act as a user network interface (UNI), an interim inter-switch protocol (IISP) user or network interface to an ATM network.

Note: The Enhanced E1 Circuit Emulation (CE) module is functionally identical to the Enhanced E1 module, except that the Enhanced E1 (CE only) module provides a license for circuit emulation functions only.

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)
- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking

ATM Forum Technical Committee Specifications:

- *Circuit Emulation Service Interoperability Specification Version 2.0* af-vtoa-0078.00
- *User-to-Network Interface Specification Version 3.0*, af-uni.0010.001
- *User-to-Network Interface Specification Version 3.1*, af-uni.0010.002
- *Private Network-Network Interface (PNNI), Specification Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Multiservices:

- ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network
- CE: Circuit emulation service (CES) with ISDN PRI using 64 Kbps clear channel; dynamic bandwidth circuit emulation service (DBCES—proprietary version); 1 X 64 Kbps structured CAS; unstructured CES
- HDLC Pass-through
- Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
- ITU-T I.370 (frame relay policing)
- Congestion management
- Traffic policing

Hardware Features

- Number of ports: six
- Connector type: RJ-45 (120-Ohm symmetrical pair [4-wire] interface)
- Line rate: 2.048 Mbps
- Framing mode: cyclic redundancy check multifrequency (CRC-mf)
- Interfaces: ITU-T G.703, ITU G.704
- Line encoding mode: HDB3

Ethernet Module

The Ethernet module provides Ethernet bridging from LAN to LAN, and from LAN to ATM. The module has five ports on the faceplate and a sixth, virtual

port built into the circuit board. The virtual port provides 70 virtual channels that transmit data through the backplane. The Ethernet module has three types of light-emitting diode (LED) indicators: FAIL, ACTIVE, and LOS (loss of signal).

Software Features

The Ethernet bridging feature includes the encapsulation of the media access control (MAC) layer data, using standards in the ATM Forum RFC 1483 specification, for filtering and bridge management (see "Ethernet LAN Bridging" for more detail).

Hardware Features

- Number of ports: six
  - ~ five physical ports
  - ~ one virtual port used for backplane connections
- Connector type: RJ-45
- Ethernet interfaces:
  - ~ Per port: port 1 supports 10 or 100 Mbps; ports 2, 3, 4, and 5 support 10 Mbps each
  - ~ Aggregate of all ports, maximum: 30 Mbps throughput
- Interfaces: IP over frame relay (RFC 1490)

High-Speed Module

The High-Speed module has one serial port and one parallel port. These two ports can operate simultaneously or independently. The serial interface operates with a line rate of 2.048–29.824 Mbps. Typically, this module is used to connect to Direct Broadcast Satellite transmitters and receivers.

Software Features

The limitless ATM network (LANET) protocol is used for both ports on this module to interface with an asynchronous transfer mode (ATM) network. The ATM protocol is optimized for high-speed environments such as DS3 and OC-3c. ATM also works well with low-speed links by offering a standards-based method for optimally interleaving constant bit rate (CBR) voice traffic and variable bit rate (VBR) data traffic in order to efficiently use bandwidth and offer multi-media capability.

The software supports the following ATM Forum Technical Committee Specifications:

- *Circuit Emulation Service Interoperability Specification Version 2.0* af_vtoa_0078.00
- User to Network Interface (UNI) Version 3.0

- User to Network Interface (UNI) Version 3.1
- *Integrated Local Management Interface (ILMI) Specification Version 4.0, af-ilmi-0065.000*
- *Private Network-Network Interface (PNNI), Version 1.0*, af-pnni-0055.000

Protocols:

- ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network, ILMI, PNNI
- CE: Circuit emulation service (CES)

Hardware Features

- Number of ports:
  - ~ One parallel (ECL/CMOS chip) (port 1)
  - ~ One serial (EIA-422 interface) (port 2)
- Connector type:
  - ~ Micro dual-row 36-pin for the parallel port
  - ~ Micro-DB25 for the serial port
- Interfaces supported on the parallel port:
  - ~ Direct Broadcast Satellite transmitters and receivers
  - ~ Video set-top boxes
- Interfaces supported on the serial port:
  - ~ EIA-422-A
  - ~ EIA-449
  - ~ EIA-530
- Data transmission rate:
  - ~ Using external clock timing: up to 30 Mbps
  - ~ Using internal clock timing: data transmission rates are given in Appendix B,"Pin Configurations"
- Protocols: ATM and circuit emulation

Medium-Density DS1 Module

The Medium-Density DS1 module provides 12 ports, each with a line rate of 1.544 Mbps. Each port can be independently configured to provide for channelized and unchannelized frame relay configurations, circuit emulation service (CES), high-level data link control (HDLC) pass-through mode, integrated services digital network with a primary rate interface (ISDN PRI) service, and ATM services.

You can configure the Medium-Density DS1 module to provide N x 64 Kbps (fractional T1) structured circuit emulation service. When configured for DS1 circuit emulation service, the module interfaces with TDM channelized DS1

circuits. It converts channelized data (usually voice data) to ATM virtual channels. By using structured (channelized) circuit emulation, this module can adapt a maximum of 24 DS1channels per port to ATM virtual channels with individual virtual path identifiers (VPIs) and virtual channel identifiers (VCIs). Signalling bit transport is also provided, based on ATM Forum standards for channel-associated signalling (CAS). With the 64 Kbps "clear channel" capability, this module can connect to a device using an ISDN PRI service. Because this structured circuit emulation service can be configured to use only a fraction of the time slots, you can configure several independent emulated circuits to share one service interface.

The Medium-Density DS1 module uses ATM Forum Specification UNI 3.0 or UNI 3.1, which allows any DS1 port to act as a user network interface (UNI), an interim inter-switch protocol (IISP) user or network interface to an ATM network.

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)
- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking

ATM Forum Technical Committee Specifications:

- *Circuit Emulation Service Interoperability Specification Version 2.0* af_vtoa_0078.00
- User to Network Interface Version 3.0
- User to Network Interface Version 3.1
- *Private Network-Network Interface (PNNI), Version 1.0*, af-pnni-0055.000
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Multi-Services:

- ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network
- CE: Circuit emulation service (CES) with ISDN PRI using 64 Kbps clear channel; 1 x 64 Kbps structured CAS; unstructured CES
- HDLC passthrough mode (N x 56 and N x 64)
- Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
- ITU-T I.370 (Frame relay policing)
- Congestion management

- Traffic policing

Hardware Features

- Number of ports: 12
- Connector type: One Mini-Champ connector that mates with the AMP cable # 1324936-1
- Line rate: 1.544 Mbps
- Framing mode: cyclic redundancy check multi-frequency (CRC-mf)
- Interfaces: ITU-T G.703, ITU G.704
- Line encoding mode: B8ZS

Multi-Serial Module

The Multi-Serial module provides six serial ports for several types of serial data interfaces, with a maximum line rate of 2.048 Mbps, and a maximum aggregate rate of 4 Mbps.

Bit Stuffing and CES Conversion

The Multi-Serial component also supports bit stuffing and 56K–64K circuit emulation service (CES) conversion, available as standard features in the R6.3 software.

The framing for SS7's Message Transfer Part (MTP) Level 2 is a modified version of HDLC. The difference between SS7 MTP framing and standard HDLC is in the opening and closing 1-byte flag. SS7 MTP messages use only the closing flag. In order to support external SS7 transport requirements, it is necessary to exchange information via T-1 circuits where each 64 kbps DS-0 of the T-1 is filled with 56 kbps of SS7 data and 8 kbps of overhead (stuffing) data.

The SS7 circuits originating from the Multiserial interface can be mapped using AAL1 to an individual ATM constant bit rate (CBR) class of service exiting on a DS3 ATM cell-bearing interface. At the far-end, the ATM circuit is adapted (based on AAL-1 adaptation) to a native Multiserial (TDM) or CES (TDM) circuit. SS7 traffic can originate from the Multiserial interface and terminate on the Enhanced DS1 interface.

Interfaces

The interfaces support RS-232 (synchronous and asynchronous), RS-449, RS-530, and V.35. For synchronous interfaces, each port can be independently configured as either data terminating equipment (DTE) or data communications equipment (DCE). Each port can be independently configured for frame relay, circuit emulation, terminal emulation and asynchronous transfer mode (ATM) (using limitless ATM network [LANET] protocol).

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

- FRF.1—User-to-Network Interface (UNI)
- FRF.2—Network-to-Network Interface (NNI)
- FRF.5—Frame Relay/ATM PVC Network Interworking
- FRF.8—Frame Relay/ATM PVC Service Interworking

ATM Forum Technical Committee Specifications:

- *Circuit Emulation Service Interoperability Specification Version 2.0* af_vtoa_0078.00
- User to Network Interface Version 3.0
- User to Network Interface Version 3.1
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

Multi-Services:

- ATM: ATM UNI 3.0 and 3.1; Interim inter-switch signaling protocol (IISP) user, IISP network
- CE: Circuit emulation service (CES)
- Frame relay UNI and NNI (FRF.1, FRF.2, FRF.5, and FRF.8)
- HDLC Passthrough
- ITU-T I.370 (frame relay policing)
- Congestion management
- Traffic policing

The following sections explain the application of the interfaces supported on the Multi-Serial module: frame relay, circuit emulation, terminal emulation, HDLC pass-through, and ATM.

Frame Relay

The Multi-Serial module has interfaces for frame-relay network-level interworking (FRF.5) and service-level interworking (FRF.8). A maximum of 350 permanent virtual circuits (PVCs) can be assigned on each frame relay user-network interface (UNI) port. These features enable the Access Concentrator system to act as a gateway between routers, remote dial-access servers, IBM SNA equipment, and other devices configured for frame-relay operation.

Frame relay policing, and user-selected point-to-point SVCs are supported on the Multi-Serial module. Frame relay policing enables the user to manage traffic at the user-network interface (UNI) or network-network interface (NNI) by setting performance parameters such as the Committed Information Rate (CIR), Excess Burst size (Be), and Committed Burst size (Bc).

Circuit Emulation

Each port on the Multi-Serial module can be configured to perform adaptation for circuit emulation. The implementation of ATM Adaptation Layer 1 (AAL-1) allows for the transmission of circuit emulation data as Constant Bit Rate (CBR) traffic across an ATM network. With circuit emulation support, the Multi-Serial module can adapt and concentrate circuit emulation traffic onto an ATM network. This feature enables the Access Concentrator system to interface with non-frame relay routers, video encoders, encryption devices, and other devices which use a synchronous interface.

Terminal Emulation

Each port on the Multi-Serial module can be configured to perform an adaptation for terminal emulation. The implementation of ATM Adaptation Layer 5 (AAL-5) allows for the transmission of terminal emulation data as Variable Bit Rate (VBR) traffic across an ATM network. With terminal emulation support, the Multi-Serial module can adapt and concentrate terminal emulation traffic onto an ATM network. This feature enables the Access Concentrator system to interface with terminal equipment such as monitors, craft interfaces, console ports, sensors, and other devices implementing an asynchronous interface.

HDLC Pass-through

Each port on the Multi-Serial module can be configured to perform adaptation for high-level data link control (HDLC) pass-through. Without this feature, AAL-1 adaptation would be required for data from HDLC devices connected to a port on the Multi-Serial module. With this feature, AAL-5 adaptation can be used to allow HDLC data to be handled as if it were VBR rather than CBR. Since ATM cells are only generated when HDLC is present, optimal bandwidth is utilized.

ATM

Each port on the Multi-Serial module can be configured for ATM service as per the ATM Forum's UNI 3.0/3.1 specifications. With this feature, a port on the Multi-Serial module can be used as an ATM network interface, using the LANET protocol.

With this feature, statistical multiplexing gains can be achieved over low speed serial links. By using LANET, the advantages of ATM can be used over serial links to optimally interleave traffic for efficient bandwidth utilization and multi-media capability. The LANET protocol efficiently adapts ATM to low speed, high noise applications such as wireless and satellite. It is a physical layer protocol that maintains cell extraction capability at bit-error rates up to 10 to the negative second power (-2). LANET overhead accounts for 0.63% of link bandwidth. It can be implemented over each of the supported serial interface types, and is independent of the transmission rate.

Hardware Features

- Number of ports: six serial
- Connector type: micro-DB15

- Interfaces supported: EIA-232-D, EIA-530, EIA-449 v.11 (subset), and V.35, with the Access Concentrator system configured as either a data terminating equipment (DTE) or a data communications equipment (DCE) device.
- Data transmission rate:
  - ~ Minimum: 75 Mbps per port
  - ~ Maximum: 2.048 Mbps per port
  - ~ Aggregate of all ports maximum: 4 Mbps
- Protocols: frame relay, circuit emulation, terminal emulation, HDLC pass-through, and ATM

Voice 2-Wire Office Module

The Voice 2-Wire Office module provides support for the office (central office or PABX switch) end of a two-wire analog telephone line. This allows a voice loop from a voice switch to be connected directly to an Access Concentrator system and communicate over an ATM network to a distant telephone or other analog device.

The Voice 2-Wire Office module has three types of LED indicators: ACTIVE, FAIL, and LOS (loss of signal). There is a LOS LED for each port on the faceplate. The LED turns on when the port goes off-hook. It also turns on and off in synchonization with an incoming ringing signal to the port.

Software Features

A PVC connection can be set up between a Voice 2-Wire Office module and a Voice 2-Wire Station module. This connection enables foreign exchange (FXO) voice service to be transmitted across an ATM network. With FXO service, the voice switch provides dial tone, ringing, and digit translation, which are not provided by the ATM network.

- Number of ports: four
- Connector type: RJ-11
- Ringing frequency: 20 Hz
- Termination impedance: 600 Ohms
- Signaling: dual tone multi-frequency (DTMF)
- Supervision: loop start

Voice 2-Wire Station Module

The Voice 2-Wire Station module provides support for the station (telephone set) end of a two-wire analog telephone line. A telephone or other analog

voice device can be connected directly to this module in the Access Concentrator system to communicate over an ATM network.

The Voice 2-Wire Station module has three types of LED indicators: ACTIVE, FAIL, and LOS (loss of signal). The LOS LED turns on when the port goes off-hook. It also turns on and off in synchronization with an incoming ringing signal to the port.

Software Features

The Voice 2-Wire Station module can be used to establish a permanent virtual circuit (PVC) on a voice circuit that originates on the same module. This module also provides private-line automatic ring-down (PLAR) service for the PVC. PLAR provides a point-to-point private line between two telephone sets. If either station goes off-hook, the other one automatically rings The ringing will stop when the called station goes off-hook or the calling station goes back on-hook. The PLAR service provides 20-Hz ring-down, loop-start supervision, and no signalling. The module also supports FXS service.

Hardware Features

- Number of ports: eight
- Connector type: RJ-11
- Ringing frequency: 20 Hz
- Termination impedance: 600 Ohms

Optical-Type I/O Modules

OC-3c Multi-mode and Single-Mode Modules

The OC-3c Multi-Mode (MM) and Single-Mode (SM) modules provide a fiber optic interface operating in the concatenated mode of the SONET-defined line rate of 155 Mbps.

- The interface on the OC-3c Multi-Mode module is intended for very short-reach applications, usually connections in a building.
- The interface on the OC-3c Single-Mode module is intended for long-reach applications, typically between LANs. This module is frequently used to connect high-speed LAN products (routers and so on) to the ATM network.

These modules are available in two variations, which differ according to the firmware installed on the circuit boards.

- One variation for both the Multi-Mode and Single-Mode types, with the names OC-3c MM AQ module and OC-3c SM AQ module, uses the *AQueMan*™ algorithm for flow control.
- The other variation for both the Multi-Mode and Single-Mode types, with the names OC-3c MM TS module and OC-3c SM TS module, uses traffic shaping for flow control.

Software Features

The software also supports the following ATM Forum Technical Committee Specifications:

- *User to Network Interface Version 3.0*
- *User to Network Interface Version 3.1*
- *Integrated Local Management Interface Specification Version 4.0,*

  af-ilmi-0065.000
- *Interim Inter-Switch Signaling Protocol*, af-pnni-0026.000
- *Private Network-Network Interface (PNNI)*, af-pnni-0055.000

  Protocol
- Traffic management:
  - AQueMan
  - AAL-5 (traffic shaping)
  - Ten quality of service (QoS) levels: constant bit rate level 1 (CBR-1), CBR-2, CBR-3, CBR-4, variable bit rate level 1 (VBR-1), VBR-2, VBR-3, VBR-4, VBR-5, and VBR-6

Hardware Features

All OC-3c Multi-Mode and Single-Mode modules have the hardware features shown in Table 3-7:

Table 3-7. OC-3c Multi-Mode and Single-Mode Hardware Specifications

Feature	Module	
	OC-3c SM	**OC-3c MM**
Number of ports	1	1
Type of connector (two for each module—transmit and receive)	SC	ST
Type of fiber optic cable	single-mode	multi-mode
Fiber optic cable reach (approximate, depending on fiber makeup)	16 miles (25.7 km)	6,560 feet or 1.2 miles (2 km)
Line rate	155 Mbps	155 Mbps

Table 3-7. OC-3c Multi-Mode and Single-Mode Hardware Specifications

Feature	Module	
	OC-3c SM	OC-3c MM
Optical wavelength (nominal value)	1,300 nm	1,330 nm
• System gain	15 dB	13.5 dB
• Transmitter—minimum optical output power (average)	-15 dBm	-19 dBm
• Transmitter—maximum optical output power (average)	-8 dBm	-14 dBm
• Receiver—minimum optical input power (average)	-31 dBm	-32.5 dBm
• Receiver—maximum optical input power (average)	-8 dBm	-14 dBm

STM-1 Multi-Mode and Single-Mode Modules

The STM-1 Multi-Mode (MM) and Single-Mode (SM) modules provide a fiber optic interface operating in the concatenated mode of the SONET-defined line rate of 155 Mbps. The interface on the STM-1 Single-Mode module is intended for long-reach applications, typically between LANs. This module is frequently used to connect high-speed LAN products (routers and so on) to the ATM network.

These modules are available in two variations, which differ according to the firmware installed on the circuit boards.

- One variation for both the Multi-Mode and Single-Mode types, with the names STM-1 MM AQ module and STM-1 SM AQ module, uses the *AQueMan*™ algorithm for flow control.
- The other variation for both the Multi-Mode and Single-Mode types, with the names STM-1 MM TS module and STM-1 SM TS module, uses traffic shaping for flow control.

Software Features

The software also supports the following ATM Forum Technical Committee Specifications:

- *User to Network Interface Version 3.0*
- *User to Network Interface Version 3.1*
- *Integrated Local Management Interface Specification Version 4.0, af-ilmi-0065.000*

- *Interim Inter-Switch Signaling Protocol, af-pnni-0026.000*
- *Private Network-Network Interface (PNNI), af-pnni-0055.000*

Protocols:

- Traffic management:
  - *AQueMan*™ algorithm (for traffic flow control)
  - AAL-5 (traffic shaping)
  - 10 quality of service (Qos) levels:
    - Constant bit rate level 1 (CBR-1), CBR-2, CBR-3, and CBR-4
    - Variable bit rate (VBR): VBR real time level 1 (VBR-RT1), VBR real time level 2 (VBR-RT2), VBR non-real time level 1 (VBR-NRT1), VBR non-real time level 2 (VBR-NRT2), VBR-express
    - Unspecified bit rate (UBR)

Hardware Features

All STM-1 Multi-Mode and Single-Mode modules have the following hardware features:

Table 3-8. STM-1 Multi-Mode and Single-Mode Hardware Specifications

Feature	Module	
	STM-1 SM	**STM-1 MM**
Number of ports	1	1
Type of connector (two for each module — transmit and receive)	SC	ST
Type of fiber-optic cable	single-mode	multi-mode
Fiber-optic cable reach (approximate, depending on fiber makeup)	25.7 km (16 miles)	2 km (6,560 feet or 1.2 miles)
Line rate	155 Mbps	155 Mbps
Optical wavelength (nominal value)	1,300 nm	1,330 nm
• System gain	15 dB	13.5 dB
• Transmitter — minimum optical output power (average)	-15 dBm	-19 dBm
• Transmitter — maximum optical output power (average)	-8 dBm	-14 dBm

Table 3-8. STM-1 Multi-Mode and Single-Mode Hardware Specifications

Feature	Module	
	STM-1 SM	STM-1 MM
• Receiver — minimum optical input power (average)	-31 dBm	-32.5 dBm
• Receiver — maximum optical input power (average)	-8 dBm	-14 dBm

Server Modules

DSP2 Voice Server Module

The DSP2C Voice Server components process voice and other digital data on a *PacketStar*™ Access Concentrator system). The modules have two internal logical ports: one to receive and transmit unprocessed voice data; the other to receive and transmit processed voice data. All three modules have two types of LED indicators: FAIL and ACTIVE.

The module processes circuit emulation voice traffic entering the chassis and applies all of the following features: voice compression, echo cancellation, silence suppression, and comfort noise. The module provides these features in conjunction with the channelized CES modules, across the entire *PacketStar*™ Access Concentrator product line: the PSAX 1250, PSAX 2300, PSAX 20, AC 30, and AC 60.

The DSP2C Voice Server module has been enhanced with expanded capabilities, combining the features of earlier voice server products on a single module. Based on improved hardware components that permit better performance, the revamped DSP2C will support both ADPCM and CS-ACELP voice compression for 128 channels.

With Release 6.3, this module now offers support for AAL2 SVC connections and AAL2 PVC multiplexing for reduced call latency. The module also monitors the presence of facsimile or model information. The module continues to support G.168 echo cancellation (64 msec and 128 msec tails), and a 224-channel echo-cancellation-only mode. The doubled channel capacity for CS-ACELP compression, longer tails for G.168 echo cancellation, and AAL2 multiplexing overcome previous performance limitations and position the DSP2C as the powerful centerpiece of the Lucent voice traffic over ATM (VToA) solution.

Existing features that remain supported include silence suppression with comfort noise, PCM code conversion, and caller ID. DSP2A and DSP2B single mode modules cannot be upgraded with System Software Release 6.3, because they lack hardware capacity.

Release 6.3.0 offers the user these new features on the DSP2C Voice Server:

- Soft permanent virtual circuit (SPVC) support for circuit emulation service (CES). SPVC connections can be used for voice traffic on all modes of the DSP2C Voice Server (A, B, and Echo Cancellation mode). This feature allows up to 247 connections per trunk, with these restrictions:
  - ~ For voice transmissions over an SPVC connection to be successful, the DSP2C at startpoint and endpoint of the SPVC must be configured with the same values for all Voice Server features.
  - ~ SPVCs using voice processing features must be configured as non-multiplexed.
- AAL2 multiplexing. The user can now multiplex up to 128 connections on DSP2A mode or DSP2B mode, in up to 32 trunk groups; for echo cancellation, the user can multiplex up to 224 connections in up to 32 trunk groups.

Software Features

Table 3-9 below summarizes the three modes and their features available on the DSP2C Voice Server module in multiplexed and non-multiplexed AAL-2.

Table 3-9. Matrix of Features and Standards Supported on the DSP2C Modes A, B and Echo Cancellation

Release 6.3.0	DSP2C Non-Multiplexed AAL2 (Non-Mux-Aal2)			DSP2C Standard AAL2		
	DSP2A	DSP2B	Echo Cancel Mode	DSP2A	DSP2B	Echo Cancel Mode
Channels	128		224	128		224
Voice Compression	G.726	G.729A	None	G.726	G.729A	None
Silence Suppression	Lucent	G.729B	N/A	Lucent	G.729AB	N/A
Comfort Noise	Lucent	G.729B	N/A	Lucent	G.729AB	N/A
Echo Cancellation (near end)	G.165 G.168	G.165 G.168	G.168	G.165 G.168	G.165 G.168	G.168
Echo Cancellation Tails Supported	Up to 64 msec	Up to 64 msec	Up to 128 msec	Up to 64 msec	Up to 64 msec	Up to 128 msec
DTMF Digit Collection /Regeneration	Not Applicable	Supported	Not Applicable	Supported for 16 and 24 Kbps	Supported for 8 Kbps only	Not Applicable

Table 3-9. Matrix of Features and Standards Supported on the DSP2C Modes A, B and Echo Cancellation

Release 6.3.0	DSP2C Non-Multiplexed AAL2 (Non-Mux-Aal2)			DSP2C Standard AAL2		
	DSP2A	DSP2B	Echo Cancel Mode	DSP2A	DSP2B	Echo Cancel Mode
Dynamic Bandwidth Circuit Emulation Service (DBCES) Functionality	Supported	Supported	Supported	N/A	N/A	N/A
Caller ID	Supported	Supported	N/A	N/A	N/A	N/A
DSP Failure Alarm/Reboot Functionality	Supported	Supported	Supported	Supported	Supported	Supported
Dynamic DSP Resource Allocation	Supported	Supported	Supported	N/A	N/A	N/A
Fax/modem Bypass of Compression and Echo Cancellation	Supported	Supported	N/A	N/A	N/A	N/A
Fax Modulation/ Demodulation	N/A	N/A	N/A	TBD	TBD	N/A
Permanent Virtual Circuits (CE-to-CE)	Supported	Supported	Supported	Not Supported	Not Supported	Not Supported
Permanent Virtual Circuits (CE-to-ATM)	Supported	Supported	Supported	Supported	Supported	Supported
Soft Permanent Virtual Circuit (SPVC)	Supported	Supported	Supported	Not Supported	Not Supported	Not Supported
DSP A/B/C Mode Hybrid Configurations on DSP2C Module	Supported	Supported	Supported	Supported	Supported	Supported
Mu-law/A-law-PCM Code Conversion	Supports ITU-T G.711	Supports ITU-T G.711	Supports ITU-T G.711	Supports ITU-T G.711	Supports ITU-T G.711	Supports ITU-T G.711

DSP2C Voice Server Features

Multiplexed or Nonmultiplexed AAL-2

The choice of multiplexed ATM Adaptation Layer 2 (AAL-2) has been added. As the capacity of the DSP2C is 32 DSPs, up to 32 trunk groups can be configured for multiplexing. Lucent recommends multiplexing voice and

data channels to reduce delay. AAL-2 implementation is based on ITU-T Standards G.363, G.366.1, and G.366.2.

In nonmultiplexed voice and data processing, the payload length is a fixed value of 40 bytes, which results in a dramatic reduction of latency (40 msec end-to-end delay on the DSP2A, 60 msec end-to-end delay on the DSP2B, and 22 msec end-to-end delay on DSP2C-Echo Canceler). See Appendix C in this user guide for a comparison of standard AAL-2 and nonmultiplexed AAL-2 cells per second (cps) at each compression rate.

Dynamic DSP Resource Allocation

If a DSP fails on a DSP2A or DSP2B module, the connection admission control (CAC) in the primary CPU will reassign the connections passing through it to another DSP, if available. It will also move all the connections from an entire module, should it fail, to another DSP2 module, if available. The only restriction preventing re-routing is if compatibly configured DSP resources are not available. (For example, a connection configured for G.168 echo cancellaton will not re-route to a DSP configured for G.165 echo cancellation.)

Caller ID/Flash Hook Signalling

Caller ID frequency shift keying (FSK) information is transmitted between the first and second ring. This is valid when the called party is on-hook. Flash signals are transmitted over flash signaling-capable trunks to initiate internal calling features (i.e., Caller ID, call forwarding). As with FSK, the transmission of flash signalling is only valid when the called end of a line is off-hook. Flash signalling consists of signalling transitions from off-hook to on-hook to off-hook, where the on-hook state last between 300 msec and 1000 msec. This feature is compliant with TIA/EIA-464-B Requirements for Private Branch Exchange (PBX) Switching Equipment.

The DSP2A, DSP2B and DSP2C modules offer limited support to the Caller ID feature, but only with a specialized configuration setup with the Enhanced DS1 Module. See *"*PacketStar™ *PSAX Access Concentrator Caller ID Application Note"* (Document No. 255-700-006) for instructions on configuration.

Hybrid A, B and C Mode Configurations

You may configure the 32 interfaces on the module in any combination of A, B, or echo cancellation modes that you need.

Previous Version Compatibility

With software releases 6.2.0 and subsequent, modules DSP2A, DSP2B, and DSP2C will re-route connections made to failed DSPs. For modules previous to release 6.2.0, the DSP2A and DSP2B onboard processor cannot detect chip failures. The CPU can route connections that require DSP resources only if compatible DSP resources are available. For example, a connection configured for G.168 echo cancellation will not re-route to a DSP configured for G.165 echo cancellation.

Soft Permanent Virtual Circuit Support

With Release 6.3.0, the DSP2C can offer its voice and data processing capabilities in an SPVC over PNNI, ATM UNI, or IISP link.Up to 247 connections are configurable on a CE-to-ATM VCC PVC connection. See Chapter 7 of the DSP2A, DSP2B, and DSP2C Module User Guide for instructions and configuration restrictions.

Voice Processing

The component can perform the following types of voice processing:

- Near-end echo cancellation only (G.165 and G.168 on DSP2A mode and DSP2B mode; G.168 in echo cancellation mode)
- Facsimile (fax)/modem call sequence detection
- Voice compression and decompression, G.726 (DSP2A mode) and G.729 (DSP2B mode)

Silence Suppression Comfort Noise

The silence suppression feature implemented on the DSP2A and DSP2B components inhibits transmission of cells across the ATM link to save bandwidth when no voice activity is detected. Silence suppression saves bandwidth when there is no voice activity, and improves the user's comfort by generating comfort noise when the line is silent. When there is no voice activity, the comfort noise feature samples the background noise and sends a few cells across the ATM link. These cells are fed into a white noise generator on the far end. The far end regenerates the background noise so that the user knows the connection is still active. The background noise level is updated every 5 seconds provided the background noise does not change. If the background does change, there is an activity burst and the background noise level is updated every 20 msec, until a steady state condition occurs again.

DSP2A and DSP2B Single-Mode Voice Server Modules (System Release 6.2.0)

▲ CAUTION:
The DSP2A and DSP2B Single-Mode Modules are not upgradable to System Software Release 6.3.0.

See Table 3-10 for a summary of DSP2A and DSP2B Single-Mode Voice Server Module features.

Table 3-10. Matrix of Features and Standards Supported on the Single-Mode DSP2A and DSP2B Voice Server Module (Release 6.2.0)

Release 6.2.0	Single Mode Modules	
	DSP2A	DSP2B
Channels	128	128
Voice Compression	G.726	G.729A
Silence Suppression	Lucent	G.729B
Comfort Noise	Lucent	G.729B
Non-Multiplexed AAL-2	Supported	Supported
Echo Cancellation (near end)	G.165 G.168	G.165 G.168
Echo Cancellation Tails Supported	Up to 32 msec	Up to 32 msec
DTMF Digit Collection /Regeneration	Not Applicable	Supported

Table 3-10. Matrix of Features and Standards Supported on the Single-Mode DSP2A and DSP2B Voice Server Module (Release 6.2.0)

Release 6.2.0	Single Mode Modules	
	DSP2A	DSP2B
Dynamic Bandwidth Circuit Emulation Service (DBCES) Functionality	Supported	Supported
Caller ID	Supported	Supported
DSP Failure Alarm/Reboot Functionality	Supported	Supported
Dynamic DSP Resource Allocation	Supported	Supported
Fax/modem Bypass of Compression and Echo Cancellation	Supported	Supported
Fax Modulation/ Demodulation	Not Applicable	Not Applicable
Soft Permanent Virtual Circuit (SPVC) Support	Not Supported	Not Supported
DSP A/B/C Mode Hybrid Configurations on DSP2C Module	Not Applicable	Not Applicable
Mu-law/A-lawPCM Code Conversion	Supports ITU-T G.711	Supports ITU-T G.711

Outstanding differences between the single-mode DSP2A and DSP2B modules and the DSP2C module include:

- On the DSP2A and DSP2B single-mode modules, the number of tails supported in echo cancellation is 32 msec fewer than in DSP2C mode in Table 3-10.
- In the DSP2B single-mode, the number of channels supported is 32 fewer than in DSP2C mode.
- The DSP2A and DSP2B modes do not offer AAL-2 multiplexing, SPVC support, or hybrid A, B or Echo Cancellation configurations.

Hardware Features

Any number of DSP2A, DSP2B and DSP2C Voice Server components can be supported per chassis. These components are connected to the CPU, I/O modules, and other components by a backplane connection.

Route Server Module

The Route Server module supports IP virtual private networks (VPNs). Each VPN supports routing information protocol (RIP) and can be assigned to multiple IP network interfaces and static routes. The module can interact with any other Access Concentrator module port that is configured for frame

relay, bridge, routing, or asynchronous transfer mode (ATM). All traffic on the Route Server module runs through IP in compliance with media access control (MAC) encapsulation:

- IP over ATM (RFC 1483)
- IP over frame relay (RFC 1490)
- IP over Ethernet

The module can be configured through either the Access Concentrator system console or through simple network management protocol (SNMP). Each Access Concentrator system may support multiple Route Server modules, but multiple Route Server modules cannot be configured for hot standby redundancy purposes.

Software Release 6.3.0 introduces routing information protocol (RIP) Version 2 to the Route Server module. The module now supports Internet Protocol virtual private networks (VPNs) by assigning multiple IP network interfaces and static routes. (The Route Server module also supports RIP v1.0, and can interact with any other Access Concentrator module port that is configured for frame relay, Ethernet bridging, or ATM.)

Release 6.3.0 software, supporting RIP v2.0, allows you to divide networks to a further extent than the traditional subnet classes (Class A, B, and C) available with RIP v1.0. RIP v2.0 enables authentication and multicasting, and allows you to run different masks on different subnets. Rip v2.0 can be either active or passive.

You can assign an authentication password to an IP network interface for maximum security. Doing so can prevent those who cannot directly access the network from sending false routing information to the routers. RIP v1.0 messages will be ignored when authentication is in use. However, authentication does not prevent RIP v1.0 routers from viewing RIP v2.0 messages. To prevent RIP v1.0 routers from viewing RIP v2.0 messages, you must use multicasting.

Multicasting reduces load on hosts not using RIP v2.0 messages. Multicasting also allows RIP v2.0 routers to share information that RIP v1.0 routers cannot access. Available bandwidth becomes the tiebreaker in calculating routes using default parameters for both IISP and PNNI routing.

Software Features

The software supports the following Frame Relay Forum (FRF) Implementation Agreements:

  - FRF.5—Frame Relay/ATM PVC Network Interworking
  - FRF.8—Frame Relay/ATM PVC Service Interworking
- Interfaces: IP over ATM (IETF RFC 1483), IP over frame relay (IETF RFC 1490), IP over Ethernet (bridge)
- Multi-service routing:
  - ICMP (RFC 792)
  - Static routing with six independent VPNs
  - IP routing

- Frame relay (FRF.5, FRF.8)
- ATM

Hardware Features

Forwarding speeds (measured in packets per second):

- 64-byte IP packet size: 22K pps (11.3 Mbps)
- 256-byte IP packet size: 16K pps (32.8 Mbps)
- 1518-byte IP packet size: 4.6K pps (55.8 Mbps)

Tones and Announcements Server Module

The Tones and Announcements Server (TAS) module offers these tests in a switch-to-switch capacity:

- SS7 (Signaling System 7) continuity test for VToA
- 1004 Hz (miliwatt) test tone support (Type 102)
- Digital, non-inverting loopback (Type 108)
- Automatic Transmisson measurement(Type 105)

These tests enable PSAX products to provide tones and signaling testing on voice equipment in the customer's premises, such as PBXs. Designed for use between central office products, such as the PSAX 2300 and the PSAX 1250, and edge devices such as the AC 60 and the PSAX 20, the module offers call routing information to a connection gateway without using an expensive circuit switch. Up to 128 circuits can be tested simultaneously using the TAS Server Module.

The SS7 Continuity Test enables PSAX products to be deployed with other applications in connection gateways involving hand-offs to ILECs which require the quality assurance of conducting the continuity test from the circuit switch.

The test features work in conjunction with the Enhanced DS1, the Enhanced E1, the High-Density E1/DS1, the Channelized DS3/STS-1e, the CPU module, and a Connection Gateway Application Programming Interface (API).

Hardware Features

The hardware of the Tones and Announcments Server is the same as the DSP2C Voice Server Module, with TAS firmware and boot loader. All modules connect to the CPU and other modules by a backplane connection.

Any number of TAS modules are supported by the *PacketStar*™ PSAX 1250 and 2300 Access Concentrators. A TAS module can be placed in any available slot on the PSAX 1250, 2300, and AC 20 and 60.

4 Configuring the Basic System

Overview of This Chapter

This chapter describes how to configure the PSAX 20 Access Concentrator system and set the system values for your site. Before you do this, be sure you have done the following tasks as described in the *PacketStar™PSAX 20 Access Concentrator Installation and Operation Guide*:

- Installed the system hardware components
- Applied power to the system

For procedures to configure the I/O and server modules, see the appropriate PacketStar™ module user's guide.

The PSAX 20 system is designed for continuous operation after power is applied.

Telnet sessions are supported on the Ethernet interface. Both the telnet session on the Ethernet interface and the console session provide a console interface for VT100 terminal emulation. See Chapter 6, "Using VT100 Terminal Emulation," for information on configuring this application.

Logging onto the System

Before beginning the following procedure, be sure that your cabling on the CONSOLE and ETHERNET ports on the chassis faceplate is connected properly (see the *PacketStar™PSAX 20 Access Concentrator Installation and Operation Guide*). To log onto the PSAX 20 system, perform the following steps.

Logging onto the PSAX 20 System

Begin

1. Configure your VT100 terminal emulator (see Chapter 6, "Using VT100 Terminal Emulation).
2. To start the console session, press Enter.

The PSAX 20 Logon window is displayed (see Figure 4-1). i

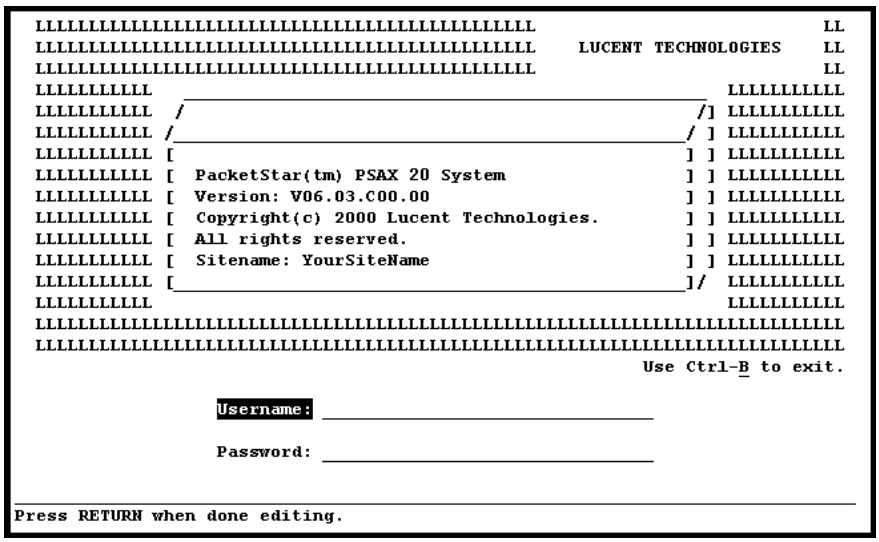

Figure 4-1. PSAX 20 ATM Access Concentrator System Logon Window

3 In the **Username** field, type one of the following values, and press Enter:

- **readwrite** if you want to view and change all configuration options
- **readonly** if you want to view configuration options without the ability to change them

4 In the **Password** field, type one of the following values, and press Enter:

- **lucenttech1** (default value) if you entered **readwrite** in the **Username** field
- **lucenttech2** (default value) if you entered **readonly** in the **Username** field

The Console Interface Main Menu window is displayed (see Figure 4-2).

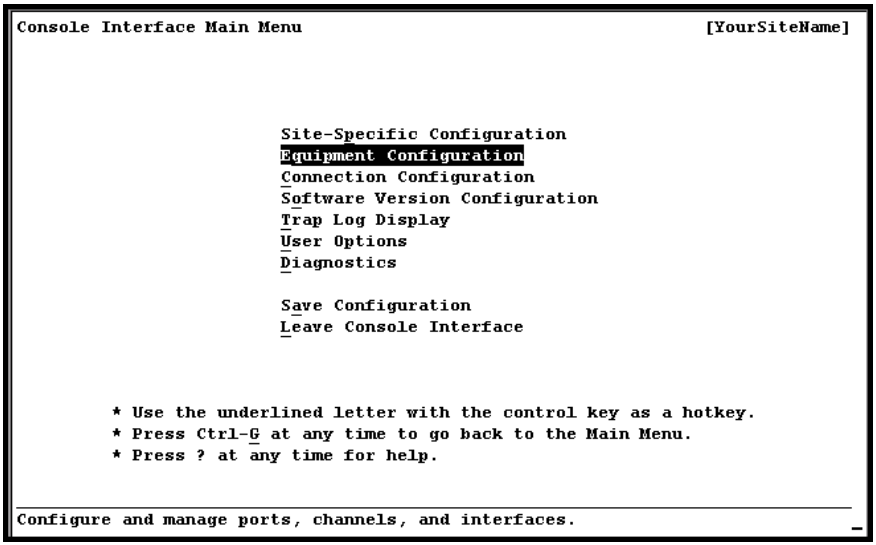

Figure 4-2. Console Interface Main Menu Window (Site-Specific Configuration Selected)

End

At the time of initial configuration, the Console Interface Main Menu window is displayed a field with a pair of opposing square brackets in the upper right corner. This field contains the site name, which you enter during site-specific configuration (see the procedure in "Configuring System Identification" on page 4-12).

Help Information

The Help windows are accessible from any window in the Access Concentrator system console interface. To access the Help windows, press the Question Mark (?) key on any window. In addition to the Help windows, the Console Interface windows have contextual help displayed in the information line at the bottom of each window. Contextual help provides information about the command or field currently highlighted on that window. The information line also is displayed error codes and responses to commands. All responses and notifications are recorded in a trap log. (See Appendix A, "SNMP Trap Messages," for details on displaying the trap log and explanations of the messages).

To view the Help windows from the Console Interface Main Menu window, perform the steps in the following procedure.

Viewing the Help Windows

Begin

1 On the Console Interface Main Menu window, press the **?** key. The first Main Menu Help window is displayed (see Figure 4-3):

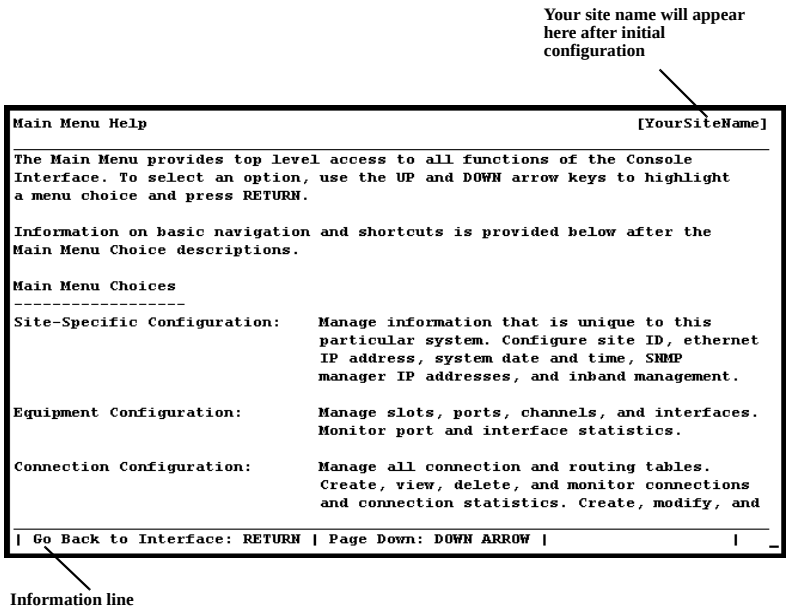

Figure 4-3. Main Menu Help Window

2 To display the second through fourth Main Menu Help windows (see Figure 4-4 through Figure 4-6), press the Down Arrow.

```
Main Menu Help                                                [YourSiteName]
_____________________________________________________________________________

                                delete routing table entries.

Software Version Configuration: Perform software upgrades and firmware
                                downloads.

Event Management:               Configure event manager filters or display
                                event logs.

Trap Log Display:               Scroll through and search the history of SNMP
                                network traps generated by this system.

User Options:                   Manage user specific options. Change password,
                                turn trap display on/off, turn bell on/off,
                                change timeout value, change alternate
                                navigation keys.
Diagnostics:   Diagnostics tools for the system and system
    usage information, such as cell test, unlock
    remote shell, remote reboot hardware
    components, or exit to command prompt.


_____________________________________________________________________________
| Go Back to Interface: RETURN | Page Down: DOWN ARROW | Page Up: UP ARROW |
```

Figure 4-4. Main Menu Help Window 2

```
Main Menu Help                                                [YourSiteName]
_____________________________________________________________________________

Save Configuration:             Permanently save the current system
                                configuration to disk. The configuration can
                                then be restored after a loss of power.

Leave Console Interface: Log out of the Console Interface.

Basic Navigation
-----------------
Move from field to field..............  UP, DOWN, LEFT, or RIGHT ARROW KEYS
Select a menu option..................  RETURN
Edit a field..........................  RETURN
Stop editing a field..................  RETURN, UP ARROW, or DOWN ARROW
Cycle forward through an options list...  RETURN
Cycle backward through an options list..  BACKSPACE or Ctrl-H
When the arrow keys won't work..........  K=UP, J=DOWN, H=LEFT, L=RIGHT
                                          (or user defined under User Options)
Shortcuts and Hotkeys
----------------------
Redraw the screen display anytime.......  Ctrl-R

_____________________________________________________________________________
| Go Back to Interface: RETURN | Page Down: DOWN ARROW | Page Up: UP ARROW |
```

Figure 4-5. Main Menu Help Window 3

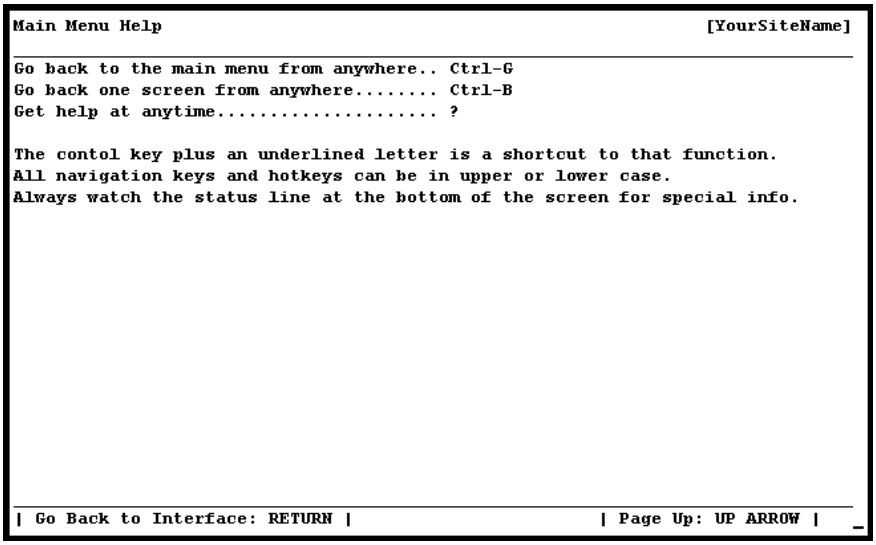

Figure 4-6. Main Menu Help Window 4

End

Selecting Options, Fields, and Commands

As described on the Help windows, follow these steps to select an option, field, or command:

1. Press the Up Arrow or the Down Arrow to highlight (reverse video image) the option name, field name, or command you want to select, and press Enter.

   ~ Or, to quickly select a command, simultaneously press Ctrl and the letter underlined in the command.

   The system responds as follows:

- For a selected option name, the window corresponding to the option name displays.
- For a selected field, the following variations occur:
  - ~ The field entry area appears blank or contains the previously entered value. You can now enter or change data in this field.
  - ~ The field entry area, like the field name, appears in reverse video image and contains a predefined set of values, which you can view by pressing Enter to cycle through these values.
- For a selected command, the following variations occur:

- ~ The information line displays a message indicating an error or successful completion of the command.
- ~ The system displays the next higher level or previous window (**Enter to <window name>**).
- ~ The system displays the next lower level or succeeding window (**<window name>**).

The following tips will also help you:

- Read-only fields, which you cannot change, are enclosed in square brackets (example: **[LineStatus]**).
- Press **Ctrl+B** on any window to to move back to the previous window.
- Press **Ctrl+G** on any window to return to the Main Menu window.

Changing the System Password and Other User Options

When initially configuring the system, you should change the initial default password (**lucenttech1**) and the default SNMP community string name (**public**) to ones of your choosing. You can change the password and SNMP community string name at any time, as needed.

▲ CAUTION:
For optimum system security, we highly recommend that you change the password and the SNMP community string name from their initial default values.

To change the system password, perform the following procedure.

Changing the System Password

Begin

1. On the Console Interface Main Menu window, select the **User Options** command.

The User Options window is displayed (see Figure 4-7).

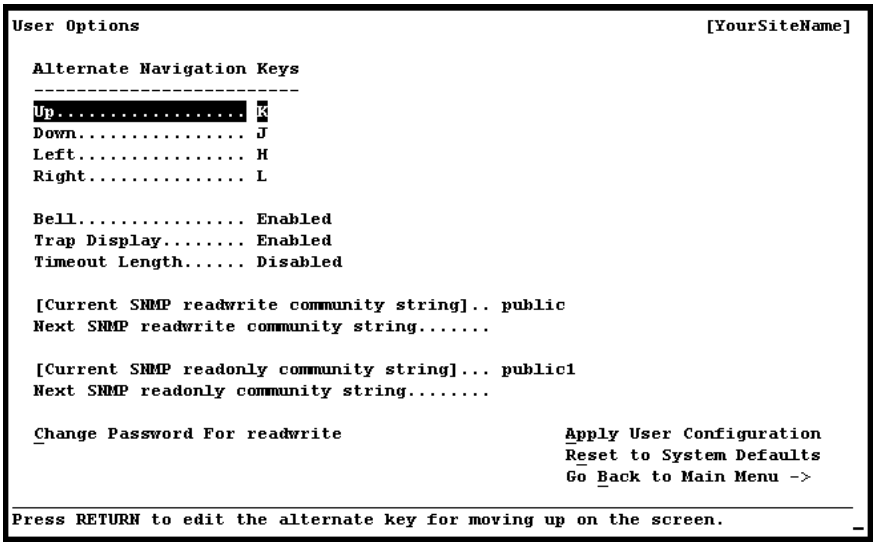

Figure 4-7. User Options Window

2 Select the **Change Password For <***username***>** field.

   a. As prompted on the window, type the current password, and press Enter.

   b. Type a new password that is at least 8 characters long, and press Enter.

   c. Retype the new password, and press Enter to confirm it.

3 To change your community name. select the **Next SNMP community string** field. Type a new string name that is a maximum of 53 characters long, and press Enter (the default strings are **public** and **private**).

Note: This step is optional.

The **[Current SNMP community string]** field is displayed the new name you just entered. This field is used as an authentication password to have an SNMP request honored.

4 Select the **Apply User Configuration** command, and press Enter.

5 To permanently save these values, press **Ctrl+G** to return to the Console Interface Main Menu window.

6 On the Console Interface Main Menu window, select the **Save Configuration** command, and press Enter to store the values in the PSAX system database. The new values will take effect after the chassis reboots.

End

Console Interface Main Menu

The Console Interface Main Menu window includes the following options:

- Site-Specific Configuration
- Equipment Configuration
- Connection Configuration (see the appropriate *PacketStar™ Module User Guide*)
- Software Version Configuration (see Chapter 7, "Upgrading and Backing Up System Software")
- Trap Log Display (see Appendix A, "SNMP Trap Messages")
- User Options (see Chapter 5, "Using System Diagnostics")
- Diagnostics (see Chapter 5, "Using System Diagnostics")
- Save Configuration
- Leave Console Interface

Configuring the System for Your Site

Before proceeding with the site configuration, you must first determine the actual values you use for the following configuration identifiers:

- Site name
- Site identifier
- Switch master IP address
- Ethernet mask address
- Gateway address
- IP addresses of remote network managers configured to receive SNMP traps

To configure your system, perform the steps in the following procedure.

System Identification Data

Configuring System Values for Your Site

Begin

1 On the Console Interface Main Menu window, select the **Site-Specific Configuration** command.

The Site-Specific Menu window is displayed (see Figure 4-8).

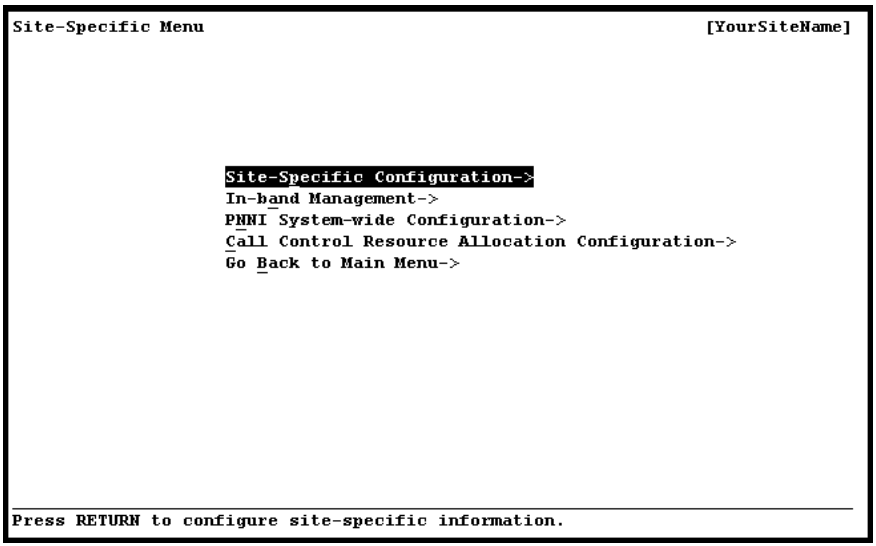

Figure 4-8. Site-Specific Menu Window

2 On the Site Specific Menu window, select the **Site-Specific Configuration** command.

The Site-Specific Configuration window is displayed (see Figure 4-9).

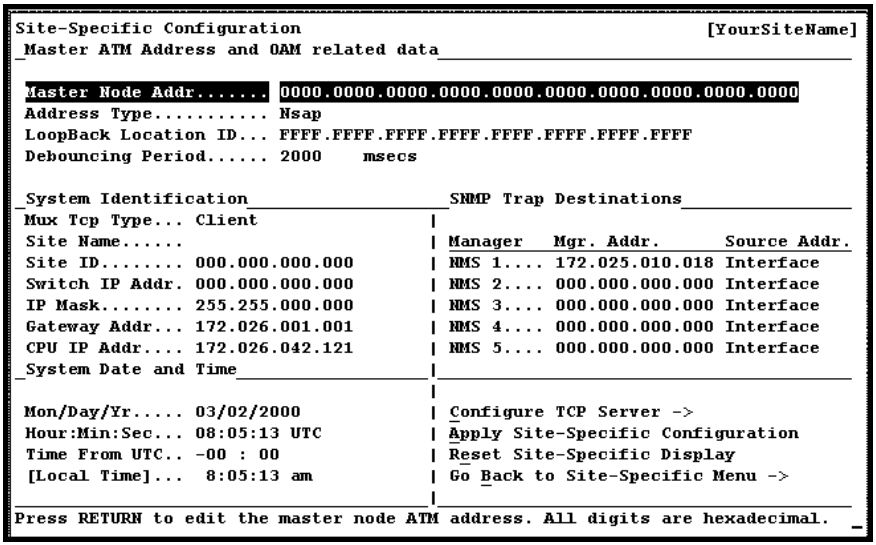

Figure 4-9. Site-Specific Configuration Window

Note: The system performs error checking on each field by highlighting any field containing an incorrect value. Use the system message displayed in the information line to help you correct any errors.

Commands

Command	Function
• Configure TCP Server	Displays the TCP Server Configuration window.
• Apply Site-Specific Configuration	Applies the values you enter in the this window.
• Reset Site-Specific Configuration	Sets the values in this window the last saved (applied) set of values.
• Go Back to Site-Specific Menu→	Redisplays the Site-Specific Menu window.

Rules for Configuring IP Addresses

Use the following rules when configuring the CPU IP address, switch IP address, and in-band IP address on the Site-Specific Configuration window:

1. The CPU IP address is always necessary. However, you should enter the switch IP address only in a redundant system.
2. CPU IP and switch IP addresses cannot be the same.

3. CPU IP and switch IP addresses cannot be on the same subnet as the in-band IP address.
4. CPU IP, switch IP, and in-band IP addresses may each be zero, but CPU IP and Switch IP addresses cannot both be zero (see Number 2 above).

Note: If the CPU IP address is zero and the **ssid** file on the CPU module is corrupted, the system cannot access the Ethernet.

5. If non-zero, then the CPU IP, switch IP, and in-band IP addresses have to be valid IP addresses.
6. If the switch IP address is not zero, then the system will respond to the Switch IP address; otherwise, the system will respond to the CPU IP address on the Ethernet port.
7. In a redundant system, both CPU modules must have a unique CPU IP address; they will have the same switch IP address and in-band IP address if either address is defined.

Rules for Configuring IP Address Masks

Use the following rules when configuring the CPU IP address and switch IP address on the Site-Specific Configuration window:

1. The CPU IP address and switch IP address share the same IP mask.
2. The CPU IP address (or switch IP address) and in-band IP address masks are independent of each other, as long as the CPU IP address (or switch IP address) and in-band IP address are in different networks.
3. If the CPU IP address (or switch IP address) and in-band IP address are in the same network, then their masks must be the same.
4. The CPU IP address (or switch IP address) and the in-band IP address are in the same subnet if the CPU IP address mask (or switch IP address mask) is the same as the in-band IP address, **and** if the CPU IP address (or switch IP address) masked out result is the same as the in-band IP address masked-out result.
5. The CPU IP address and switch IP address must always be on a different network from the in-band IP address (see Number 3 of the previous section).

Configuring System Identification

ATM Addresses and OAM Properties

The Master ATM Address and OAM related data panel allows you to enter and display information about the Master ATM address, the loopback, and OAM debouncing period.

Entering and Displaying ATM Addresses and OAM Properties

Perform the steps in the following procedure to configure the loopback parameters on modules that support loopback configuration.

Viewing OAM Properties

Begin

1 Select the values for the fields in the Master ATM Address and OAM related data panel as described in Table 4-1.

Table 4-1. Field Values for Master ATM Address and OAM Related Data Panel

Field	Description
Master Node Addr	Enter the master node address to where the traps will be sent (10 octets).
Address Type	Select an address type from the pull-down menu: **Nsap, E164**, or **E164nsap.**
Loopback Location ID	Enter the unique identifier of the ATM node where the loopback is to occur (8 octets). **Loopback Location ID** is the location identifier of the local switch. It is used as "Source Location Id" in all the outgoing OAM loopback cells and will be compared with the "Destination Location Id" of a received OAM loopback cell to decide if the received OAM loopback cell should be looped back by this switch or not. You must enter a unique value in the **Loopback Location ID** field to perform OAM loopback tests. (For more information about OAM loopback tests, see Chapter 5, "Using System Diagnostics.")
Debouncing Period	Enter a value between **1000** and **300000** (default value is **2000**). This field is used in OAM; it is the maximum time (in milliseconds) for clearing OAM AIS and RDI alarms.

2 Select the **Apply Site-Specific Configuration** command and press Enter.

3 To return to the Console Interface Main Menu window, press **Ctrl+B**.

End

Entering the System Identification

Begin

To set the system identification for your site, select the values for the fields on the **System Identification** panel on the Site-Specific Configuration window as described in Table 4-2.

Table 4-2. Field Values for the System Identification Panel

Field	Description
Mux Tcp Type	Select **Client** to configure the PSAX 20 as the client device. Select **Server** to configure the PSAX 20 as the server device. The **Mux Tcp Type** field is used for the TCP connection between the PSAX 20 and the connection gateway for messages of the Connection Gateway API. The **Mux Tcp Type** field indicates whether the PSAX 20 is a server device or a client device when the TCP connection is established. If the PSAX 20 is designated as the server, the connection gateway establishes the connection to the PSAX 20. If the PSAX 20 is designated as the client, the PSAX 20 establishes the connection to the connection gateway.
Site Name	Enter a site name with no more than 53 characters: • A valid site name starts with an alphanumeric character • A valid site name is a consecutive string which can have the following types of characters: alphanumeric, -, and _ • Do not use any spaces or periods
Site ID	Select the **Site ID** field, and type the value you have already determined. The Site ID number has four subnets, each containing a 3-digit number not to exceed 255 (for example, 123.087.232.003). The site ID is used to identify the system for future ATM routing, remote management, and in-band management.

Table 4-2. Field Values for the System Identification Panel

Switch IP Addr	Select the **Switch IP Addr** field, and type the IP address value you have already determined. The PSAX 20 system, that can accommodate only one CPU per chassis, does not have redundancy. This field cannot be used.
IP Mask	Type the IP mask for ethernet access to your site. This field is used to determine which part of the IP address is the network identifier; shows the network's subnet mask.
Gateway Addr	Enter the IP address for local gateway access to your site. Displays the IP address of the gateway the PSAX system should use to access other networks. Leave this field blank if you are not using a router.
CPU IP Addr (display only)	Displays the IP address of the active CPU for the PSAX 20.

4 Select the **Apply Site-Specific Configuration** command, and either press Enter to save these values now, or after you have entered data in all the fields on this window.

End

Configuring System Date and Time

System Date and Time Data

Entering the System Date and Time

Begin

To set the date and time for your PSAX 20, select the values for the fields on the **System Date and Time** panel on the Site-Specific Configuration window as described in Table 4-3.

Table 4-3. Field Values for the System Date and Time Panel

Field	Description
Mon/Day/Yr	Enter the current date in the format shown here: *mm/dd/yyyy* (2-digit values for the month and the day, and a 4-digit value for the year). Displays the current date in month (*mm*), day (*dd*), and year (*yyyy*).
Hour: Min:Sec UTC	Enter the current time in Universal Time Coordinated (UTC) format, also known as Greenwich Mean Time (GMT).
Time from UTC	Sets local time display by adding or subtracting hours and minutes from the UTC. **Note:** Both negative and positive hourly time selections are available. The time selected represents the difference between your local time and the UTC. **Note:** Select **00** for all countries except those whose time zones operate at intervals 30 minutes ahead (and behind) all others. For these locations, select **30**. Press Enter to cycle through the predefined set of values and select a value, according to your local time custom.
[Local Time] (display only)	Displays local time of the PSAX system. **Note:**

5 Select the **Apply Site-Specific Configuration** command, and either press Enter to save these values now, or wait until you have entered data in all the fields on this window.

Note: The local time is automatically calculated and displayed in the **[Local Time]** field after you apply the values. The local time is calculated based on the values in the **Hour:Min:Sec** field and the selected value in the **Time From UTC** field.

End

Configuring the TCP Client/Server for a Connection Gateway

If you are using the Connection Gateway API with your *PacketStar* PSAX 20 system, you need to configure the system as either a transmission control protocol (TCP) client or as a TCP server. If you set up the connection gateway (CG) device as a TCP server, you can connect multiple PSAX 20 systems as TCP clients (see Figure 4-10)

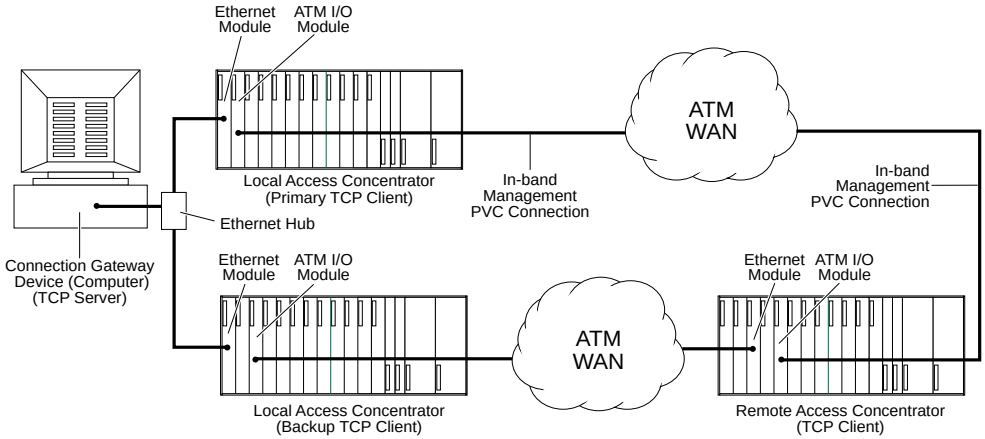

Figure 4-10. *PacketStar*™ PSAX 20 as a TCP Client

You can also set up the PSAX 20 system as a TCP server with the CG device as the client. As an option, you can connect two CG devices (clients), set up as primary and backup CG devices, to the PSAX 20 system (server) (see Figure 4-11).

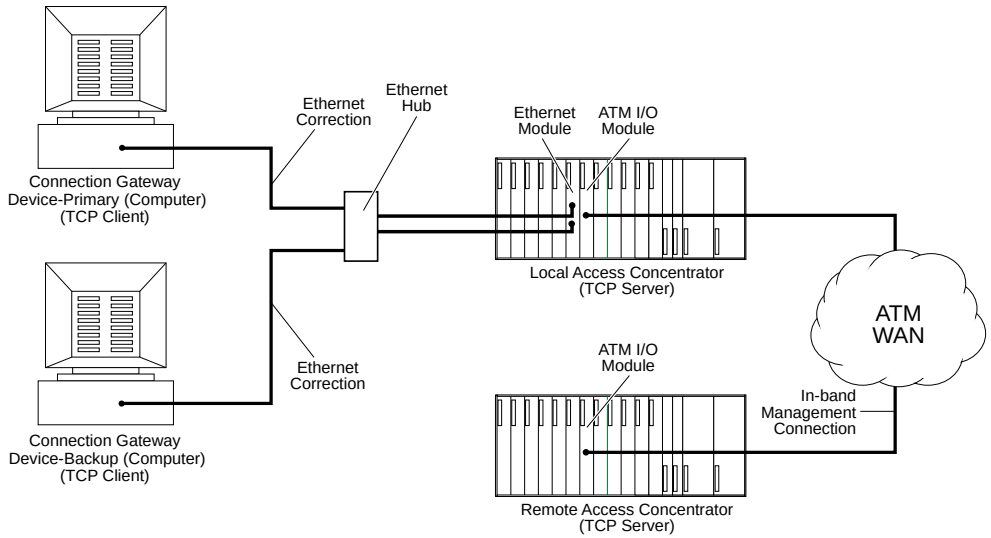

Figure 4-11. *PacketStar*™ PSAX 20 as a TCP Server

Connection Gateway Application Programming Interface

API is a protocol that can be used instead of SNMP to manage the Lucent Technologies PSAX systems. It provides an interface to the PSAX system so an external workstation, which is acting as a gateway, can control ATM switching with non-native ATM networking protocols. With the API, the gateway and the PSAX system can perform the interworking of ATM, integrated services digital network (ISDN), signalling system 7 (SS7), channel associated signalling (CAS), and additional protocols. The PSAX system must be configured with the IP address of this external call controller.

To configure the PSAX 20 system as a TCP client or server, perform the steps in the following procedure.

Configuring the TCP Server

Viewing TCP Server Configuration Data

Begin

1. In the Site-Specific Configuration window, select the **Configure TCP Server** command and press Enter.
2. The TCP Server Configuration window is displayed (see Figure 4-12 for Client, and Figure 4-13 for Server).

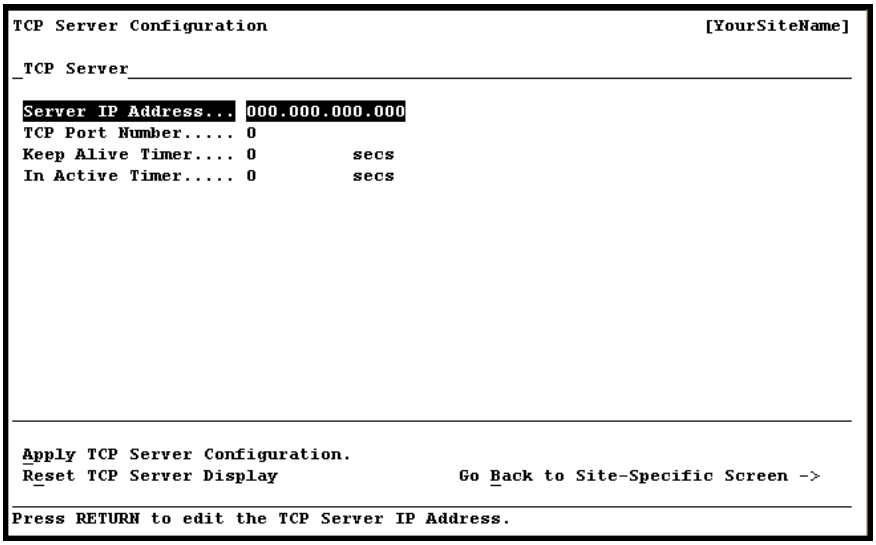

Figure 4-12. TCP Server Configuration Window (Client TCP Type)

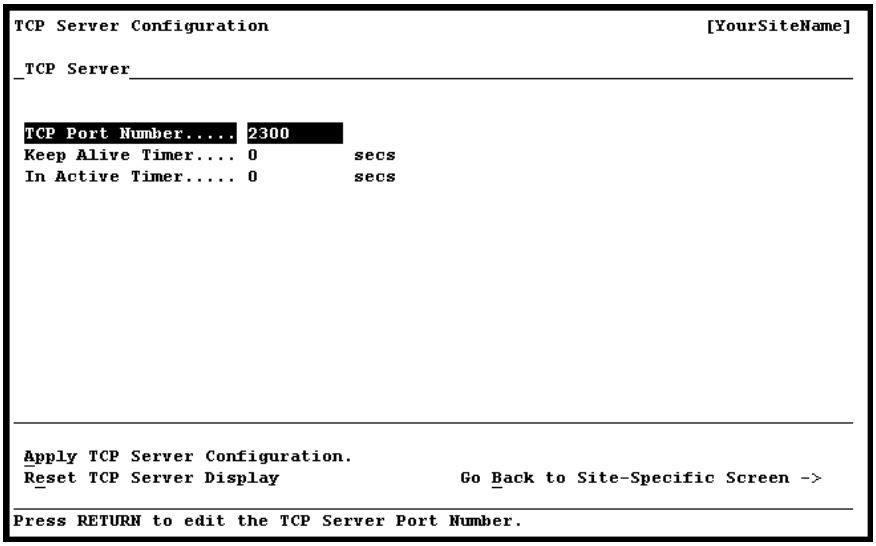

Figure 4-13. TCP Server Configuration Window (Server TCP Type)

Commands The commands on this window have the following functions:

Command	Function
• Apply TCP Server Configuration	Applies the configuration.
• Reset TCP Server Display	Resets the display.
• Go Back to Site-Specific Screen	Redisplays the Site-Specific Configuration window.

3 You can enter data into the fields on the TCP Server Configuration window as described in Table 4-4.

Table 4-4. Field Values for the TCP Server Configuration Panel

Field	Description
Server IP Address	Enter the IP address of the server, such as the call control gateway. This field is only available for configuration if the PSAX system has been designated as a client. This field is display-only if the PSAX system is acting as the TCP server.
TCP Port Number	Enter the server port number.
Keep Alive Timer (secs)	Enter the frequency at which the keep-alive message is to be sent for the connection (in seconds).
In Active Timer (secs)	Enter the amount of time that the server must be inactive, in seconds, before the TCP/IP session is automatically terminated.

Select the **Apply TCP Server Configuration** command and press Enter.

4 To return to the Site-Specific Configuration window, select the **Go Back to Site-Specific Screen** command and press Enter.

End

Configuring SNMP Trap Destinations

You can send SNMP traps to a remote network management system (NMS), to alert it of a problem with the PSAX 20. To set the destinations for SNMP trap messages from your PSAX 20 system, perform the steps in the following procedure.

Entering the SNMP Trap Destinations

Begin

1. Select the **NMS 1** field, and type the IP address value of the remote management station to which you want to send SNMP traps.
2. Under the **Source Addr** field, select one of the following values (see Table 4-5):

Table 4-5. Field Values for the SNMP Trap Destinations Panel

Field Value	Description
Interface (default)	Sets the source address used in all SNMP traps to the IP address of the interface from which they are sent
Ethernet	Sets the source address used in all SNMP traps to the Ethernet IP address from which they are sent
Ibm	Sets the source address used in all SNMP traps to the inband IP address from which they are sent

3. Press **Enter** to exit edit mode.
4. Repeat steps 1-3 for each network management station to be defined (up to a total of five).
5. Select the **Apply Site-Specific Configuration** command and press Enter.

   System Response: After you apply (save) the values on this window, the system does the following:

   - Writes the values you entered to the PSAX 20 system database
   - Displays your site name in the upper right corner of the window
   - Displays the local time in the **[Local Time]** field.

6. To return to the Console Interface Main Menu window, press **Ctrl+B**.

End

Configuring In-Band Management

If you want to manage one or more Access Concentrator systems over an ATM wide-area network (WAN), you can set up an Access Concentrator or a network management system (NMS) computer to provision either PVC or SVC connections to the remote Access Concentrator systems to be managed.

For a PVC connection, you set up the management host, which is usually a Unix workstation running an SNMP client that manages one or more Access

Concentrator systems over an Ethernet network. See the appendix "Configuring In-Band Management."

Three basic methods for configuration are possible:

- Direct connection

The management host connects directly to the Access Concentrator system being managed.

- Routed connection

The management host connects over an Ethernet network to an Access Concentrator system acting as a router. The router Access Concentrator system in turn has direct in-band management PVC connections to remote Access Concentrator systems (managed targets).

- Hybrid connection

To configure the primary IP address for the management host, perform the steps in the following sections, "Adding an In-Band Management ATM SVC Connection" and "Adding an In-Band Management ATM SVC Connection".

Adding an In-Band Management ATM SVC Connection

A Unix workstation is used as the address resolution protocol (ARP) server. The host Access Concentrator system and all remote systems on the same ATM network register their IP addresses on the ARP server when they are initialized (booted). When you want to create an in-band management SVC connection to one or more remote Access Concentrator systems, you use the host Access Concentrator system to request the IP addresses of the remote Access Concentrator systems. After you obtain these IP addresses, you can create the SVC connections (see Figure 4-14).

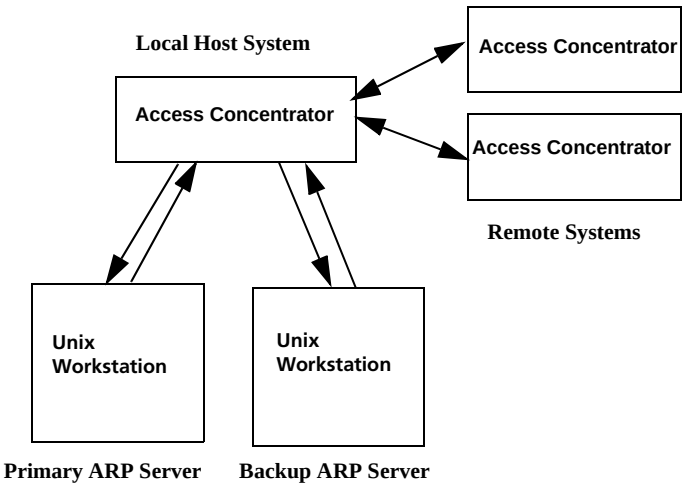

Figure 4-14. In-Band SVC Connections

Before creating an SVC connection, you need to set up the Unix workstation as the ARP server, and each of the Access Concentrator systems. To do this, perform the steps in the following procedure.

Preparing for an In-Band Management SVC Connection

Preparing to Create an In-Band Management SVC Connection

Begin

1. To configure the Solaris workstation to act as an ARP router, you must install an ATM Network Interface Card (NIC) and configure the card as an ATM ARP Server. To do this, consult the procedures in the appropriate section of your Sun Solaris ATM User Guide.
2. Log on to your PSAX system, and go to the Equipment Configuration window.
3. In the Equipment Configuration window, select the module you will use. The OC-3c module is the most often used I/O module for this connection.
4. Configure the OC-3c module (or the module you have selected) for **Interface Type ATMUNI 3.1** and select **Apply Port and Channel Configuration.**
5. Select **Configure the Interface**.
6. On the ATM UNI 3.1 Configuration window, in the **ATM Signaling** field, select **Enabled**. In the **Interface Type** field, select **Network**.

7 Enter the **Address Prefix**. This is the Address Prefix of the node address of the OC-3c module.

8 Configure the ILMI interface. (This is an optional step, but strongly recommended.)

9 On the ILMI Configuration window enable **ILMI Protocol**, **Address Registration**, and **Connectivity Procedure**.

10 Select **Apply ILMI Configuration**, and **Go Back to Previous Screen**.

11 Check the ILMI Register User Address window to see that the address has been created, and return to the Main Menu.

12 From the Site-Specific Menu, select **PNNI System-Wide Configuration**.

13 Select **Create a Node** and follow the instructions in the "PNNI System-Wide Configuration" section in this chapter.

14 Return to the Site-Specific window to create the In-Band SVC Connection.

An in-band management SVC connection can be created between a configured in-band management address and any module that supports ATM interfaces. This connection supports the UBR and VBR-express service types.

Creating an In-Band-Management SVC Connection

Creating an In-Band Management SVC Connection

Begin

Follow the steps below to create an in-band management SVC connection.

1 From the Console Interface Main Menu, select **Site Specific Configuration.**

The Site Specific window is displayed (see Figure 4-15).

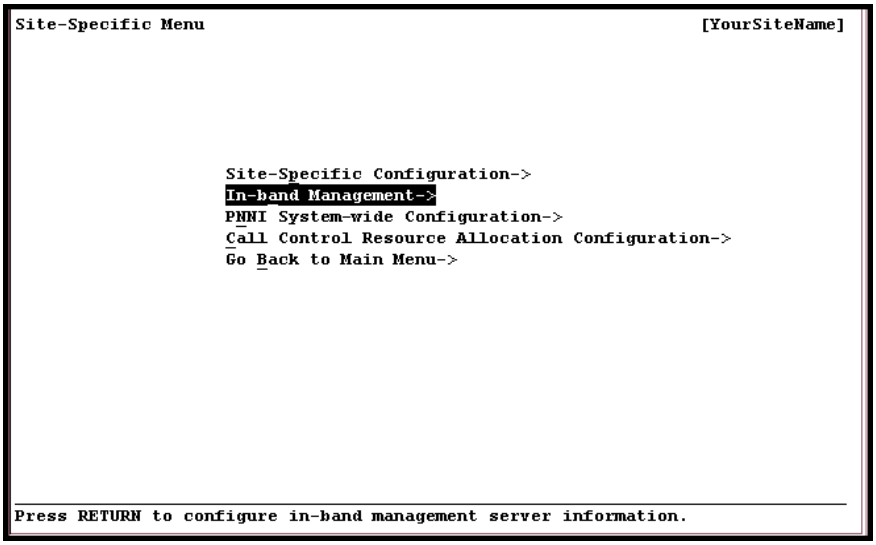

Figure 4-15. Site-Specific Window

2 Select the **In-Band Management** option and press Enter.

The In-Band Management Configuration Window displays (see Figure 4-16).

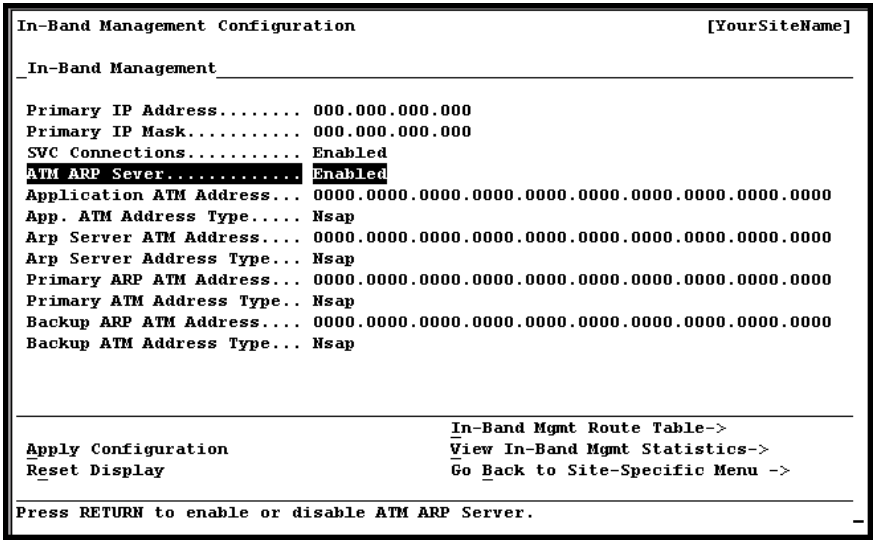

Figure 4-16. In-Band Management Configuration Window (SVC Disabled)

Commands The commands on this window have the following functions:

Command	Function
• Apply Configuration	Applies the configuration.
• Reset Display	Resets the display.
• In-Band Mgmt Route Table	Displays the In-Band Mgmt Route Table.
• View In-Band Mgmt Statistics	Displays the In-Band Mgmt Statistics window.
• Go Back to Site-Specific Menu	Returns you to the Site-Specific window.

3 In the In-Band Management Configuration window, enter the IP address and IP Mask for the PSAX unit.

Note: This address must be on a different subnet from the subnet that is assigned to the Ethernet interface for the management host.

4 In the **SVC Connections** field, select **Enabled**.

The In-Band Management Configuration Window with SVC enabled displays (see Figure 4-17).

```
In-Band Management Configuration                              [YourSiteName]

_In-Band Management_____________________________________________________

 Primary IP Address........ 000.000.000.000
 Primary IP Mask........... 000.000.000.000
 SVC Connections........... Enabled
 ATM ARP Sever............. Enabled
 Application ATM Address... 0000.0000.0000.0000.0000.0000.0000.0000.0000.0000
 App. ATM Address Type..... Nsap
 Arp Server ATM Address.... 0000.0000.0000.0000.0000.0000.0000.0000.0000.0000
 Arp Server Address Type... Nsap
 Primary ARP ATM Address... 0000.0000.0000.0000.0000.0000.0000.0000.0000.0000
 Primary ATM Address Type.. Nsap
 Backup ARP ATM Address.... 0000.0000.0000.0000.0000.0000.0000.0000.0000.0000
 Backup ATM Address Type... Nsap




                                    In-Band Mgmt Route Table->
 Apply Configuration                View In-Band Mgmt Statistics->
 Reset Display                      Go Back to Site-Specific Menu ->

Press RETURN to enable or disable ATM ARP Server.
```

Figure 4-17. In-Band Management Configuration Window (SVC and ARP Enabled)

Field Descriptions

5 Select the values for the fields on this window from the values given in Table 4-6.

Table 4-6. Field Values for the In-Band Management Configuration Window

Field Name	Values	Description
Primary IP Address	Valid dotted-quad	Enter the in-band management IP address of the Access Concentrator.
Primary IP Mask	Valid dotted-quad	Enter the in-band management IP mask of the Access Concentrator
SVC Connections	Disabled	Disables SVC connection provisioning. The fields below will disappear. The server is used for PVC connection provisioning when SVC is disabled.
	Enabled	Enables SVC connection provisioning.
ATM ARP Server	Disabled (default)	Indicates that this PSAX system is not acting as an ARP server.
	Enabled	Indicates that this PSAX system is acting as an ARP server.
Application ATM Address		Enter the application ATM address of the Access Concentrator in hexadecimal notation.
App. ATM Address Type	Default: Nsap E164, E164nsap	Select the application ATM address type of the Access Concentrator.
Arp Server ATM Address		This field is displayed only if **Enabled** is selected in the **ATM ARP Server** field. Enter the address of the ATM address of the ARP server.
Arp Server ATM Address Type	Default: Nsap E164, E164nsap	The format of the ATM address of the ARP server. This field is displayed only if **Enabled** is selected in the **ATM ARP Server** field. Select the ATM address type of the ARP server.
Primary ARP ATM Address		Enter the address of the primary ATM ARP server. (Use Solaris workstation address.)
Primary ATM Address Type	Default: Nsap E164, E164nsap	Select the ATM address type of the primary ARP server.

Table 4-6. Field Values for the In-Band Management Configuration Window

Field Name	Values	Description
Backup ARP ATM Address		Enter the address of the backup ATM ARP server. (Use Solaris workstation address.)
Backup ATM Address Type	Default: Nsap E164, E164nsap	Select the ATM address type of the backup ARP server.

6 Select the **Apply Configuration** command and press Enter.

7 Select the **In-Band Mgmt Route Table** command and press Enter.

The Inband Management Route Table window is displayed (see Figure 4-18).

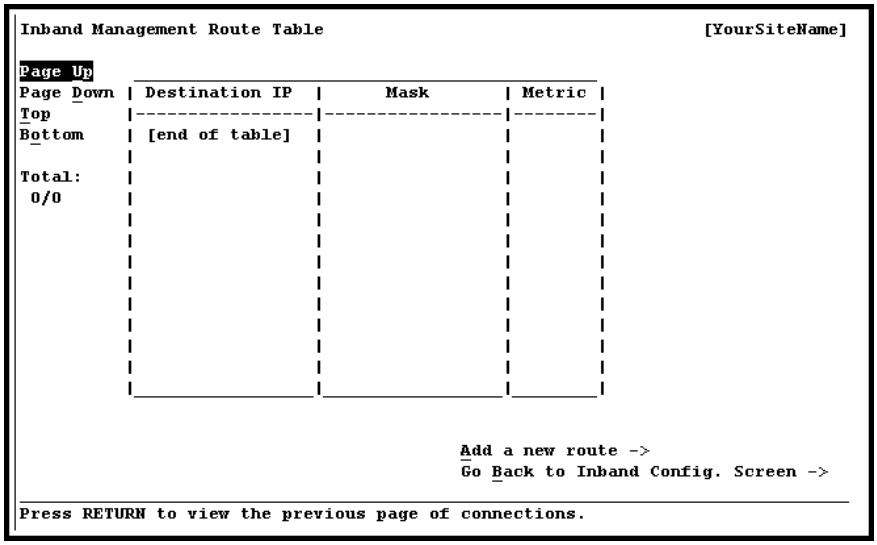

Figure 4-18. Inband Management Route Table Window

Commands

The commands on this window have the following functions:

Command	Function
• Add a new route→	Use to add a new route.
• Go Back to In-Band Config. Screen→	Returns you to the In-Band Management-Configuration window.

8 Select the **Add a new route** command and press Enter.

The Inband Management Route Configuration window displays (see Figure 4-19).

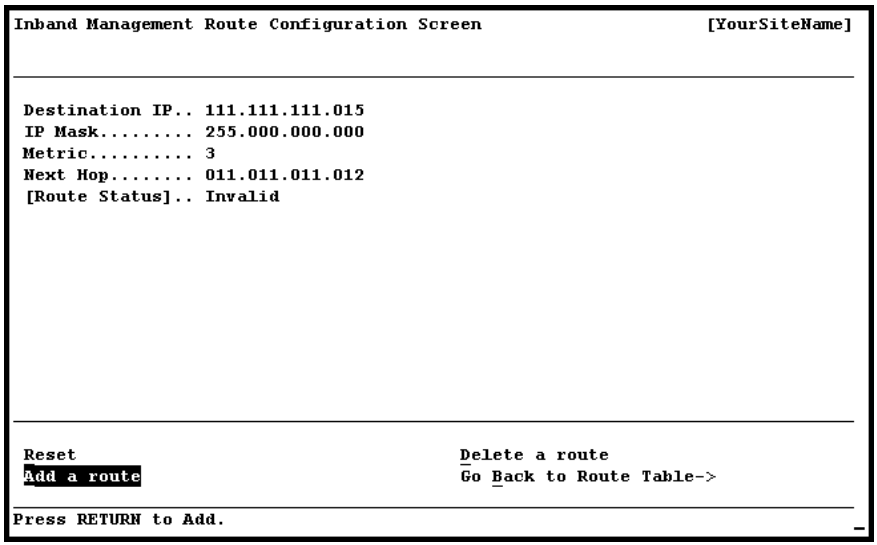

Figure 4-19. Inband Management Route Configuration Window

Note: At the time of initial setup, the In-Band Management Table window is empty. After you have set up routes, this window displays all the routes of this type in the system.

9 Select the **Add a route** command and press Enter.

10 Click **Create.**

Commands

The commands on this window have the following functions:

Command	Function
• Reset	Resets the display.
• Add a route	Use to add the newly configured route.
• Delete a route	Use to delete a route.
• Go Back to Route Table	Returns you to the In-Band Management Route Table window.

Field Descriptions

11 Select the values for the fields in this window as described in Table 4-7.

Table 4-7. Field Values for the In-Band Management Route Configuration Window

Field Name	Values	Description
Destination IP	Variable	Enter the destination network IP address.
IP Mask		Enter the destination network IP mask.
Metric	Variable, any number	The number of Hops to reach to the destination.
Next Hop	IP Address	Gateway to the destination network
	Invalid	Display only.

The route is now added.

12 Select the **Go Back to Route Table** command and press Enter

The Inband Management Route Table window displays with the new route added (see Figure 4-20).

```
Inband Management Route Table                                  [YourSiteName]

Page Up
Page Down | Destination IP  |      Mask        | Metric |
Top       |-----------------|------------------|--------|
Bottom    | 111.111.111.015 | 255.000.000.000  |    3   |
          | [end of table]  |                  |        |
Total:    |                 |                  |        |
 1/1      |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |                 |                  |        |
          |_________________|__________________|________|

                                        Add a new route ->
                                        Go Back to Inband Config. Screen ->

Press RETURN to view the previous page of connections.
```

Figure 4-20. Inband Management Route Table (Route Displayed)

Viewing In-Band Statistics Data

To view the In-Band Management Interface Statistics window, return to the In-Band Management Configuration window (see Figure 4-16), and select the **View In-Band Mgmt. Statistics** command. The In-Band Management Interface Statistics window displays (see Figure 4-21).

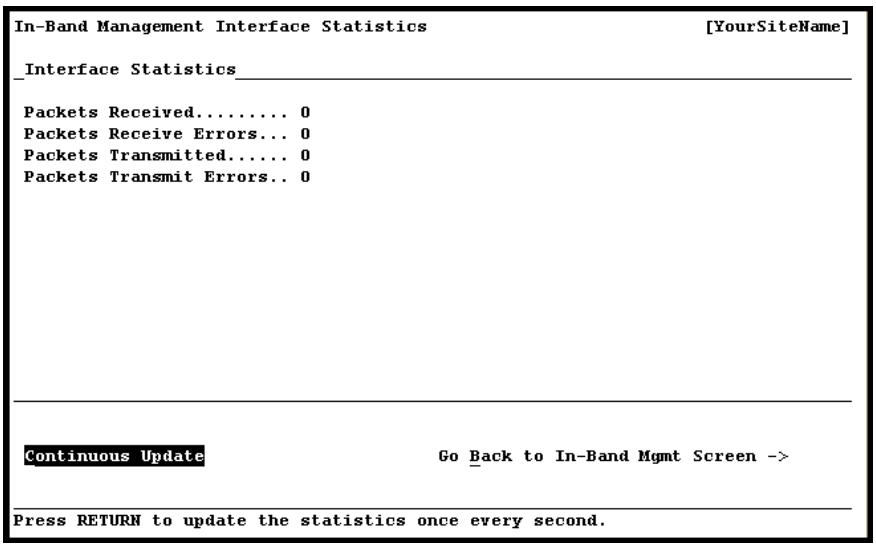

Figure 4-21. In-Band Management Interface Statistics Window

Commands

The commands on this window have the following functions:

Command	Function
• Continuous Update	Continuously updates the information in the fields every second. Select this command and press Enter to turn the continuous updating on and off as needed (similar to a toggle switch).
• Go Back to In-Band Mgmt→	Returns you to the In-Band Management-Configuration window.

Field Descriptions

The statistics in this window are described in Table 4-8.

Table 4-8. Field Values for the In-Band Management Statistics

Field Name	Description
Packets Received	Displays the number of packets received.
[Packet Receive Errors]	Displays the number of packet receive errors.

Table 4-8. Field Values for the In-Band Management Statistics

Field Name	Description
Packets Transmitted	Displays the number of packets transmitted.
Packet Transmit Errors	Displays the number of packet transmit errors.

End

Deleting an In-Band Management SVC Route

Deleting an In-Band Management SVC Route

Perform the steps in the following procedure to delete an In-Band SVC route.

Deleting an In-Band SVC Route

Begin

1. In the Inband Management Route Configuration window (see Figure 4-18 on page 4-28), select the **Delete a route** command and press Enter.
2. Select the **Go Back to Route Table** command to check that the Inband Management Route Table (see Figure 4-19 on page 4-29) does not contain the route you just deleted.

End

Using the Equipment Configuration Window

To configure the Stratum 3–4 module or any I/O module, you select an item from the Equipment Configuration window.

From the Console Interface Main Menu window, select the **Equipment Configuration** option.

The Equipment Configuration window is displayed (see Figure 4-22).

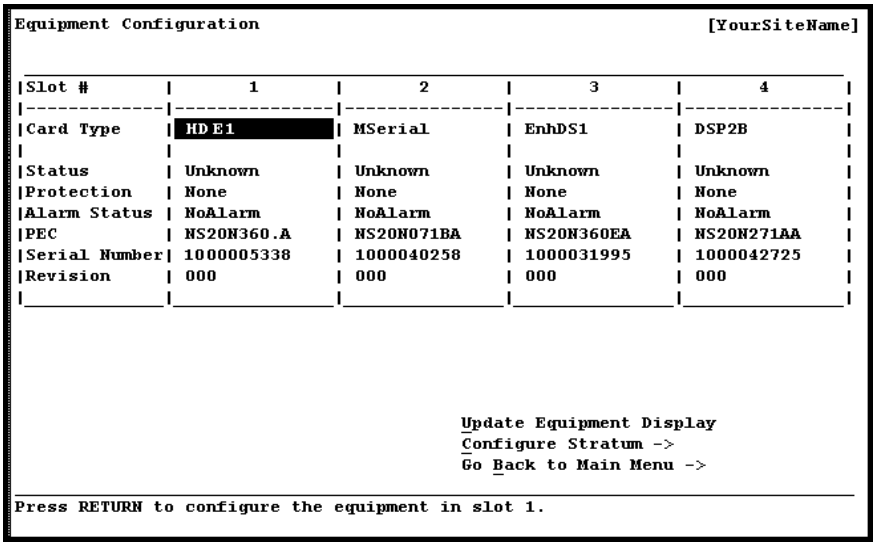

Figure 4-22. Sample Equipment Configuration Window (As Displayed on the PSAX 20 or AC 60 Systems)

The Equipment Configuration window displays the following:

- All the input/output (I/O) and server modules in the chassis
- Each module location by slot number
- Status of the modules (whether they are configured)
- Alarm status (whether a loss of signal has been detected)

When a module is inserted into the chassis, its module name appears on the window. When the module is removed from the chassis, its module name disappears from the window. The fields displayed on the Equipment Configuration window are described in Table 4-9.

Table 4-9. Field Values for the Equipment Configuration Window

Field	Description
Slot	Indicates the slot number location on the PSAX 20 chassis. You can configure only user-selectable I/O and server modules, and the Stratum 3–4 clock timing.
Card Type	Indicates what kind of module is inserted in the slot.
Status	Indicates that the module operates in primary mode. This field applies to the I/O and server modules.
Alarm Status	Indicates whether any alarms are active. The **Alarm Status** fields are described in more detail in Table 4-12 on page 4-38.

Table 4-9. Field Values for the Equipment Configuration Window

Field	Description
PEC	Indicates the product element code (PEC).
Serial # (serial number)	Indicates the unique identifying number to identify a particular hardware component.
SW Version	Indicates the current software version level of the module.

Configuring the Stratum 3–4 Clock Timing

Data and voice transmit most efficiently (with the least amount of cells lost per second) if a proper clock timing source is present in the PSAX 20. Therefore, we recommend that you configure the Stratum 3–4 clock timing before configuring any I/O or server modules.

Note: You can avoid any system timing errors by configuring the Stratum 3–4 clock timing before you configure and run traffic through any I/O and server modules, DSP, or T1/E1 components.

Note: On the Stratum Configuration window, you establish the source of the system synchronization. You must configure the Stratum 3–4 module before configuring any user-selected I/O or server modules. You must configure the Stratum 3–4 clock timing before configuring any user-selected I/O or server modules. After you have configured the Stratum 3–4 clock timing, it provides the reference clock to all I/O module ports configured for local timing.

Setting the Stratum Configuration Values

To configure the Stratum 3–4 clock timing, perform the steps in the following procedure.

Configuring the Stratum 3–4 Clock Timing

Begin

1. On the Console Interface Main Menu window, select the **Equipment Configuration** command.

   The Equipment Configuration window (see Figure 4-22 on page 4-33) is displayed:

2. On the Equipment Configuration window, select the **Stratum** 3–4 clock timing and press Enter.

The Stratum Configuration window is displayed (see Figure 4-23).

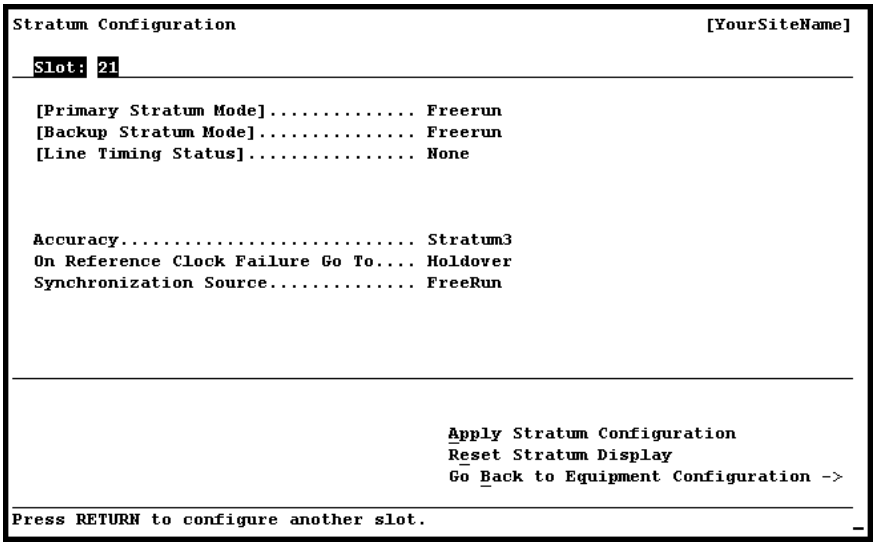

Figure 4-23. Stratum Configuration Window (Freerun)

Note: The **[Primary Stratum Mode]** and **[Line Timing Status]** fields indicate the current modes of operation for the Stratum 3–4 clock timing. Table 4-10 describes the possible values for these fields.

Table 4-10. Field Values for the Primary Stratum Window

Field Name	Mode of Operation	Description
(display only)	Default: Holdover	Indicates a loss of timing.
	Freerun	Indicates the initial state of no timing source.
	Synchronized3	Indicates timing has Stratum3 precision.
	Synchronized4	Indicates timing has Stratum4 precision.
	CardRemoved	Indicates that a Stratum 3–4 module is not present.

Table 4-10. Field Values for the Primary Stratum Window

Field Name	Mode of Operation	Description
(display only)	Default: None	Indicates that the system timing is not being provided by the line source.
	PrimaryLine	Indicates that system timing is provided by the slot and port of the module specified as the Primary Line Source.
	SecondaryLine	Indicates that system timing is provided by the slot and port of the module specified as the Secondary Line Source.
Accuracy	Default: Stratum3	Indicates timing has Stratum3 precision.
	Stratum4	Indicates timing has Stratum4 precision.
On Reference Clock Failure Go To	Default: Freerun	Indicates that the Stratum 3–4 module should switch to freerun status if a reference clock failure occurs.
	Holdover	Indicates that the Stratum 3–4 module should switch to holdover status if a reference clock failure occurs.
Synchronization Source	Default: LineTiming	Indicates the clock will be provided through the slot and port specified in the **Primary Line Source** and **Secondary Line Source** fields.
	Freerun	Indicates the system is running on its internal clock.
	CompositeClock	Indicates the clock will be provided through an external clock connected to the front of the primary Stratum 3–4 module.

3 Select the **Accuracy** field, and press Enter to cycle through the predefined set of values (**Stratum3** or **Stratum4**).

4 Select the **Synchronization Source** field, and press Enter to cycle through the predefined set of values (see Table 4-11).

Table 4-11. Field Values for the Synchronization Source Field

Value	Description
Freerun (default)	Indicates the PSAX 20 system is running on its internal clock.
LineTiming	Indicates the clock timing is provided through the slot and port specified in the **Primary Line Source** and **Secondary Line Source** fields.

Note: The following steps 5 and 6 in this procedure apply only if you select the **LineTiming** value in the **Synchronization Source** field. When you select this value, the **Primary Line Source** and the **Secondary Line Source** fields and the **Switch Line Timing Source** command are displayed (see Figure 4-24).

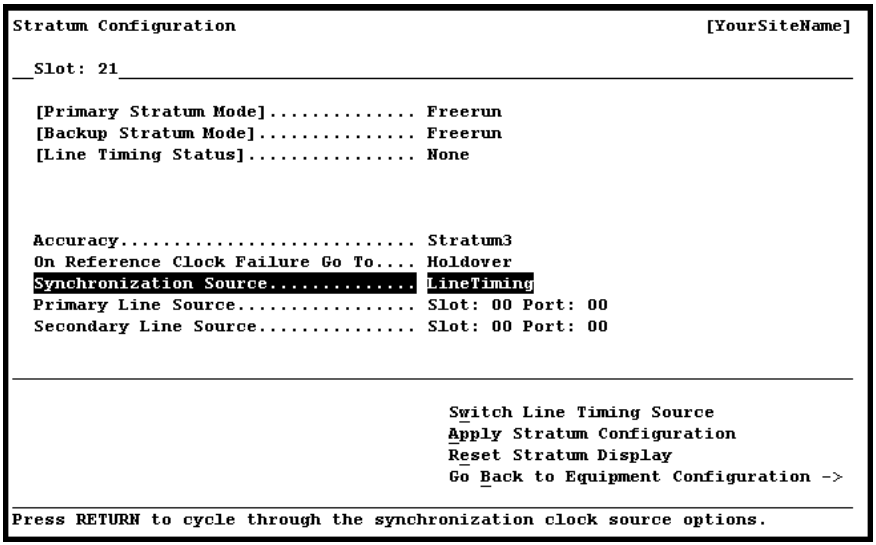

Figure 4-24. Stratum Configuration Window (LineTiming Synchronization)

5 Select the **Primary Line Source** field, and enter the values for the slot and the port.

Press Enter to exit edit mode.

6 Select the **Secondary Line Source** field, and enter the values for the slot and the port. Enter zeros (00) if you do not want to specify a secondary line source.

Press Enter to exit edit mode.

7 Select the **Apply Stratum Configuration** command, and press Enter to execute the command.

End

Switching the Line Timing Source

At any time after initial configuration of the Stratum 3–4 clock timing when you have selected **LineTiming** as your synchronization source, you can switch between the primary line source or the secondary line source, as follows:

1 Select the **Switch Line Timing Source** command.

2 Press Enter.

The value displayed in the **[Line Timing Status]** field is changed.

Configuring I/O and Server Modules

Once the Stratum 3–4 clock timing has been configured, I/O and server modules are configured by returning to the Equipment Configuration window (see Figure 4-22 on page 4-33).

Alarm Status Values

I/O and server modules display the status value of **Primary** if they are configured, or **Unknown** if they are unconfigured. The Alarm Status column for unconfigured modules still can have a number listing the ports that are available to be configured. If numbers in the Alarm Status column are underlined, this condition indicates a loss of signal. Table 4-12 describes the values in the **Alarm Status** field as shown on the Equipment Configuration window.

The Alarm Status field on the Equipment Configuration window displays the current status of all *PacketStar* I/O, server , and common equipment module in your PSAX Access Concentrator system. The alarm status descriptions are provided in Table 4-12.

Table 4-12. Alarm Status Descriptions for PSAX Access Concentrator Modules

Number	Alarm Status	Module Type Affected	Description
1	NoAlarm/Card-Present	I/O	No module is inserted in the chassis.
2	WrongCardType	I/O	One type of module was configured in this slot in the chassis, but a different module now occupies this slot.
3	LineFailed	All	The line has failed.
4	CardRemoved	All	A module has been configured and then removed.
5	ReferenceClock-Failed	Stratum	The timing reference clock has failed.
6	CompositeClock-Failed	Stratum	The timing composite clock has failed.
7	Overload	Power Supply	The Power Supply is operating under an overload condition.
8	Plus5vFailed	Power Supply	The 5 V Power Supply has failed.
9	Plus120vFailed	Power Supply	The 120 V ac Power Supply has failed.
10	Minus48vFailed	Power Supply	The -48 V dc Power Supply has failed.

Table 4-12. Alarm Status Descriptions for PSAX Access Concentrator Modules

Number	Alarm Status	Module Type Affected	Description
11	UnknownAlarm	I/O	The reason for failure is not known.
12	CompleteClock-Failed	Stratum	The timing complete clock has failed.
13	BackplaneCir-cuitryFailed	All	The chassis backplane circuit board is not operating.
14	PowerFailed	Power Supply	Power failed

PNNI System-Wide Configuration

For an overview of PNNI and the PNNI features supported on the PSAX 20 system, see the section about PNNI in Chapter 3.

To configure a PNNI node for your PSAX 20 system, perform the steps in the following procedure.

Note: Before you can configure an I/O module with the ATM PNNI 1.0 interface, you must configure PNNI for your PSAX 20 system.

Configuring PNNI

PNNI System-Wide Configuration

Begin

1. At the Console Interface Main Menu, select **Site-Specific Configuration**.
2. On the **Site-Specific Menu,** select **PNNI System-Wide Configuration**.

   The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

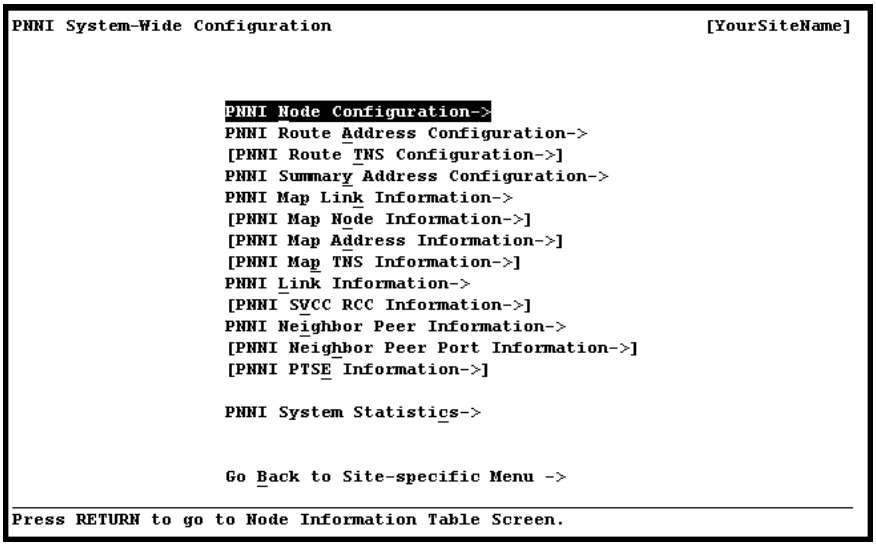

Figure 4-25. PNNI System-Wide Configuration Window

Commands

The commands in this window have the following functions:

Command	Function
• PNNI Node Configuration	Configures the PNNI Node.
• PNNI Route Address Configuration	Adds the route address.
• Go Back to Site-Specific Menu	Re-displays the Site-Specific window.

The other commands on this screen provide read-only information to assist in monitoring PNNI status.

Menu Option	Description
• PNNI Route TNS Configuration	Not currently supported.
• PNNI Summary Address Configuration	Displays ATM NSAP addresses for all nodes to which this link table is attached by PNNI interfaces.

Menu Option	Description
• PNNI Map Link Information	Displays the mapping for the nodes and their links, and all original port and remote port PNNI topology state element (PTSE) identifiers and the metrics tag number.
• PNNI Map Node Information	Not currently supported.
• PNNI Map Address Information	Not currently supported.
• PNNI Map TNS Information	Not currently supported.
• PNNI Link Information	Displays an index of nodes and their associated links for this PSAX 20 system.
• PNNI SVCC RCC Information	Not currently supported.
• PNNI Neighbor Peer Information	Displays nodes that are on the same level as this node.
• PNNI Neighbor Peer Port Information	Not currently supported.
• PNNI PTSE Information	Not currently supported.
• PNNI System Statistics	Displays PNNI statistics.

3 Select the **PNNI Node Configuration** command and press Enter.

The PNNI Node Table window is displayed (see Figure 4-26).

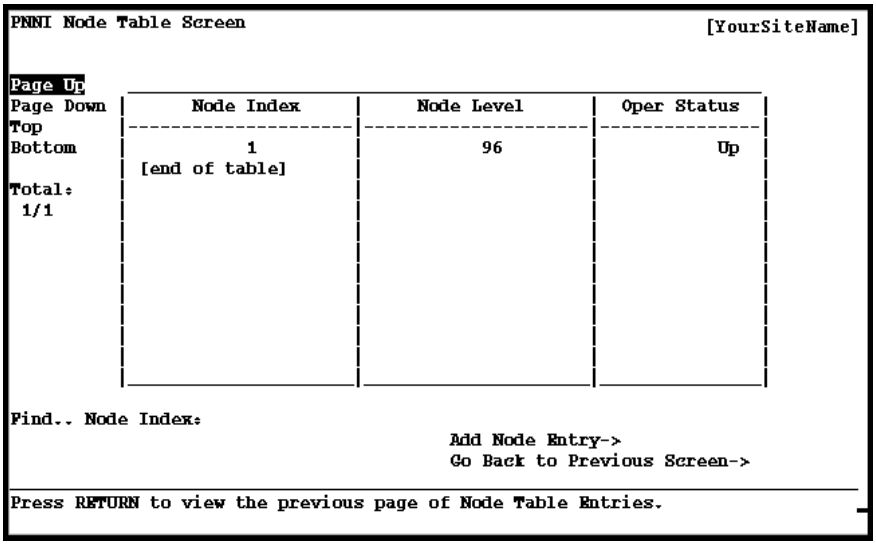

Figure 4-26. PNNI Node Table Window

Commands

The commands on this window have the following functions:

Command	Function
• Find Node Index	Displays default five-number value on the Node Table window.
• Add Node Entry	Adds only one node entry in the PSAX system.
• Go Back to Previous Screen	Redisplays the PNNI System-Wide configuration window.

4 Select **Add Node Entry** and press Enter.

The PNNI Node Configuration window is displayed (see Figure 4-27).

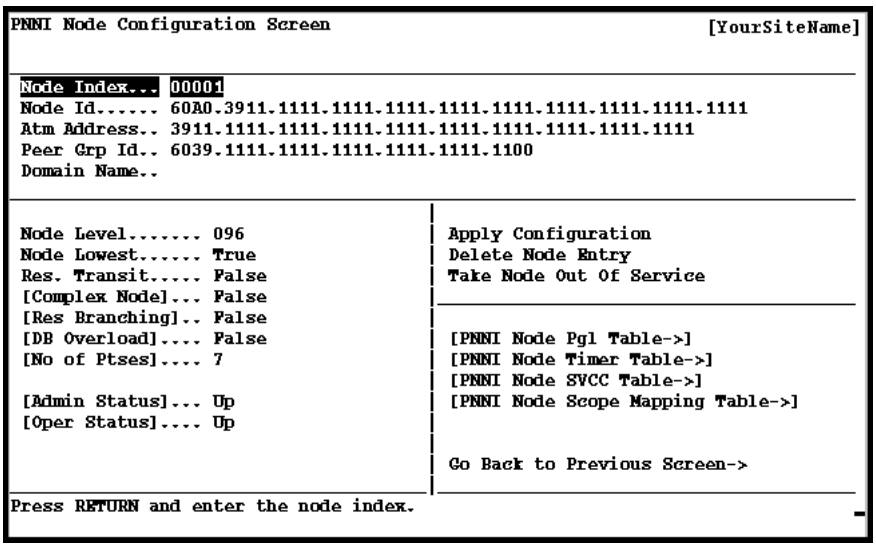

Figure 4-27. PNNI Node Configuration Window

Commands

The commands on this window have the following functions:

Command	Function
• Create Node Entry	Create a new PNNI node.
• Delete Node Entry	Delete an existing PNNI node.
• Bring Node Into Service	Bring an existing PNNI node into or out of service.
• Go Back to Previous Screen	Redisplays the PNNI Node Table Screen.

Field Descriptions

5 Select the values for the fields on this window from the values given in Table 4-13.

Table 4-13. Field Values for the PNNI Node Configuration Window

Field Name	Values	Description
Node Index	00000 (default); Range: 1–65535	The node index identifies a logical PNNI entity in the PSAX system. Enter **1** in this field. **Note:** It is not recommended that you use the default value, because parent node and multiple node configuration are not currently supported.
Node Id		The system generates your Node Id automatically.
Atm Address		A unique Enter your ATM NSAP address, a hexadecimal number within the network's PNNI hierarchy that must beginning with 39, 45, or 47.
Peer Group Id		The first 13 bytes of the ATM IP address. This value is generated and displayed by the system automatically. For more information, see Section 5.3.3, Node Identifiers, in the ATM Forum Specification, *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0, af-pnni-0055.000*.
Domain Name		Routing domain in which this node participates.
Node Level	096 (default); Range: 96 (decimal)=60 (hexadecimal); 0–104 maximum	Number of significant bits in the network portion of the ATM address on the PSAX system; related to the first octet (two digits) of the node identifier. All PSAX systems should be in the same node level. Enter in decimal form and the system will generate and display the value automatically.

Table 4-13. Field Values for the PNNI Node Configuration Window

Field Name	Values	Description
Node Lowest	True (default), False	Specifies the root node (true if the current node is root). Select **True** for this field. **Note:** It is recommended that you use the default value of **True**, because parent node and multiple node configuration are not currently supported.
Res. Transit (display only)	False (default), True	Restricted transit indicates whether the node is restricted to not allowing support of SVCs transitting this node.
[Complex Node] (display only)	True, False	Specifies whether this node uses the complex node representation. This attribute determines the setting of the nodal representation bit in the nodal information group originated by this node. **True** indicates that the complex node representation is used. **False** indicates that the simple node representation is used.
[Res Branching] (display only)	True, False	Indicates whether the node is able to support additional point-to-multipoint branches. This attribute reflects the setting of the restricted branching bit in the nodal information group originated by this node. **True** indicates that additional branches cannot be supported. **False** indicates that additional branches can be supported.
[DB Overload] (display only)	True, False	Specifies whether the node is currently operating in a topology database overload state. This attribute has the same value as the non-transit for PGL election bit in the nodal information group originated by this node.
[No of Ptses] (display only)	0 (default)	Displays the total number of PTSEs currently in the topology database(s) for this node.

Table 4-13. Field Values for the PNNI Node Configuration Window

Field Name	Values	Description
[Admin Status] (display only)	Up, Down	The administrative status for this node.
[Oper Status] (display only)	Up, Down	The operational status for this node.

6 Select the **Create Node Entry** command and press Enter.

The Node entry is created and the Node Id field is displayed the node identifier of your PSAX 20 system.

7 Select the **Bring Node Into Service** command and press Enter.

The **OperStatus** display field indicates that the node is up.

Note: You must bring the node into service to enable PNNI support on your PSAX 20 system. The ATM PNNI interface cannot be brought into service until a PNNI node is created and in service. If you need to take the node out of service, you must first delete any ATM PNNI interfaces you have configured on your PSAX 20 system.

8 Select the **Go Back to Previous Screen** command and press Enter.

The PNNI Node Table Screen (see Figure 4-26) is displayed, showing your current node index, node level, and operating status. Use this screen to check a node's status whenever you create, delete, or bring a node into service.

9 Press **Ctrl+G** to go back to the Console Interface Main Menu window.

10 Select the **Equipment Configuration** option and press Enter.

The Equipment Configuration window is displayed.

11 Select an I/O module that supports the ATM PNNI 1.0 interface type.

The Port and Channel Configuration window is displayed.

12 In the **Interface Type** field, select **AtmPnni1-0**.

The ATM PNNI 1.0 Interface Configuration window is displayed.

13 Configure the fields for this interface as described in the appropriate *PacketStar™ Module User Guide*.

14 Select the **Apply Configuration command and press Enter.**

15 Select the **Bring Interface Into Service command and press Enter.**

16 Type **Ctrl+G** to return to the Console Interface Main Menu window.

End

The PNNI node you just configured has been brought into service. At this time, you can select a route address using the PNNI System-Wide

Configuration window. The following procedure is not necessary to follow unless you want to advertise the reachable addresses that the system cannot learn or automatically detect. The Route Address table displays the rachable addresses and other information that the PSAX 20 system learns from other switches in the same network as the PSAX 20 system.

Configuring PNNI Route Addresses

Steps for Configuring PNNI Route Addresses

Begin

Note: If you are configuring an SPVC as **ActiveSvc**, do not configure a route address. If you configuring an SPVC as **PassiveSvc**, configure a route address.

1. Select the **Site-Specific Configuration** option, and press Enter.

   The Site-Specific Menu is displayed.

2. Select the **PNNI System-Wide Configuration** option, and press Enter.

   The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3. Select the **PNNI Route Address Configuration** option.

   The PNNI Route Address Table window is displayed (see Figure 4-28).

```
PNNI Route Address Table Screen                                  [YourSiteName]
 Page Up   Page Down    Top     Bottom    Total:   1/6

| Node  |                Route Address                          |Prefix|Address| S |
| Index |                                                       | Len  | Index |   |
|-------|-------------------------------------------------------|------|-------|---|
| 00001 | 4722.2222.2222.2222.2222.2222.2222.2222.2222.00       | 152  | 00012 |   |
| 00001 | 4722.2222.2222.2222.2222.2222.2222.2222.2222.22       | 152  | 00001 |   |
| 00001 | 4733.3333.3333.3333.3333.3333.3333.3333.0000.00       | 152  | 00001 |   |
| 00001 | 4733.3333.3333.3333.3333.3333.3333.3333.0000.00       | 152  | 00003 |   |
| 00001 | 4744.4444.4444.4444.4444.4444.4444.4444.4444.44       | 152  | 04369 |   |
| 00001 | 4755.5555.5555.5555.5555.5555.5555.5555.5555.55       | 152  | 00001 |   |
|[end]  |                                                       |      |       |   |
|       |                                                       |      |       |   |
|       |                                                       |      |       |   |
|       |                                                       |      |       |   |
|       |                                                       |      |       |   |
|       |                                                       |      |       |   |
|_______|_______________________________________________________|______|_______|___|
 * Route Address Operational (S)tatus is inactive.
Find.. Node Index:        Prefix Length:       Address Index:
       Route Address:     .    .    .    .    .    .    .    .    .    .
Add Route Address Entry->              Go Back to Previous Screen->

Press RETURN to view the previous page of Route Address Entries.
```

Figure 4-28. PNNI Route Address Table Window

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index, Prefix Length, Address Index**, or **Route Address** fields.
• Add Route Address Entry	Displays the PNNI Route Address Configuration window.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

4 Select the **Add Route Address Entry** command.

The PNNI Route Address Configuration window is displayed (see Figure 4-29).

```
PNNI Route Address Configuration Screen                    [YourSiteName]

                          Route Address Information

 Node Index............. 00001
 Route Address Prefix.. 4722.2222.2222.2222.2222.2222.2222.2222.2222.00
 Adv Node Id............ 60A0.3911.1111.1111.1111.1111.1111.1111.1111.1111

 Interface Index.... 0000000000        | Metrics Tag..... 0000000000
 Adv Port Id........ 0000000000        | [Time Stamp].... 00:00:02
 Prefix Length...... 152               |
                                       | [Oper Status]... Advertised
 Address Index...... 00012             |
 Address Type....... Exterior          |---------------------------------------
 Address Scope...... 000               | Apply configuration.
 VP Capability...... True              | Delete Route Address Entry
 Org Advertisement.. True              |
                                       | View Metrics Table->
 [Adv Ptse Id]...... 0000000000        |
 [Address Proto].... Mgmt              | Go Back to Previous Screen->
                                       |

Press RETURN and enter the Node Index.
```

Figure 4-29. PNNI Route Address Configuration Window

Commands

The commands in this window have the following functions:

Command	Function
• Create Route Address Entry	Adds the route address to the PNNI Route Address table.
• Delete Route Address Entry	Deletes the route address from the PNNI Route Address table.

Command	Function
• View Metrics Table	Displays the PNNI Metrics Table window.
• Go Back to Previous Screen	Displays the PNNI Route Address Table window.

Field Descriptions

5 Select the values for the fields in this window as described in Table 4-14.

Table 4-14. Field Values for the PNNI Route Address ConfigurationWindow

Field Name	Values	Description
Node Index	0 (default) Range: 1–65535	Unique indentifier for this PNNI system node. Enter **1** in this field.
Route Address Prefix	(hexadecimal)	The address prefix of the ATM end system, in 19 bytes (it does not include the NSAP address selector byte).
Adv Node Id	(hexadecimal)	The node ID of the node advertising connectivity to the specified prefix. If the local node ID is 0, then this must be zeroes. This value is generated and displayed by the PSAX system automatically.
Interface Index	0 (default)	The local interface over which the advertised node is reachable. If the node is only reachable through a remote node, this must be set to 0. If the node is not set to zero, the Address Protocol (**Address Proto** field) must not be **PNNI**, and the **Address Type** field should not be set to **Reject**.
Adv Port Id	0 (default)	Advertised port identifier. For an SVC endpoint, enter **SS** (SlotSlot) **PP** (PortPort) **CCC** (ChannelChannelChannel). You may create up to 50 routes manually, to display in the Route Address table. More than 50 routes may be displayed by the PSAX system because route addresses are also learned dynamically.
Prefix Length	0 (default)	Enter a value that does not exceed 152 (19 octets = 152 bits). For an SPVC, enter the length of the Address Prefix which is accessible through this PNNI node for SPVC (1–152 bits).

Table 4-14. Field Values for the PNNI Route Address ConfigurationWindow

Field Name	Values	Description
Address Index	1 (default)	This number references an entry in a table that keeps track of which nodes can access which prefixes.
Address Type	Exterior (default)	The type of connectivity from the advertising node to the address prefix. Belongs to an external domain address.
	Other	Belongs to a a domain address that is not defined as internal or external.
	Reject	Indicates that messages from a matching address prefix should be discarded as unreachable.
	Internal	Belongs to the same domain address, administrative authority, or attached device.
Address Scope	0 (default)	The level of the PNNI hierarchy where the connectivity between the advertising node and the address prefix is located.
VP Capability	True (default); False	Indicates whether VPCs can be established between the advertising node and the address prefix.
Org Advertisement	True (default); False	Indicates whether the local node should advertise the reachable address on its domain (where it originates).
[Adv Ptse Id] (display only)	0 (default)	The advertised PTSE identifer of the PTSE being originated by the originating node, if this was learned through PNNI 1.0.
[Address Proto] (display only)	Mgmt (default)	The connectivity mechanism by which connectivity from the advertising node to the address prefix was learned.
Metrics Tag	0 (default)	The primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the **Address Proto** value of the route. If this metric is not used, enter **1** in this field.
[Time Stamp]	00:00:00 (default)	Indicates when connectivity became known to the local node.

Table 4-14. Field Values for the PNNI Route Address ConfigurationWindow

Field Name	Values	Description
Operational Status	Inactive (default)	Indicates that the reachable address prefix is not operationally valid and not being advertised by this node.
	Advertised	Indicates that the reachable address prefix is operationally valid and being advertised by this node. The system will display this value if the ATM PNNI 1.0 interface is in service, and at least two nodes must have connectivity to each other.

6 Press **Ctrl+A** to **Create Route Address Entry**.

The route is completed.

7 Using the instructions in the appropriate *PacketStar™ Module User Guide*, configure a second port with the ATM UNI interface (you must create the ATM UNI interface if it does not yet exist) and bring the ATM UNI interface into service.

8 To add additional route addresses, repeat this procedure.

End

Configuring PNNI Metrics

The Metrics table displays the PNNI parameters associated with a PNNI entity, or connectivity between a node and a reachable address or transit network. The PSAX 20 system learns such information as advertised service categories, bandwidth, and so on. You can also view traffic patterns and other information about routes advertised on other nodes in the Route Address Table window (see Figure 4-28).

Configuring PNNI Metrics

Begin

1 From the PNNI Route Address Configuration window, select the **View Metrics Table** command.

The PNNI Metrics Table window is displayed (see Figure 4-30).

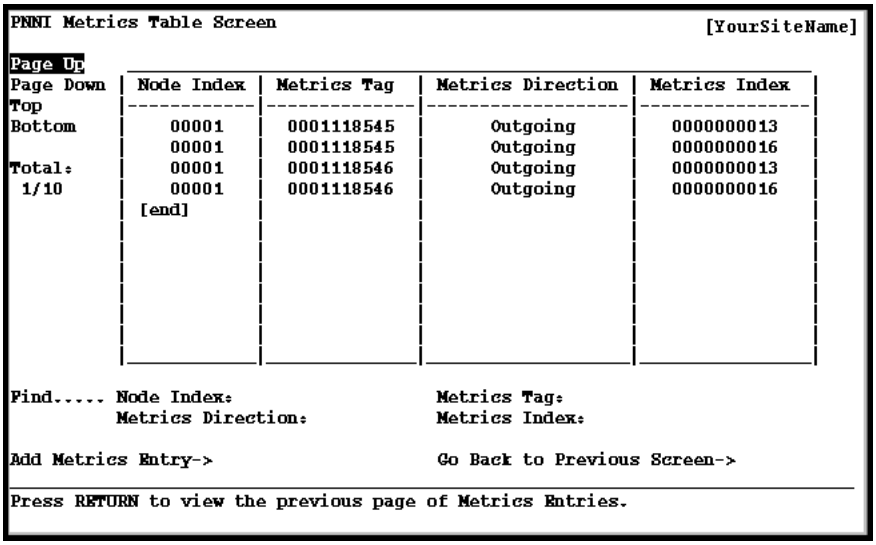

Figure 4-30. PNNI Metrics Table Window

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index, Metrics Direction, Metrics Tag**, or **Metrics Index** fields.
• Add Metrics Entry	Displays the PNNI Metrics Configuration window.
• Go Back to Previous Screen	Displays the PNNI Route Address Configuration window.

2 Select the **Add Metrics Entry** command.

The PNNI Metrics Configuration window is displayed (see Figure 4-31).

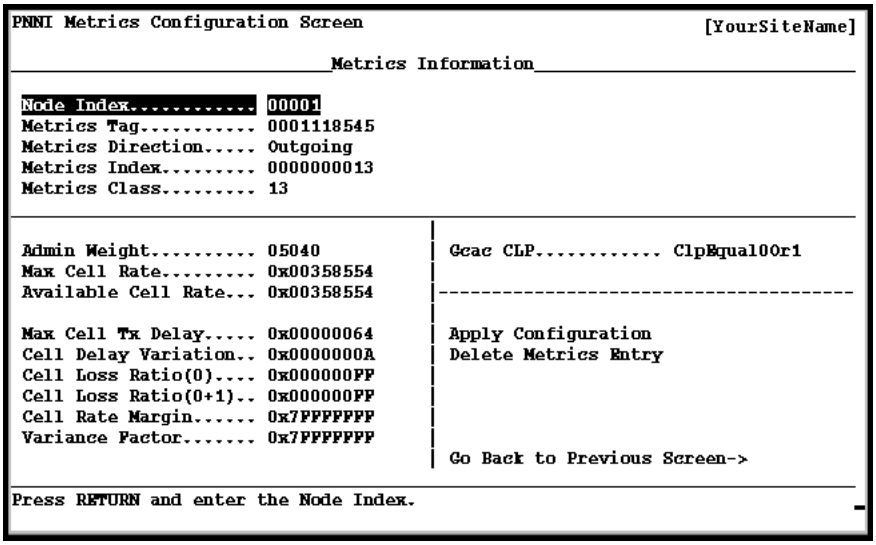

Figure 4-31. PNNI Metrics Configuration Window

Commands

The commands in this window have the following functions:

Command	Function
• Create Metrics Entry (displays upon initial metrics configuration)	Adds the metric entry to the PNNI Metrics table.
• Apply Configuration	Applies the configuration values you set.
• Delete Metrics Entry	Deletes the metric entry from the PNNI Metrics table.
• Go Back to Previous Screen	Displays the PNNI Metrics Table window.

Field Descriptions

3 Select the values for the fields in this window as described in Table 4-15.

Table 4-15. Field Values for the PNNI Metrics Configuration Window

Field Name	Values	Description
Node Index	0 (default) Range: 1–65535	The unique identifier for this node. Enter **1** in this field.
Metrics Tag	0 (default)	A user-defined number that identifies this set of traffic parameters. A single metrics tag can be assigned to multiple routes if they all have the same set of traffic parameters.
Metrics Direction	Incoming (default); Outgoing	The direction, with respect to the advertising node, to which these parameters apply (may have multiple service categories).
Metrics Index	0 (default)	An index into a set of parameters associated with the given tag and direction.
Metrics Classes	0 (default) Range: 0–31	The service class to which this metric belongs. Service classes displayed are as follows: • CBR • rt_VBR • nrt_VBR • ABR (displayed but not supported by PSAX systems) • UBR
Admin Weight	0 (default) Range: 1–16777215	The administrative weight from the advertising node to the remote end of the PNNI entity or to the reachable address or transit network, for the specified service categories. The lower the value of the administrative weight, the more preferable this interface.
Max Cell Rate	0xFFFFFFFF (default)	Maximum cell rate, in hexadecimal notation, for one directions and specific service category (see the descriptions for **Metrics Direction** and **Metrics Classes**.
Available Cell Rate	0xFFFFFFFF (default)	Available bandwidth on this interface, in hexadecimal notation.
Max Cell Tx Delay	0xFFFFFFFF (default)	Amount of delay in the transit of cells from point A to point B, in hexadecimal notation.

Table 4-15. Field Values for the PNNI Metrics Configuration Window

Field Name	Values	Description
Cell Delay Variation	0xFFFFFFFF (default)	Variation in the cell transit delay, in hexadecimal notation.
Cell Loss Ratio (0)	0xFFFFFFFF (default)	Cells lost/number of cells sent for the peak cell rate 0 category, in hexadecimal notation.
Cell Loss Ratio (0+1)	0xFFFFFFFF (default)	Cells lost/number of cells sent for the peak cell rate 0+1 category, in hexadecimal notation.
Cell Rate Margin	0xFFFFFFFF (default)	Difference between the effective bandwidth allocation and the allocation for sustainable cell rate (the safety margin above the sustainable cell rate), in hexadecimal notation.
Variance Factor	0xFFFFFFFF (default)	Relative measure of the square root of cell rate margin, normalized by the variance of some of the cell rates of all existing connections, in hexadecimal notation.
Gcac CLP	ClpEqual0 (default); ClpEqual0or1	Cell loss priority for generic connection admission control (GCAC).

4 Select the **Create Metrics Entry** command.

This entry is added to the PNNI Metrics Table window.

5 If you are making changes to an existing metric configuration, select the **Apply Configuration** command.

6 Type **Ctrl+G** to return to the Console Interface Main Menu window and save the configuration.

End

Configuring Summary Addresses

To configure PNNI summary addresses, perform the steps in the following procedure.

Summary Address Configuration

Begin

1 On the Console Interface Main Menu, select the **Site-Specific Configuration** option, and press Enter.

The Site-Specific Menu is displayed.

2 Select the **PNNI System-Wide Configuration** option, and press Enter.

The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3 Select the **PNNI Summary Address Configuration** command.

The PNNI Summary Address Table window is displayed (see Figure 4-32).

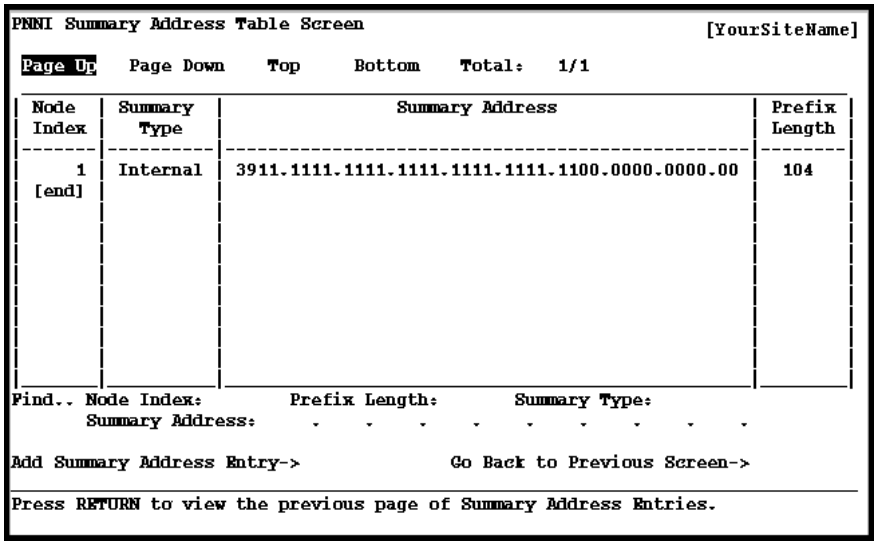

Figure 4-32. PNNI Summary Address Table

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index, Prefix Length, Summary Type**, or **Summary Address** fields.
• Add Metrics Entry	Displays the PNNI Summary Address Configuration window.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

4 Select the **Add Summary Address Entry** command.

The PNNI Summary Address Entry window is displayed (see Figure 4-33).

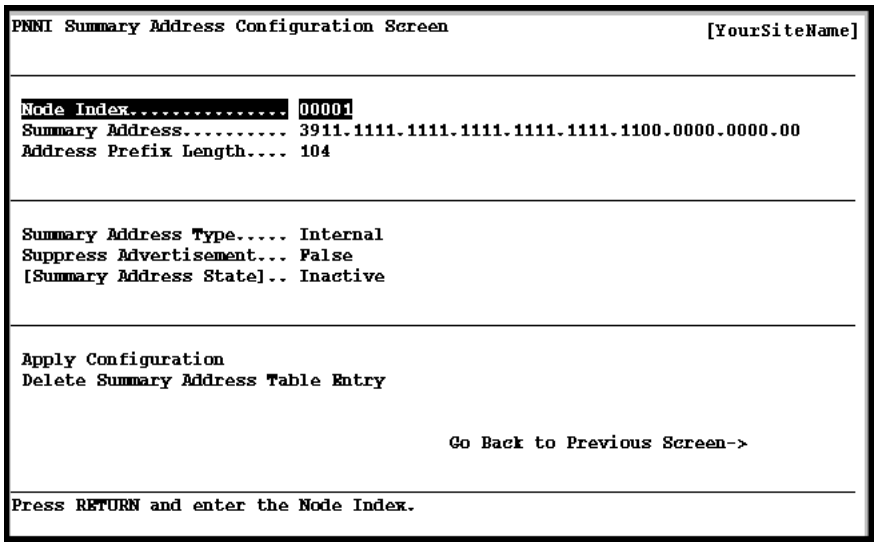

Figure 4-33. PNNI Summary Address Configuration Window

Commands

The commands in this window have the following functions:

Command	Function
• Create Summary Address Entry (displays upon initial summary address configuration)	Adds the route address to the PNNI Summary Address table.
• Apply Configuration	Applies the configuration values you set.
• Delete Summary Address Entry	Deletes the route address from the PNNI Summary Address table.
• Go Back to Previous Screen	Displays the PNNI Summary Address Table window.

Field Descriptions

5 Select the values for the fields in this window as described in Table 4-16.

Table 4-16. Field Values for the PNNI Summary Address Configuration Window

Field Name	Values	Description
Node Index	0 (default) Range: 1–65535	The unique identifier for this node. Enter **1** in this field.
Summary Address	0 (default) (hexidecimal)	The address prefix of the ATM end system. This tells a node how to summarize reachability information.
Address Prefix Length	0 (default)	A string of 0–152 bits that is the lead portion of one or more ATM addresses.
Summary Address Type	Internal (default); Exterior	Internal denotes that a link, node, or reachable address is inside of a PNNI routing domain. Exterior denotes that a link, node, or reachable address is outside of a PNNI routing domain.
Suppress Advertisement	False (default), True	Determines whether the summary is advertised within this peer group.
[Summary Address State] (display only)	Advertising (default); Active, Inactive	Indicates whether the summary is currently being advertised by the node within the PSAX system into its peer group.

6 Select the **Create Summary Address Entry** command.

This entry is added to the PNNI Summary Address Table window.

7 Type **Ctrl+G** to return to the Console Interface Main Menu window and save the configuration.

End

Viewing the PNNI Map Link Table

PNNI Map Link Table contains attributes necessary to find and analyze the operation of all links and nodes within the PNNI hierarchy, as seen from the perspective of a local node. It also provides information for network management to map port identifiers from the nodes at both ends to the link between them.

The PNNI Map Link table is read-only, reflecting the fact that the map is discovered dynamically during operation of the PNNI protocol, not manually configured.

To view PNNI map links, perform the steps in the following procedure.

Viewing PNNI Map Links

Begin

1. On the Console Interface Main Menu, select the **Site-Specific Configuration** option, and press Enter.

   The Site-Specific Menu is displayed.

2. Select the **PNNI System-Wide Configuration** option, and press Enter.

   The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3. Select the **PNNI Map Link Information** command.

   The PNNI Map Link Table window is displayed (see Figure 4-34).

```
PNNI Map Link Table Screen                                    [YourSiteName]
 Page Up   Page Down    Top     Bottom    Total:   1/2
 ____________________________________________________________________________
|Node |        Originating Node Identifier                      | Org     | Map |
|Index|                                                         | Port Id | Index|
|-----|---------------------------------------------------------|---------|-----|
|    1|60A0.3911.1111.1111.1111.1111.1111.1111.1111.0000.1111  |  301001 |    1|
|    1|60A0.3911.1111.1111.1111.1111.1111.1111.1111.1111.1111  |  201001 |    1|
|[end]|                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|     |                                                         |         |     |
|_____|_________________________________________________________|_________|_____|

Find.. Node Index:       Org. Port Id:            Map Index:
       Org. Node Id:     .    .    .    .    .    .    .    .    .    .
                                        Go Back to Previous Screen->

Press RETURN to view the previous page of Map Link Entries.
```

Figure 4-34. PNNI Map Link Table Window

The PNNI Map Link Table window displays the node index, originating node identifier, originating port identifier, and map index for various map links.

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index, Org. Port Id, Map Index**, or **Org. Node Id** fields.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

The **Originating Node Identifier** is the node identifier of the node whose connectivity within itself or to other nodes is being described.

The **Org Port Id** is the port identifier of the port as assigned by the originating node, to which the port is attached.

The **Map Index** is an index into the set of link and nodal connectivity associated with the originating node and port. This index is needed since multiple entries for nodal connectivity from a specific node and port pair can exist, in addition to any entry for a horizontal link or uplink.

4 If a node has been created, select the node for which you want to view information and press Enter.

The PNNI Map Link Configuration window is displayed (see Figure 4-35).

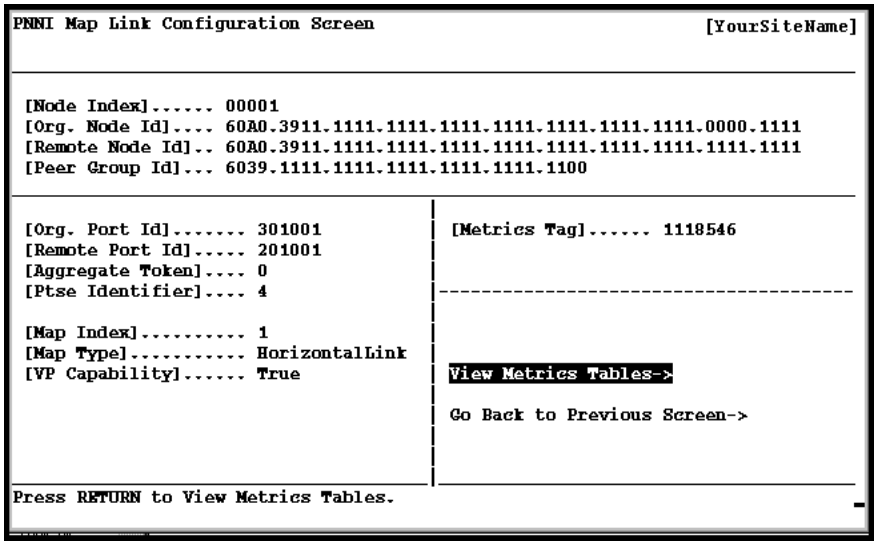

Figure 4-35. PNNI Map Link Configuration Window

Commands The commands in this window have the following functions:

Command	Function
• View Metrics Tables	Displays the PNNI Metrics Configuration window.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

Field Descriptions

5 The values for the fields in this window are described in Table 4-17.

Table 4-17. Field Values for the PNNI Map Link Configuration Window

Field Name	Values	Description
[Node Index] (display only)	Range: 1–65535	The unique identifier for this node.
[Org. Node Id] (display only)	(Numerical data)	Node identifier of the node whose connectivity within itself or to other nodes is being described.
[Remote Node Id] (display only)	(Numerical data)	Node identifier at the other end of the link from the originating node. A value of all zeroes means the node identifier is unknown.
[Peer Group Id] (display only)	(Numerical data)	Peer group identifier of the originating node.
[Org. Port Id] (display only)	(Numerical data)	Port identifier of the port as assigned by the originating node, to which the port is attached.
[Remote Port Id] (display only)	(Numerical data)	Port identifier of the port at the remote end of the link as assigned by the remote node. A value of all zeroes means the port identifier is unknown.
[Aggregate Token] (display only)	(Numerical data)	Hierarchical PNNI is currently not supported, so the value is 0.
[Ptse Identifier] (display only)	(Numerical data)	PTSE identifier containing the information describing this link or node.
[Map Index] (display only)	(Numerical data)	An index into the set of link and nodal connectivity associated with the originating node and port. This index is needed since there may be multiple entries for nodal connectivity from a specific node and port pair, in addition to any entry for a horizontal link or uplink.

Table 4-17. Field Values for the PNNI Map Link Configuration Window

Field Name	Values	Description
[Map Type] (display only)	Horizontal Link	The type of PNNI entity being described in this entry.
[VP Capability] (display only)	True, False	Indicates whether VPCs can be established across the PNNI entity being described in this entry
[Metrics Tag] (display only)	(Numerical data)	Associates a set of traffic parameters that are always advertised together. It is used as an index into the PNNI Metrics Table. A value of zero indicates no metrics are associated with this PNNI entity.

6 To view the Metrics table, select **View Metrics Tables** and press Enter.

The Metrics Table window is displayed (see Figure 4-30).

7 To return to the Map Link Table window, **Go Back to Previous Screen** and press Enter.

The Map Link Table window is displayed (see Figure 4-34).

End

Viewing the PNNI Link Table

The PNNI Link table contains the attributes necessary to describe the operation of logical links attached to the PSAX system and the relationship with the neighbor nodes on the other end of the links. Links are attached to a specific node within the PSAX system. Links may represent horizontal links between lowest level neighboring peers, outside links, uplinks, or horizontal links to or from logical group nodes (LGNs).

The PNNI Link table is read-only because the information in the Link table is discovered dynamically by the PNNI protocol, not manually configured. For more information, see the ATM Forum Specification, *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0, af-pnni-0055.000,* Section 5.6.

To view PNNI links, perform the steps in the following procedure.

Viewing PNNI Links

Begin

1 On the Console Interface Main Menu, select the **Site-Specific Configuration** option, and press Enter.

The Site-Specific Menu is displayed.

2 Select the **PNNI System-Wide Configuration** option, and press Enter.

The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3 Select the **PNNI Link Information** command.

The PNNI Link Table window is displayed (see Figure 4-36).

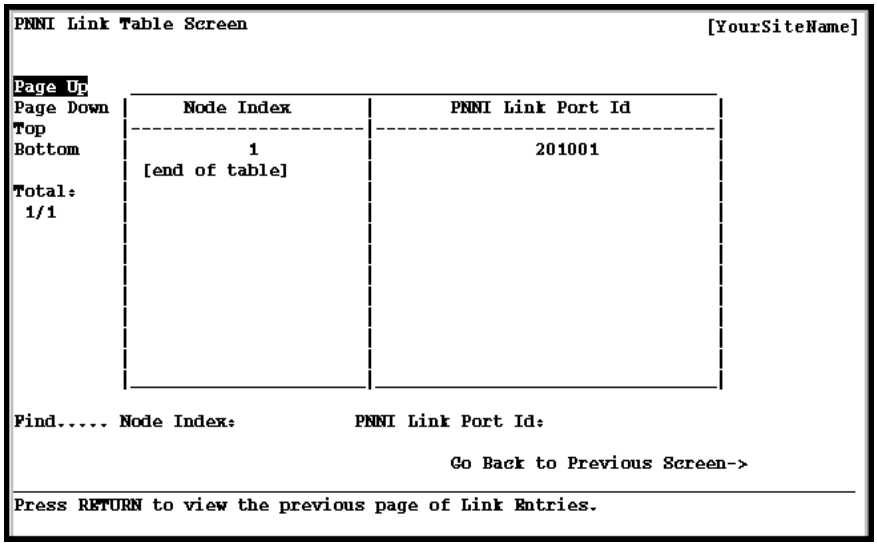

Figure 4-36. PNNI Link Table

The PNNI Link Table window displays the node index, and link port identifier for various PNNI links.

The **PNNI Link Port Id** is the port identifier of the link as selected by the local node. This value has meaning only within the context of the node to which the port is attached.

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index** or **PNNI Link Port Id** fields.
• Add Metrics Entry	Displays the PNNI Link Configuration window.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

4 If a node has been created, select the node for which you want to view information and press Enter.

The PNNI Link Configuration window is displayed (see Figure 4-37).

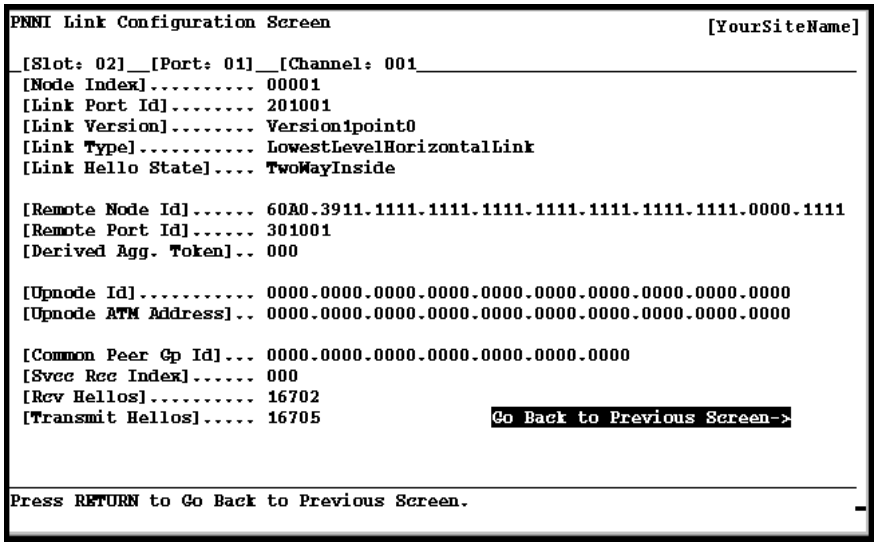

Figure 4-37. PNNI Link Configuration Window

Commands

The command in this window has the following function:

Command	Function
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

Field Descriptions

5 The values for the fields in this window are described in Table 4-18.

Table 4-18. Field Values for the PNNI Link Configuration Window

Field Name	Values	Description
[Node Index] (display only)	Range: 1–65535	The unique identifier for this node.
[Link Port Id] (display only)	(Numerical data)	Port identifier of the link as selected by the local node. This value has meaning only within the context of the node to which the port is attached.

Table 4-18. Field Values for the PNNI Link Configuration Window

Field Name	Values	Description
[Link Version] (display only)	Version1point0 Unknown	For horizontal and outside links between lowest-level nodes and for links of unknown type, this attribute indicates the version of PNNI routing protocol used to exchange information over this link. If communication with the neighbor node has not yet been established, the version is set to **Unknown**. For uplinks (where the port ID is not also used for the underlying outside link) or links to/from LGNs, the version is set to **Unknown**.
[Link Type] (display only)	Unknown LowestLevel HorizontalLink HorizontalLink ToFromLgn LowestLev-elOutsideLink Uplink OutsideLin-kAndUplink	Indicates the type of link being described.
[Link Hello State] (display only)	TwoWayInside	For horizontal and outside links between lowest-level nodes and for links of unknown type, this attribute indicates the state of the Hello protocol exchange over this link. For links to or from LGNs, this attribute indicates the state of the corresponding LGN Horizontal Link Hello State Machine. For uplinks (where the port ID is not also used for the underlying outside link), this attribute is set to "not appli-cable."
[Remote Node Id] (display only)	(Numerical data)	Node identifier.

Table 4-18. Field Values for the PNNI Link Configuration Window

Field Name	Values	Description
[Remote Port Id] (display only)	(Numerical data)	Indicates the port identifier of the port at the remote end of the link as assigned by the remote node. If "outsideLinkAndUplink" is displayed in the **Link Type** field, this is the port identifier assigned by the lowest-level neighbor node to identify the outside link. If "unknown" is displayed in this field, or if "uplink" is displayed in the **Link Type** field, the remote port ID is set to zero.
[Derived Agg. Token] (display only)	(Numerical data)	A PNNI aggregation token - this is used to determine which links to a given neighbor node are to be aggregated and advertised as a single logical link.
[Upnode Id] (display only)	(Numerical data)	For outside links and uplinks, this attribute contains the Node Identifier of the upnode (the neighbor node's identity at the level of the common peer group). When the upnode has not yet been identified, this attribute is set to zero. For horizontal links or when the link type is not yet known, this attribute is set to zero.
[Upnode ATM Address] (display only)	(Numerical data)	For outside links and uplinks, this attribute contains the ATM end system address used to establish connections to the upnode. When the upnode has not yet been identified, this attribute is set to zero. For horizontal links or when the link type is not yet known, this attribute is set to zero.

Table 4-18. Field Values for the PNNI Link Configuration Window

Field Name	Values	Description
[Common Peer Gp Id] (display only)	(Numerical data)	The common peer group identifier. For outside links and uplinks, this attribute contains the peer group identifier of the lowest level common peer group in the ancestry of the neighboring node and the node within the PSAX system. The value of this attribute takes on a value determined by the Hello exchange of hierarchical information that occurs between the two lowest-level border nodes. When the common peer group has not yet been identified, this attribute is set to zero. For horizontal links or when the link type is not yet known, this attribute is set to zero.
[Svcc Rcc Index] (display only)	(Numerical data)	The value of this object identifies the SVCC-based RCC for which the entry contains management information.
Rcv Hellos (display only)	(Numerical data)	For horizontal and outside links between lowest-level nodes and for links of unknown type, this attribute contains a count of the number of Hello packets received over this link. If "horizontalLinkToFromLgn" or "uplink," is displayed in the **Link Type** field, this field is set to zero.
[Transmit Hellos] (display only)	(Numerical data)	For horizontal and outside links between lowest-level nodes and for links of unknown type, this attribute contains a count of the number of Hello packets transmitted over this link. If "horizontalLinkToFromLgn" or "uplink," is displayed in the **Link Type** field, this field is set to zero.

6 To return to the Link Table window, **Go Back to Previous Screen** and press Enter.

The Link Table window is displayed (see Figure 4-36).

End

Viewing the PNNI Neighbor Peer Table

The PNNI Neighbor Peer table contains all the attributes necessary to describe the relationship a node in the PSAX system has with a neighboring node within the same peer group.

The PNNI Neighbor Peer table is read-only because neighboring peers are discovered dynamically by the PNNI protocol, not manually configured. For more information, see the ATM Forum Specification, *Private Network-Network Interface (PNNI 1.0) Specification Version 1.0, af-pnni-0055.000,* Sections 5.7 and 5.8.

To view PNNI neighbor peers, perform the steps in the following procedure.

Viewing PNNI Neighbor Peers

Begin

1. On the Console Interface Main Menu, select the **Site-Specific Configuration** option, and press Enter.

   The Site-Specific Menu is displayed.

2. Select the **PNNI System-Wide Configuration** option, and press Enter.

   The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3. Select the **PNNI Neighbor Peer Information** command.

   The PNNI Neighbor Peer Table window is displayed (see Figure 4-38).

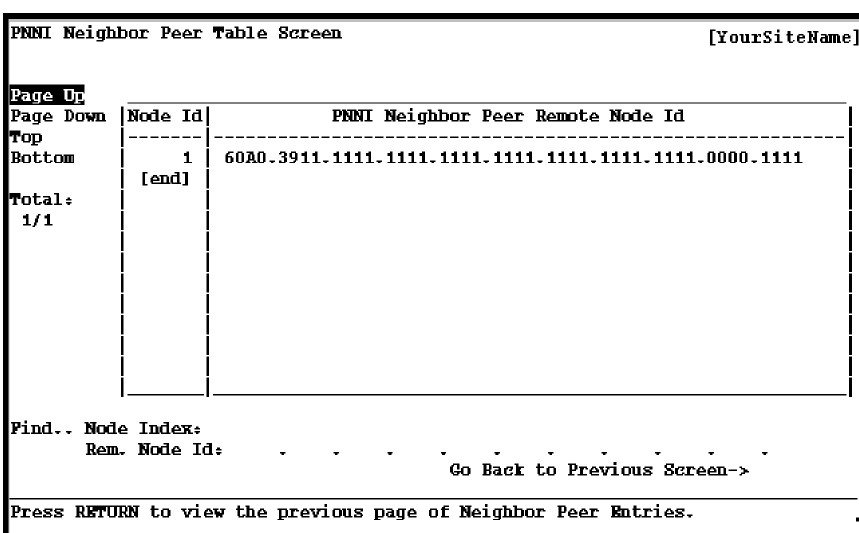

Figure 4-38. PNNI Neighbor Peer Table

The PNNI Neighbor Peer Table window displays the node index and neighbor peer remote node index for various neighbor peers.

The **PNNI Neighbor Peer Remote Node Id** is the node identifier of the neighboring peer node.

Commands

The commands in this window have the following functions:

Command	Function
• Find..	Searches this table by the values you enter in the **Node Index** or **Rem. Node Id** fields.
• Add Metrics Entry	Displays the PNNI Neighbor Peer Configuration window.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

4 If a node has been created, select the node for which you want to view information and press Enter.

The PNNI Neighbor Peer Configuration window is displayed (see Figure 4-39).

```
PNNI Neighbor Peer Configuration Screen                    [YourSiteName]


 [Node Index]............. 00001
 [NbrPeer Rem Node Id]... 60A0.3911.1111.1111.1111.1111.1111.1111.1111.0000.1111
 [NbrPeer State]......... Full
 [NbrPeer Svcc Rcc Id]... 0
 [NbrPeer Port Count].... 1

 [NbrPeer Rcv DbSums].... 3
 [NbrPeer Xmt DbSums].... 2
 [NbrPeer Rcv Ptsps]..... 419
 [NbrPeer Xmt Ptsps]..... 568

 [NbrPeer Rcv Ptse Req].. 1
 [NbrPeer Xmt Ptse Req].. 0
 [NbrPeer Rcv Ptse Ack].. 567
 [NbrPeer Xmt Ptse Ack].. 416

                                          Go Back to Previous Screen->


Press RETURN to Go Back to Previous Screen
```

Figure 4-39. PNNI Neighbor Peer Configuration Window

Commands

The commands in this window have the following functions:

Command	Function
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

Field Descriptions

5 The values for the fields in this window are described in Table 4-19.

Table 4-19. Field Values for the PNNI Neighbor Peer Configuration Window

Field Name	Values	Description
[Node Index] (display only)	Range: 1–65535	The unique identifier for this node.
[NbrPeer Rem Node Id] (display only)	(Numerical data)	Node identifier of the neighboring peer node.
[NbrPeer State] (display only)	Npdown Negotiating Exchanging Loading Full	Indicates the state of this node's neighboring peer state machine associated with the neighbor peer remote node ID.
[NbrPeer Svcc Rcc Index] (display only)	(Numerical data)	Identifies the SVCC-based RCC being used to communicate with the neighboring peer if one exists. If both the local node and the neighboring peer node are lowest-level nodes, this field is set to zero.
[NbrPeer Port Count] (display only)	(Numerical data)	A count of the total number of ports that connect to the neighboring peer. If the neighboring peer only communicates via an SVCC-based RCC, the value of this field is set to zero. Otherwise it is set to the total number of ports to the neighboring peer in the Hello state two-way inside.
[NbrPeer Rcv DbSums) (display only)	(Numerical data)	A count of the number of database summary packets received from the neighboring peer.
[NbrPeer Xmt DbSums) (display only)	(Numerical data)	A count of the number of database summary packets transmitted to the neighboring peer.
[NbrPeer Rcv Ptsps] (display only)	(Numerical data)	A count of the number of PTSPs received from the neighboring peer.

Table 4-19. Field Values for the PNNI Neighbor Peer Configuration Window

Field Name	Values	Description
[NbrPeer Xmt Ptsps] (display only)	(Numerical data)	A count of the number of PTSPs (re)transmitted to the neighboring peer.
[NbrPeer Rcv Ptse Req] (display only)	(Numerical data)	A count of the number of PTSE request packets received from the neighboring peer.
[NbrPeer Xmt Ptse Req] (display only)	(Numerical data)	A count of the number of PTSE request packets transmitted to the neighboring peer.
[NbrPeer Rcv Ptse Ack] (display only)	(Numerical data)	A count of the number of PTSE acknowledgement packets received from the neighboring peer.
[NbrPeer Xmt Ptse Ack] (display only)	(Numerical data)	A count of the number of PTSE acknowledgement packets transmitted to the neighboring peer.

6 To return to the Link Table window, **Go Back to Previous Screen** and press Enter.

The Neighbor Peer Table window is displayed (see Figure 4-38).

End

Viewing PNNI System Statistics

To view PNNI system statistics, perform the steps in the following procedure.

Viewing PNNI PNNI System Statistics

Begin

1 On the Console Interface Main Menu, select the **Site-Specific Configuration** option, and press Enter.

The Site-Specific Menu is displayed.

2 Select the **PNNI System-Wide Configuration** option, and press Enter.

The PNNI System-Wide Configuration window is displayed (see Figure 4-25).

3 Select the **PNNI System Statistics** command.

The PNNI System Statistics window is displayed (see Figure 4-40).

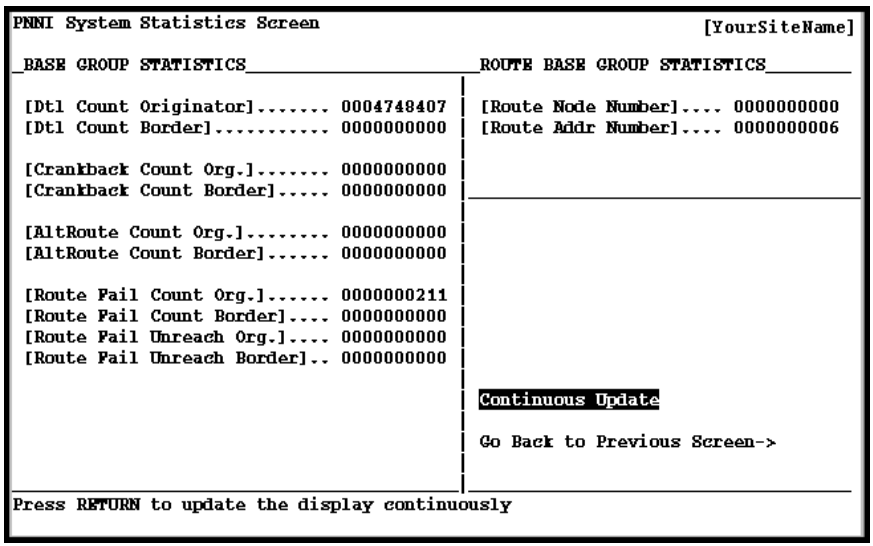

Figure 4-40. PNNI System Statistics Window

Commands

The commands in this window have the following functions:

Command	Function
• Continuous Update	Updates the values in the fields on this window continuously. Use this command as a toggle switch to view the statistics.
• Go Back to Previous Screen	Displays the PNNI System-Wide Configuration window.

Field Descriptions

The fields in this window are described in Table 4-20.

Table 4-20. Field Values for the PNNI System Statistics Window

Field Name	Description
[Dtl Count Originator]	The total number of designated transit list (DTL) stacks that the PSAX 20 system has originated as the DTL originator and placed into signaling messages. This includes the initial DTL stacks computed by the PSAX 20 system and any alternate route. DTL stacks computed by the PSAX 20 system in response to crankbacks.
[Dtl Count Border]	The number of partial DTL stacks that the PSAX 20 system has added into signaling messages as an entry border node. This includes the initial partial DTL stacks computed by the PSAX 20 system and any alternate route. Partial DTL stacks computed by the PSAX 20 system in response to crankbacks.
[Crankback Count Org.]	The count of the total number of connection setup messages including DTL stacks originated by the PSAX 20 system that have cranked back to PSAX 20 system at all levels of the hierarchy.
[Crankback Count Border]	The count of the total number of connection setup messages including DTLs added by the PSAX 20 system as an entry border node that have cranked back to the PSAX 20 system at all levels of the hierarchy. This count does not include crankbacks for which the PSAX 20 system was not the crankback destination. Only those crankbacks that were directed to the PSAX 20 system are counted here.
[AltRoute Count Org.]	The total number of alternate DTL stacks that the PSAX 20 system has computed and placed into signaling messages as the DTL originator.
[AltRoute Count Border]	The total number of alternate partial DTL stacks that the PSAX 20 system has computed and placed into signaling messages as an entry border node.

Table 4-20. Field Values for the PNNI System Statistics Window

Field Name	Description
[Route Fail Count Org.]	The total number of times where the PSAX 20 system failed to compute a viable DTL stack as the DTL originator for a call. It indicates the number of times a call was cleared from the PSAX 20 system due to originator routing failure.
[Route Fail Count Border]	The total number of times where the PSAX 20 system failed to compute a viable partial DTL stack as an entry border node for some call. It indicates the number of times a call was either cleared or cranked back from the PSAX 20 system due to border routing failure.
[Route Fail Unreach Org.]	The total number of times where the PSAX 20 system failed to compute a viable DTL stack as the DTL originator because the destination was unreachable, i.e., calls that are cleared with the cause "specified transit network unreachable" or the cause "destination unreachable" in the cause incoming exclusion (IE).
[Route Fail Unreach Border]	The total number of times where the PSAX 20 system failed to compute a viable partial DTL stack as an entry border node because the target of the path calculation was unreachable, i.e., calls that are cleared or cranked back with the cause "specified transit network unreachable" or the cause "destination unreachable" in the cause IE.
[Route Node Number]	The number associated with the route node from which the statistics on this window are being generated.
[Route Addr Number]	The number associated with the route address from which the statistics on this window are being generated.

End

Configuring Call Control Resource Allocation

Perform the steps in the following procedure to configure the call control resource allocations for your Access Concentrator system.

Setting the Configuration Values

Allocating Call Resources

Begin

1 From the Console Interface Main Menu, select Site-Specific Configuration. The Site-Specific Menu is displayed (see Figure 4-41).

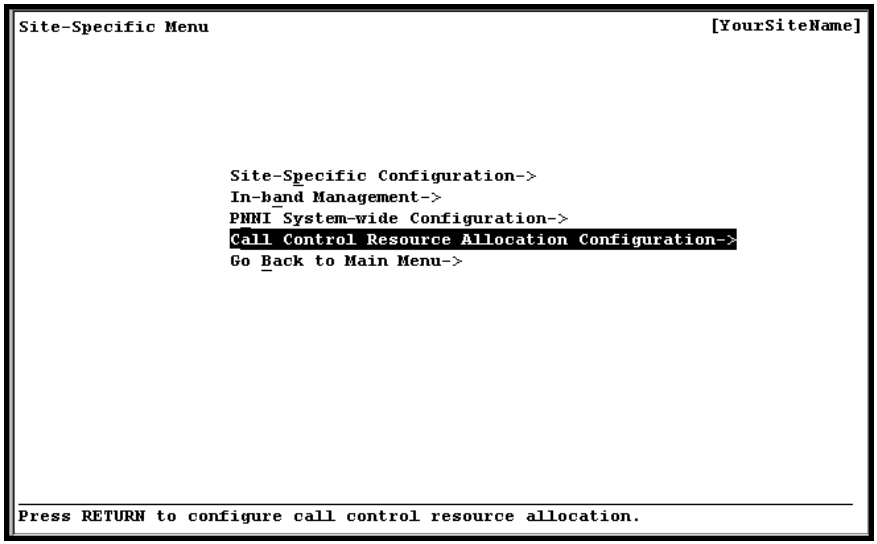

Figure 4-41. Site Specific Menu

2 Select **Call Control Resource Allocation Configuration** option and press Enter.

The Call Control Resource Allocation Configuration window is displayed (see Figure 4-42).

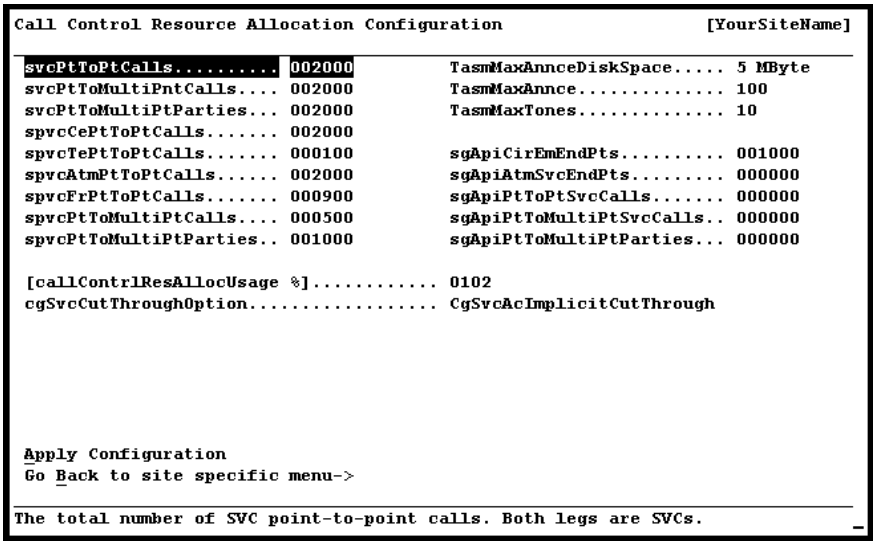

Figure 4-42. Call Control Resource Allocation Configuration Window

Commands

The commands on this window have the following functions:

Command	Function
• Apply Configuration	Applies the values you enter in the this window.
• Go Back to site specific menu→	Reis displayed the Site-Specific Menu window.

Configuration Guidelines

Note: Read the following configuration guidelines before you enter values in the fields.

When you are entering values in the fields, follow these guidelines for successfully allocating call control resources:

- The maximum value for **svcPointToPointCalls** is **10950** if the other fields in the Call Control Resource Allocation Configuration window are set to **0**.
- The maximum value for **svcPointToMultiPointCalls** is **6000**, and the maximum value for **svcPointToMultiPointParties** is **6000**, if the values in the other fields on the Call Control Resource Allocation Configuration window are set to **0**.

Note: The value for **svcPointToMultiPointParties** must be greater than or equal to the value for **svcPointToMultiPointCalls**,

because each point-to-multipoint call must have at least one party.

~ The sum of the values in the following fields cannot exceed 5000: **spvcCePointToPointCalls**, **spvcTePointToPointCalls**, **spvcAtmPointToPointCalls**, and **spvcFrPointToPointCalls**

Note: If you already have an existing, configured Access Concentrator system, the sum of the values in the SPVC point-to-point calls fields cannot be less that the actual number of SPVC connections already configured in the SPVC table, which resides in the MIB.

~ When changing the values in these fields to suit your needs, keep in mind that the system calculates the percentage of the memory allocation usage from the combination of values you have entered in the fields. This calculation is displayed in the **callContrlResAllocUsage** field. When all the values of SVC calls and parties, SPVC calls, connection gateway API endpoints, and connection gateway API calls and parties are calculated as a percentage, which cannot exceed 100 percent of the memory allocation. If you enter a combination of values that, when calculated, exceeds 100 percent, an error message is displayed at the bottom of the window:

```
T-CallControlResAllocFail
```

If you get this error message, adjust the values in the fields and use the **Apply Configuration** command to calculate the allocation usage percentage value. When you enter a combination of values that results in a value of 100 percent or less, the following informational message is displayed:

```
Resource allocation configuration has been applied.  Need
to save configuration and reboot the system to take
effect.
```

Field Descriptions

3 Select the values for the fields on this window from the values given in Table 4-21.

Table 4-21. Field Values for the Call Control Resource Allocation Configuration Window

Field Name	Values	Description
svcPoint-ToPointCalls	Default: 002000	The total number of SVC point-to-point calls to be supported by the PSAX system.
svcPointToMul-tiPointCalls	Default: 002000	The total number of SVC point-to-multipoint calls to be supported by the PSAX system.
svcPointToMulti PointParties	Default: 002000	The total number of parties on SVC point-to-multipoint calls to be supported by the PSAX system.

Table 4-21. Field Values for the Call Control Resource Allocation Configuration Window

Field Name	Values	Description
spvcCePointTo PointCalls	Default: 002000	The total number of circuit emulation point-to-point calls to be supported by the PSAX system.
spvcTePointTo PointCalls	Default: 00100	The total number of terminal emulation point-to-point calls to be supported by the PSAX system.
spvcAtmPointTo PointCalls	Default: 002000	The total number of ATM point-to-point calls to be supported by the PSAX system.
spvcFRPointTo PointCalls	Default: 000900	The total number of frame relay point-to-point calls to be supported by the PSAX system.
spvcPoint-ToMultiPoint-Calls	Default: 002000	The total number of SPVC point-to-multipoint calls to be supported by the PSAX system.
spvcPoint-ToMulti PointParties	Default: 002000	The total number of parties on SPVC point-to-multipoint calls to be supported by the PSAX system.
TasmMax-Annce-DiskSpace (MByte)		Currently not supported. Maximum disk size reserved for compressed announcements.
TasmMaxAnnce		Currently not supported. Maximum number of announcements on the CPU hard disk.
TasmMaxTones		Currently not supported. Maximum number of standard tones to supported by the system.
sgApiCirE-mEndPoints	Default: 001000	The total number of circuit emulation end points for Connection Gateway application programming interface (API) to be supported by the PSAX system.
sgApiAtmSvc EndPoints	Default: 000000	The total number of ATM SVC end points for Connection Gateway API to be supported by the PSAX system.

Table 4-21. Field Values for the Call Control Resource Allocation Configuration Window

Field Name	Values	Description
sgApiPointTo PointSvcCalls	Default: 000000	The total number of point-to-point SVC calls for Connection Gateway API to be supported by the PSAX system.
sgApiPointTo MultiPointSvc Calls	Default: 000000	The total number of point-to-multi-point SVC calls for Connection Gateway API to be supported by the PSAX system.
sgApiPointTo MultiPoint Parties	Default: 000000	The total number of parties for Connection GatewayConnection Gateway API to be supported by the PSAX system.
[callContrlRes AllocUsage %] (display only)	100 or less	The percentage of the current usage of the total call control resource memory allocated by the system to be supported by the PSAX system.
cgSvcCut ThroughOption	Default: cgSvcAcImplicit CutThrough	**Note:** The value in this field is not used if you do not have the Connection Gateway API feature enabled. The PSAX system sends a message to the connection manager to make a connection.
	cgSvcAcExplicit CutThrough	**Note:** The value in this field is not used if you do not have the Connection Gateway API feature enabled. The Connection Gateway device determines when to send a cut-through message to the connection manager.

4 To apply the values you have entered, select the **Apply Configuration** command and press Enter.

Once you modify a configuration and click **Apply**, the changes are temporarily stored in the CPU module in the PSAX device. To store them permanently, save changes selecting **Device > Save PSAX Configuration** from the *AQueView*™ Menu Bar.

End

Saving the Configuration and Rebooting the System

Perform the steps in the following procedure to save the values you have set, and reboot the Access Concentrator system

Saving Configuration Values and Rebooting System Components

Begin

1. To save the values you have entered, select the **Go Back to Site-Specific Menu** command and press Enter.

   The Site-Specific Menu window is displayed.

2. Select the **Go Back to Main Menu** command and press Enter.

   The Console Interface Main Menu is displayed.

3. Select the **Save Configuration** option and press Enter.

4. Select the **Diagnostics** option and press Enter.

   The Diagnostics Menu window is displayed (see Figure 4-43).

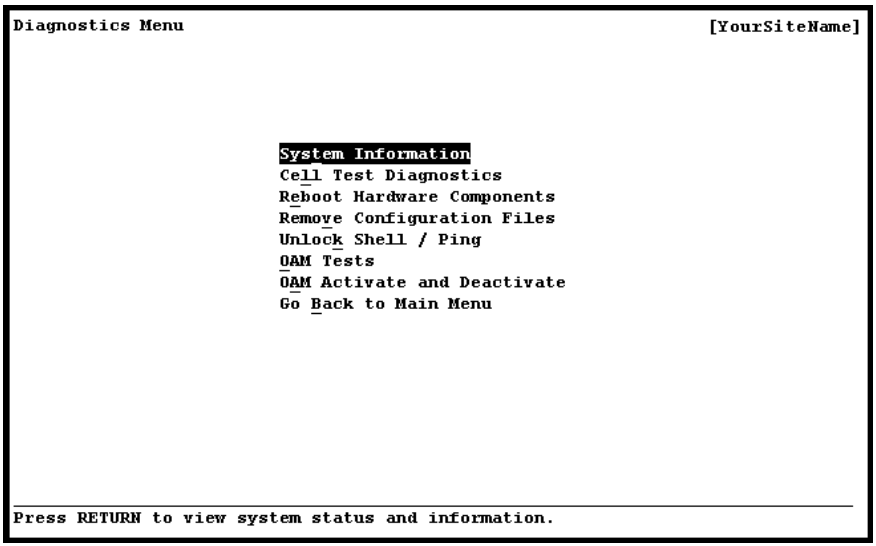

Figure 4-43. Diagnostics Menu

5. Select the **Reboot Hardware Components** option and press Enter.

The Remote Reboot Configuration window is displayed (see Figure 4-44).

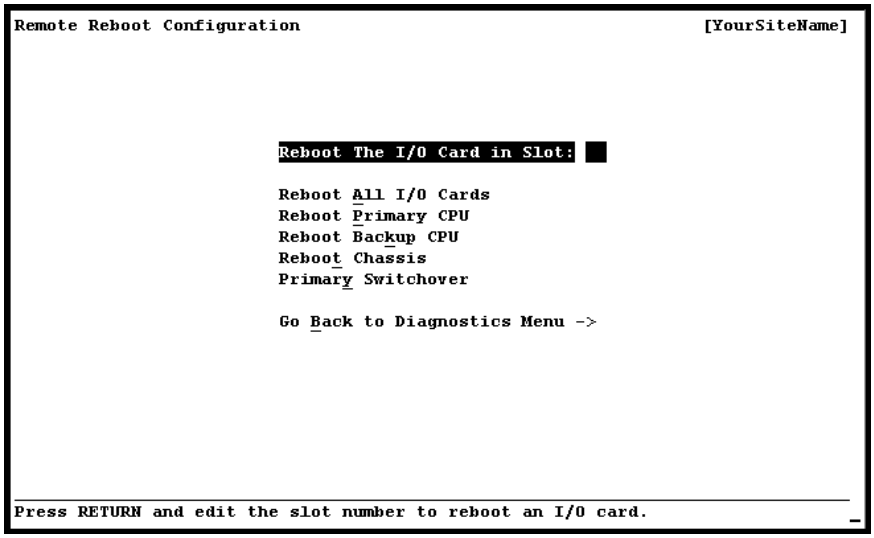

Figure 4-44. Remote Reboot Configuration Window

6 Select the **Reboot Chassis** command and press Enter.

The CPU module(s), I/O and server modules, T1/E1, and DSP components are rebooted.

The configuration values you entered in the procedure are now in effect.

End

Backing Up Your Configuration Data

You can back up the data on the Call Control Resource Allocation window by backing up the file ssid.def, which resides on the CPU module system disk. We highly recommend that you back up the ssid.def file, which contains your configuration data. See Chapter 7 for procedures on backing up your system software data.

After configuring the module ports and channels, the interface types for each port and channel, and the connections, you must save the configuration permanently, before you exit the current session of the PSAX Access Concentrator system console interface. We recommend that you save your configuration frequently, after you configure each module, and then again after configuring the connections of each type you will have in your system. Finally, before you quit your current session, be sure you save your configuration for the last time.

▲ CAUTION:
If you lose power or your current session ends abnormally while you are in the process of configuring the system, and you have not yet saved the values permanently, you will lose the values that you have applied in the various windows.

To save values permanently to the PSAX Access Concentrator system database, perform the steps in the following procedure.

Saving the Access Concentrator System Values

Begin

1. Press Ctrl+G while on any window to display the Console Interface Main Menu window.
2. Select the **Save Configuration** command and press Enter (or press Ctrl+A).

   Wait a few seconds while the system writes the values permanently to the Access Concentrator system database. The system displays the following message while it is executing this command:

`Saving the equipment and connection information` …

   When the command is completed, the system displays the following message:

`T-SaveConfiguration: saveConfigurationReasonCode=All-OK`

   You can now safely exit the current session.

3. Select the **Leave Console Interface** command and press Enter.

You are now logged off the PSAX Access Concentrator system console interface.

End

5 Using System Diagnostics

Overview of This Chapter

The PSAX system diagnostics functions give you the ability to:

- View the status of the PSAX system including:
  - ~ Version of the PSAX system software currently running
  - ~ Status of the hard disk on the CPU
  - ~ Statistics on the message pool and the cell buffers
- Run cell test diagnostics to determine whether a specified port is operating correctly
- Reboot (reinitialize) the PSAX chassis, CPU, user-selected I/O modules, or all components in the chassis
- Unlock a telnet session remotely
- Perform OAM loopback tests
- Configure activate or deactivate OAM functions

Viewing System Status

To view the status of the PSAX system, perform the steps in the following procedure.

Viewing System Status

Begin

1 From the Console Interface Main Menu window (see Figure 5-1), select the **Diagnostics** option and press Enter.

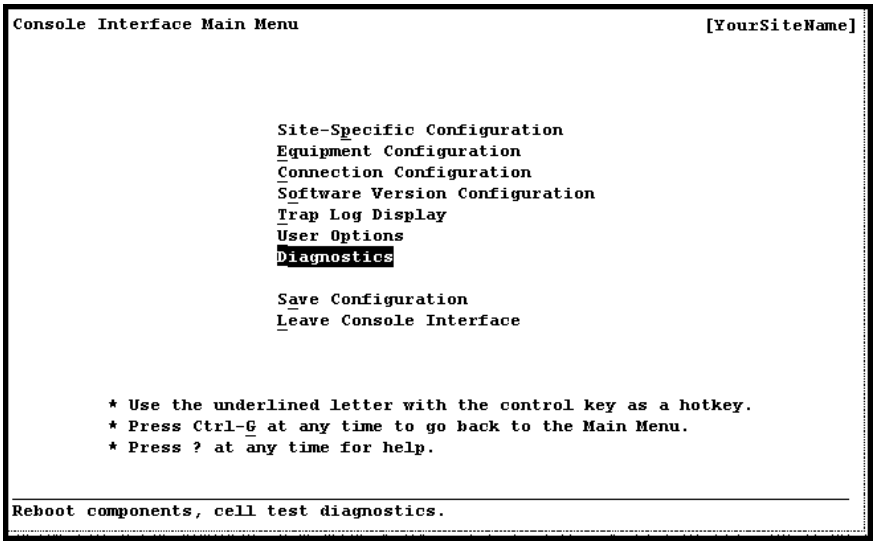

Figure 5-1. Console Interface Main Menu Window (Diagnostics Option Selected)

The Diagnostics Menu window is displayed (see Figure 5-2).

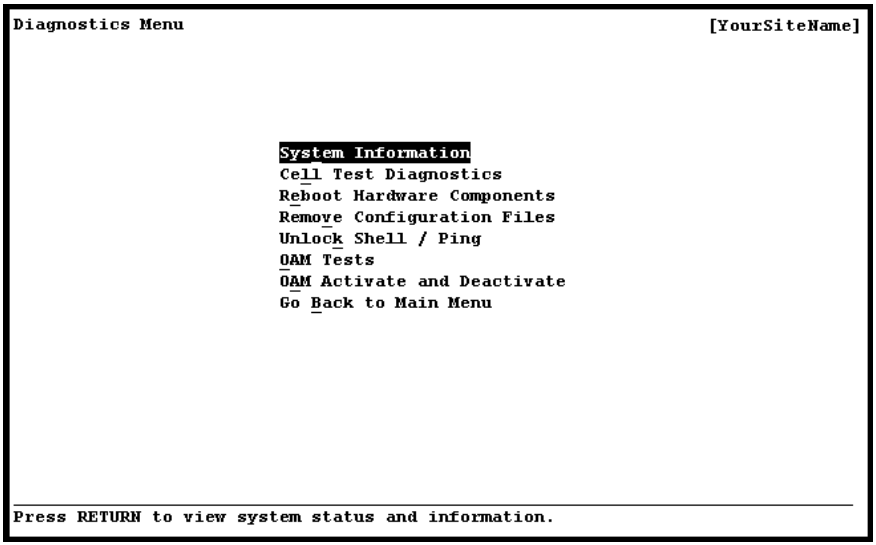

Figure 5-2. Diagnostics Menu Window

2 Select the **System Information** option and press Enter.

The System Information window is displayed (see Figure 5-3).

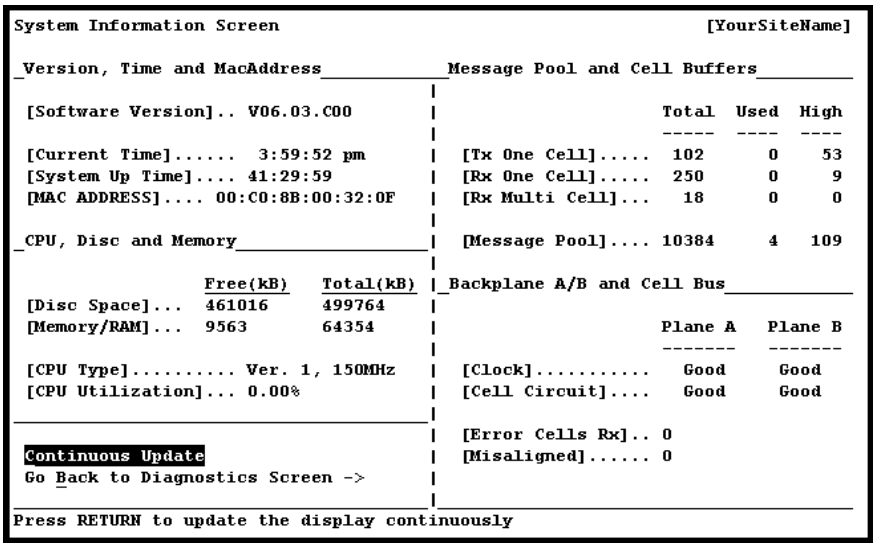

Figure 5-3. System Information Window

Commands

The commands on this window have the following functions:

Command	Function
• Continuous Update	Continuously updates the information in the fields every second. Select this command and press Enter to turn the continuous updating on and off as needed (similar to a toggle switch).
• Go Back to Diagnostics Screen→	Redisplays the Diagnostics Menu window (see Figure 5-2).

Field Descriptions

The display-only fields on this window are described in Table 5-1.

Table 5-1. Field Values for the System Information Window

Field Name	Description
[Software Version]	The version of the system software currently running on the CPU.
[Current Time]	Displays Universal Coordinated Time (UTC). This time value for the PSAX 20 system is set on the Site-Specific Configuration window.
[System Up Time]	The amount of time the PSAX 20 system has been running since the last time you applied power to the system, or rebooted (initialized) the CPU.
[Disc Space] (Free kBytes)	The amount of free space (in kilobytes) on the hard disk of the CPU.
[CPU Utilization]	The percentage of time the processor uses for processing data traffic.
Message Pool and Cell Buffers panel	Used primarily by technical support for diagnostic problems.
[Tx One Cell]	**Total**: Total amount of cells within the transmit one cell pool. **Used**: Amount of cells currently being used within the transmit one cell pool. **High**: High-water mark of cells used within the transmit one cell pool.
[Rx One Cell]	**Total**: Total amount of cells within the receive one cell pool. **Used**: Amount of cells currently being used within the receive one cell pool. **High**: High-water mark of cells used within the receive one cell pool.
[Rx Multi Cell]	**Total**: Total amount of multi-cells within the receive multi-cell pool. **Used**: Amount of multi-cells currently being used within the receive multi-cell pool. **High**: High-water mark of multi-cells used within the receive multi-cell pool.
[Message Pool]	**Total**: Total amount of messages within the message pool. **Used**: Amount of messages currently being used within the message pool. **High**: High-water mark of messages used within the message pool.

Table 5-1. Field Values for the System Information Window

Field Name	Description
[Error Cells Rx]	The number of bad cells (BIP16) received so far.
[Misaligned]	The number of misaligned cells received so far.

End

Running Cell Test Diagnostics

To determine whether a port is operating correctly, perform the steps in the following procedure.

Cell Test Diagnostics

Running Cell Tests

Begin

1. On the Console Interface Main Menu window (see Figure 5-1), select the **Diagnostics** option and press Enter.

   The Diagnostics Menu window is displayed (see Figure 5-2).

2. On the Diagnostics Menu window, select the **Cell Test Diagnostics** option and press Enter.

   The Cell Test Diagnostics window is displayed (see Figure 5-4).

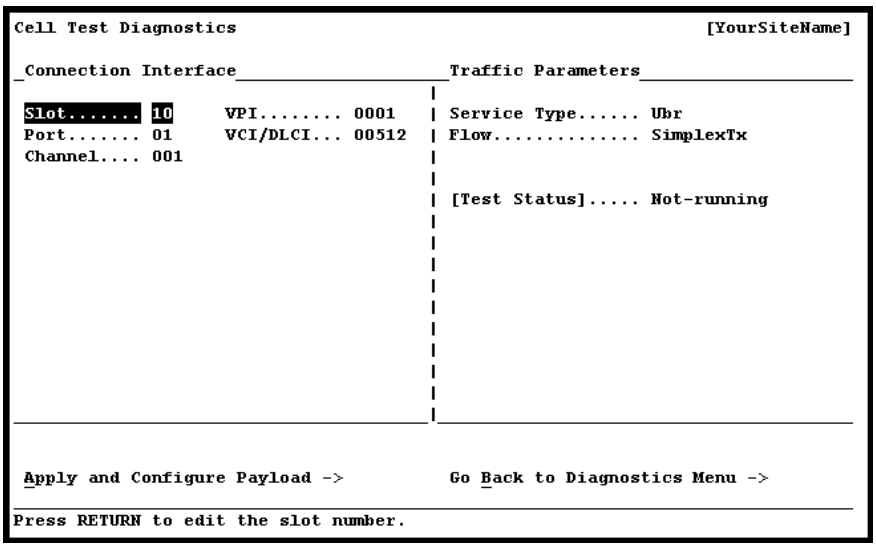

Figure 5-4. Cell Test Diagnostics Window

Commands

The commands on this window have the following functions:

Command	Function
• Apply and Configure Payload	Applies the traffic parameters you set, and displays the Cell Test Payload Configuration window.
• Go Back to Diagnostics Menu	Redisplays the Diagnostics Menu window.

Field Descriptions

3 To set up a connection for the port you want to test, select the values for the fields on this window from the values given in Table 5-2.

Table 5-2. Field Values for the Cell Test Diagnostics Window

Field Names	Values	Description
Slot	Range: The total number of slots in the Access Concentrator system	The slot number containing the module you want to test.
Port	Range: The total number available, per module	The port number on the module you want to test.
Channel	Range: The total number available, per module	The channel number for the port you want to test.
VPI	Range: 0–255	The virtual path identifier (VPI) for the channel you want to test.
VCI/DLCI	VCI range: 32–65535 DLCI range: 16–1024	The virtual channel identifier (VCI) or the data link connection identifier (DLCI) for the channel you want to test.
Service Type	Ubr (default), Vbr-nrt2, Vbr-rt2, Vbr-rt1, Vbr-express, Cbr4, Cbr3, Cbr2, Cbr1	The service type you have set up for the connection.

Table 5-2. Field Values for the Cell Test Diagnostics Window

Field Names	Values	Description
Flow	SimplexTx (default), SimplexRx, Duplex	The type of traffic flow you want to set up for the test: one-way transmit, one-way receive, or two-way flow.
[Test Status]	Running, Not-running	Indicates whether or not cell test payload is currently being transmitted or received or both.

4 Select the **Apply Test Parameters** command and press Enter.

The Cell Test Payload Configuration window is displayed (see Figure 5-5).

```
Cell Test Payload Configuration                              [YourSiteName]

_Payload Formats_____________________________Statistics_____________________

                                            |
 [Received Payload:]                        | [Protocol].......... Atm
 XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX    | [Test Status]....... Not-running
 XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX    |
 XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX    | [Packets Transmitted].. 0000000000
                                            | [Packets Received]..... 0000000000
                                            | [Packets Mismatched]... 0000000000
                                            |
                                            |
 Transmitted Payload:                       |
 0000 0000 0000 0000 0000 0000 0000 0000    |
 0000 0000 0000 0000 0000 0000 0000 0000    |
 0000 0000 0000 0000 0000 0000 0000 0000    | Continuous Update
                                            | Reset Cell Counters
                                            |_____________________________
                                            | Send Payload Once
                                            | Send Payload Continuously
 Apply Transmit Payload                     |
 Reset Display                              | Go Back to Cell Test Diagnostics ->
____________________________________________|_____________________________
```

Figure 5-5. Cell Test Payload Configuration Window

Commands

The commands on this window have the following functions:

Command	Function
• Apply Transmit Payload	Applies the values you enter in the **Transmitted Payload** field.
• Reset Display	Sets the values in the **Transmitted Payload** field to the last saved (applied) set of values.

Command	Function
• Continuous Update	Continuously updates the information in the **[Packets Transmitted, Received, and Mismatched]** fields every two seconds. Select this command and press Enter to turn the continuous updating on and off as needed (similar to a toggle switch).
• Reset Cell Counters	Sets the values in the **[Packets Transmitted, Received, and Mismatched]** fields to zero.
• Send Payload Once	Sends the payload one time.
• Send Payload Continuously	Sends the payload continuously 10 times per second.
• Delete Connection (displayed only after you have sent a payload one time)	Deletes the connection you set up on the Cell Test Diagnostics window. Use this command after you have sent a test payload by using the **Send Payload Once** command.
• Stop Cell Test (displayed only after you have sent a payload continuously)	Stops a continuously running test and deletes the connection you set up on the Cell Diagnostics window. Use this command after you have sent a test payload by using the **Send Payload Continuously** command.
• Go Back to Cell Test Diagnostics→	Redisplays the Cell Test Diagnostics window.

Field Descriptions

5 Select the values for the fields on this window from the values given in Table 5-3.

Table 5-3. Field Values for the Cell Test Payload Window

Field Names	Values	Description
[Received Payload] (display only)	Dependent on the your input in the Transmitted Payload field	The packets received.
Transmitted Payload	Any digits	The values you enter in this field are transmitted by the system
[Protocol] (display only)	Atm	Indicates the type of protocol in use.
[Test Status] (display only)	Running, Not-running	Indicates whether or not the cell test payload is currently being transmitted or received or both.

Table 5-3. Field Values for the Cell Test Payload Window

Field Names	Values	Description
[Packets Transmitted] (display only)	System-generated	The number of packets transmitted.
[Packets Received] (display only)	System-generated	The number of packets received.
[Packets Mismatched] (display only)	System-generated	The number of packets that are not associated with the number transmitted/number received pairs.

6 Select the first line in the **Transmitted Payload** field and enter numbers in any sequence and press Enter. Repeat this step for the second and third lines of this field.

7 Select the **Refresh Transmit Payload** command and press Enter.

This command applies the values for the test payload.

8 Select the **Send Payload Once** or the **Send Payload Continuously** command and press Enter.

The system displays the protocol, cells transmitted or the cells received or both, depending on the type of flow you selected on the Cell Test Diagnostics window (see Figure 5-4).

End

Rebooting PSAX Hardware Components

Specific hardware components may need to be restarted for several reasons, including:

- When you want to revert back to a saved configuration
- When a module is not adhering to its configuration
- When timing problems cannot be resolved automatically
- When firmware changes on a module

To reboot (initialize) one or more components in an Access Concentrator chassis, use the steps in the following procedure.

Rebooting the PSAX System Hardware Components

Rebooting the PSAX System Hardware Components

Begin

1 On the Console Interface Main Menu window (see Figure 5-1), select the **Diagnostics** option and press Enter.

The Diagnostics Menu window is displayed (see Figure 5-2).

2 On the Diagnostics Menu window, select the **Reboot Hardware Components** option and press Enter.

The Remote Reboot Configuration window is displayed (see Figure 5-6).

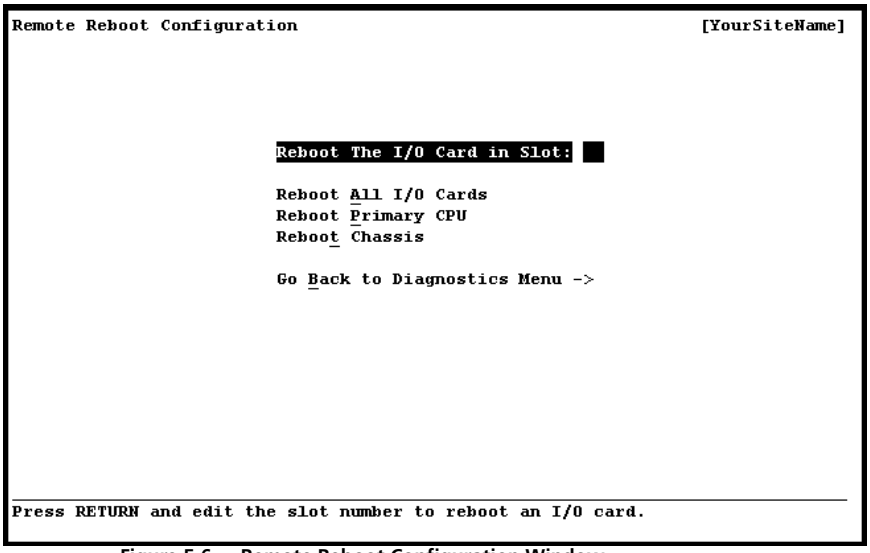

Figure 5-6. Remote Reboot Configuration Window

3 Select one of the commands shown in the following table as needed and press Enter.

Command	Function
• Reboot the I/O Card in Slot:__	This command reboots the I/O module, server module, T1/E1, or DSP component in the slot you designate (slot number range 1–4). This command is the equivalent to physically deinserting the module from and then reinserting it into the chassis.
• Reboot All I/O Cards	Reboots I/O and server modules, the T1/E1, and DSP components in the chassis, without affecting the CPU. This command is the equivalent to physically deinserting the modules from and then reinserting them into the chassis.
• Reboot Primary CPU	Reboots (reinitializes) the CPU. This command also reboots all I/O and server modules in the chassis, as instructed by the system software initialization process. This command also reboots the T1/E1 and DSP components in the chassis, as instructed by the system software initialization process.
• Reboot Chassis	Reboots the CPU, I/O and server modules, and the T1/E1 and DSP components in the chassis. This command is equivalent to a system cold start; that is, removing the power from the chassis and then reapplying the power.
• Go Back to Diagnostics Menu	Displays the Diagnostics Menu window.

End

Removing Configuration Files

To remove configuration files, use the steps in the following procedure, starting at the Console Interface Main Menu window (see Figure 5-1).

Removing Configuration Files

Removing Configuration Files

Begin

1. On the Console Interface Main Menu window, select the **Diagnostics** option and press Enter.

   The Diagnostics Menu window is displayed (see Figure 5-2).

2. On the Diagnostics Menu window, select the **Remove Configuration Files** option and press Enter.

   The following prompt is displayed.

   ```
   Are you sure that you want to remove all the
   configuration files? (y/n)
   ```

3. Answer **y** to remove the files or **n** to cancel.

End

Unlocking a Telnet Session

Once in a while, a lockup condition of a telnet session you are using to connect to an PSAX 20 system may occur. If this happens, you need to use another Access Concentrator system in the network to remotely access and unlock the PSAX 20 system with the telnet lock-up problem.

Unlocking a Telnet Session

Unlocking a Telnet Session

Begin

To unlock the telnet session of an Access Concentrator system, or to check the connectivity of an Access Concentrator system, perform the steps in the following procedure.

1. From another Access Concentrator system, log on the Access Concentrator system console interface.
2. On the Console Interface Main Menu window (see Figure 5-1), select the **Diagnostics** option and press Enter.

   The Diagnostics Menu window is displayed (see Figure 5-2).

3. On the Diagnostics Menu window, select the **Unlock Shell / Ping** option and press Enter.

   The Unlock Shell / Ping window is displayed (see Figure 5-7).

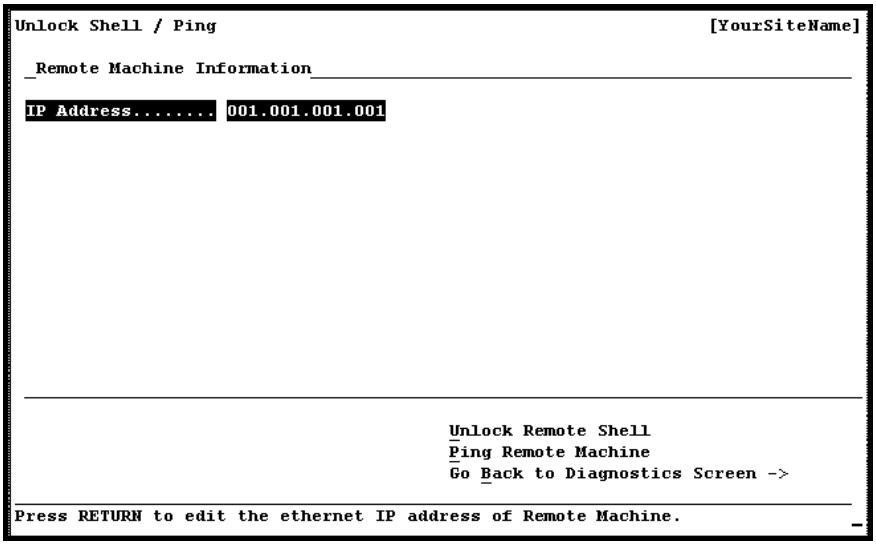

Figure 5-7. Unlock Shell / Ping Window

4 Type the IP address of the PSAX 20 system that is connected to the locked-up telnet session in the **IP Address** field, and press Enter.

5 Select the **Unlock Remote Shell** command and press Enter.

This command corrects a telnet lock-up condition, and enables you to access the PSAX 20 system to which you previously could not get any response.

6 Select the **Ping Remote Machine** command and press Enter.

This command sends a ping command to a remote PSAX system or other switching device to indicate whether or not you can connect to that remote device.

End

Operations and Maintenance (OAM)

For more information about OAM, see the chapter "System Features," in Chapter 3.

Creating OAM Connections

The OAM loopback test is supported for end-to-end connections only. In order to support OAM functionality, you must have already configured one I/O module for circuit emulation and one I/O module for ATM as follows:

- The first port is assigned to the near-end user.
- The second port is assigned to the far-end user, using the same configuration as the first port.

Creating an OAM Connection

Begin

1 On the Console Interface Main Menu Window (see Figure 5-8), select the **Connection Configuration** option and press Enter.

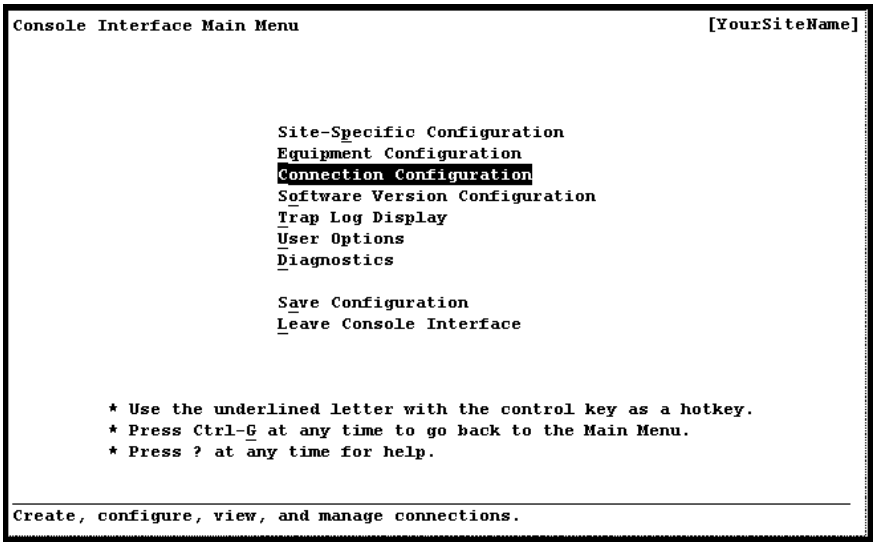

Figure 5-8. Console Interface Main Menu (Connection Configuration Selected)

The Connection Configuration window is displayed (see Figure 5-9).

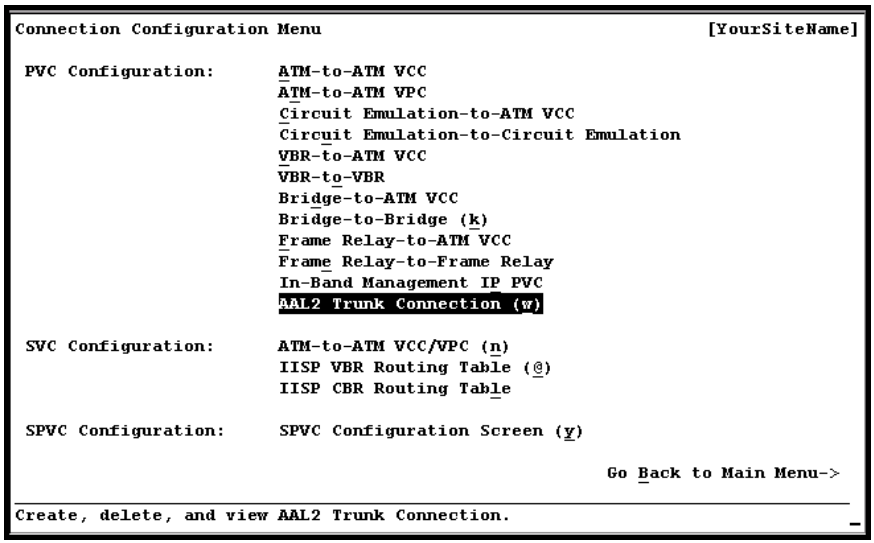

Figure 5-9. Connection Configuration Window (As Displayed on the PSAX 1250)

2 On the Connection Configuration window, select the **Circuit Emulation-to-ATM VCC** configuration and press Enter.

The Circuit Emulation-to ATM VCC PVC Table Window is displayed (see Figure 5-10).

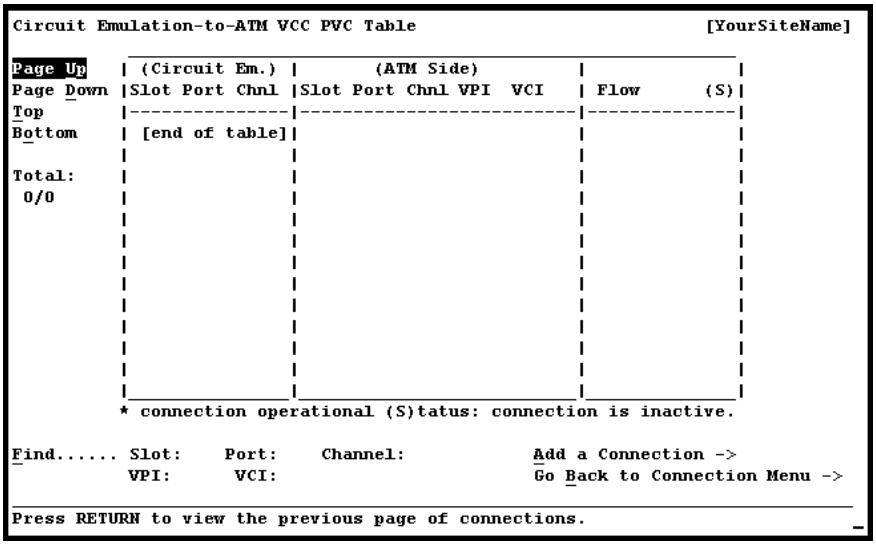

Figure 5-10. Circuit Emulation-to-ATM VCC PVC Table Window

Note: At the time of initial installation, the Circuit Emulation-to-ATM VCC PVC Table window is empty. After you have set up connections, this window displays all the connections of this type in the system.

Commands

The commands on this window have the following functions:

Command	Function
• Find . . .	To find a particular connection, enter values in the **Slot, Port, Chnl, VPI**, and **VCI** fields. If the connection exists, it is displayed on the first line of the table.
• Add a Connection→	Displays the Circuit Emulation-to-ATM VCC PVC Connection window.
• Go Back to Connection Menu→	Redisplays the Connection Configuration Menu window.

Display Fields

The display fields on this window provide the following information about all the circuit emulation-to-ATM VCC PVC connections in the Access Concentrator system:

Display Field	Description
• Circuit Emulation Side	This column displays the information for all circuit emulation sides of the connections. The connection entries are displayed in ascending numerical order by slot, then by port and channel.
• ATM Interface Side	This column displays the information for all ATM interface sides of the connections. The connection entries are displayed in ascending numerical order by slot, then by port, channel, VPI, and VCI.
• Flow	This column displays the direction of the data traffic flow for the connections.
• Total: 0/0	The first number in this field indicates the number of the connection table entry on the first line of the currently displayed window. The second number indicates the total number of connection table entries for this connection type.

3 Select the **Add a Connection** command and press Enter.

The Circuit Emulation-to-ATM VCC PVC Connection Window is displayed (see Figure 5-11).

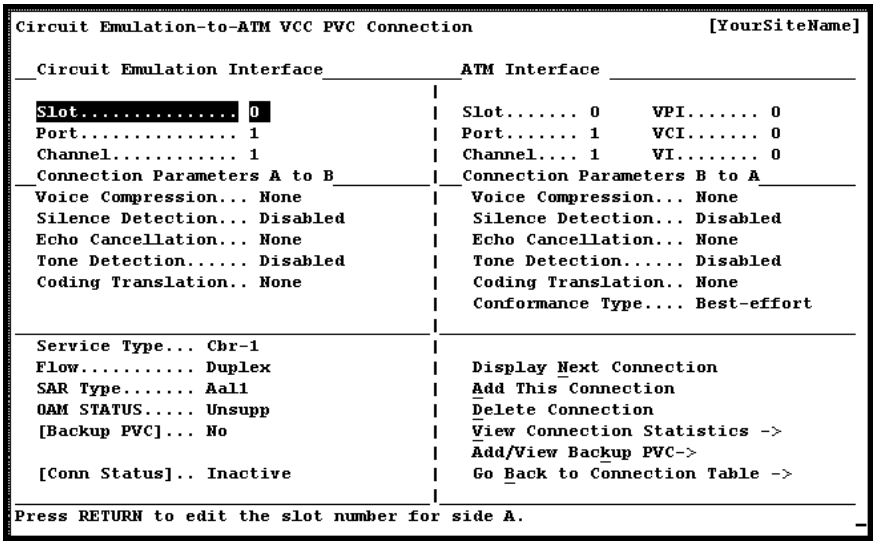

Figure 5-11. Circuit Emulation-to-ATM VCC PVC Connection Window

Commands

The commands on this window have the following functions:

Command	Function
• Display Next Connection	Displays the next connection of this type in the table.
• Add This Connection	Adds a connection having the values currently displayed on the window.
• Delete Connection	Deletes the connection having the values currently displayed on the window.
• View Connection Statistics→	Displays the Circuit Emulation-to-ATM VCC PVC Statistics window.
• Add/View Backup PVC→	
• Go Back to Connection Table→	Redisplays the Circuit Emulation-to-ATM VCC PVC Connection Table window.

Field Descriptions

4 Select the values for the fields on this window from the values given in Table 5-4.

Table 5-4. Field Values for the Circuit Emulation-to-ATM VCC PVC Connection Window

Field Names	Values	Description
Circuit Emulation Interface		The circuit emulation side of the connection that will send and receive signals.
ATM Interface		The ATM interface side of the connection that will send and receive signals.
Slot	Variable depending on chassis type	Enter the slot number containing the module for which you are creating a connection. Enter slot numbers for both sides of the connection.
Port	Range: Variable	Enter the port number on the module for which you are creating a connection. Enter port numbers for both sides of the connection.
Channel	CE side: Range: 1–24 (DS1), 1–31 (E1), 1–28 (DS3) ATM side: 1	On the Circuit Emulation Interface side, enter the channel number of the port on the module for which you are creating a connection. On the ATM Interface side, do not change the default value (**1**) in this field.
VPI	Range: 0-255 (ATM UNI); 0-4095 (NNI)	Virtual path identifier. Enter a value for ATM side of the connection.
VCI	Range: 32–65535	Virtual channel identifier. Enter a value for the ATM side of the connection.
VI	Default: 0 Range: 0-255	Virtual interface, which provides bandwidth allocation restrictions. Currently available only on the OC-3c APS and STM-1 MSP modules. When disabled, default is 0.
AAL2 Cid (display only unless SAR type is Aal2Std)	Default: 0 Range: 8-255 per trunk (0-7 not available; reserved)	If **Aal2Std** is selected in the **SAR Type** field, enter a channel identifier.

Table 5-4. Field Values for the Circuit Emulation-to-ATM VCC PVC Connection Window

Field Names	Values	Description
Voice Compression	None (default), G726-16k, G726-24k, G726-32k, G726-40k, G729a-8k	If you want data traffic for this connection to be processed through the DSP2A,DSP2B, or DSP2C Voice Server modules, do not use the default value. Instead, select the desired type and rate of voice compression from the list of choices.
Silence Detection	Disabled (default), Enabled	If you want data traffic for this connection to be processed through the DSP2A, DSP2B or DSP2C Voice Server modules, do not use the default value. Choosing **Enabled** enables Silence Detection.
Echo Cancellation	None (default), G.165-nearEnd G.168	If you want data traffic for this connection to be processed through the DSP2A, DSP2B or DSP2C Voice Server modules, do not use the default value. Select **G165-nearEnd** if you want to enable Echo Cancellation on this connection.
Tone Detection	Disabled (default) Bypass	If you want data traffic for this connection to be processed through the DSP2A, DSP2B or DSP2C Voice Server modules, use **Bypass**. The value **Bypass** indicates that the fax tones are to be recognized and data sent by fax is not to be processed by compression and echo cancellation.
Coding Translation	None (default), MuLaw2muLaw, ALaw2aLaw, MuLaw2aLaw, ALaw2MuLaw	If you want data traffic for this connection to be processed through the DSP2A, DSP2B, or DSP2C Voice Server modules, do not use the default value. The other values indicate the desired type of pulse code modulation (PCM) translation. You must specify one of these PCM types to enable data traffic processing through the DSP2A, DSP2B or DSP2C Voice Server modules.

Table 5-4. Field Values for the Circuit Emulation-to-ATM VCC PVC Connection Window

Field Names	Values	Description
Conformance Type		The type of traffic control option used for ATM cells. The traffic descriptor combination specifies which traffic parameters are used for traffic control, determines the number and type of cells that are admitted into a congested queue, and determines whether high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds. **Note:** See the appendix for a detailed description of the values for this field.
	Default: Best-effort	This traffic descriptor allows the system to attempt to send all cells in a "best effort" fashion, without specifying traffic parameters, similar to the *AQueMan*™ algorithm.
	1B-NT-0+1	This traffic descriptor uses the parameters one bucket, no tagging, cell loss priority (CLP)=0+1 cells (high and low priority).
	2B-NT-0+1-0+1	This traffic descriptor uses the parameters two buckets, no tagging, CLP=0+1 cells (high and low priority) for bucket 1, and CLP=0+1 cells (high and low priority) for bucket 2.
	2B-NT-0+1-0	This traffic descriptor uses the parameters two buckets, no tagging, CLP=0+1 cells (high and low priority) for bucket 1, and CLP=0 cells (high priority) for bucket 2.
	2B-T-0+1-0	This traffic descriptor uses the parameters two buckets, CLP=0+1 cells (high and low priority) for bucket 1, and tagging for CLP=0 cells (high priority) in bucket 2.
	Best-effort-tag	This traffic descriptor allows the system to tag all CLP=0 (high priority) cells to change them to CLP=1 (low priority) cells during congestion, and then attempt to send all cells in a "best effort" fashion, without specifying any other traffic parameters, similar to the *AQueMan*™ algorithm.

Table 5-4. Field Values for the Circuit Emulation-to-ATM VCC PVC Connection Window

Field Names	Values	Description
Service Type	Ubr (default) Vbr-nrt2, Vbr-nrt1, Vbr-rt2, Vbr-rt1, Vbr-express Cbr-4, Cbr-3, Cbr-2, Cbr-1	Access Concentrator system-supported quality of service (QoS) class. See the appendix for a detailed description of the values for this field.
Flow	Duplex (default), SimplexA2B, SimplexB2A PointToMulti-pointA2B PointToMulti-pointB2A	Direction of the flow of data traffic in this connection. **Note:** The values change on either side of the connection window as you scroll through this field.
SAR Type		The segmentation and reassembly (SAR) type should correspond to the SAR type of the incoming data stream.
	Aal1 (default)	AAL-1
	Aal2Std	AAL-2 Standard. **Note:** Choose this type for AAL-2 trunking. Enter the associated channel identifier in the **Cid** field in the upper right panel.
	Non-Mux-Aal2	Non-multiplexed AAL-2 (Lucent proprietary)
OAM STATUS	Unsupp (default)	OAM is not in use.
	End-Pt	The Access Concentrator is used as a termination point for ATM. Use this value to enable trunk conditioning. For more information, see the *Trunk Conditioning Application Note for PacketStar™ Access Concentrators*.
[Backup PVC] (display only)	Default: No, Yes	This field displays a backup PVC, if configured.
[Conn Status] (display only)	Inactive, Active	This field displays the current status of the connection. The value indicates whether the connection is passing traffic.

5 In the Circuit Emulation Interface section of the window, add the the slot, port, and channel designations for the near end user from your circuit emulation module.

6 In the ATM Interface section section of the window, add the slot, port, channel designation, VPI and VCI for the near end user from your ATM module.

7 Select **End-Pt** in the **OAM STATUS** field.

8 Select the **Add a Connection** command and press Enter.

9 Return to the top of the screen and repeat steps three through five for the far end user.

End

Monitoring OAM Functionality

Perform the steps in the following procedure to monitor OAM functionality, using the Circuit Emulation-to-ATM Statistics window.

Using the CE-to-ATM Statistics Window to Monitor OAM Functionality

Begin

1 From the Circuit Emulation-to-ATM VCC PVC Connection Window, select **View Connection Statistics** and press Enter.

The Circuit Emulation-to-ATM VCC PVC Statistics window is displayed (see Figure 5-12).

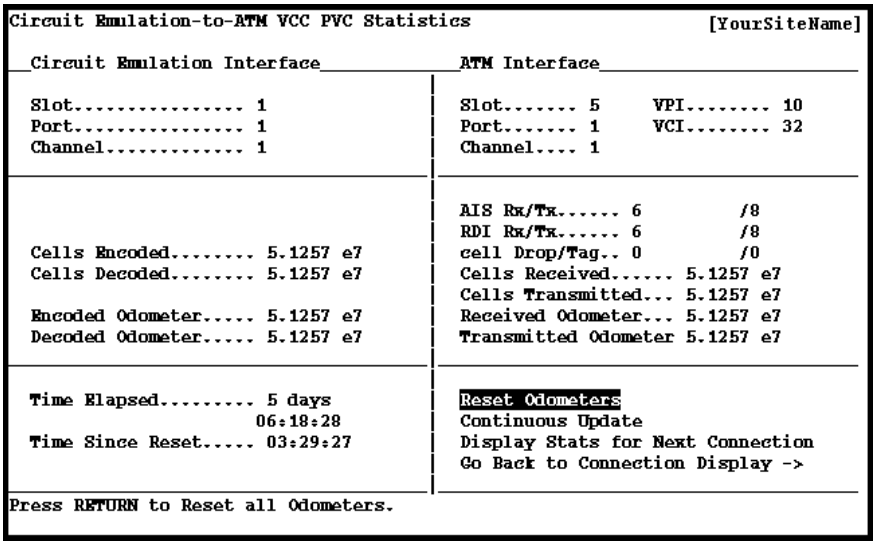

Figure 5-12. Circuit Emulation-to-ATM VCC PVC Statistics Window

Commands

The commands on this window have the following functions:

Command	Function
• Reset Odometers	Resets all statistics odometers back to their default.
• Continuous Update	Starts the counters for a continuous update of all OAM statistics fields.
• Display Stats for Next Connection	Displays statistical information for the far end user.
• Go Back to Connection Display	Redisplays the Circuit Emulation-too ATM VCC PVC Connection window.

Field Descriptions

The values for the fields on this window are described in Table 5-5.

Table 5-5. Field Values for the Circuit Emulation-to-ATM VCC PVC Statistics Window

Field Names	Values	Description
Circuit Emulation Interface		The circuit emulation side of the connection that will send and receive signals.
ATM Interface		The ATM interface side of the connection that will send and receive signals.

Table 5-5. Field Values for the Circuit Emulation-to-ATM VCC PVC Statistics Window

Field Names	Values	Description
Slot	Variable depending on the chassis type	Enter the slot number containing the module for which you are creating a connection. Enter slot numbers for both sides of the connection.
Port	Range:1 to 8	Enter the port number on the module for which you are creating a connection. Enter port numbers for both sides of the connection.
Channel	CE side: Range: 1 to 24 (DS1), 1 to 31 (E1), ATM side:1	On the Circuit Emulation Interface side, enter the channel number of the port on the module for which you are creating a connection. On the ATM Interface side, do not change the default value (**1**) in this field.
VPI	Range: 0 to 255	Virtual path identifier. Enter a value for ATM side of the connection.
VCI	Range: 32 to 65535	Virtual channel identifier. Enter a value for the ATM side of the connection.
Cells Encoded	0.0000 e0 (default)	The total number of encoded (transmitted) user cells going into interface side A during the amount of time shown in **Time Elapsed** field (i.e., since the circuit was created).
Cells Decoded	0.0000 e0 (default)	The total number of decoded (received) user cells going out of interface side A during the amount of time shown in **Time Elapsed** field (i.e., since the circuit was created).
Encoded Odometer	0.0000 e0 (default)	The total number of encoded user cells going into interface side B since the connection was created.
Decoded Odometer	0.0000 e0 (default)	The total number of decoded user cells decoded going out of interface side B since the connection was created.
Time Elasped		Total time elasped for OAM statistics collection since the circuit was established.

Table 5-5. Field Values for the Circuit Emulation-to-ATM VCC PVC Statistics Window

Field Names	Values	Description
Time Since Reset		Total time elapsed for OAM statistics collection since the last time the **Reset Odometers** command was used. **Note:** The **Reset Odometers** command on the statistics window resets only the odometer fields and the corresponding clock. Other counters increment for the life of the circuit.
AIS Rx/Tx	0/0 (default)	Number of OAM alarm indication signal cells received and transmitted.
RDI	0/0 (default)	Number of OAM remote defect indication cells received and transmitted.
Cells Received	6.5000 e1 (default)	Total number of OAM cells received.
Cells Transmitted	6.5000 e1 (default)	Total number of OAM cells transmitted.
Received Odometer	6.5000 e1 (default)	Total number of ATM cells received since odometer was last reset.
Transmitted Odometer	6.5000 e1 (default)	Total number of ATM cells transmitted since odometer was last reset.

Note: To view statistics for the far end user, select **Display Stats for Next Connection**. The Circuit Emulation-to-ATM VCC PVC Statistics window is displayed with statistical information for the far end.

Performing OAM Tests

To perform OAM tests, perform the steps in the following procedure.

OAM Tests

Performing OAM Tests

Begin

1. On the Console Interface Main Menu window, select the **Diagnostics** option and press Enter.

   The Diagnostics Menu window is displayed (see Figure 5-2).

2. On the Diagnostics Menu window, select the **OAM Tests** option and press Enter.

   The OAM Loopback Test window is displayed (see Figure 5-13).

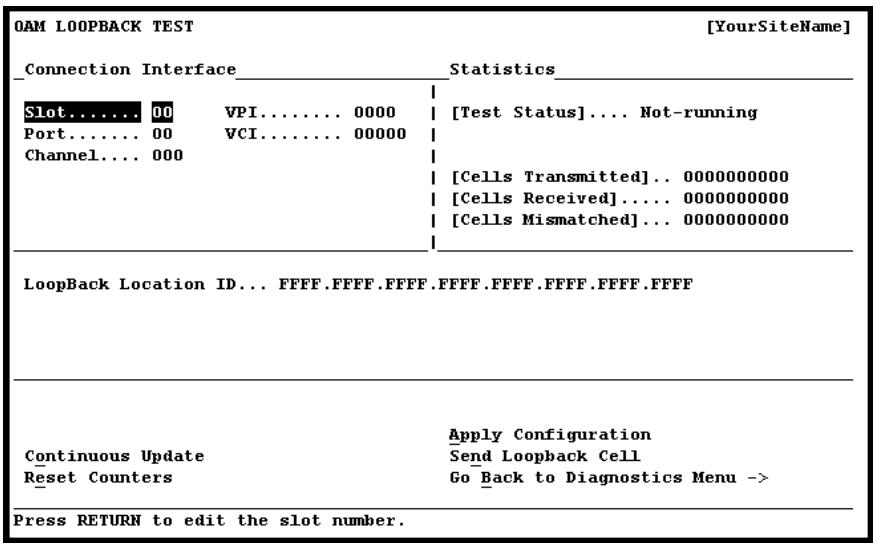

Figure 5-13. OAM Loopback Test Window

Commands

The commands on this window have the following functions:

Command	Function
• Continuous Update	Continuously updates the fields in the **Statistics** panel every two seconds. Select this command and press Enter to turn the continuous updating on and off as needed (similar to a toggle switch). **Note:** The test display update does not always keep pace with the actual Access Concentrator device operation. Use this command to avoid misinterpretation of test results.
• Reset Counters	Sets the values in the **Statistics** panel to the last saved (applied) set of values.
• Apply Configuration	Applies the values you enter in the this window.
• Send Loopback Cell	Sends the loopback cells.
• Go Back to Diagnostics Menu→	Redisplays the Diagnostics Menu window (see Figure 5-2).

Field Desciptions

3 Select the values from the fields on this window from Table 5-6.

Table 5-6. Field Values for the OAM Loopback Test Window

Field Name	Values	Description
Connection Interface Panel		
Slot	Default: 0	The module slot number of the ATM connection for the loopback test.
Port	Default: 0	The port number of the ATM connection for the loopback test.
Channel	Default: 0	The channel number of the ATM connection for the loopback test.
VPI	Default: 0	The virtual path identifier of the connection.
VCI	Default: 0	The virtural channel identifier of the connection. Must be zero for virtual path connections
Statistics Panel		
[Test Status] (display only)	Default: 0	The current status of the test.
[Cells Transmitted] (display only)	Default: 0	The number of loopback cells transmitted.
[Cells Received] (display only)	Default: 0	The number of loopback cells received correctly.
[Cells Mismatched] (display only)	Default: 0	The current status of the test.
[Loopback Location ID] (display only)	Default: FFFF.FFFF.FFFF.FFFF.FFFF.FFFF.FFFF.FFFF	The destination loopback location ID where the loopback must occur.

4 Select the **Apply Configuration** command and press Enter.

End

OAM Activation and Deactivation

The **OAM Activate and Deactivate** option can perform continuity checks on the circuit running between PSAX systems when the traffic is down.

To perform an OAM continuity check, perform the steps in the following procedure.

Activating and Deactivating OAM

Activating or Deactivating OAM

Begin

1 On the Console Interface Main Menu window, select the **Diagnostics** option and press Enter.

The Diagnostics Menu window is displayed (see Figure 5-2).

2 On the Diagnostics Menu window, select the **OAM Activate and Deactivate** option and press Enter.

The OAM ACTIVATION -DEACTIVATION window is displayed (see Figure 5-14) .

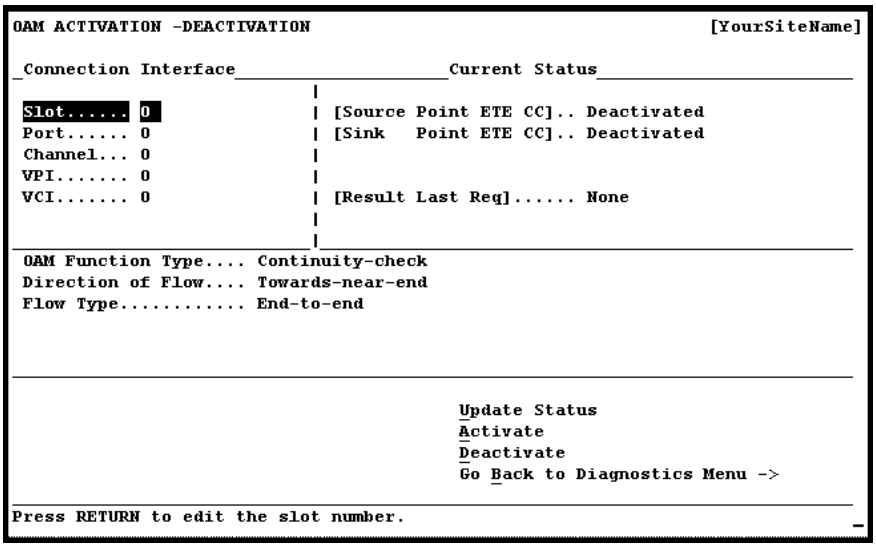

Figure 5-14. OAM ACTIVATION -DEACTIVATION Window

Commands

The commands on this window have the following functions:

Command	Function
• Update Status	Updates the information in the **Current Status** panel.
• Activate	Starts the OAM test.
• Deactivate	Terminates the OAM test.
• Go Back to Diagnostics Menu→	Redisplays the Diagnostics Menu window (see Figure 5-2).

Field Descriptions

3 Select the values for the fields in this window as described in Table 5-7.

Table 5-7. Field Values for the OAM Activation-Deactivation Window

Field Name	Values	Description
Connection Interface Panel		
Slot	Default: 0	The module slot number of the ATM connection.
Port	Default: 0	The port number of the ATM connection.
Channel	Default: 0	The channel number of the ATM connection.
VPI	Default: 0 Range: 0–4095	VPI value for an OAM CC connection.
VCI	Default: 0 Range: 0–65535	VCI value for OAM CC connection.
Current Status Panel		
[Src Point ETE CC] (display only)	Default: Deactivated , Activated, WaitAct, Confirm, WaitDeact, Confirm	Displays the current status of activation or deactivation request for the source point.
[Snk Point ETE CC] (display only)	Default: Deactivated, Activated, WaitAct, Confirm, WaitDeact Confirm	Displays the current status of activation or deactivation request for the sink point.
[Result Last Req] (display only)	Default: None, Denied, Timedout, LocResrc Unavl, OamUnsupported, ReqCancelled, FuncNot Implemented, Successful	Shows the reasons of failure of the last activation request on this connection from the local user.

Table 5-7. Field Values for the OAM Activation-Deactivation Window

Field Name	Values	Description
OAM Function Type	Default: Continuity-check, Fpm-and br, Fpm only	Represents the OAM flow for activation or deactivation for this connection.
Direction of Flow	Default: Towards-near-end, Both-way, Towards-far-end	The direction in which cells will be transmitted.
Flow Type	Default: End-to-end, Segment	Direction of the flow of data traffic in this connection.

4 To begin the test, select the **Activate** command and press Enter.

5 To terminate the test, select the **Deactivate** command and press Enter.

End

6 Configuring the VT100 Terminal Emulator

Overview of This Chapter

VT100 terminal emulation is used in configuring and managing the PSAX 20 system from the serial interface port labeled CONSOLE on the faceplate. The PSAX 20 Access Concentrator system software supports the following terminal emulation software:

- Microsoft Windows 3.1 terminal emulator
- Microsoft Windows 95 HyperTerminal terminal emulator
- Alternate terminal emulation software

Use the serial cable (RS-11 with specific pinouts) supplied with your installation kit to connect the Access Concentrator system with the PC.

Setting Up The Windows 3.1 Terminal Emulator

To configure the terminal settings using the Microsoft Windows 3.1 terminal emulator, perform the following procedure.

Setting Up The Windows 3.1 Terminal Emulator

Begin

1. From the Terminal menu, select the **Settings** option.
2. Select the **Terminal Emulation** option from the Settings Menu.
3. Set the **Terminal Emulation** field to **DEC VT100 (ANSI)**.
4. Select **OK**.
5. Return to the Settings Menu.
6. Select the **Terminal Preferences** option from the Settings Menu.
7. Select the settings in Table 6-1 for each option.

Table 6-1. Settings for VT100 Terminal Preferences Using the Windows 3.1 Terminal Emulator

Option	Setting
Line wrap:	off
Local echo:	off
Sound:	on
CR->CR/LF inbound and outbound:	off
Columns:	80
Cursor:	underline is recommended

Table 6-1. Settings for VT100 Terminal Preferences Using the Windows 3.1 Terminal Emulator

Option	Setting
Cursor Blink:	blink is not recommend
Terminal font:	Courier 13 is recommended
Translations:	none
Fonts:	optional
Show scroll:	off
Use function, arrow, and Ctrl keys for Windows:	off
Buffer lines:	100

8 Select **OK**.

9 Return to the Settings Menu.

10 From the Settings Menu, select the **Communications** option.

11 Select the settings in Table 6-2 for each option.

Table 6-2. Port Settings for VT100 Terminal Communication

Option	Setting
Baud:	9600
Data bits:	8
Stop bits:	1
Parity:	none
Flow control:	none
Connector:	user defined
Parity check:	off
Carrier detect:	off

12 Select **OK**.

13 From the File Menu, select the **Save** option.

14 Maximize the terminal window.

End

Setting Up The Windows 95 HyperTerminal Emulator

To configure VT100 terminal emulation using the Windows 95 HyperTerminal emulator, use the settings in Table 6-3.

Table 6-3. Windows 95 HyperTerminal Settings

Option	Setting
Phone number:	Connect Using **Direct to COM1**
Configure:	9600 baud
Data bits:	8
Parity:	none
Stop bits:	1
Flow control:	none
Advanced Settings:	
(Port settings):	turn off FIFO buffers
Settings:	select terminal keys
Emulation:	VT100
Terminal setup:	
Cursor:	block or underline, no blink
Font:	Fixedsys 15
Translations:	none
Scroll bars:	off
Keys for window:	off

Other Software for VT100 Terminal Emulation

The console interface supports the standard VT100 terminal emulator configuration. When using various types of workstations or other terminal emulation software with the PSAX 20 console interface, use the settings listed in Table 6-4.

Table 6-4. Preference Settings for Other VT100 Terminal Emulation Programs

Typical Option	Preferred Setting
Terminal emulation:	VT100
Terminal preferences: •	
• Communications:	9600 baud, 8 bits, 1 stop bit, no parity
• Flow control:	none
Terminal modes:	
• Line Wrap:	off
• Local Echo:	off
• Sound:	on (optional)

Table 6-4. Preference Settings for Other VT100 Terminal Emulation Programs

• CR	CR/LF
• Inbound:	off
• Outbound:	off
Columns:	80
Cursor:	block or underline
Translations:	none
Scroll bars:	off
Keys for window:	off

Setting Up a U.S. Robotics-Compatible Modem

Table 6-5 shows the list of commands to configure the modem on your computer to the PSAX 20 for interoperability.

⚠ WARNING:
Set echo reply OFF (AtE0 command) on the modem you connect to the PSAX 20. Failure to do so may cause the PSAX 20 to hang up and fail to boot properly.

⚠ WARNING:
Set the quiet mode (AtQ1 command). Failure to do so could possibly cause subsequent logins or CPU communication to fail after the initial login.

Table 6-5. Modem Set-Up Commands For a Modem Connected to a Remote PSAX 20 System

Command	Result
AtE0	sets local echo off
At&B1	sets fixed port serial rate
At&H0	sets flow control disabled
At&I0	sets software flow control disabled
At&N6	sets connect speed to 9600 bps
At&R1	modem ignored request to send (RTS)
At&S0	data set ready (DSR) override
AtY0	sets profile 0 setting in non-volatile random access memory (NVRAM) as default

Table 6-5. Modem Set-Up Commands For a Modem Connected to a Remote PSAX 20 System

Command	Result
AtQ1	sets quiet mode, no result codes
At&W0	writes current configuration to NVRAM 0 template

7 Upgrading and Backing Up System Software

Overview of This Chapter

This chapter describes how to upgrade, back up, and restore the Access Concentrator system software and firmware.

Note: If the system software release to which you are upgrading requires a firmware update, you need to perform the remote software upgrade procedure, or arrange for an in-factory or on-site upgrade by Lucent Technologies, Inc. personnel. The Release Note for the system software version to which you are upgrading identifies any affected modules. Your Lucent Technologies customer engineer or a NetworkCare[SM] representative can provide you with details about the return materials authorization (RMA) process or, depending on the type of service agreement you have, the on-site upgrade procedure. For information on these services, contact Lucent Technologies NetworkCare (see "Technical Support" in Chapter 1, "Getting Started").

The following procedures are presented:

- Installing a new software or firmware release by using the following methods:
  - ~ Upgrading to the new release using FTP (see ”Upgrading System Software Using FTP” on page 7-4)
  - ~ Upgrading from Release 3.1.1 to later releases using X/Modem/YModem file transfer (see ”Upgrading Using XModem/YModem File Transfer Method” on page 7-9)
- Upgrading the firmware of I/O modules (see ”Upgrading Using XModem/YModem File Transfer Method” on page 7-9)
- Falling back to the previous software release (see ”Falling Back to the Previous Software Release” on page 7-22)
- Backing up Access Concentrator system, module, and connection configuration database files by using the following methods:
  - ~ Backing up database files using FTP (see ”Falling Back to the Previous Software Release” on page 7-22)
  - ~ Backing up database files using XModem/YModem file transfer (see ”Backing Up Database Files Using XModem/YModem File Transfer” on page 7-26)
- Restoring Access Concentrator configuration and connection database files by using the following methods:
  - ~ Restoring database files using FTP (see ”Restoring Database Files Using FTP” on page 7-30)

- Restoring database files using XModem/YModem file transfer (see "Restoring Database Files Using XModem/YModem File Transfer" on page 7-32)

Directory Structures

In DOS environments, specify the drive letter as follows:

/*x*/FTP/V6.1.C5/upgrade.lib

where *x* is the drive letter.

Note: Always use forward slashes (/)when typing directory strings.

Software upgrades for the Access Concentrator systems are provided on the CD-ROM. The directory structure on the CD-ROM is the following:

- The directory **/*version*/next**, where *version* stands for the new software release number.
- The directory **/*version*/mib**, which contains the V1 and V2 management information bases (MIBs), which you can use with an SNMP manager.

The following directory structure is resident on the hard disk of the CPU module:

- **/scsi/current/**—This directory contains the initialization files for the current, operational version of the system software.
  - **/scsi/current/bin**—This directory contains the library files for the current version of the software.
  - **/scsi/current/snmpagt**—This directory contains the SNMP agent files for the current version of the software.
  - /**scsi**/**current**/**firmware**—This directory contains the firmware files for the current version of the firmware.
- **/scsi/fallback/**—This directory contains all the files for the previous version of system software and database files.
  - /**scsi**/**fallback**/**firmware**—This directory contains the firmware files for the previously downloaded version of the firmware.
- **/scsi/next/**—This is the directory where all files for future system software upgrades are received.
  - /**scsi**/**next**/**firmware**—This directory contains the firmware files for the when the next version of the firmware is received.

Installing a New Software Release

Installing a new release of the Access Concentrator System software includes the following tasks:

- If you are using FTP server software:
  - Performing the downloading of the software upgrade files to the CPU module hard disk
- If you are using the XModem or YModem file transfer method:

~ Transferring the software upgrade files to the CPU hard disk

Note: Upgrading the software on your Access Concentrator system affects its operation.

This process is shown in Figure 7-1:

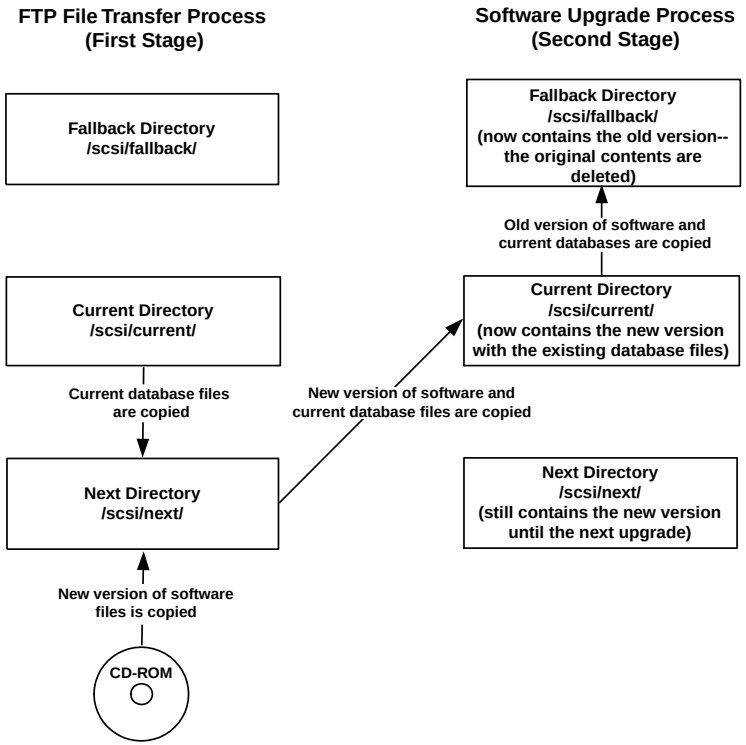

Figure 7-1. Migration of System Software and Databases During the Software Upgrade Process

Setting Up a Windows FTP Server

If you are using a PC workstation or laptop PC running Windows 3.1, Windows 95 or higher to upgrade your Access Concentrator system software, you need to obtain an FTP server software program. If you are running Windows NT, you can use the FTP server function that is included in this operating system. For Windows 95, you need to obtain an FTP server software program, which is available from several Internet web sites, including:

- War FTP Daemon from http://www.jgaa.com

- Serv-U from http://www.cat-soft.com
- Wftpd234 from http://www.shareware.com

If you plan to use a shareware program, you are responsible for following the terms of the author's licensing agreement, including payment. To set up your FTP server software, perform the steps in the following procedure.

Setting Up a Windows FTP Server

Begin

1. Obtain an FTP server software program (freeware, shareware, or commercial) for Windows 95 or Windows 3.1.
2. Set up the FTP server software as follows:
   a. Create an account and password.
   b. Assign read-only, recursive access privileges to the pathname containing the drive ID and directory where the CD-ROM drive resides.

End

Upgrading System Software Using FTP

To upgrade your Access Concentrator system software to Release 6.3.0 from an earlier release, perform the steps in the following procedure.

Upgrading System Software Using FTP

Begin

1 From the Console Interface Main Menu window (see Figure 7-2), select the Software Version Configuration option and press Enter.

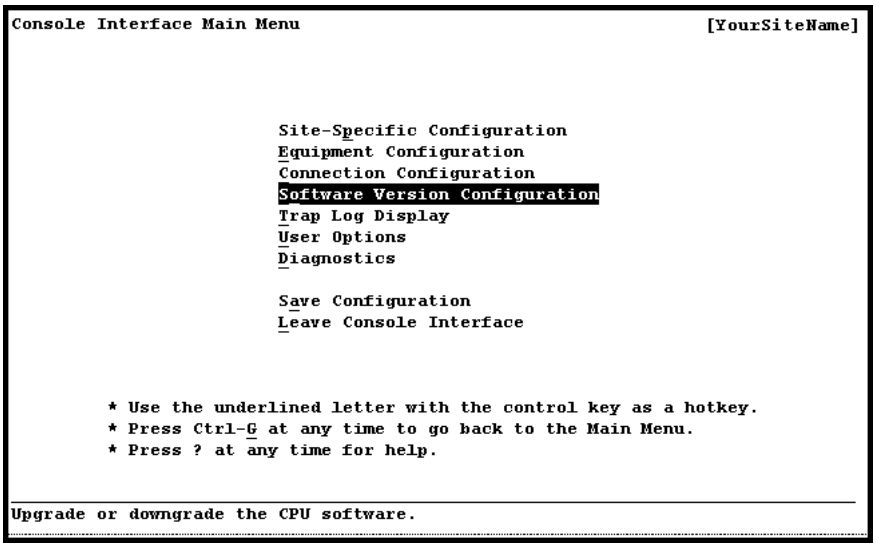

Figure 7-2. Console Interface Main Menu Window (Software Version Configuration Selected)

The Software Version Configuration window (see Figure 7-3) is displayed.

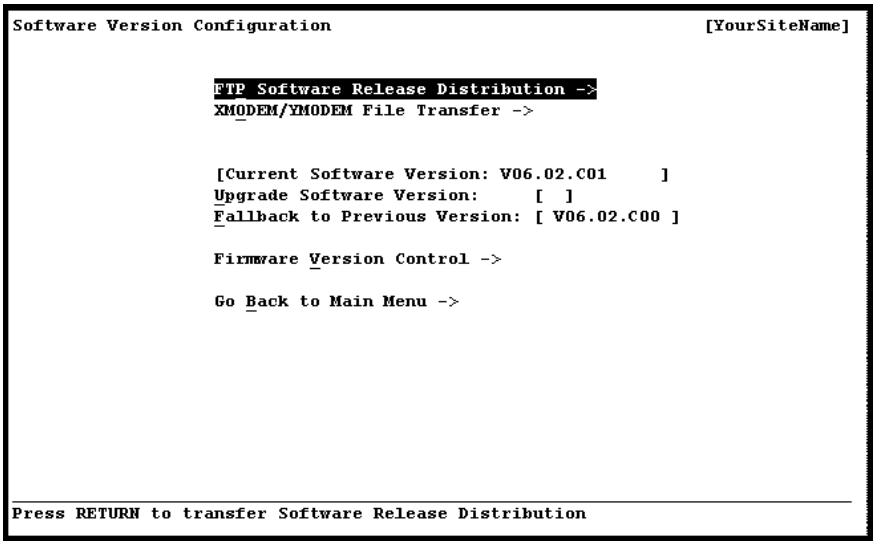

Figure 7-3. Software Version Configuration Window (FTP Software Release Distribution Selected)

2 Select the FTP Software Release Distribution option and press Enter.

The SRD Download Configuration window (see Figure 7-2 on page 7-5) is displayed.

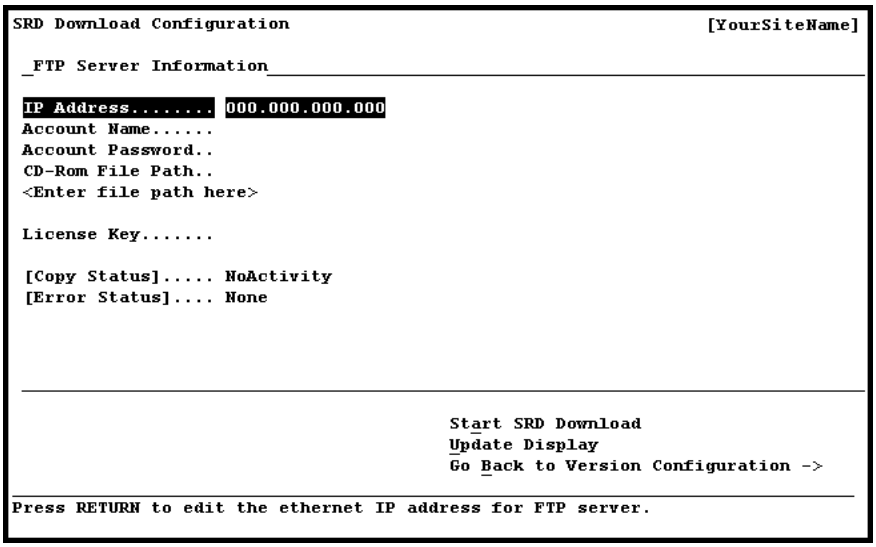

Figure 7-4. SRD Download Configuration Window

Commands

The commands on the SRD Download Configuraton window have the following functions:

Command	Function
• Start SRD Download	Begins the software release downoad via the FTP connection.
• Update Display	Reads database and refreshes the screen.
• Go Back to Version Configuration→	Returns user to the Version Configuration window to upgrade software after a successful download.

Field Descriptions

3 Select the values for the fields on this window from the values given in Table 7-1:

⚠ WARNING:
If your current system software release is prior to release 6.0.0 and you mistakenly download the incorrect file, the system will crash after the FTP download process finishes. See the corrective action to take at the end of this procedure.

Table 7-1. Field Values for the SRD Download Configuration Window

Field Names	Values/Variables	Description
IP Address Directory	Default: 000.000.000.000	Location from which files are retrieved. Example: **172.26.46.78**
Account Name	Range:	Example: **testftp**
Account Password	Range:	Example: **test1**
CD-Rom File Path	Values: **x:/V06.02.C00/upgradec.lib**, where **x** = CD-ROM drive letter, and the value following the slash (/) is the software version you are downloading. **x:/V06.02.C00/upgrade.lib,** where **x** = CD-ROM drive letter, and the value following the slash (/) is the software version you are downloading.	If upgrading from any sytem software release **prior** to release 6.0.0, enter **V06.02.C00/upgradec.lib** If upgrading from system software release 6.0.0 **or later**, enter **V06.02.C00/upgrade.lib** **Note:** Two separate files for the CD-ROM file path exist because the operating system that the CPU uses has changed library formats for the modules that are loaded into memory.
License Key		Lucent software license. Not currently supported.
[Copy Status]	Default: No Activity	Displays FTP software copy status. After download starts, message displayed is "Working."
[Error Status]	Default: None, or one of several error messages.	Message tells user what mistake was made if download is unsuccessful.

4 After entering the values in the SRD Download Configuration window, complete the download by competing these steps:

5 Select the **Start SRD Download** command and press Enter.

The Copy Status displays the message, "Working," and the bottom of the window displays "Filetransferstatus : percentcomplete = 100." After the file transfer is complete, the Copy Status displays "DoneSuccessfully."

6 Select the **Go Back to Version Configuration** command.

The Software Version Configuration window (see Figure 7-3 on page 7-6) is displayed.

7 Select the **Upgrade Software Version** option and press Enter.

8 On the bottom of the window, the following message is displayed:

```
Are you sure that you want to upgrade the software? (y/n)
```

9 Type **y** to continue the upgrade process.

The following message is displayed:

```
Upgrade the software to the next version...
```

The CPU software upgrades to the system software release you specified, which is displayed in the brackets ([ ]) to the right of the **Upgrade Software Version** command. The Access Concentrator chassis reboots, and all firmware of the I/O modules in the chassis are upgraded as the CPU system software is being upgraded.

Corrective Action If Incorrect File Is Downloaded

If your current system software release is prior to release 6.0.0, you mistakenly download the incorrect file (upgrade.lib), and you experience a system crash, the following events will occur:

- In a non-redundant CPU environment, the CPU reinitializes, but you will still be able to upgrade the CPU as if the crash had not occurred. Perform the FTP download again using the correct file, **upgradec.lib**.

End

Perform the FTP download again using the correct file, **upgradec.lib**.

Upgrading Using XModem/YModem File Transfer Method

You can use the XModem/YModem file transfer method to load new system software to the CPU component.

Upgrading using the XModem/YModem file transfer method includes two major tasks:

- First, you set up the cabling and connections between the PC workstation and the Access Concentrator system CPU component, start up the VT100 terminal emulation software on the PC workstation, and ensure you have communication between the two devices (see the following procedure, “Steps to Set Up for the File Transfer Process”).
- Second, you perform the file transfer process for the new software upgrade files to the Access Concentrator system, and the upgrading process on the CPU component (see the procedure ”Steps to Transfer the Software Upgrade Files to the System” on page 7-10).

Setting Up for the File Transfer Process

Steps to Set Up for the File Transfer Process

Begin

1 To set up the cabling and connections between the PC workstation, the local modem, and the telephone line do one of the following:

a. If you are using an external modem, connect a cable from the EIA-232 interface port on the PC workstation to the modem, and a cable from the modem to the telephone line.

b. If you are using an internal modem, connect a cable from the modem port on the PC to the telephone line.

2 To set up the cabling and connections between the Access Concentrator system CPU component, the remote modem, and the telephone line.

a. Connect a cable from the CONSOLE port on the front of the Access Concentrator system to the modem.

b. Connect a cable from the modem to the telephone line.

3 On the PC workstation, start up the VT100 terminal emulation software, and set up the configuration preferences.

4 Using the terminal emulator modem communication function, enter the telephone number of the line connected to the modem connected to the Access Concentrator system.

End

Transferring Software Upgrade Files

Steps to Transfer the Software Upgrade Files to the System

Begin

1 Using the terminal emulator, log on the Access Concentrator System

2 On the Console Interface Main Menu window (see Figure 7-2 on page 7-5), select the **Software Version Configuration** option and press Enter.

The Software Version Configuration window (see Figure 7-5) is displayed.

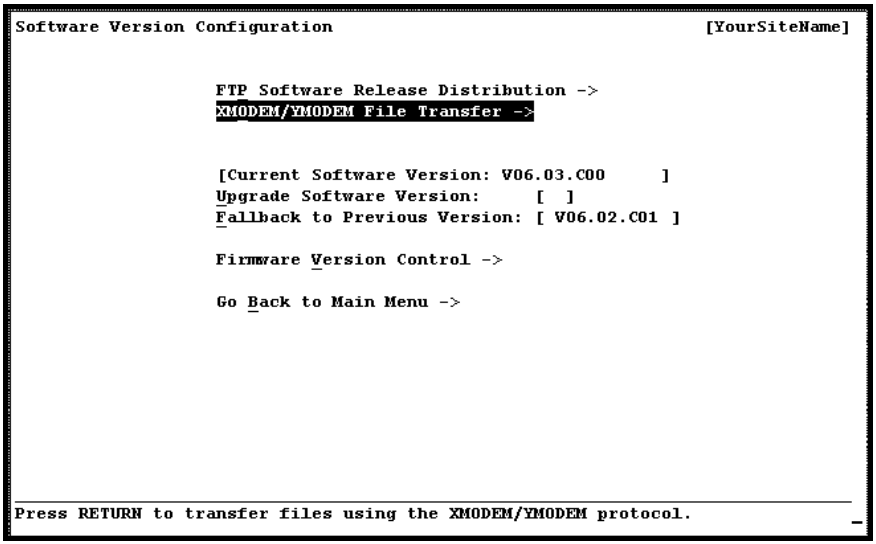

Figure 7-5. Software Version Configuration Window (XMODEM/YMODEM File Transfer Selected)

3 On the Software Version Configuration window, select the **XMODEM/YMODEM File Transfer** option and press Enter.

The XMODEM/YMODEM File Transfer window (see Figure 7-6) is displayed.

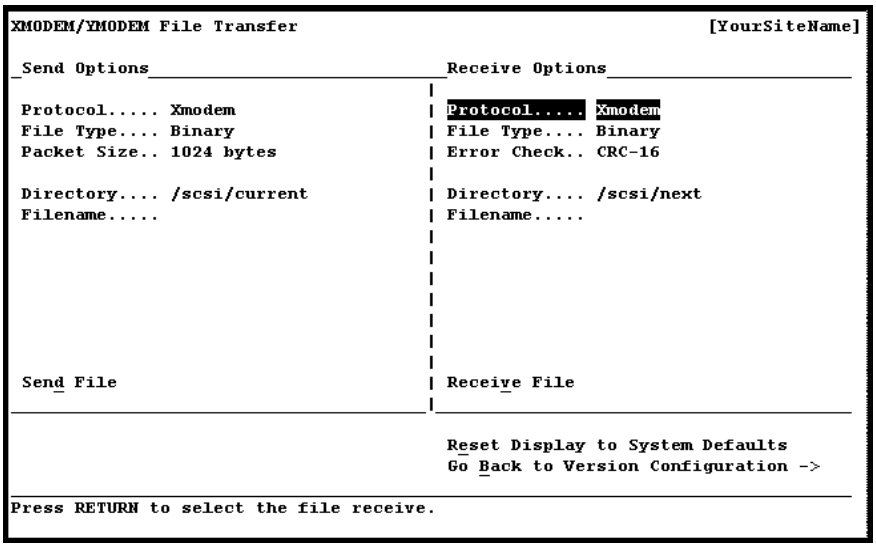

Figure 7-6. XMODEM/YMODEM File Transfer Window (Receive Options Panel Selected)

Note: For the upgrade software process, use only the **Receive Options** panel.

Commands

The commands on this window have the following functions:

Command	Function
• Send File	Initiates the send function of the file transfer process from the CPU hard disk to a storage medium (such as a PC workstation hard disk).
• Receive File	Initiates the receiving function of the file transfer process to the CPU hard disk from the CD-ROM containing the software upgrade files (running in a CD-ROM drive in a PC workstation).
• Reset Display to System Defaults	Redisplays the default values in the fields.
• Go Back to Version Configuration→	Redisplays the Software Version Configuration window (see Figure 7-5 on page 7-11).

Field Descriptions

4 Select the values for the fields on this window from the values given in Table 7-2.

Table 7-2. Field Values for the XMODEM/YMODEM File Transfer Window (Receive Options Panel)—Upgrading with Software Release Files

Field Names	Values/Variables	Description
Protocol	Default: YModem	YModem protocol for receiving the upgrade software files.
	YModem-G	YModem-G protocol for receiving the upgrade software files.
	XModem	XModem protocol for receiving the upgrade software files.
File Type	Default: Binary	Binary format is the type you use most of the time.
	Text	Text or ASCII format is available but do not use it for software upgrade files.
Error Check (displayed only when the value **XModem** is selected in the **Protocol** field)	Default: CRC-16	Indicates that the error checking method is cyclical redundant checking, 16 bits.
	Checksum	Indicates that the error checking method is arithmetic summation checking, 8 bits.

Table 7-2. Field Values for the XMODEM/YMODEM File Transfer Window (Receive Options Panel)—Upgrading with Software Release Files

Field Names	Values/Variables	Description
Directory	**/scsi/next/** *directoryname***/**	Subdirectory on the CPU hard disk where the software upgrade files are received (stored). For each subdirectory contained in the package of software upgrade files, you must enter the subdirectory name in this field, and then receive this directory on the CPU hard disk. **Note:** All subdirectory and file names are listed in the readme.txt file accompanying the software upgrade files on the CD-ROM.
Filename (displayed only when the value **XModem** is selected in the **Protocol** field)	filename	Filename on the CPU hard disk where the software upgrade files are received (stored). For each file contained in the package of software upgrade files, you must enter the filename in this field, and then receive this file on the CPU hard disk. **Note:** All subdirectory and file names are listed in the readme.txt file accompanying the software upgrade files on the CD-ROM.

Note: We recommend that you use either the YModem or the YModem-G protocol. Use the XModem protocol if that is the only one you have available to use.

- The YModem-G protocol allows the fastest transmission of the three types; however, this protocol does not acknowledge receipt of packets. You can receive all files grouped under a subdirectory at one time.
- The YModem protocol is a slower method of transmission, but is more reliable because it acknowledges receipt of packets. You can receive all files grouped under a subdirectory at one time.
- The XModem protocol is a laborious method of transmission because you must enter the filename of each file in the complete package of software upgrade files to accomplish the upgrade task.

5 Select the **Receive Files** command and press Enter.

The terminal emulator displaying the Access Concentrator system window interface brings the XMODEM/YMODEM File Transfer window

out of view. A message is displayed indicating that you can cancel the transfer by pressing Ctrl+X several times. A second message is displayed indicating that you must start the terminal emulator send function.

6 Using the terminal emulator send function, select one of the three protocol types: 1) YModem, 2) YModem-G, or 3) XModem. Be sure to select the same protocol as the one you selected on the Send Options panel of the XMODEM/YMODEM File Transfer window (see Figure 7-6 on page 7-12).

7 In the terminal emulator field for the location of the file, specify the drive where the Access Concentrator system upgrade software files reside (normally, the CD-ROM drive) and the directory pathname.

For example, specify a pathname like one of the following:

- **<***x***:/scsi/next/***subdirectory****.*>** if you are using YModem or YModem-G
  where *x* is the drive letter for the CD-ROM drive
- **<***x***:/scsi/next/***subdirectory******filename**>** if you are using XModem
  where *x* is the drive letter for the CD-ROM drive

Be sure you enter the subdirectory name (or the subdirectory and filename if using XModem) exactly so that it matches the names you previously entered on the XMODEM/YMODEM File Transfer window (see Figure 7-6 on page 7-12). All subdirectory and file names are listed in the readme.txt file accompanying the software upgrade files on the CD-ROM.

8 Select the **OK** or **Send** button or command in the terminal emulator send function dialog box.

9 Repeat steps 4–8 to specify another subdirectory name (for YModem or YModem-G) or another subdirectory name and filename (for XModem) until you have transferred all files for the Access Concentrator system software upgrade.

Note: The new version of the software and the existing database files are now resident in the directory **/scsi/next/** (see Figure 7-1 on page 7-3).

10 Redisplay the Access Concentrator system Software Version Configuration window (see Figure 7-5 on page 7-11).

11 Select the **Upgrade Software Version** command and press Enter.

The following message is displayed:

```
Are you sure that you want to upgrade the software? (y/n)
```

12 Select the y key (to indicate yes) to continue.

While the system performs the software upgrade process, the follow message is displayed:

```
Upgrading the software to the next version ...
```

During the process, the system sends several trap messages indicating events that are occurring. When the process is completed, the system displays a message indicating successful completion.

Upgrading Firmware

Access Concentrator I/O and server modules released with Access Concentrator 6.0.0 software release are supported by the Firmware Release Control feature. Access Concentrator I/O and server modules released prior to the Access Concentrator 6.0.0 software release will work in the Access Concentrator chassis, but are not supported by the Firmware Release Control feature.

Note: Use the Firmware Version Control window (see Figure 7-7) described in the following procedure only with the advice of Lucent Technologies NetworkCare (see the "Technical Support" section in Chapter 1, "Getting Started").

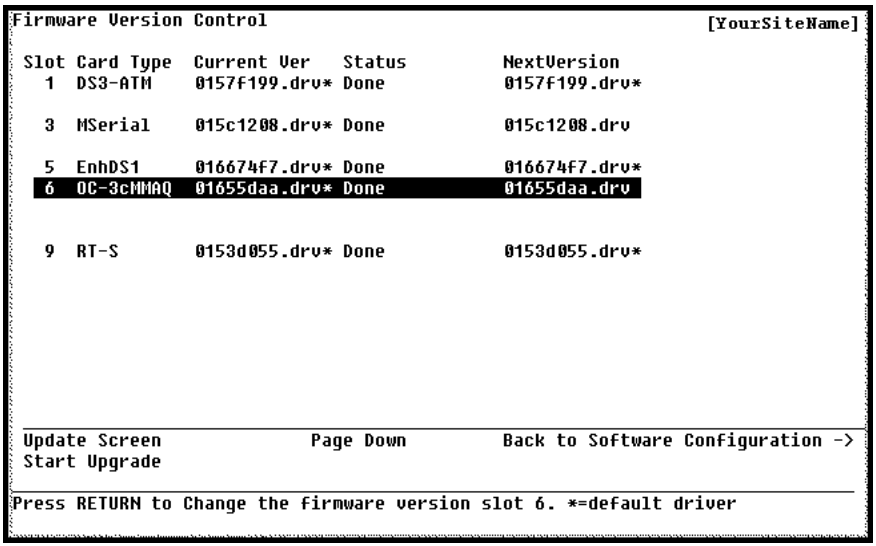

Figure 7-7. Firmware Version Control Window

Firmware Drivers

The firmware driver is a binary file that is automatically downloaded from the system software resident on the CPU module to the I/O module or server, and is used to initialize the module. The default driver and the nondefault (configurable) driver are the two types of drivers you can choose from (although on some I/O and server modules, only one type of driver is available).

Note: We recommend that you use the default driver unless you know which specific driver to select. The default driver contains the most current version of the firmware.

The Access Concentrator system selects only the default driver when the I/O or server module initializes for the first time. When selecting the version of the firmware you want to download to the module, the drivers displayed represent the only downloadable versions for the module highlighted under the **Card Type** field.

During the upgrade of Access Concentrator system software or a firmware patch, one of three scenarios can occur, according to which driver you initially select. The three scenarios are described as follows:

- If you select the default driver on the Firmware Version Control window, and you upgrade the system software to a version that has both types of drivers, the system will upgrade the driver to the next version of the default driver, because that is the type of driver you initially chose.
- If you select the nondefault driver on the Firmware Version Control window, and you upgrade the system software to a version that has both types of drivers, the system will upgrade the driver to the next version of the nondefault driver, because that is the type of driver you initially chose.
- If you select either type of driver on the Firmware Version Control window, and you upgrade the system software to a version that has only one type of driver, the system will upgrade the driver to the one available driver, even if you did not originally select that type of driver before the upgrade.

To download firmware to the I/O and server modules, perform the steps in the following procedure, beginning at the Console Interface Main Menu window (see Figure 7-8).

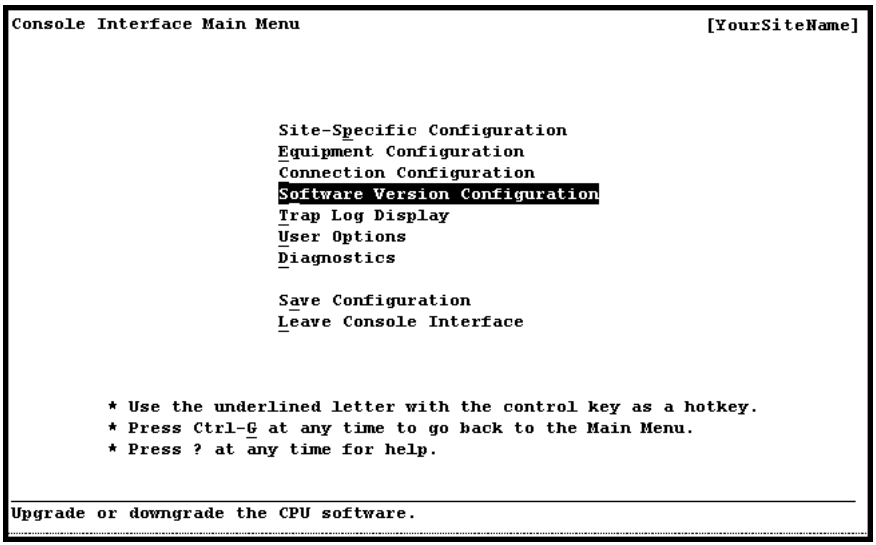

Figure 7-8. Console Interface Main Menu Window (Software Version Configuration Selected)

Upgrading I/O and Server Module Firmware

Steps to Upgrade I/O and Server Module Firmware

Begin

1 On the Console Interface Main Menu window, select the **Software Version Configuration** command.

The Software Version Configuration window (see Figure 7-9) is displayed.

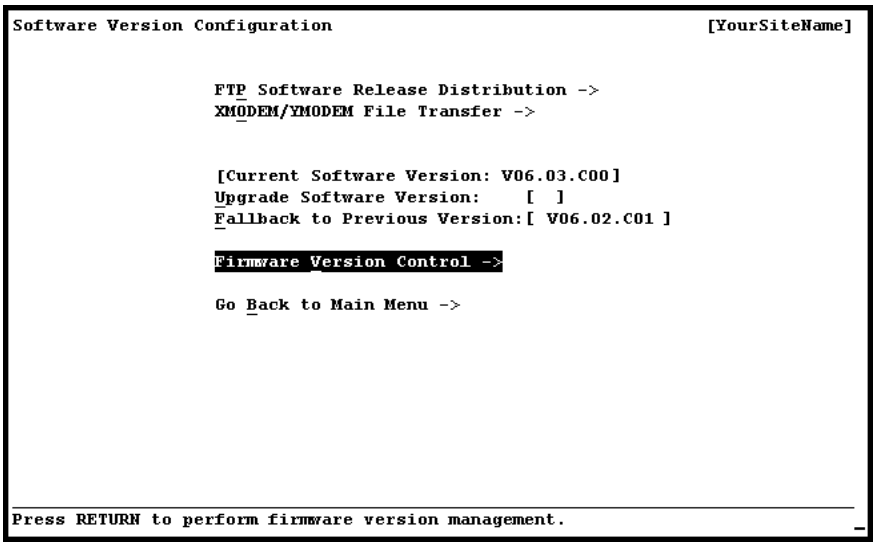

Figure 7-9. The Software Version Configuration Window (Firmware Version Control Selected)

2 Select the **Firmware Version Control** option.

The Firmware Version Control window (see Figure 7-10) is displayed.

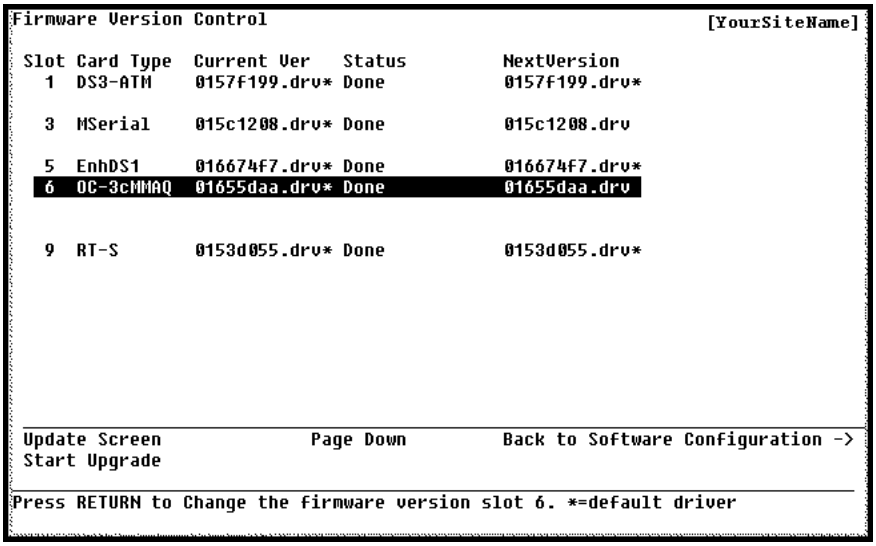

Figure 7-10. Firmware Version Control Window

Commands

The commands in this window have the following functions:

Command	Function
• Update Screen	Refreshes this window to the module's current firmware configuration.
• Start Upgrade	Initiates the downloading of firmware by the selected driver under **NextVersion**.
• Back to Software Configuration→	Redisplays the Software Version Configuration window (see Figure 7-9 on page 7-19).

Field Descriptions

The read-only fields in this window are described in Table 7-3.

Table 7-3. Field Descriptions for the Firmware Version Control Window

Field Name	Description
Slot	The physical slot where the module is installed.
Card Type	The I/O or server module in the slot.

Table 7-3. Field Descriptions for the Firmware Version Control Window

Field Name	Description
Current Version	The version of the firmware on this module. **Note:** An asterisk (*)at the end of the driver name indicates the default version of this driver. Some modules have only one driver that you may select.
Status	This field indicates whether or not the firmware on the module was successfully upgraded. The values that may appear in this field are **Failed**, **Progress**, **Retry, Done,** and **Wrong Card Type**. A status message will appear at the bottom of the window.
NextVersion	The version of the firmware you select to download onto the module. An asterisk followed by the driver name indicates the default driver. **Note:** An asterisk (*)at the end of the driver name indicates the default version of this driver. Some modules have only one driver that you may select.

3 Under the **NextVersion** field, select the driver that represents the version of the firmware you want to download onto the module, and press Enter. Pressing Enter displays the next available driver, thus the Enter key is used to move to the next driver.

The first four digits of the driver code correspond to the firmware release number. The last four digits of the driver code correspond to the checksum.

Selecting Firmware Drivers

You can select either a default driver or nondefault driver from the list of available drivers (see Step 3):

- If you select the default driver, you can install any I/O or sever module into the slot.
- If you select a nondefault driver, you can install only the particular I/O or server module into the slot that is meant for this driver. If you install an I/O or server module that was not meant for this driver, the message **wrongcardtype** is displayed at the bottom of the Firmware Version Control window.

The Access Concentrator system attempts to download the driver for this I/O or server module for approximately six minutes. The Access Concentrator system will recognize the I/O or server module automatically when you install the configured I/O or server module during the download time (six minutes). If the correct I/O or server module is not installed during the

download time, you must select the **Start Upgrade** command on the Firmware Version Control window.

- If you wish to install an I/O or server module other than the I/O or server module with a non-default driver in any particular slot, you must select the default driver in that slot, and select the **Start Upgrade** command on the Firmware Version Control window. The new I/O or server module you have installed is displayed on the Firmware Version Control window.

4. To download the version you selected in Step 3, select the **Start Upgrade** command and press Enter.

   When the confirmation message, **FirmwareDownloadSucceeded,** is displayed at the bottom of the window, the downloading procedure is complete.

5. Select the **Back to Software Configuration** command and press Enter.

   The Software Version Configuration window is displayed.

6. Select the **Go Back to Main Menu** command and press Enter.

   The Console Interface Main Menu (see Figure 7-8 on page 7-18) is displayed.

7. Select the **Equipment Configuration** option.

   The Equipment Configuration window is displayed.

Information about the upgraded module will be updated in a few seconds. A confirmation message is displayed at the bottom of the window.

End

Falling Back to the Previous Software Release

▲ CAUTION:
Use the fallback procedure only if you have previously upgraded your CPU component as described in the section, "Upgrading System Software Using FTP" on page 7-4.

To fall back (return) to the previous software release, perform the steps in the following procedure, starting at the Console Interface Main Menu window (see Figure 7-2 on page 7-5).

Steps to Revert Software to a Previous Version

Begin

1. On the Console Interface Main Menu window, select the **Software Version Configuration** option and press Enter.

The Software Version Configuration window (see Figure 7-11) is displayed.

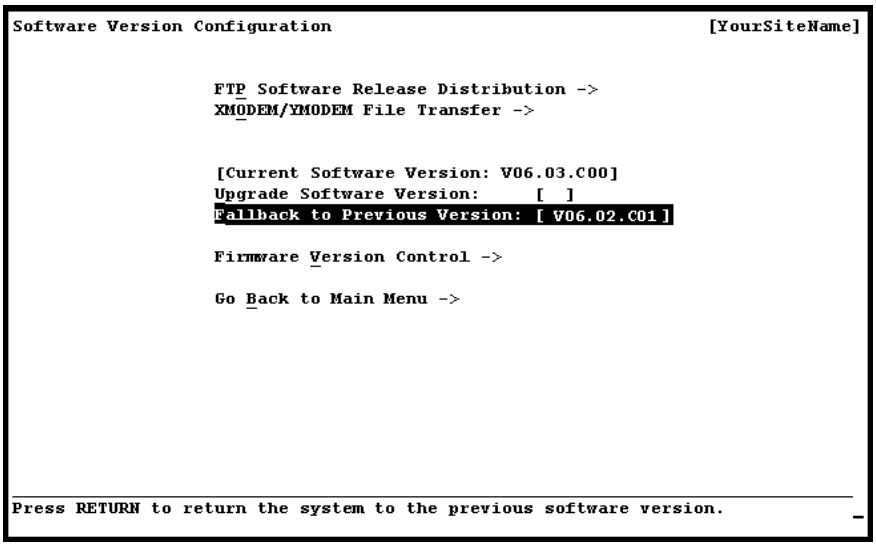

Figure 7-11. Software Version Configuration Window (Fallback to Previous Version Selected)

2 Select the **Fallback to Previous Version** option and press Enter.

The following message is displayed:

```
Are you sure that you want to Return to the previous
version? (y/n)
```

3 Select the **y** key (to indicate yes) to continue.

While the system completes the fallback process, the following message is displayed:

```
Returning the software to the previous version ...
```

When the process is completed, the system displays a message indicating successful completion.

Note: The previous version is restored as the current functional system, and the later version is still stored on the hard disk under the directory structure **/scsi/next/**.

End

Backing Up System Database Files

We recommend that you back up your system, module, and connection configuration database files to a storage medium separate from the hard disk on the CPU component.

▲ CAUTION:
After initially configuring your Access Concentrator system, and after every configuration modification, be sure to back up the files to a separate storage medium.

You can use one of the following methods:

- Upload the database files using FTP server software (see the following section, "Backing Up Database Files Using FTP")
- Transfer files using the XModem or YModem serial transfer protocol (see "Backing Up Database Files Using XModem/YModem File Transfer" on page 7-26)

Configuration and Connections Data Files

The files containing your configuration and connection data are named as follows:

- System configuration database—ssid.def
- System backup file database—ssid.bak
- Password setup—console.def (this file exists only if you have changed your password from the system default password)
- Module configuration database—ecd.bak
- Module backup file database—ecd.def
- Pnni configuration database—pnnimib.db
- Pnni backup file database—pnnimib.bak
- Connection configuration database—cnctn.db
- Vipr task configuration database—vipr.cfg
- Soft-pvc configuration database—spvc.db
- Firmware configuration database—fwc.def
- Event management configuration information—eventmgr.cfg
- IISP CBR route table—iisp.cbr (this file exists even if you have no configured SVCs on your Access Concentrator system)
- IISP VBR route table—iisp.vbr (this file exists even if you have no configured SVCs on your Access Concentrator system)

Backing Up Database Files Using FTP

To back up database files to a separate storage medium using FTP, perform the steps in the following procedure.

Backing Up Database Files Using FTP

Steps to Back Up Database Files Using FTP

Begin

1. Connect a standard 10Base-T Ethernet cable to the Ethernet port on the primary CPU module. Ensure that you have a stable connection from the source PC or network management workstation to the CPU module.
2. Use the DOS drive and change directory commands to access the drive and directory on the computer to which you want to copy (store) the databases.
3. At the DOS prompt, enter:

   <ftp -n *xxx.xxx.xxx.xxx*>

   where

   xxx.xxx.xxx.xxx is the IP address of the Access Concentrator CPU component.

   Press Enter.
4. At the prompt **`ftp>`**, type:

   user readwrite *currentpassword*

   where

   currentpassword is the password you currently have for the Access Concentrator system software.

   Press Enter.
5. To be sure you have the correct path selected, type **cd /scsi/current** (Windows); **cd \scsi\current** (UNIX) and press Enter.
6. To provide a visual indicator during the backup process, type **hash** and press Enter.
7. Type **bin** and press Enter.
8. Type **get "ssid.def"** and press Enter.
9. Type **get "console.def"** and press Enter.
10. Type **get "ecd.def"** and press Enter.
11. Type **get "pnnimib.db"** and press Enter.
12. Type **get "cnctn.db"** and press Enter.
13. Type **get "spvc.db"** and press Enter.
14. Type **get "fwc.def"** and press Enter.
15. Type **get "eventmgr.cfg"** and press Enter.
16. If you have SVCs configured on your system, type **get "iisp.cbr"** and press Enter.
17. If you have SVCs configured on your system, type **get "iisp.vbr"** and press Enter.

18 Type **bye** and press Enter.

End

Backing Up Database Files Using XModem/YModem File Transfer

You can use the XModem/YModem file transfer option to copy the Access Concentrator system databases from the CPU hard disk to a separate storage medium. Backing up the databases using the XModem/YModem file transfer option includes two major tasks:

- First, you set up the cabling and connections between the PC workstation and the Access Concentrator system CPU component, start up the VT100 terminal emulation software on the PC workstation, and ensure you have communication between the two devices (see the following procedure, "Setting Up for the File Transfer Process").
- Second, you perform the file transfer (copy) process for the databases to the separate storage medium (see the procedure, "Copying the Database Files to a Storage Medium" on page 7-27).

Setting Up for the File Transfer Process

Steps to Set Up for the File Transfer Process

Begin

1 Set up the cabling and connections between the PC workstation, the local modem, and the telephone line. Do one of the following:

a. If you are using an external modem, connect a cable from the EIA-232 interface port on the PC workstation to the modem, and a cable from the modem to the telephone line.

b. If you are using an internal modem, connect a cable from the modem port on the PC to the telephone line.

2 Set up the cabling and connections between the Access Concentrator system CPU component, the remote modem, and the telephone line.

~ Connect a cable from the CONSOLE port on the front of the Access Concentrator system to the modem.

~ Connect a cable from the modem to the telephone line.

3 On the PC workstation, start up the VT100 terminal emulation software, and set up the configuration preferences (see Chapter 6, "Configuring the VT100 Terminal Emulator").

4 Using the terminal emulator modem communication function, Return the telephone number of the line connected to the modem connected to the Access Concentrator system.

End

Copying the Database Files to a Storage Medium

Steps to Copy Database Files to a Storage Medium

Begin

1. Using the terminal emulator, log on the Access Concentrator system.
2. On the Console Interface Main Menu window (see Figure 7-2 on page 7-5), select the **Software Version Configuration** option and press Enter.

   The Software Version Configuration window (see Figure 7-12) is displayed.

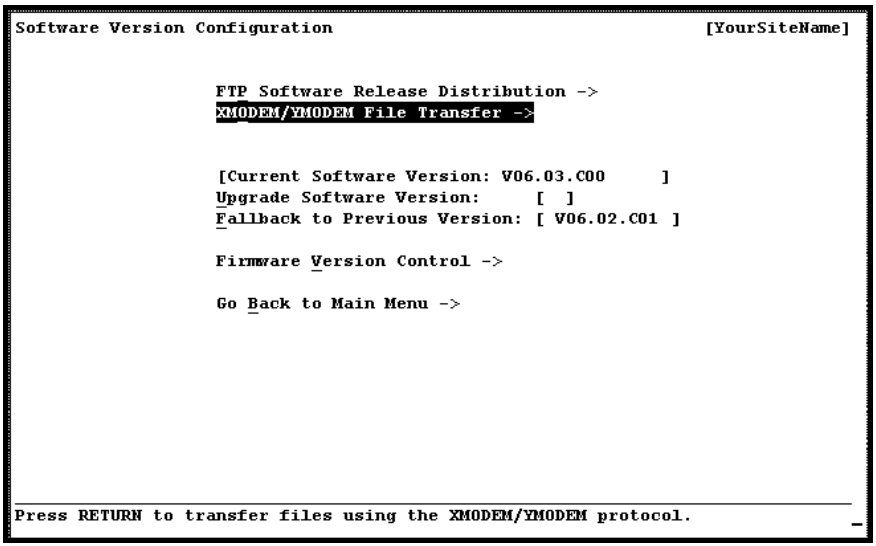

Figure 7-12. Software Version Configuration window (XMODEM/YMODEM File Transfer Selected)

3. On the Software Version Configuration window, select the **XMODEM/YMODEM File Transfer** option and press Enter.

The XMODEM/YMODEM File Transfer window (see Figure 7-13) is displayed.

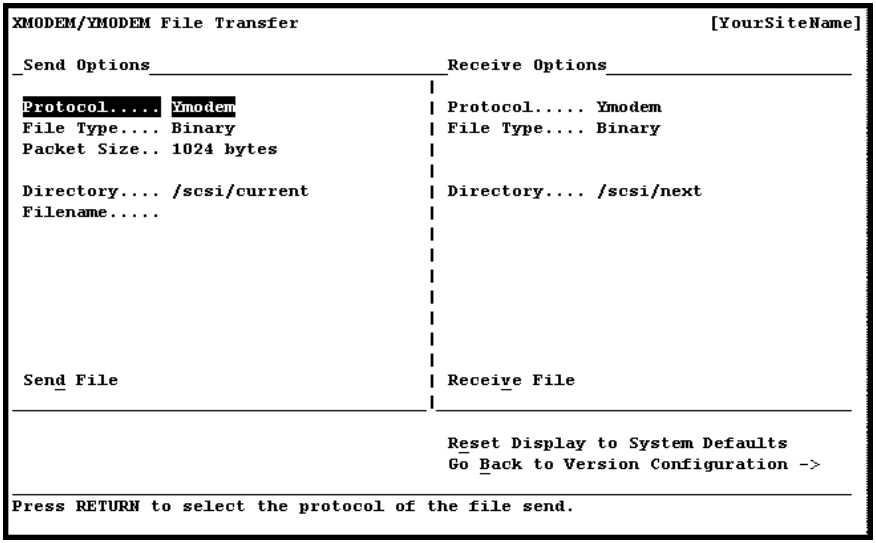

Figure 7-13. XMODEM/YMODEM File Transfer Window (Send Options Panel Selected)

Note: For the database file transfer process, use only the **Send Options** panel.

Commands

The commands on this window have the following functions:

Command	Function
• Send File	Initiates the send function of the file transfer process from the CPU hard disk to a storage medium (such as a PC workstation hard disk).
• Receive File	Initiates the receiving function of the file transfer process to the CPU hard disk from the CD-ROM containing the software upgrade files (running in a CD-ROM drive in a PC workstation).
• Reset Display to System Defaults	Redisplays the default values in the fields.
• Go Back to Version Configuration→	Redisplays the Software Version Configuration window (see Figure 7-12 on page 7-27).

Field Descriptions

4 Select the values for the fields on this window from the values given in Table 7-4.

Table 7-4. Field Values for the XMODEM/YMODEM File Transfer Window (Send Options Panel)

Field Names	Values/Variables	Description
Protocol	Default: YModem	YModem protocol for receiving the upgrade software files.
	XModem	XModem protocol for receiving the upgrade software files.
File Type	Default: Binary	Binary format is the type you use most of the time.
	Text	Text or ASCII format. If you specify text format here, you must specify the text (ASCII) format setting in the terminal emulator.
Packet Size	Default: 1024 bytes	Indicates that the packet size is 1024 bytes.
	128 bytes	Indicates that the packet size is 128 bytes.
Directory	/scsi/current/ *directoryname/*	Subdirectory on the CPU hard disk where the Access Concentrator system databases are stored.
Filename	filename	Filename on the CPU hard disk of the database file. You can specify only one filename at a time. **Note:** The files you need to copy are given on "Steps to Back Up Database Files Using FTP" on page 7-25.

5 Select the **SendFiles** command and press Enter.

The terminal emulator displaying the Access Concentrator system interface window scrolls the XMODEM/YMODEM File Transfer window out of view. A message is displayed indicating that you can cancel the transfer by pressing Ctrl+X several times. A second message is displayed indicating that you must start the terminal emulator receive function.

6 Using the terminal emulator receive function, select one of the two protocol types: 1) YModem, or 2) XModem. Be sure to select the same protocol as the one you selected on the Access Concentrator system XMODEM/YMODEM File Transfer window.

7 In the terminal emulator field for the location of the file, specify the drive and the directory pathname on the PC hard disk where you want to transfer (copy) the database file.

For example, specify a pathname like the following:

<*x*:/directory/*filename*>** where *x* is the drive letter for the PC hard disk and *directory* is any name you choose (such as **acdbase**)

Be sure you enter the filename of the database file exactly so that it matches the name you previously entered on the Access Concentrator system XMODEM/YMODEM File Transfer window.

8 Select the **OK** or **Receive** button or command in the terminal emulator receive function dialog box.

9 Repeat steps 4–8 to specify another database filename until you have transferred all the database files to the PC hard disk.

End

Restoring System Database Files

If your system, module, and connection configuration database files become corrupted or otherwise unusable, you must restore them from your backup storage medium to the CPU hard disk by using one of the following methods:

- Download the database files using FTP server software (see "Restoring Database Files Using FTP" on page 7-30)
- Transfer files using the XModem or YModem serial transfer protocol (see "Restoring Database Files Using XModem/YModem File Transfer" on page 7-32)

Configuration and Connection Data Files

The files containing your configuration and connection data are named as follows:

- System configuration database—ssid.def
- Password setup—console.def (this file exists only if you have changed your password from the system default password)
- Module configuration database—ecd.def
- Pnni configuration database—pnnimib.db
- Connection configuration database—cnctn.db
- Soft-pvc configuration database—spvc.db
- Firmware configuration database—fwc.def
- Event management configuration information—eventmgr.cfg
- IISP CBR route table—iisp.cbr (this file exists even if you have no configured SVCs on your Access Concentrator system)
- IISP VBR route table—iisp.vbr (this file exists even if you have no configured SVCs on your Access Concentrator system)

Restoring Database Files Using FTP

To restore database files from a separate storage medium using FTP, perform the steps in the following procedure.

Restoring Database Files Using FTP

Steps to Restore Database Files Using FTP

Begin

1. Connect a standard 10Base-T Ethernet cable to the Ethernet port on the front of the Access Concentrator system. Ensure that you have a stable connection from the source PC or network management workstation to the CPU component.
2. Use the DOS drive and change directory commands to access the drive and directory on the computer where you have stored the databases.
3. At the DOS prompt, enter:

   <ftp -n *xxx.xxx.xxx.xxx***>**

   where

   xxx.xxx.xxx.xxx is the IP address of the Access Concentrator CPU component.

   Press Enter.
4. At the prompt **`ftp>`**, enter:

   user readwrite *currentpassword*

   where

   currentpassword is the password you currently have for the Access Concentrator System software.

   Press Enter.
5. To be sure you have the correct path selected, type **cd /scsi/current** (Windows); **cd \scsi\current** (UNIX) and press Enter.
6. To provide a visual indicator during the backup process, type **hash** and press Enter.
7. Type **bin** and press Enter.
8. Type **put "ssid.def"**and press Enter.
9. Type **put "console.def"** and press Enter.
10. Type **put "ecd.def"** and press Enter.
11. Type **put "pnnimib.db"** and press Enter.
12. Type **put "cnctn.db"** and press Enter.
13. Type **put "spvc.db"** and press Enter.
14. Type **put "fwc.def"** and press Enter.
15. Type **put "eventmgr.cfg"** and press Enter.
16. If you have SVCs configured on your system, type **put "iisp.cbr"** and press Enter.
17. If you have SVCs configured on your system, type **put "iisp.vbr"** and press Enter.

18 Type **bye** and press Enter.

End

At this point, you must reboot (reinitialize) the Access Concentrator system chassis, so all components are synchronized. To reboot the Access Concentrator system, perform the steps in the following procedure.

Rebooting the AC System

Steps to Reboot the Access Concentrator System

Begin

1 Log on the Access Concentrator system.

The Console Interface Main Menu window (see Figure 7-2 on page 7-5) is displayed.

2 On the Console Interface Main Menu window, select the **Diagnostics** option.

The Diagnostics Menu window is displayed.

3 On the Diagnostics Menu window, select the **Reboot Hardware Components** command.

The Remote Reboot Configuration window is displayed.

4 On the Remote Reboot Configuration window, select the **Reboot Chassis** command.

This command reboots (reinitializes) the CPU component, and the I/O and server modules.

End

Restoring Database Files Using XModem/YModem File Transfer

You can use the XModem/YModem file transfer option to restore the Access Concentrator system databases from a separate storage medium to the CPU hard disk. Restoring the databases using the XModem/YModem file transfer option is a process transferring files from the PC workstation to the Access Concentrator system. This procedure includes two major tasks:

- First, set up the cabling and connections between the PC workstation and the Access Concentrator system CPU component, start up the VT100 terminal emulation software on the PC workstation, and ensure you have communication between the two devices (see the following procedure,"Steps to Set Up for the File Transfer Process").
- Second, you perform the file transfer (copy) process for the backup database files to the Access Concentrator system (see the procedure, "Steps to Copy Database Files to a Storage Medium" on page 7-27).

Setting Up for the File Transfer Process

Steps to Set Up for the File Transfer Process

Begin

1 Set up the cabling and connections between the PC workstation, the local modem, and the telephone line. Do one of the following:

a. If you are using an external modem, connect a cable from the RS-232 interface port on the PC workstation to the modem, and a cable from the modem to the telephone line.

- The single modem kit consists of a rack-mounted modem, cables, and connectors.

b. If you are using an internal modem, connect a cable from the modem port on the PC to the telephone line.

2 Set up the cabling and connections between the Access Concentrator system CPU module, the remote modem, and the telephone line.

a. Connect a cable (or cables) from the CONSOLE port on the CPU module (or modules) to the modem as follows.

- If you have a redundant modem kit, connect cables from the switching modem to the CONSOLE ports on both CPU modules, and set up the switching modem to establish a connection with the primary CPU module.

3 Set up the cabling and connections between the Access Concentrator system CPU component, the remote modem, and the telephone line.

a. Connect a cable (or cables) from the CONSOLE port on the front of the Access Concentrator system to the modem.

b. Connect a cable from the modem to the telephone line.

4 On the PC workstation, start up the VT100 terminal emulation software, and set up the configuration preferences (see Appendix B).

5 Using the terminal emulator modem communication function, Return the telephone number of the line connected to the modem connected to the Access Concentrator system.

Copying the Backup Files to the System

Steps to Copy the Backup Database Files to the System

Begin

1 Using the terminal emulator, log on the Access Concentrator system.

2 On the Console Interface Main Menu window (see Figure 7-2 on page 7-5), select the **Software Version Configuration** option and press Enter.

The Software Version Configuration window (see Figure 7-5 on page 7-11) is displayed.

3 On the Software Version Configuration window, select the **XMODEM/YMODEM File Transfer** option and press Enter.

The XMODEM/YMODEM File Transfer window (see Figure 7-14) is displayed.

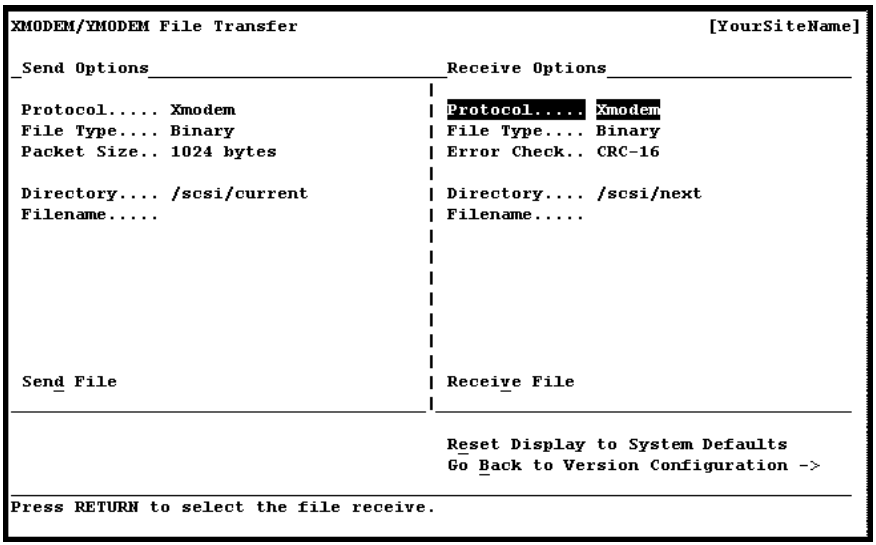

Figure 7-14. XMODEM/YMODEM File Transfer Window (Receive Options Panel Selected)

Note: For the software upgrade process, use only the **Receive Options** panel.

Commands

The commands on this window have the following functions:

Command	Function
• Send File	Initiates the send function of the file transfer process from the CPU hard disk to a storage medium (such as a PC workstation hard disk).
• Receive File	Initiates the receiving function of the file transfer process to the CPU module hard disk from the separate storage medium containing the backup database files.
• Reset Display to System Defaults	Redisplays the default values in the fields.
• Go Back to Version Configuration→	Redisplays the Software Version Configuration window (see Figure 7-3 on page 7-6).

Field Descriptions

4 Select the values for the fields on this window from the values given in Table 7-5.

Table 7-5. Field Values for the XMODEM/YMODEM File Transfer Window (Receive Options Panel)—Restoring Backup Files

Field Names	Values/Variables	Description
Protocol	Default: YModem	YModem protocol for receiving the upgrade software files.
	Ymodem-G	YModem-G protocol for receiving the upgrade software files.
	XModem	XModem protocol for receiving the upgrade software files.
File Type	Default: Binary	Binary format is the type you use most of the time.
	Text	Text or ASCII format is available but do not use it for restoring database files.
Error Check (displayed only when the value **XModem** is selected in the **Protocol** field)	Default: CRC-16	Indicates that the error checking method is cyclical redundant checking, 16 bits.
	Checksum	Indicates that the error checking method is arithmetic summation checking, 8 bits.
Directory	/scsi/current/	Directory on the CPU module hard disk where the backup database files are to be restored.
Filename (displayed only when the value **XModem** is selected in the **Protocol** field)	filename	Filename on the CPU module hard disk, which the backup database file (of the same name) will overwrite.

Note: We recommend that you use either the YModem or the YModem-G protocol. Use the XModem protocol if that is the only one you have available to use.

- The YModem-G protocol allows the fastest transmission of the three types; however, this protocol does not acknowledge receipt of packets. You can receive all files grouped under a subdirectory at one time.
- The YModem protocol is a slower method of transmission, but is more reliable because it does acknowledge receipt of packets. You can receive all files grouped under a subdirectory at one time.
- The XModem protocol is a laborious method of transmission because you must enter the filename of each file in the complete package of software upgrade files to accomplish the upgrade task.

5 Select the **Receive** command and press Enter.

The terminal emulator displaying the Access Concentrator system window interface scrolls the XMODEM/YMODEM File Transfer window out of view. A message is displayed indicating that you can cancel the transfer by pressing Ctrl+X several times. A second message is displayed indicating that you must start the terminal emulator send function.

6 Using the terminal emulator send function, select one of the three protocol types: 1) YModem, 2) YModem-G, or 3) XModem. Be sure to select the same protocol as the one you selected on the Access Concentrator system XMODEM/YMODEM File Transfer window.

7 In the terminal emulator field for the location of the file, specify the drive where the Access Concentrator system backup database files reside and the directory pathname.

For example, specify a pathname like one of the following:

- **<*x*:\acbackup*.*>** if you are using YModem or YModem-G where *x* is the drive letter where the backup database files reside
- **<*x*:\acbackup*filename*>** if you are using XModem where *x* is the drive letter where the backup database files reside

Be sure you enter the directory name (or the directory and filename if using XModem) exactly so that it matches the names you previously entered on the Access Concentrator system XMODEM/YMODEM File Transfer window.

8 Select the **OK** or **Send** button or command in the terminal emulator send function dialog box.

9 Repeat steps 4 through 8 to specify another filename (for XModem) until you have transferred all the backup files to the CPU hard disk.

End

At this point, you must reboot (reinitialize) the Access Concentrator system chassis, so all components are synchronized. To reboot the Access Concentrator system, perform the steps in the following procedure.

Rebooting the AC System

Steps to Reboot the Access Concentrator System

Begin

1 Redisplay the Console Interface Main Menu window (see Figure 7-2 on page 7-5).

2 On the Console Interface Main Menu window, select the **Diagnostics** option.

The Diagnostics Menu window is displayed.

3 On the Diagnostics Menu window, select the **Reboot Hardware Components** command.

The Remote Reboot Configuration window is displayed.

4 On the Remote Reboot Configuration window, select the **Reboot Chassis** command.

This command reboots (reinitializes) the CPU component, and the I/O and server modules.

End

A SNMP Trap Messages

This appendix describes the SNMP trap and notification messages generated by the Access Concentrator Console Interface system SNMP agent. External SNMP managers can perform various functions in the Access Concentrator system, and can receive the trap and notification messages. Access the Trap Log Display window to view the messages, as described in the following procedure.

An electronic copy of the full ASN.1 version of the SNMP MIB is available upon request.

Viewing SNMP Trap Messages

Use the following steps to view SNMP trap and notification messages, starting at the Console Interface Main Menu window (see Figure A-1).

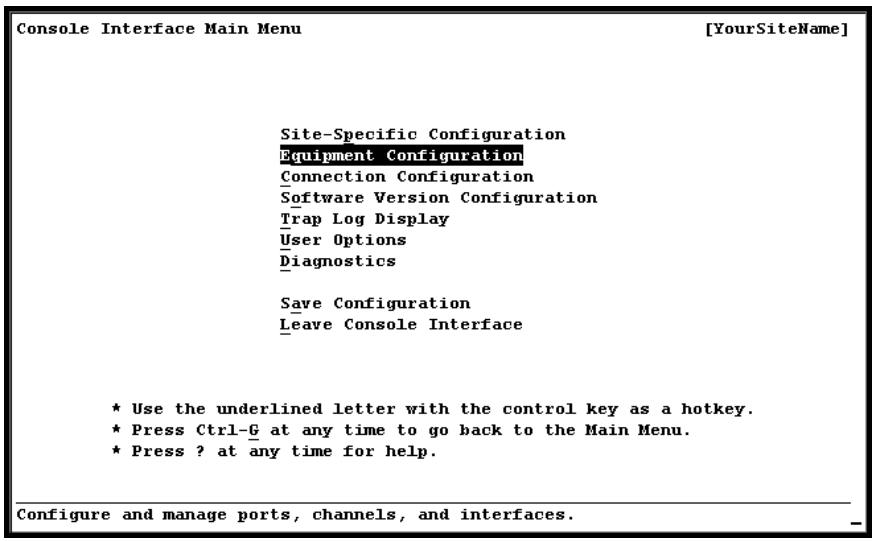

Figure A-1. Console Interface Main Menu Window (Trap Log Display Selected)

1. Select the **Trap Log Display** option.

The Trap Log Display window is displayed (see Figure A-2) .

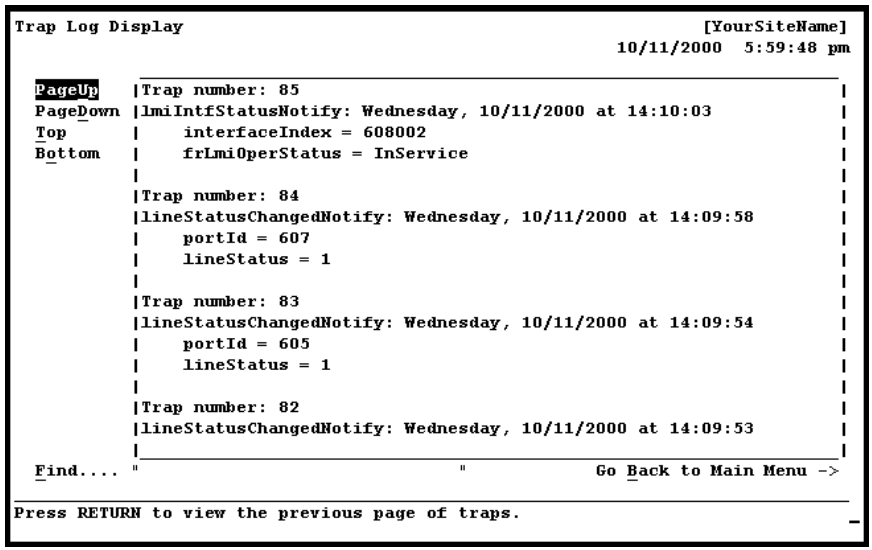

Figure A-2. Trap Log Display Window

To find a description of what a trap message means, follow these steps.

2. Look for the message that you want information about in Table A-1 on page A-3.

   For example, you might want information about the trap message **cardInsertionNotify**. You would find this message under the enterprise object identifier **Module Events**.

3. Look for the message that you want information about in Table A-2 on page A-9.

   Using the preceding example, you would find the message **cardInsertionNotify** and find the following information:

   - Type of event that caused the message: a system, module, interface, or connection event
   - System indicator for the trap message
   - The MIB objects associated with the trap message
   - Description of the trap message indicating what happened.

4. To find out more information about the MIB objects, find the object that you want more information about in "Definitions of MIB Objects Used for Traps" on page A-43.

   The description of the object includes the type of information the object presents. If the object has enumerated types, the integer values and their definitions are also listed. In the preceding example, **cardInsertionNotify**

has four associated MIB objects, **cardSlot**, **cardType**, **cardProtectionStatus**, and **cardOperStatus**, which are all enumerated-type objects.

Table A-1 lists the enterprise-specific trap names and trap numbers in the four groups of enterprise object identifiers: 1) system events; 2) module events; 3) interface events; and 4) connection events.

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
System Events (Enterprise Object Identifier):	
1	systemColdStartNotify
2	systemWarmStartNotify
3	ecdBootFailureNotify
4	referenceClockFailNotify
5	referenceClockClearedNotify
6	compositeClockFailNotify
7	compositeClockClearedNotify
8	stratumModeChangeNotify
9	powerSupplyStatusNotify
10	softwareDownloadStatusNotify
11	muxReadyConfirmReceivedNotify
12	muxReadyConfirmNotReceivedNotify
13	oneWayMessageWhileInTwoWayStateNotify
14	inactivityTimerExpiredNotify
15	keepAliveTimerExpiredInLlDownStateNotify
16	keepAliveTimerExpiredInOneWayStateNotify
17	completeClockFailedNotify
18	completeClockRecoveredNotify
19	backplaneCircuitryFailedNotify
20	backplaneCircuitryRecoveredNotify
21	remoteRebootNotify
22	saveConfigurationNotify
23	versionConfigurationNotify
24	fileTransferStatusNotify
25	ipOrMaskInvalidNotify
26	alarmCardInputChangeNotify
27	removeConfigFilesNotify
28	alarmCardOutputChangeNotify
29	alarmCardAcoChangeNotify
30	snmpCommunityStringsChangedToPublicNotify

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
31	pnniNodeCfgNotify
32	pnniNodeCfgFailNotify
33	pnniNodeModFailNotify
34	pnniNodeDelFailNotify
35	pnniNodeOOSFailNotif
36	pnniNodeISFailNotify
37	pnniRtAddrCfgNotify
38	pnniRtAddrCfgFailNotify
39	pnniRtAddrModFailNotify
40	pnniRtAddrDelFailNotify
41	pnniRtAddrAddByIlmiNotify
42	pnniRtAddrDelByIlmiNotify
43	callContrlResAllocFailNotify
44	differentSystemSoftwareNotify
Module Events (Enterprise Object Identifier):	
1	cardInsertionNotify
2	cardRemovedOrFailedNotify
3	lineStatusChangedNotify
4	firmwareDownloadSucceededNotify
5	firmwareDownloadFailedNotify
6	moduleRebootNotify
7	oc3APSStateChangeNotify
8	oc3APSSSwitchoverNotify
9	portModifyFailNotify
Interface Events (Enterprise Object Identifier):	
1	interfaceCreatedNotify
2	interfaceDeletedNotify
3	interfaceModifiedNotify
4	interfaceModifyFailNotify
5	interfaceOutOfServiceNotify
6	interfaceInServiceNotify
7	bridgeDomainFullNotify
8	bridgeDomainExceededForSlotNotify
9	bridgeDomainNumberInUseNotify
10	bridgeDomainInServiceNotify

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
11	bridgeDomainNumberInvalidNotify
12	signalingModifyFailNotify
13	lmiIntfStatusNotify
14	isdnLapdDownNotify
15	isdnLapdUpNotify
16	bridgeDomainTimingRelationshipNotify
17	ts16UsageModifyFailNotify
18	ceServiceTypeModifyFailNotify
19	channelizationModifyFailNotify
20	cirEmSpvcConfiguredNotify
21	cirEmSpvcConfigFailNotify
22	cirEmSpvcDeletedNotify
23	cirEmSpvcModifiedNotify
24	cirEmSpvcModifyFailNotify
25	vbrSpvcConfiguredNotify
26	vbrSpvcConfigFailNotify
27	vbrSpvcDeletedNotify
28	vbrSpvcModifiedNotify
29	vbrSpvcModifyFailNotify
30	atmSpvcConfiguredNotify
31	atmSpvcConfigFailNotify
32	atmSpvcDeletedNotify
33	atmSpvcModifiedNotify
34	atmSpvcModifyFailNotify
35	cRC4ModifyFailNotify
36	imaGrpChannelFailNotify
37	imaGrpChannelFailNotify
38	imaGrpChannelClearedNotify
39	atmImaIntfClearedNotify
40	pnniProtLnkUpAndAdv
41	pnniProtLinkUpAndNotAdv
42	pnniProtLnkStatDown
43	pnniIntfCfgFailNotify
44	viprPingTrap
45	viprArpTrap

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
46	viprRoutingTrap
47	viprVpnTrap
48	viprIpIntfTrap
49	viprSubChanTrap
50	viprRtSrvTrap
51	atmSvcIntfLayer2Up
52	atmSvcIntfLayer2Down
53	apsConfigurationModifyFailNotify
54	viprStatRtTrap
55	interfaceCreateFailNotify
Connection Events (Enterprise Object Identifier):	
1	atmPvcVccReqFailNotify
2	atmPvcVpcReqFailNotify
3	ipAtmAppPvcVccReqFailNotify
4	cirEmAtmPvcVccReqFailNotify
5	vbrAtmPvcVccReqFailNotify
6	frAtmPvcVccReqFailNotify
7	frFrPvcReqFailNotify
8	cirEmCirEmPvcReqFailNotify
9	vbrVbrPvcReqFailNotify
10	atmPvcVccSetupNotify
11	atmPvcVpcSetupNotify
12	ipAtmAppPvcVccSetupNotify
13	cirEmAtmPvcVccSetupNotify
14	vbrAtmPvcVccSetupNotify
15	frAtmPvcVccSetupNotify
16	frFrPvcSetupNotify
17	cirEmCirEmPvcSetupNotify
18	vbrVbrPvcSetupNotify
19	atmPvcVccTearDownNotify
20	atmPvcVpcTearDownNotify
21	ipAtmAppPvcVccTearDownNotify
22	cirEmAtmPvcVccTearDownNotify
23	vbrAtmPvcVccTearDownNotify
24	frAtmPvcVccTearDownNotify

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
25	frFrPvcTearDownNotify
26	cirEmCirEmPvcTearDownNotify
27	vbrVbrPvcTearDownNotify
28	bridgeBridgePvcReqFailNotify
29	bridgeBridgePvcSetupNotify
30	bridgeBridgePvcTearDownNotify
31	bridgeAtmPvcVccReqFailNotify
32	bridgeAtmPvcVccSetupNotify
33	bridgeAtmPvcVccTearDownNotify
34	cellTestReqFailNotify
35	lmiDlciStatusNotify
36	cirEmAtmBkPvcVccReqFailNotify
37	cirEmAtmBkPvcVccSetupNotify
38	cirEmAtmBkPvcVccTearDownNotify
39	vbrAtmBkPvcVccReqFailNotify
40	vbrAtmBkPvcVccSetupNotify
41	vbrAtmBkPvcVccTearDownNotify
42	atmBkPvcVccReqFailNotify
43	atmBkPvcVccSetupNotify
44	atmBkPvcVccTearDownNotify
45	frAtmBkPvcVccReqFailNotify
46	frAtmBkPvcVccSetupNotify
47	frAtmBkPvcVccTearDownNotify
48	atmBkPvcVpcReqFailNotify
49	atmBkPvcVpcSetupNotify
50	atmBkPvcVpcTearDownNotify
51	bridgeAtmBkPvcVccReqFailNotify
52	bridgeAtmBkPvcVccSetupNotify
53	bridgeAtmBkPvcVccTearDownNotify
54	ipAtmBkAppPvcVccReqFailNotify
55	ipAtmBkAppPvcVccSetupNotify
56	ipAtmBkAppPvcVccTearDownNotify
57	cirEmAtmSpvcVccSetUpNotify
58	vbrAtmSpvcVccSetUpNotify
59	atmSpvcVccSetUpNotify

Table A-1. Enterprise-Specific SNMP Trap Names and Trap Numbers by Enterprise Object Identifier

Enterprise-Specific Trap Number	Enterprise-Specific Trap Name
60	cirEmAtmSpvcVccTearDownNotify
61	vbrAtmSpvcVccTearDownNotify
62	atmSpvcVccTearDownNotify
63	oamTestReqFailNotify
Virtual Interface Events (Enterprise Object Identifier):	
219	vi-Cannot-Be-0
220	vi-OOR
221	vi-Mod-Limit-Exceeded
222	vi-Resource-Unavail
223	vi-Already-Exists
224	vi-Does-Not-Exist
225	vi-0-Non-Ubr-Conn-Not-Supp
226	vi-OS-Cannot-Be-0
227	vi-OS-OOR
228	vi-CellRate-Too-Lo
229	vi-CellRate-Too-Hi
230	intf-CBR-CellRate-Exceeded
231	intf-VBR-CellRate-Exceeded
232	vi-Conn-CellRate-Exceeded
233	vi-Not-Enabled
234	vi-Should-Be-0
235	vi-OOR-A
236	vi-OOR-B
237	vi-0-Non-Ubr-Conn-Not-SuppA2B
238	vi-0-Non-Ubr-Conn-Not-SuppB2A
239	vi-Should-Be-0-A
240	vi-Should-Be-0-B
241	vi-Cbr-Bw-Unavailable-Egrs
242	vi-Cbr-Bw-Unavailable-Egrs-A
243	vi-Cbr-Bw-Unavailable-Egrs-B
244	vi-Vbr-Bw-Unavailable-Egrs
245	vi-Vbr-Bw-Unavailable-Egrs-A
246	vi-Vbr-Bw-Unavailable-Egrs-B
247	vi-Not-Enabled-A
248	vi-Not-Enabled-B

Table A-2 on page A-9 provides information about the SNMP enterprise-specific trap messages, including the following:

- Enterprise-specific trap name
- Type of event that caused the message: a system, module, interface, or connection event
- System indicator for the trap message
- The MIB objects associated with the trap message
- Description of the trap message indicating what happened.

The system indicators for the trap messages are defined as follows:

System Indicator for the Trap (Column 3 in Table A-2)	Definition
• System Response ("Response" in Table A-2)	A system-supplied reply to a command a user enters, usually indicating the success or failure of a requested action.
• System Information ("Info" in Table A-2)	A system-supplied informational message indicating the completion of a particular process (for example, a maintenance function).
• Minor Problem ("Minor" in Table A-2)	A notification of a problem that does not affect service or function of a component of the Access Concentrator system (for example, the failure of a redundant power supply module).
• Major Problem ("Major" in Table A-2)	A notification of a problem that affects service of function of a component of the Access Concentrator system (for example, failure of a DS1/T1 module).
• Critical Problem ("Critical" in Table A-2)	A notification of a problem that affects functioning of the whole Access Concentrator system (for example, failure of a nonredundant Stratum 3–4 module). Critical notifications indicate that all traffic flow through the system has ceased.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
aal2TrunkConfig ReqFailNotify	Connection	Response	aal2TrunkConfigIf aal2TrunkConfigVpi aal2TrunkConfigVci pvcFailureReasonCode	The PVC VCC aal2 trunk could not be setup.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
aal2TrunkConfig TearDownNotify	Connection	Response	aal2TrunkConfigIf aal2TrunkConfigVpi aal2TrunkConfigVci	The PVC VCC AAL2 Trunk has been deleted.
aal2TrunkConfig SetupNotify	Connection	Response	aal2TrunkConfigIf aal2TrunkConfigVpi aal2TrunkConfigVci	The PVC VCC connection for aal2 trunk.
alarmCardAco-ChangeNotify	System	Info	alarmCardReasonCode	Indicates the action taken by the indicated type of the audible alarm.
alarmCardIn-putChangeNotify	System	Info	alarmCardReasonCode deviceId	Indicates that the **deviceId** with **alarmCardReasonCode** has changed its status.
alarmCardOut-putChangeNotify	System	Info	alarmCardReasonCode deviceId	Indicates that the **deviceId** with **alarmCardReasonCode** has changed its status.
atmAtmSpvcConfigFailNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr spvcConfigFailureCode	Notification that an attempt to configure an endpoint as ATM SPVC endpoint has failed.
atmAtmSpvcConfiguredNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr	Notification that an endpoint has been configured as ATM SPVC endpoint.
atmAtmSpvcDeletedNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr	Notification that ATM SPVC configuration has been deleted.
atmAtmSpvc-ModifiedNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr	Notification that a SPVC endpoint has been modified.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
atmAtmSpvcModifyFailNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr spvcConfigFailureCode	Notification that an attempt to modify a TE SPVC endpoint has failed.
atmAtmSpvcVccSetUpNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr atmAtmSpvcVccIfB atmAtmSpvcVccVpiB atmAtmSpvcVccVciB	Notification that a SPVC connection between ATM and ATM endpoints has been made successfully.
atmAtmSpvcVccTearDownNotify	Interface	Info	spvcAddrIfA atmAtmSpvcVccVpiA atmAtmSpvcVccVciA atmAtmSpvcVccRemoteAtmPortAddr atmAtmSpvcVccIfB atmAtmSpvcVccVpiB atmAtmSpvcVccVciB	Notification that a SPVC connection between ATM and ATM endpoints has been deleted.
atmBkPvcVccReqFailNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB pvcFailureReasonCode	The DHPVC VCC backup connection request between an ATM interface and an ATM interface has failed.
atmBkPvcVccSetupNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB	The DHPVC VCC backup connection between an ATM interface and an ATM interface has been created.
atmBkPvcVccTearDownNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB	The DHPVC VCC backup connection between an ATM interface and an ATM interface has been deleted.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
atmBk-PvcVpcReqFail-Notify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB pvcFailureReasonCode	The DHPVC VPC backup connection request between an ATM interface and an ATM interface has failed.
atmBkPvcVpc-SetupNotify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB	The DHPVC VPC backup connection between an ATM interface and an ATM interface has been created.
atmBkPvcVpc-TearDownNotify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB	The DHPVC VPC backup connection between an ATM interface and an ATM interface has been deleted.
atmImaIntf-ClearedNotify	Interface	Info	atmImaIntfIndex atmImaIntfStatus	The **atmImaIntf-ClearedNotify** trap indicates a failure has been cleared in an IMA interface. The **atmImaIntfSta-tus** field indicates the failure that has been cleared.
atmImaIntfFail-Notify	Interface	Info	atmImaIntfIndex atmImaIntfStatus	The **atmImaIntfFail-Notify** trap indicates a failure in the physical IMA interface. The **atmImaIntfSta-tus** field indicates the reason for the failure.
atmPvcVccReq-FailNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB pvcFailureReasonCode	The PVC VCC connection request between two ATM interfaces failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
atmPvcVccSetupNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB	The PVC VCC connection between two ATM interfaces has been created.
atmPvcVccTearDownNotify	Connection	Response	atmPvcVccIfA atmPvcVccVpiA atmPvcVccVciA atmPvcVccIfB atmPvcVccVpiB atmPvcVccVciB	The PVC VCC connection between two ATM interfaces has been deleted.
atmPvcVpcReqFailNotify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB pvcFailureReasonCode	The PVC VPC connection request between two ATM interfaces failed.
atmPvcVpcSetupNotify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB	The PVC VPC connection between two ATM interfaces has been created.
atmPvcVpcTearDownNotify	Connection	Response	atmPvcVpcIfA atmPvcVpcVpiA atmPvcVpcIfB atmPvcVpcVpiB	The PVC VPC connection between two ATM interfaces has been deleted.
atmSpvcConfigFailNotify	Interface	Info	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA spvcConfigFailureCode	Notification that an attempt to configure an endpoint as ATM SPVC endpoint has failed.
atmSpvcConfiguredNotify	Interface	Info	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA	Notification that an endpoint has been configured as ATM SPVC endpoint.
atmSpvcDeletedNotify	Interface	Info	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA	Notification that ATM SPVC configuration has been deleted.
atmSpvcModifiedNotify	Interface	Info	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA	Notification that a SPVC endpoint has been modified.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
atmSpvcModify-FailNotify	Interface	Info	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA spvcConfigFailureCode	Notification that an attempt to modify a TE SPVC endpoint has failed.
atm-SpvcVccSetUp-Notify	Connec-tion	Response	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA atmSpvcVccIfB atmSpvcVccVpiB atmSpvcVccViB	Notification that a SPVC connection between ATM and ATM endpoints has been made success-fully.
atmSpvcVccTe-arDownNotify	Connec-tion	Response	atmSpvcVccIfA atmSpvcVccVpiA atmSpvcVccVciA atmSpvcVccIfB atmSpvcVccVpiB atmSpvcVccViB	Notification that a SPVC connection between ATM and ATM endpoints has been deleted.
backplaneCir-cuitryFailedNo-tify	System	Critical	< NO OBJECTS >	There is no activity on the cell bus. Please call Technical Support immediately to resolve the prob-lem.
backplaneCir-cuitryRecov-eredNotify	System	Info	< NO OBJECTS >	The CPU module is able to detect activity on the cell bus.
bridgeAtmBk-PvcVccReqFail-Notify	Connec-tion	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccViB pvcFailureReasonCode	The DHPVC VCC backup connection request between a bridge interface and an ATM interface has failed.
bridgeAtmBk-PvcVccSetupNo-tify	Connec-tion	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccViB	The DHPVC VCC backup connection between a bridge interface and an ATM interface has been created.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
bridgeAtmBk-PvcVccTear-DownNotify	Connection	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccVciB	The DHPVC VCC backup connection between a bridge interface and an ATM interface has been deleted.
bridgeAt-mPvcVccReq-FailNotify	Connection	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccVciB pvcFailureReasonCode	The PVC VCC connection request between a bridge interface and an ATM interface has failed.
bridgeAt-mPvcVccSetup-Notify	Connection	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccVciB	The PVC VCC connection between a bridge interface and an ATM interface has been created.
bridgeAt-mPvcVccTear-DownNotify	Connection	Response	bridgeAtmPvcVccIfA bridgeAtmPvcVccIfB bridgeAtmPvcVccVpiB bridgeAtmPvcVccVciB	The PVC VCC connection between a bridge interface and an ATM interface has been deleted.
bridge-BridgePvcReq-FailNotify	Connection	Response	bridgeBridgePvcIfA bridgeBridgePvcIfB pvcFailureReasonCode	The PVC connection request between two bridge interfaces has failed.
bridge-BridgePvcSetup-Notify	Connection	Response	bridgeBridgePvcIfA bridgeBridgePvcIfB	The PVC connection between two bridge interfaces has been created.
bridge-BridgePvcTear-DownNotify	Connection	Response	bridgeBridgePvcIfA bridgeBridgePvcIfB	The PVC connection between two bridge interfaces has been deleted.
bridgeDomain-Exceeded-ForSlotNotify	Interface	Info	cardSlot	The bridge domain number has been exceeded for the slot.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
bridgeDomain-FullNotify	Interface	Info	bridgeDomainNumber	The 15 ports available for the bridge domain are being used, leaving no space for an additional port.
bridgeDomain-InServiceNotify	Interface	Info	bridgeDomainNumber	Notification that a bridge domain is now in service.
bridgeDomain-NumberInUse-Notify	Interface	Info	bridgeDomainNumber	Notification that a bridge domain number is currently in use.
bridgeDomain-NumberInvalid-Notify	Interface	Info	interfaceIndex	Indicates that this interface contains an invalid bridge domain number. In order to create a domain, associate a port with a domain, or bring an interface in service, a valid domain number must be provided.
bridgeDomain-TimingRelationshipNotify	Interface	Info	bridgeDomainNumber timingReasonCode	Trap sent when one of the following relationships is violated: (1) 2 * (**BridgeForwardDelay** - 1.0 sec) >= **BridgeMaxAge** (2) **BridgeMaxAge** >= 2 * (**BridgeHelloTime** + 1.0 sec).
cRC4ModifyFailNotify	Interface	Info	portId interfaceFailureReasonCode	
cardInsertion-Notify	Module	Info	cardSlot cardType cardProtectionStatus cardOperStatus	The indicated slot has had a module inserted into it.
cardRemove-dOrFailedNotify	Module	Major	cardSlot	The indicated slot has changed state.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
ceServiceType-ModifyFailNotify	Interface	Info	portId interfaceFailureReasonCode	Indicates that configuring unstructured CE failed. Possible reasons: (1) The port has been channelized (2) The port has CAS turned on.
cellTestReqFail-Notify	Connection	Response	cellTestIfB cellTestVpiB cellTestVcidB pvcFailureReasonCode	The PVC connection request has failed.
channelization-ModifyFailNotify	Interface	Info	portId interfaceFailureReasonCode	Indicates that channelizing/unchannelizing failed. Possible reasons: (1) The port has been configured for unstructured CE (2) The port has CAS turned on.
cirAtmSpvcConfigFailNotify	Interface	Info	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr spvcConfigFailureCode	Notification that an attempt to configure an endpoint as CE SPVC endpoint has failed.
cirAtmSpvcConfiguredNotify	Interface	Info	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr	Notification that an endpoint has been configured as CES SPVC endpoint.
cirAtmSpvcDeletedNotify	Interface	Info	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr spvcConfigFailureCode	Notification that an attempt to configure an endpoint as CE SPVC endpoint has failed.
cirAtmSpvc-ModifiedNotify	Interface	Info	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr	Notification that a SPVC endpoint has been modified.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
cirAtmSpvc-ModifyFailNo-tify	Interface	Info	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr spvcConfigFailureCode	Notification that an attempt to modify a CE SPVC endpoint has failed.
cirAtm-SpvcVccSetUp-Notify	Connec-tion	Response	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr cirAtmSpvcVccIfB cirAtmSpvcVccVpiB cirAtmSpvcVccVciB	Notification that a SPVC connection between CE and ATM endpoints has been made success-fully.
cirAtmSpvcVcc-TearDownNotify	Connec-tion	Response	spvcAddrIfA cirAtmSpvcVccRemote-CePortAddr cirAtmSpvcVccIfB cirAtmSpvcVccVpiB cirAtmSpvcVccVciB	Notification that a SPVC connection between CE and ATM endpoints has been deleted.
cirEmAtmBk-PvcVccReqFail-Notify	Connec-tion	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB pvcFailureReasonCode	The DHPVC VCC backup connection request between a circuit emulation interface and an ATM interface has failed.
cirEmAtmBk-PvcVccSetupNo-tify	Connec-tion	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB	The DHPVC VCC backup connection between a circuit emulation interface and an ATM inter-face has been cre-ated.
cirEmAtmBk-PvcVccTear-DownNotify	Connec-tion	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB	The DHPVC VCC backup connection between a circuit-emulation interface and an ATM inter-face has been deleted.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
cirEmAtmPvcVccReqFailNotify	Connection	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB pvcFailureReasonCode	The PVC VCC connection request between a circuit emulation interface and an ATM interface has failed.
cirEmAtmPvcVccSetupNotify	Connection	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB	The PVC VCC connection between a circuit emulation interface and an ATM interface has been created.
cirEmAtmPvcVccTearDownNotify	Connection	Response	cirEmAtmPvcVccIfA cirEmAtmPvcVccIfB cirEmAtmPvcVccVpiB cirEmAtmPvcVccVciB	The PVC VCC connection between a circuit-emulation interface and an atm interface has been deleted.
cirEmAtmSpvcVccSetUpNotify	Connection	Response	cirEmAtmSpvcVccIfA cirEmAtmSpvcVccIfB cirEmAtmSpvcVccVpiB cirEmAtmSpvcVccVciB	Notification that a SPVC connection between CE and ATM endpoints has been made successfully.
cirEmAtmSpvcVccTearDownNotify	Connection	Response	cirEmAtmSpvcVccIfA cirEmAtmSpvcVccIfB cirEmAtmSpvcVccVpiB cirEmAtmSpvcVccVciB	Notification that a SPVC connection between CE and ATM endpoints has been deleted.
cirEmCirEmPvcReqFailNotify	Connection	Response	cirEmCirEmPvcIfA cirEmCirEmPvcIfB pvcFailureReasonCode	The PVC connection request between two circuit emulation interfaces has failed.
cirEmCirEmPvcSetupNotify	Connection	Response	cirEmCirEmPvcIfA cirEmCirEmPvcIfB	The PVC connection between two circuit-emulation interfaces has been created.
cirEmCirEmPvcTearDownNotify	Connection	Response	cirEmCirEmPvcIfA cirEmCirEmPvcIfB	The PVC connection between two circuit emulation interfaces has been deleted.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
cirEmSpvcConfigFailNotify	Interface	Info	interfaceIndex spvcConfigFailureCode	Notification that an attempt to configure an endpoint as CE SPVC endpoint has failed.
cirEmSpvcConfiguredNotify	Interface	Info	interfaceIndex	Notification that an endpoint has been configured as CES SPVC endpoint.
cirEmSpvcDeletedNotify	Interface	Info	interfaceIndex	Notification that CE SPVC configuration has been deleted.
cirEmSpvcModifiedNotify	Interface	Info	interfaceIndex	Notification that a SPVC endpoint has been modified.
cirEmSpvcModifyFailNotify	Interface	Info	interfaceIndex spvcConfigFailureCode	Notification that an attempt to modify a CE SPVC endpoint has failed.
completeClockFailedNotify	System	Critical	< NO OBJECTS >	The Stratum 3–4 modules have either been removed or have failed,resulting in no clock being provided.
completeClockRecoveredNotify	System	Info	< NO OBJECTS >	A Stratum 3–4 module is now available to provide a clock source.
compositeClockClearedNotify	System	Info	< NO OBJECTS >	The error in the composite clock has been corrected.
compositeClockFailNotify	System	Critical	< NO OBJECTS >	The composite clock has failed. Please call Technical Support immediately to resolve the problem.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
differentSystem-SoftwareNotify	System	Critical	primarySoftwareVersion backupSoftwareVersion	Indicates that the primary and backup CPU modules are running different versions of software. This could cause system problems since the database files will not be transferred between CPU modules so a change of CPU will result.
ecdBootFail-ureNotify	System	Critical	< NO OBJECTS >	System failed in the Boot (startup) procedures. Please call Technical Support immediately to resolve the problem.
fileTransferSta-tusNotify	System	Info	percentComplete	Indicates the percent complete of the current upgrade, downgrade, or ftp download in progress.
firmwareDown-loadFailedNotify	Module	Minor	fwReleaseSlot firmwareDownloadReason-Code	The indicated slot had the indicated failure during a firmware download.
firmwareDown-loadSucceeded-Notify	Module	Info	fwReleaseSlot	The indicated slot has successfully completed a firmware download.
frAtmBkPvcVc-cReqFailNotify	Connec-tion	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB pvcFailureReasonCode	The DHPVC VCC backup connection request between a frame relay interface and an ATM interface has failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
frAtmBk-PvcVccSetupNotify	Connection	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB	The DHPVC VCC backup connection between a frame relay interface and an ATM interface has been created.
frAtmBkPvcVcc-TearDownNotify	Connection	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB	The DHPVC VCC backup connection between a frame relay interface and an ATM interface has been deleted.
frAtmPvcVc-cReqFailNotify	Connection	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB pvcFailureReasonCode	The PVC VCC connection request between a frame-relay interface and an ATM interface has failed.
frAt-mPvcVccSetup-Notify	Connection	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB	The PVC VCC connection between a frame-relay interface and an ATM interface has been created.
frAtmPvcVccTe-arDownNotify	Connection	Response	frAtmPvcVccIfA frAtmPvcVccDlciA frAtmPvcVccIfB frAtmPvcVccVpiB frAtmPvcVccVciB	The PVC VCC connection between a frame-relay interface and an ATM interface has been deleted.
frFrPvcReqFail-Notify	Connection	Response	frFrPvcIfA frFrPvcDlciA frFrPvcIfB frFrPvcDlciB pvcFailureReasonCode	The PVC connection request between two frame-relay interfaces has failed.
frFrPvcSetupNotify	Connection	Response	frFrPvcIfA frFrPvcDlciA frFrPvcIfB frFrPvcDlciB	The PVC connection between two frame-relay interfaces has been created.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
frFrPvcTear-DownNotify	Connection	Response	frFrPvcIfA frFrPvcDlciA frFrPvcIfB frFrPvcDlciB	The PVC connection between two frame-relay interfaces has been deleted.
frAtmSpvcConfigFailNotify	Interface	Info	spvcAddrIfA frAtmSpvcVccDlciA spvcConfigFailureCode	Notification that an attempt to configure an endpoint as FR SPVC endpoint has failed.
frAtmSpvcConfiguredNotify	Interface	Info	spvcAddrIfA frAtmSpvcVccDlciA	Notification that an endpoint has been configure as FR SPVC endpoint.
frAtmSpvcDeletedNotify	Interface	Info	spvcAddrIfA frAtmSpvcVccDlciA	Notification that FR SPVC configuration has been deleted.
frAtmSpvcModifiedNotify	Interface	Info	spvcAddrIfA frAtmSpvcVccDlciA	Notification that a SPVC endpoint has been modified.
frAtmSpvcModifyFailNotify	Interface	Info	spvcAddrIfA frAtmSpvcVccDlciA spvcConfigFailureCode	Notification that an attempt to modify a FR SPVC endpoint has failed.
frAtm-SpvcVccSetUp-Notify	Connection	Response	spvcAddrIfA frAtmSpvcVccDlciA frAtmSpvcVccIfB frAtmSpvcVccVpiB frAtmSpvcVccVciB	Notification that a SPVC connection between FR and ATM endpoints has been made successfully.
frAtmSpvcVcc-TearDownNotify	Connection	Response	spvcAddrIfA frAtmSpvcVccDlciA frAtmSpvcVccIfB frAtmSpvcVccVpiB frAtmSpvcVccVciB	Notification that a SPVC connection between FR and ATM endpoints has been deleted.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
imaGrpChannelClearedNotify	Interface	Info	imaGrpChannelId imaGrpChannelStatus	The **imaGrpChannelClearedNotify** trap indicates a failure has been cleared in an IMA group. The **imaGrpChannelStatus** field indicates the failure that has been cleared.
imaGrpChannelFailNotify	Interface	Info	imaGrpChannelId imaGrpChannelStatus	The **imaGrpChannelFailNotify** trap indicates a failure in the IMA group. The **imaGrpChannelStatus** field indicates the reason for the failure.
inactivityTimerExpiredNotify	System	Major	< NO OBJECTS >	Sent by the Access Concentrator system when the inactivity timer of the keep-alive protocol expires; that is, when the Access Concentrator system does not see a message from the Signalling Gateway on the TCP link during the time period specified by the inactivity timer value setting
inputPortClockClearedNotify	System	Info	< NO OBJECTS >	The error in the input port clock has been corrected.
inputPortClockFailNotify	System	Critical	< NO OBJECTS >	The input port clock has failed. Please call Support immediately to resolve the problem.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
interfaceCreatedNotify	Interface	Info	interfaceIndex interfaceType	Notification that an interface has been created.
interfaceCreateFailNotify	Interface	Info	interfaceIndex interfaceType interfaceFailureReasonCode	Notification that an attempt to create an interface has failed. interfaceFailureReasonCode gives details.
interfaceDeletedNotify	Interface	Info	interfaceIndex	Notification that an interface has been deleted.
interfaceInServiceNotify	Interface	Info	interfaceIndex interfaceType	Notification that an interface is now in service.
interfaceModifiedNotify	Interface	Info	interfaceIndex interfaceType	Notification that an interface has been modified.
interfaceModifyFailNotify	Interface	Info	interfaceIndex interfaceType interfaceFailureReasonCode	Notification that an attempt to modify an interface has failed.
interfaceOutOfServiceNotify	Interface	Major	interfaceIndex interfaceType	Notification that an interface is now out of service.
intf-CBR-Cell-Rate-Exceeded	Interface			Indicated that the available CBR cell rate has been exceeded.
intf-VBR-Cell-Rate-Exceeded	Interface			Indicates that the available VBR cell rate has been exceeded.
ipAtmApp-PvcVccReqFail-Notify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnet-MaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVciB pvcFailureReasonCode	The PVC VCC connection request between in-band management and an ATM interface has failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
ipAtmApp-PvcVccSetupNotify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnetMaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVccVciB	The PVC VCC connection between in-band management and an ATM interface has been created.
ipAtmApp-PvcVccTear-DownNotify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnetMaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVccVciB	The PVC VCC connection between in-band management and an ATM interface has been deleted.
ipAtmBkApp-PvcVccReqFail-Notify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnetMaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVccVciB pvcFailureReasonCode	The DHPVC VCC backup connection request between an in-band management interface and an ATM interface has failed.
ipAtmBkApp-PvcVccSetupNotify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnetMaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVccVciB	The DHPVC VCC backup connection between an in-band management interface and an ATM interface has been created.
ipAtmBkApp-PvcVccTear-DownNotify	Connection	Response	ipAtmAppPvcVccDestAddrA ipAtmAppPvcVccSubnetMaskA ipAtmAppPvcVccIfB ipAtmAppPvcVccVpiB ipAtmAppPvcVccVciB	The DHPVC VCC backup connection between an in-band management interface and an ATM interface has been deleted.
ipOrMaskInvalidNotify	System	Response	ipTypeReasonCode	The indicated ip address is invalid.
isdnLapdDown-Notify	Interface	Info	interfaceIndex isdnIntfDChanId	This trap indicates that LAPD on the ISDN interface has gone down.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
isdnLapdUpNotify	Interface	Info	interfaceIndex isdnIntfDChanId	This trap indicates that LAPD is functional on the specified ISDN interface.
keepAliveTimerExpiredInLlDownStateNotify	System	Major	< NO OBJECTS >	Sent by the Access Concentrator system when the keep-alive timer expires in the LLDOWN state of the keep-alive protocol; that is, when the Access Concentrator system does not see a keep-alive message from the Connection Gateway on the TCP link during the time period specified by the keep-alive timer setting.
keepAliveTimerExpiredInOneWayStateNotify	System	Major	< NO OBJECTS >	Sent by the Access Concentrator system when the keep-alive timer expires in the ONE-Way state of the keep-alive protocol; that is, when the Access Concentrator system does not see a keep-alive message from the Signalling Gateway on the TCP link during the time period specified by the keep-alive timer setting.
lineStatusChangedNotify	Module	Major	portId lineStatus	The indicated port has had a change in the line status.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
lmiDlciStatus-Notify	Connection	Response	interfaceIndex d1ciNumber lmiDlciOperStatus	Indicates the end-to-end status of the PVC of which this DLCI is a segment .
lmiIntfStatusNotify	Interface	Info	interfaceIndex frLmiOperStatus	This trap indicates the status of an interface from the LMI perspective.
moduleReboot-Notify	Module	Major	cardSlot cardType	This trap indicates that a **cardType** in **cardSlot** becomes busy and the CPU module reboots it. This is different from when an I/O module is actually removed.
muxReadyConfirmNotReceivedNotify	System	Major	< NO OBJECTS >	If Access Concentrator system is configured as TCP client, this trap is sent if the MUX_READY_CONF message is not received after sending the MUX_READY_IND message three times. This trap indicates unexpected behavior on the Access Concentrator system to Connection Gateway link.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
muxReadyConfirmReceivedNotify	System	Info	< NO OBJECTS >	Indicates that the MUX (the Access Concentrator system) has received a MUX_READY_CONF message in response to the MUX_READY_IND message when the Access Concentrator system is configured as the TCP client for the Access Concentrator system to Connection Gateway connection.
oamActDeactResultNotify	Connection	Response	oamActDeactIfB oamActDeactVpiB oamActDeactVciB oamActDeactResultCode	the final status of oam Activation-Deactivation request.
oamTestReqFailNotify	Connection	Response	oamTestIfB oamTestVpiB oamTestVciB oamTestFailureReasonCode	OAM loopback test request has failed.
oc3APSStateChangeNotify	Module	response	oc3APSPairPortIndex$oc3APSReasonCode$oc3APSK1K2Rx$oc3APSK1K2Tx$oc3APSSelectorState$oc3APSWorkingLineSignalStatus$oc3APSProtectionLineSignalStatus	Notification
oc3APSSwitchoverNotify	Module	response	oc3APSPairPortIndex$oc3APSReasonCode$oc3APSK1K2Rx$oc3APSK1K2Tx$oc3APSSelectorState$oc3APSWorkingLineSignalStatus$oc3APSProtectionLineSignalStatus	Notification

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
oldStratum-CardNotify	System	Critical	< NO OBJECTS >	This trap indicates that the primary stratum card does not support this mode of operation being applied in the stratum configuration. Card must be upgraded. A default configuration is being applied to stratum.
oneWayMessageWhileInTwoWayStateNotify	System	Major	< NO OBJECTS >	This trap indicates that a one way message is received from the Connection Gateway (CG) when the Access Concentrator system is in the two way state of the keep-alive protocol on the TCP link between the Access Concentrator system and the CG.
pnniIntfCfgFail-Notify	Interface	Info	interfaceIndex pnniCode	Indicates that a PNNI Interface has failed to be created.
pnniNodeCfg-FailNotify	System	Info	swtchNodeIndx pnniCode	Indicates that a PNNI Node Creation has failed.
pnniNodeCf-gNotify	System	Info	swtchNodeIndx pnniCode	Indicates that a PNNI Node has been created.
pnniNodeDel-FailNotify	System	Info	swtchNodeIndx pnniCode	Indicates that a PNNI Node Deletion has failed.
pnniNodeISFail-Notify	System	Info	swtchNodeIndx pnniCode	Indicates that the action of bringing a PNNI Node into service has failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
pnniNodeMod-FailNotify	System	Info	swtchNodeIndx pnniCode	Indicates that a PNNI Node Modification has failed.
pnniNodeOOS-FailNotify	System	Info	swtchNodeIndx pnniCode	Indicates that the action of taking a PNNI Node Out of Service has failed.
pnniProtLinkU-pAndNotAdv	Interface	Info	interfaceIndex pnniCode	Indicates that the Protocol Status of the PNNI Link is Up but not Advertising.
pnniProtLnk-StatDown	Interface	Info	interfaceIndex pnniCode	Indicates that the Protocol Status of the PNNI Link is Down.
pnniProtLnkU-pAndAdv	Interface	Info	interfaceIndex pnniCode	Indicates that the Protocol Status of the PNNI Link is Up and Advertising.
pnniRtAddrAd-dByIlmiNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that an end system Address has been dynamically added to PNNI by ILMI.
pnniRtAddrCfg-FailNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that a PNNI Route Address Configuration has failed.
pnniRtAddrCf-gNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that a new PNNI Route Address has been created.
pnniRtAddrDel-ByIlmiNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that an end system Address has been dynamically deleted from PNNI by ILMI.
pnniRtAddrDel-FailNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that a PNNI Route Address Deletion has failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
pnniRtAddrModFailNotify	System	Info	swtchNodeIndx interfaceIndex pnniCode	Indicates that a PNNI Route Address Modification has failed.
portModifyFailNotify	Module	Info	portId portFailureReasonCode	Notification that an attempt to modify a port parameter has failed.
powerSupplyStatusNotify	System	Minor	powerSupplyReasonCode	Indicates the status of the power supply.
referenceClockClearedNotify	System	Info	< NO OBJECTS >	The error in the backplane reference clock has been corrected.
referenceClockFailNotify	System	Critical	< NO OBJECTS >	The reference clock used for the operation of the bus-based backplane has failed. Please call Technical Support immediately to resolve the problem.
remoteRebootNotify	System	Info	remoteRebootReasonCode	Indicates the result of the requested reboot action.
removeConfigFilesNotify	System	Info	removeConfigFiles	Indicates the status of the removal of the configuration files.
saveConfigurationNotify	System	Info	saveConfigurationReasonCode	Indicates the result of the requested save configuration.
signalingModifyFailNotify	Interface	Info	interfaceIndex interfaceType interfaceFailureReasonCode	This trap indicates that signaling has already been configured for this port and to change, you must bring all interfaces out of service, including the channel specified in **interfaceIndex**.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
snmpCommunityString-sChangedToPublicNotify	System	Critical	< NO OBJECTS >	An error has been detected in the **agt.pty** file and the community strings have been changed to be public.
softwareDownloadStatusNotify	System	Info	upgradeSwCopyStatus upgradeSwErrorStatus	Indicates the completion status of the ftp download of a software upgrade.
stratumActivitySwitchOverNotify	Module	Info	activeStratum	The secondary stratum card has become the primary primary card.
stratumCardMismatchNotify	System	Critical	< NO OBJECTS >	Indicates that the secondary stratum card does not support this mode of operation being applied to the primary stratum. Card must be upgraded.
stratumModeChangeNotify	System	Info	stratumMode	The current operational status of the Stratum 3–4 module has changed.
systemColdStartNotify	System	Info	< NO OBJECTS >	System has successfully completed initialization from a complete power down stage and is ready for operation.
systemWarmStartNotify	System	Info	< NO OBJECTS >	System has successfully completed initialization from a user or other system level interrupt or restart and is ready for operation.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
tasCmprsAnnceNotify	System	Info	tasCmprsAnnceReasonCode	Indicates the result of the requested compress announcement operation.
tasTstLineNotify	System	Info	tasTstLineReasonCode	Indicates the result of the requested line test initiation operation.
ts16UsageModifyFailNotify	Interface	Info	interfaceIndex interfaceFailureReasonCode	Indicates that either TS16 has been in use for data while trying to change e1 TS16 from CCS to CAS, or signalling is on for at least one of the channels while trying to change e1 TS16 from CAS to CCS.
vbrAtmBkPvcVccReqFailNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB pvcFailureReasonCode	The DHPVC VCC backup connection request between a variable-bit rate interface and an ATM interface has failed.
vbrAtmBkPvcVccSetupNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB	The DHPVC VCC backup connection between a variable-bit rate interface and an ATM interface has been created.
vbrAtmBkPvcVccTearDownNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB	The DHPVC VCC backup connection between a variable-bit rate interface and an ATM interface has been deleted.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vbrAtmPvcVccReqFailNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB pvcFailureReasonCode	The PVC VCC connection request between a variable-bit rate interface and an ATM interface has failed.
vbrAtmPvcVccSetupNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB	The PVC VCC connection between a variable-bit rate interface and an ATM interface has been created.
vbrAtmPvcVccTearDownNotify	Connection	Response	vbrAtmPvcVccIfA vbrAtmPvcVccIfB vbrAtmPvcVccVpiB vbrAtmPvcVccVciB	The PVC VCC connection between a variable-bit rate interface and an ATM interface has been deleted.
vbrAtmSpvcConfigFailNotify	Interface	Info	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr spvcConfigFailureCode	Notification that an attempt to configure an endpoint as TE SPVC endpoint has failed.
vbrAtmSpvcConfiguredNotify	Interface	Info	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr	Notification that an endpoint has been configured as TE SPVC endpoint.
vbrAtmSpvcDeletedNotify	Interface	Info	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr	Notification that TE SPVC configuration has been deleted.
vbrAtmSpvcModifiedNotify	Interface	Info	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr	Notification that a SPVC endpoint has been modified.
vbrAtmSpvcModifyFailNotify	Interface	Info	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr spvcConfigFailureCode	Notification that an attempt to modify a TE SPVC endpoint has failed.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vbrAtmSpvcSetUpNotify	Connection	Response	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr vbrAtmSpvcIfB vbrAtmSpvcVpiB vbrAtmSpvcVciB	Notification that a SPVC connection between TE and ATM endpoints has been made successfully.
vbrAtmSpvcTearDownNotify	Connection	Response	spvcAddrIfA vbrAtmSpvcRemoteVbrPortAddr vbrAtmSpvcIfB vbrAtmSpvcVpiB vbrAtmSpvcVciB	Notification that a SPVC connection between TE and ATM endpoints has been deleted.
vbrAtmSpvcVccSetUpNotify	Connection	Response	vbrAtmSpvcVccIfA vbrAtmSpvcVccIfB vbrAtmSpvcVccVpiB vbrAtmSpvcVccVciB	Notification that a SPVC connection between TE and ATM endpoints has been made successfully.
vbrAtmSpvcVccTearDownNotify	Connection	Response	vbrAtmSpvcVccIfA vbrAtmSpvcVccIfB vbrAtmSpvcVccVpiB vbrAtmSpvcVccVciB	Notification that a SPVC connection between TE and ATM endpoints has been deleted.
vbrSpvcConfigFailNotify	Interface	Info	interfaceIndex spvcConfigFailureCode	Notification that an attempt to configure an endpoint as TE SPVC endpoint has failed.
vbrSpvcConfiguredNotify	Interface	Info	interfaceIndex	Notification that an endpoint has been configured as TE SPVC endpoint.
vbrSpvcDeletedNotify	Interface	Info	interfaceIndex	Notification that TE SPVC configuration has been deleted.
vbrSpvcModifiedNotify	Interface	Info	interfaceIndex	Notification that a SPVC endpoint has been modified.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vbrSpvcModify-FailNotify	Interface	Info	interfaceIndex spvcConfigFailureCode	Notification that an attempt to modify a TE SPVC endpoint has failed.
vbrVbrPvcReq-FailNotify	Connection	Response	vbrVbrPvcIfA vbrVbrPvcIfB pvcFailureReasonCode	The PVC connection request between two variable-bit rate interfaces has failed.
vbrVbrPvc-SetupNotify	Connection	Response	vbrVbrPvcIfA vbrVbrPvcIfB	The PVC connection between two variable-bit rate interfaces has been created.
vbrVbrPvcTear-DownNotify	Connection	Response	vbrVbrPvcIfA vbrVbrPvcIfB	The PVC connection between two variable-bit rate interfaces has been deleted.
versionConfiguRationNotify	System	Info	versionConfigurationReasonCode	Indicates the completion status of the upgrade or downgrade.
vi-0-Non-Ubr-Conn-Not-Supp	Connection	Response		Notification that a non-UBR connection on virtual interfaces is not supported for duplex connections.
vi-0-Non-Ubr-Conn-Not-SuppA2B	Connection	Response		Notification that a non-UBR connection on virtual interfaces is not supported for simplex connections.
vi-0-Non-Ubr-Conn-Not-SuppB2a	Connection	Response		Notification that a non-UBR connection on virtual interfaces is not supported for duplex connections.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vi-Already-Exists	Connection	Info		Notification that a virtual interface associated with that number has already been created.
vi-Cannot-Be-0	Connection	Response		Notification that VI=0 already exists
vi-Cbr-Bw-Unavailable-Ergs	Connection	Response		Notification that the requested amount of egress CBR bandwidth is unavailable for duplex connections.
vi-Cbr-Bw-Unavailable-Ergs-A	Connection	Response		Notification that the requested amount of egress CBR bandwidth is unavailable for simplex connections (Side A.)
vi-Cbr-Bw-Unavailable-Ergs-B	Connection	Response		Notification that the requested amount of egress CBR bandwidth is unavailable for simplex connections (Side B.)
vi-CellRate-Too-Hi	Connection	Response		Notification that the requested virtual interface cell rate connection exceeds the available range.
vi-CellRate-Too-Lo	Connection	Response		Notification that the requested cell rate connection is below the available range.
vi-Conn-Cell-Rate-Exceeded	Connection	Response		Notification that the requested cell rate exceeds available bandwidth.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vi-Does-Not_Exist	Connection	Response		Notification that a virtual interface connection no longer exists.
vi-Mod-Limit-Exceeded				Indicates that the number of virtual interfaces per card has been exceeded.
vi-Not-Enabled	Interface	Info		Notification that the virtual interface feature is not enables for duplex connection.
vi-Not-Enabled-A				Notification that the virtual interface feature is not enables for duplex connection (Side A).
vi-Not-Enabled-B				Notification that the virtual interface feature is not enables for duplex connection (Side B).
vi-OOR				Notification that the requested VI number is out of range for duplex connections.
vi-OOR-A				Notification that the requested VI number is out of range for simplex connections (Side A).
vi-OOR-B				Notification that the requested VI number is out of range for simplex connections (Side B).

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vi-OS-Cannot-Be-0				Indicates that the virtual interface oversubscription cannot be 0. Must be at least 1.
vi-OS-OOR				Indicates that the virtual interface oversubscription is not in the range 1-10.
vi-Resource-Unavail				Notification that the requested bandwidth for a virtual interface is not available.
vi-Should-Be-0				Notification that a UBR connection has been attempted on a virtual interface with a designation other than VI=0 for a duplex connection.
vi-Should-Be-0-A				Notification that a UBR connection has been attempted on a virtual interface with a designation other than VI=0 for a simplex connection (Side A).
vi-Should-Be-0-B				Notification that a UBR connection has been attempted on a virtual interface with a designation other than VI=0 for a simplex connection (Side B).

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
vi-Vbr-Bw-Unavailable-Egrs				Notification that the requested amount of egress VBR bandwidth is unavailable for a duplex connection.
vi-Vbr-Bw-Unavailable-Egrs-A				Notification that the requested amount of egress VBR bandwidth is unavailable for a simplex connection (Side A).
vi-Vbr-Bw-Unavailable-Egrs-B				Notification that the requested amount of egress VBR bandwidth is unavailable for a simplex connection (Side B).
viprArpTrap	Interface	Info	viprSlot$viprRouterId$arpStatus	The Vipr Task is notifying Network Management of the disposition of a previous ARP Table Request.
viprIpIntfTrap	Interface	Info	viprSlot viprRouterId viprIntfId ipIntfStatus	Indicates success/fail of IP Network Interface level operations.
viprPingTrap	Interface	Info	viprSlot$viprRouterId$ipAddrNumber$pingStatusReasonCode	The Vipr Task is notifying Network Management of the disposition of a previous Ping Request.
viprRoutingTrap	Interface	Info	viprSlot$viprRouterId$routingStatus	The Vipr Task is notifying Network Management of the disposition of a previous Routing Table Request.
viprRtSrvTrap	Interface	Info	cardSlot routeSrvStatus	Indicates success/fail of Vipr (Route Server) operations.

Table A-2. SNMP Trap Names and Descriptions with Associated MIB Object Names

Enterprise-Specific Trap Name	Event Type for the Trap	System Indicator for the Trap	MIB Object Name	Trap Description
viprStatRtTrap	Interface	Info	viprSlot$viprRouterId$viprRouteId$statRtStatus	Indicates success/fail of Static Route operations.
viprSubChanTrap	Interface	Info	viprSlot$viprRouterId$viprIntfId$viprSubChnlId$subChanStatus	Indicates success/fail of Sub Channel level operations.
viprVpnTrap	Interface	Info	viprSlot$viprRouterId$vpnTrapStatus	Indicates success/fail of VPN level operations.
virtualIntfCreatedNotify	Interface	Response	virtualIntfConfigIf virtualIntfConfigVi	Response to creation of VI.
virtualIntfDeleteNotify	Interface	Response	virtualIntfConfigIf virtualIntfConfigVi	Response to modification of VI.
virtualIntfModifiedNotify	Interface	Response	virtualIntfConfigIf virtualIntfConfigVi	Response to deletion of VI.
virtualIntfModifyFailNotify	Interface	Response	virtualIntfConfigIf virtualIntfConfigVi pvcFailureReasonCode	Response to Modify Fail of VI, Overload pvcFailureReasonCode
virtualUNIIntfCreateFailNotify	Interface	Info	virtualUNIIfIndex virtualUNIVUNIId interfaceFailureReasonCode	Notification that an attempt to create an interface has fail.
virtualUNIIntfCreatedNotify	Interface	Response	virtualUNIIfIndex virtualUNIVUNIId	Response to creation of Virtual UNI.
virtualUNIIntfDeleteNotify	Interface	Response	virtualUNIIfIndex virtualUNIVUNIId	Response to deletion of Virtual UNI.
virtualUNIIntfInServiceNotify	Interface	Info	virtualUNIIfIndex virtualUNIVUNIId	Notification of virtualUNI in Service.
virtualUNIIntfModifiedNotify	Interface	Response	virtualUNIIfIndex virtualUNIVUNIId	Response to modification of Virtual UNII.
virtualUNIIntfModifyFailNotify	Interface	Response	virtualUNIIfIndex virtualUNIVUNIId interfaceFailureReasonCode	Response to Modify Fail of Virtual UNI, Overload interfaceFailureReasonCode.
virtualUNIIntfOutOfServiceNotify	Interface	Info	virtualUNIIfIndex virtualUNIVUNIId	Notification of virtualUNI Out Of Service.

Definitions of MIB Objects Used for Traps

The following list contains the definitions of the MIB objects that are associated with the SNMP enterprise-specific trap names. This list is provided in alphabetical order.

alarmCardReasonCode Valid range is a number between 1 and 8. See table below for a mapping between numbers and their enumerated type.

Table A-3. Alarm Reason Codes

Number Value	Enumerated Type
1	inputContactClosed
2	inputContactOpen
3	outputActivated
4	outputDactivated
5	audibleLocalAlarmEnable
6	audibleLocalAlarmCutoff
7	audibleRemoteAlarmEnable
8	audibleRemoteAlarmCutoff

apsFailureReasonCode APS failure reason. Valid range is a number between 1 and 10. See table below for a mapping between numbers and their enumerated type.

Table A-4. APS Failure Reason Codes

Number Value	Enumerated Type
1	protectionCard-notPresent
2	protectionCardType-notAPS3#
3	protectionCardType-incompatible
4	protectionCard-notInUnconfiguredState
5	protectionCard-notUnprotected
6	resource-access-failure
7	incorrect-APSconfiguration
8	protectionPort-Active
9	workingPort-localLoop-notAllowed
10	protectionPort-localLoop-notAllowed

arpStatus Success: Arp Data is Available. Failure: Reply from RS Card timed-out. Valid range is a number between 1 and 2. See table below for a mapping between numbers and their enumerated type.

Table A-5. ARP Status Codes

Number Value	Enumerated Type
1	success
2	failure

atmImaIntfIndex Interface index for the atm Ima interface. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

atmImaIntfStatus The return value for the atmImaIntfFailNotify trap.

- lif -- Persistence of LIF defect at near-end (Loss of IMA Frame)
- lods -- Persistence of LODS defect at near-end (Link Out of Delay Synchronization)
- txMisConnect -- The link is mis-connected (not connected to the same far-end as the other links in the group.)
- rfi -- Persistence of RDI-IMA defect at near-end (Remote Failure Indicator)
- fault -- Implementation specific fault at near-end
- txUnusableFe -- Tx link forced to unusable due to far-end behavior
- rxUnusableFe -- Rx link forced to unusable due to far-end behavior

Valid range is a number between 1 and 7. See table below for a mapping between numbers and their enumerated type.

Table A-6. ATM IMA Interface Status Codes

Number Value	Enumerated Type
1	lif
2	lods
3	txMisConnect
4	rfi
5	fault
6	txUnusableFe
7	rxUnusableFe

atmPvcVccIfA Interface index for side A of an ATM-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

atmPvcVccIfB Interface index for side B of an ATM-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

atmPvcVccVciA	VCI value for side A of an ATM-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.
atmPvcVccVciB	VCI value for side B of an ATM-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.
atmPvcVccVpiA	VPI value for side A of an ATM-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.
atmPvcVccVpiB	VPI value for side B of an ATM-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.
atmPvcVpcIfA	Interface index for side A of an ATM-to-ATM PVC VPC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.
atmPvcVpcIfB	Interface index for side B of an ATM-to-ATM PVC VPC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.
atmPvcVpcVpiA	VPI value for side A of an ATM-to-ATM PVC VPC connection. Valid range is a number between 0 and 4095.
atmPvcVpcVpiB	VPI value for side B of an ATM-to-ATM PVC VPC connection. Valid range is a number between 0 and 4095.
atmSpvcVccIfA	Interface index for side A of an ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.
atmSpvcVccIfB	Interface index for side B of an ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.
atmSpvcVccVciA	VCI value for side A of an ATM SPVC VCC connection. Valid range is a number between 0 and 65535.
atmSpvcVccVciB	VCI value for side B of an ATM SPVC VCC connection. Valid range is a number between 0 and 65535.
atmSpvcVccVpiA	VPI value for side A of an ATM SPVC VCC connection. Valid range is a number between 0 and 4095.
atmSpvcVccVpiB	VPI value for side B of an ATM SPVC VCC connection. Valid range is a number between 0 and 4095.
backupSoftwareVersion	Software version running on the backup CPU module.

bridgeAtmPvcVccIfA Interface index for side A, the bridge side, of a Bridge-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

bridgeAtmPvcVccIfB Interface index for side B, the ATM side, of a Bridge-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

bridgeAtmPvcVccVciB VCI value for side B, the ATM side, of a Bridge-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.

bridgeAtmPvcVccVpiB VPI value for side B, the ATM side, of a Bridge-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.

bridgeBridgePvcIfA Interface index for side A of a Bridge-to-Bridge PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

bridgeBridgePvcIfB Interface index for side B of a Bridge-to-Bridge PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

bridgeDomainNumber The bridge number of the bridge that includes this interface. If the interface is currently not associated with any bridge this will be set to none.

cardOperStatus Current operational status of the module. Valid range is a number between 1 and 3. See table below for a mapping between numbers and their enumerated type.

Table A-7. Module Operational Status Codes

Number Value	Enumerated Type
1	primary
2	standby
3	unknown

cardProtectionStatus Current protection status of the module. Valid range is a number between 1 and 3. See table below for a mapping between numbers and their enumerated type.

Table A-8. Module Protection Status Codes

Number Value	Enumerated Type
1	none
2	protected
3	wrongType

cardSlot Physical slot location. Valid range is a number between 1 and 4.

cardType Type of module in a physical slot. A specific type of module is associated with each number. Valid range is a number between 1 and 42. See table below for a mapping between numbers and their enumerated type.

Table A-9. Module Type Codes

Number Value	Enumerated Type
1	none
3	oC-3c
4	dS3-ATM
5	dS1-CircuitEm
6	dS1-ATM
7	e1-CircuitEm
8	e3-ATM
9	highSpeed
10	multiSerial
11	dSPI
12	twoWireStation
13	twoWireOffice
14	cPU
15	stratum
16	powerSupply
17	protectionCard
18	e1-ATM
19	ethernet
20	enhancedDS1
21	enhancedE1
22	oC-3cMMAQ
23	oC-3cMMTS
24	oC-3cSMAQ
25	oC-3cSMTS
26	sTM-1MMAQ
27	sTM-1SMTS
28	sTM-1MMAQ
29	sTM-1MMTS
30	dS3-FR
31	dSP2A
32	ds1Ima

Table A-9. Module Type Codes

Number Value	Enumerated Type
33	e1Ima
34	alarm
35	dSP2B
36	aps-OC-3cSM
37	aps-OC-3cMM
38	aps-STM-1SM
39	aps-STM-1MM
40	cH-DS3
41	cH-STS1
42	rT-S

cellTestIfB Interface index used for testing cell transfer. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cellTestVcidB Virtual Check Id for testing cell transfer to an I/O module. Valid range is a number between 0 and 65535. If the I/O module interface is frame relay, this field acts as DLCI and the valid range is a number between 0 and 1023. If the I/O module interface is circuit emulation, then this will always be 0.

cellTestVpiB VPI value for testing cell transfer to an I/O module. Valid range is a number between 0 and 4095. If the I/O module interface is not ATM, then this will always be zero.

cirEmAtmPvcVccIfA Interface index for side A, the circuit emulation side, of a circuit emulation-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cirEmAtmPvcVccIfB Interface index for side B, the ATM side, of a circuit emulation-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cirEmAtmPvcVccVciB VCI value for side B, the ATM side, of a circuit emulation-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.

cirEmAtmPvcVccVpiB VPI value for side B, the ATM side, of a circuit emulation-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.

cirEmAtmSpvcVccIfA Interface index for side A, the circuit emulation side, of a circuit emulation-to-ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cirEmAtmSpvcVccIfB Interface index for side B, the ATM side, of a circuit emulation-to-ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cirEmAtmSpvcVccVciB VCI value for side B, the ATM side, of a circuit emulation-to-ATM SPVC VCC connection. Valid range is a number between 0 and 65535.

cirEmAtmSpvcVccVpiB VPI value for side B, the ATM side, of a circuit emulation-to-ATM SPVC VCC connection. Valid range is a number between 0 and 4095.

cirEmCirEmPvcIfA Interface index for side A of a circuit emulation-to-circuit emulation PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

cirEmCirEmPvcIfB Interface index for side B of a circuit emulation-circuit emulation PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

d1ciNumber The number of the d1ci being used.

deviceId The device ID is used as the number of external devices. Each device can be an external input device or control output device.

firmwareDownload ReasonCode The suspected reasons why a firmware download would fail. Valid range is a number between 1 and 17. See table below for a mapping between numbers and their enumerated type.

Table A-10. Firmware Download Reason Codes

Number Value	Enumerated Type
1	cardInService
2	errorInFile
3	wrongCardType
4	wrongCardSubType
5	driverUnavailable
6	driverInvalidHeaderChecksum
7	driverInvalidrecordChecksum
8	requestReplyTimeout
9	completeReplyTimeout
10	mapFileCorrupted
11	mapFileUnavailable
12	mapFileInvalidChecksum
13	mapFileNameImproper
14	cfgFileCorrupted

Table A-10. Firmware Download Reason Codes

Number Value	Enumerated Type
15	cfgFileUnavailable
16	cfgFileInvalidChecksum
17	wrongCardType

frAtmPvcVccDlciA DLCI value for side A, the frame relay side, of a frame relay-atm PVC VCC connection. Valid range is a number between 0 and 1023.

frAtmPvcVccIfA Interface index for side A, the frame relay side, of a frame relay-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

frAtmPvcVccIfB Interface index for side B, the ATM side, of a frame relay-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

frAtmPvcVccVciB VCI value for side B, the ATM side, of a frame relay-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.

frAtmPvcVccVpiB VPI value for side B, the ATM side, of a frame relay-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.

frFrPvcDlciA DLCI value for side A of a frame relay-to-frame relay PVC connection. Valid range is a number between 0 and 1023.

frFrPvcDlciB DLCI value for side B of a frame relay-to-frame relay PVC connection. Valid range is a number between 0 and 1023.

frFrPvcIfA Interface index for side A of a frame relay-to-frame relay PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

frFrPvcIfB Interface index for side B of a frame relay-to-frame relay PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

frLmiOperStatus The operational status of the LMI protocol. Valid range is a number between 1 and 2. See the table below for a mapping between numbers and their enumerated type.

Table A-11. LMI Operational Status Codes

Number Value	Enumerated Type
1	outOfService
2	inService

fwReleaseSlot Physical slot location. Valid range is a number between 1 and 16.

imaGrpChannelId Interface index - SSPPCCC

imaGrpChannelStatus The return value for the imaGrpChannelFailNotify trap.

- startupFe -- Far-end started up
- cfgAbort -- Far-end tried to use unacceptable configuration parameters
- cfgAbortFe -- Far-end reported unacceptable configuration parameters
- insuffLinks -- Less than the minimum number of Tx links are active or less than the minimum number of Rx links are active
- insuffLinksFe -- Far-end reported that less than minimum number of Rx links or min number of Tx links are active
- blockedNe -- Near-end is blocked
- blockedFe -- Far-end reported that it is blocked
- timingSynch -- A possible configuration mismatch has occurred (CTC and CTC modes are not the same at both ends of the IMA virtual links).

Valid range is a number between 1 and 8. See table below for a mapping between numbers and their enumerated type.

Table A-12. IMA Group Channel Status Codes

Number Value	Enumerated Type
1	startupFe
2	cfgAbort
3	cfgAbortFe
4	insuffLinks
5	insuffLinksFe
6	blockedNe
7	blockedFe
8	timingSynch

interfaceFailureReason Code Identification of cause for failure in changing the status of an interface.

- interfaceInService: Most, if not all, modifications require that the interface be out of service.
- interfaceNotNew: Some modifications require that the interface must never have been in service.
- interfaceExists: Some modifications, such as setting the interface type, require that no interface exists. (Type must be unconfigured).
- bridgeGroupActive: For setting the bridgeDomainNumber in bridge or router interfaces. To add an interface to a bridgeGroup, the bridgeGroup must be in service.
- signalingNotEnabled: For this interface to be created, signaling must be enabled.

- firmwareOutOfDate: The firmware for the I/O module does not work with this interface.
- ts16ForData: ts16 has been set for passing data and the user is attempting to turn on signaling.
- dbcesConfigured: Signaling cannot be disabled because this interface is configured as dbces.
- signalingEnabled: Signaling is on for at least one of the channels while trying to change e1 TS16 from CAS to CCS.
- channelizationEnabled: A port can not be channelized in order to support unstructured CE.
- unstructuredCEConfigured: A port which has been channelized can not be configured to support unstructured CE.
- otherInterfacesExistOnThisPort: ISDN interface needs all 24 channels on the port.

If any of the channels on that interface are already configured, the ISDN interface can not be defined on that port. Valid range is a number between 1 and 28. See table below for a mapping between numbers and their enumerated type.

Table A-13. Interface Failure Reason Codes

Number Value	Enumerated Type
1	interfaceInService
2	interfaceNotNew
3	interfaceExists
4	bridgeGroupActive
5	signallingNotEnabled
6	firmwareOutOfDate
8	ts16ForData
9	dbcesConfigured
10	signalingEnabled
15	channelizationEnabled
16	unstructuredCEConfigured
17	firmwareOutOfDate-ts16CAS-unsup-ported
18	firmwareOutOfDate-interfaceType-unsup-ported
19	firmwareOutOfDate-ts16-unsupported
20	invalidPortMap
21	otherInterfacesExisOnThisPort
22	intfInIMAgroup
23	errorCTC-portTxClkSrc-notLocal
24	different-LoopbackConfig-on-Ports
25	imaGChanNeTxClkMode-unsupported

Table A-13. Interface Failure Reason Codes

Number Value	Enumerated Type
26	intfChange-Disallowed-on-APS-Protec-tionPort
27	intferfaceCurrentlyNotSupported
28	failure-at-call-handler

interfaceIndex Interface index used for identifcation in traps. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

interfaceType Interface type used for identification in traps. A specific interface is associated with each number. Valid range is a number between 1 and 20. See table below for a mapping between numbers and their enumerated type.

Table A-14. Interface Type Codes

Number Value	Enumerated Type
1	atmUni3-0
2	atmUni3-1
3	iispUser
4	iispNetwork
5	circuitEmulation
6	frameRelayUni
7	pri-isdn-user
8	pri-isdn-network
9	terminalEmulation
10	dsp
11	hdlcPassThrough
12	bridge
13	routing
14	dbCirEm
15	frameRelayNni
16	dsp2
17	atmIma
18	atmPnni1-0
19	atmUni4-0
20	atmVnnUni3-1

ipAddrNumber The IP address of the host/network to be echoed.

ipAtmAppPvcVccDest AddrA Destination IP address of an in-band management-ATM connection. Value is an IP address.

ipAtmAppPvcVccIfB Interface index for side B, the ATM side, of an in-band management ATM connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

ipAtmAppPvcVccSubnet MaskA The subnet mask of the destination IP address. Value is an IP address.

ipAtmAppPvcVccVciB VCI value for side B, the ATM side, of an in-band management-to-ATM connection. Valid range is a number between 0 and 65535.

ipAtmAppPvcVccVpiB VPI value for side B, the ATM side, of an in-band management-to-ATM connection. Valid range is a number between 0 and 4095.

ipIntfStatus Return codes for the Route Server module's IP interface operations. Valid range is a number between 1 and 16. See table below for a mapping between numbers and their enumerated type.

Table A-15. IP Interface Status Codes

Number Value	Enumerated Type
1	intOK
2	intIntFailure
3	intTooMany
4	intBadSlot
5	intBadId
6	intBadState
7	intBadTimer
8	intExists
9	intCantFind
10	intDelInProgress
11	intLockedIdle
12	intBadNetMask
13	intShutting
14	intDisabled
15	intNotHostAddr
16	intBadIpAddr

ipTypeReasonCode Indicator of which ip address had the problem. Valid range is a number between 1 and 31. See table below for a mapping between numbers and their enumerated type.

Table A-16. IP Type Reason Codes

Number Value	Enumerated Type
1	siteEtherIpAddr
2	siteEtherIpMask
3	siteGatewayAddr
4	siteRemoteMgrAddr1
5	siteRemoteMgrAddr2
6	siteRemoteMgrAddr3
7	siteRemoteMgrAddr4
8	siteRemoteMgrAddr5
9	inBandPrimaryIpAddress
10	inBandPrimaryIpMask
11	inBandBackupIpAddress
12	inBandBackupIpMask
13	siteIncorrectGatewaySubnet
14	siteGatewayInbandAddrMatch
15	siteIncorrectInbandSubnet
16	siteIncorrectEthernetSubnet
17	cpuIpSameAsSwitchIpAddr
18	cpuIpAddrInvalid
19	cpuAndIpMaskInvalid
20	switchAndCpuIpSubnetMismatch
21	switchIpAddrInvalid
22	switchAndIpMaskInvalid
23	cpuIpMaskClashWithInbandSubnet
24	switchIpMaskClashWithInbandSubnet
25	siteGatewayAddrInvalid
26	siteGatewayInbandAddrClash
27	unableToApplyGatewayIpAddr
28	unableToSetCpuIpInEPROM
29	unableToApplyCpuIpAddr
30	unableToApplySwitchIpAddr
31	unableToRevertBackToCpuIpAddr

isdnIntfDChanId D-Channel Number - if the Dchannel number is 0 no LAPD will run on this PRI-ISDN interface.

lineStatus

- Bit map of the status of a line connected to a port. The bit maps for the I/O modules are shown in the following tables:

~ The following bit map table shows line statuses for the DS1/T1 and Enhanced DS1 modules:

Table A-17. Enhanced DS1 Line Status Codes

Bit Value	Alarm	Description
1	dsx1NoAlarm	No alarm present
2	dsx1RcvFarEndLOF	Far end LOF (that is, Yellow Alarm)
4	dsx1XmtFarEndLOF	Near end sending LOF Indication
8	dsx1RcvAIS	Far end sending AIS
16	dsx1XmtAIS	Near end sending AIS
32	dsx1LossOfFrame	Near end LOF (a.k.a., Red Alarm)
64	dsx1LossOfSignal	Near end Loss Of Signal
128	dsx1LoopbackState	Near end is looped
256	dsx1T16AIS	E1 TS16 AIS
512	dsx1RcvFarEndLOMF	Far End Sending TS16 LOMF
1024	dsx1XmtFarEndLOMF	Near End Sending TS16 LOMF
2048	dsx1RcvTestCode	Near End detects a test code
4096	dsx1OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the DS3 module:

Table A-18. DS3 ATM and DS3 Frame Relay Module Line Status Codes

Bit Value	Alarm	Description
1	dsx3NoAlarm	No alarm present
2	dsx3RcvRAIFailure	Receiving Yellow/Remote Alarm Indication
4	dsx3XmitRAIAlarm	Transmitting Yellow/Remote Alarm Indication
8	dsx3RcvAIS	Receiving AIS failure state
16	dsx3XmitAIS	Transmitting AIS failure statue
32	dsx3LOF	Receiving LOF failure state
64	dsx3LOS	Receiving LOS failure state
128	dsx3LoopbackState	Looping the received signal
256	dsx3RcvTestCode	Receiving a Test Pattern
512	dsx3OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the Enhanced E1 module:

Table A-19. Enhanced E1 Line Status Codes

Bit Value	Alarm	Description
1	e1NoAlarm	No Alarm Present
2	e1RcvFarEndLOF	Far end LOF (a.k.a., Yellow Alarm)
4	e1XmtFarEndLOF	Near end sending LOF Indication
8	e1RcvAIS	Far end sending AIS
16	e1XmtAIS	Near end sending AIS
32	e1LossOfFrame	Near end LOF (a.k.a., Red Alarm)
64	e1LossOfSignal	Near end Loss Of Signal
128	e1LoopbackState	Near end is looped
256	e1T16AIS	E1 TS16 AIS
512	e1RcvFarEndLOMF	Far End Sending TS16 LOMF
1024	e1XmtFarEndLOMF	Near End Sending TS16 LOMF
2048	e1RcvTestCode	Near End detects a test code
4096	e1OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the E3 module:

Table A-20. E3 ATM Module Line Status Codes

Bit Value	Alarm	Description
1	e3NoAlarm	No alarm present
2	e3RcvRAIFailure	Receiving Yellow/Remote Alarm Indication
4	e3XmitRAIAlarm	Transmitting Yellow/Remote Alarm Indication
8	e3RcvAIS	Receiving AIS failure state
16	e3XmitAIS	Transmitting AIS failure statue
32	e3LOF	Receiving LOF failure state
64	e3LOS	Receiving LOS failure state
128	e3LoopbackState	Looping the received signal
256	e3RcvTestCode	Receiving a Test Pattern
512	e3OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the Ethernet module:

Table A-21. Ethernet Line Status Codes

Bit Value	Line Status
1	Down
2	10baseT-FullDuplex
4	10baseT-HalfDuplex
8	100baseT-FullDuplex
16	100baseT-HalfDuplex

~ The following bit map table shows line statuses for the OC-3c and STM-1 modules:

Table A-22. OC-3c and STM-1 Modules Line Status Codes

Bit Value	Alarm	Description
1	oc3NoAlarm	No alarm present
2	oc3RcvRAIFailure	Receiving Yellow/Remote Alarm Indication
4	oc3XmitRAIAlarm	Transmitting Yellow/Remote Alarm Indication
8	oc3RcvAIS	Receiving AIS failure state
16	oc3XmitAIS	Transmitting AIS failure statue
32	oc3LOF	Receiving LOF failure state
64	oc3LOS	Receiving LOS failure state
128	oc3LoopbackState	Looping the received signal
256	oc3RcvTestCode	Receiving a Test Pattern
512	oc3OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the Voice 2-Wire Office (2W Sink) module:

Table A-23. Voice 2-Wire Office Module Line Status Codes

Bit Value	Alarm	Description
1	NoAlarm	No alarm present
2	SignalingFailureState	Signals Failure State
4	FacilityLoopBack	Not currently supported
8	Maintenance	Maintenance
16	Out Of Service	Out of Service
32	OtherFailure	Any other line status not shown in this table

~ The following bit map table shows line statuses for the Voice 2-Wire Station (2W Source) module:

Table A-24. Voice 2-Wire Station Module Line Status Codes

Bit Value	Alarm	Description
1	NoAlarm	No alarm present
2	SignalingFailureState	Signals Failure State
4	FacilityLoopBack	Not currently supported
8	Maintenance	Maintenance
16	OutOfService	Out of Service
32	OtherFailure	Any other line status not shown in this table

lmiDlciOperStatus

The operational status of the LMI protocol. Valid range is a number between 1 and 2. See the table for a mapping between numbers and their enumerated type.

Table A-25. LMI DLCI Operational Status Codes

Number Value	Enumerated Type
1	outOfService
2	inService

oamTestFailureReason Code

An identified reason why an OAM Loopback Test request has failed. Valid range is a number between 1 and 7. See the following table for a mapping between numbers and their enumerated type.

Table A-26. OAM Test Failure Reason Codes

Number Value	Enumerated Type
1	invalidSPCforOAM
2	invalidIntfForOAM
3	invalidLocationLength
4	oamNotSupportedForThisConnection
5	loopbackTestAlreadyRunning
6	loopbackTestNotRunning
7	oamLocalResourcesUnavailable

oamTestIfB

Interface index used for starting loopback test. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

oamTestVciB

VCI value under testing for oam loopback test. Valid range is a number between 0 and 65535.

oamTestVpiB

VPI value under testing for oam loopback test. Valid range is a number between 0 and 4095.

oc3APSK1K2Rx Rx K1/K2 followed by hex value of K1, K2

oc3APSK1K2Tx Tx K1/K2 followed by hex value of K1, K2

oc3APSPairPortIndex APS Pair Port index - SSPP

oc3APSProtectionLine SignalStatus Valid range is a number between 1 and 1024. See table below for a mapping between numbers and their enumerated type.

Table A-27. OC-3c APS Protection Line Signal Status Codes

Number Value	Enumerated Type
1	noAlarm
2	signalDegradation
4	signalFailure
8	lostCellDelineation
16	switchByteFailure
32	ais-l
64	ais-p
128	lop
256	lof
512	los
1024	moduleFailure

oc3APSReasonCode Valid range is a number between 1 and 62. See table below for a mapping between numbers and their enumerated type.

Table A-28. OC-3c APS Reason Codes

Number Value	Enumerated Type
1	localprotectDoNotRe-vert
8	localprotectManualSw
10	localprotectSD
12	localprotectSF
14	localprotectForced
15	localprotectLockOut
17	localworking-DoNotRevert
24	localworkingManu-alSw
26	localworkingSD
28	localworkingSF
30	localworkingForced
33	remoteprotect-DoNotRevert

Table A-28. OC-3c APS Reason Codes

Number Value	Enumerated Type
40	remoteprotectManu-alSw
42	remoteprotectSD
44	remoteprotectSF
46	remoteprotectForced
47	remoteprotectLockOut
48	noRequest
49	remoteworking-DoNotRevert
56	remoteworkingManu-alSw
58	remoteworkingSD
60	remoteworkingSF
62	remoteworkingForced

oc3APSSelectorState

W: active/standby P: standby/active Valid range is either the number 1 or 2. See table below for a mapping between numbers and their enumerated type.

Table A-29. OC-3c APS Selector State Codes

Number Value	Enumerated Type
1	w-active-p-standby
2	w-standby-p-active

oc3APSWorkingLine SignalStatus

Valid range is a number between 1 and 1024. See table below for a mapping between numbers and their enumerated type.

Table A-30. OC-3c APS Working Line Signal Status Codes

Number Value	Enumerated Type
1	no alarm
2	signalDegradation
4	signalFailure
8	lostCellDeliniation
16	switchByteFailure
32	ais-1
64	ais-p
128	lop
256	lof
512	los
1024	moduleFailure

oc3PortId interface index - SSPP

percentComplete Used for the trap message **fileTransferStatusNotify**, and the value equals the percent of the upgrade, downgrade, or FTP download completed.

pingStatusReasonCode The response value - Alive/Not Alive. Valid range is a number between 1 and 2. See table below for a mapping between numbers and their enumerated type.

Table A-31. Ping Status Reason Codes

Number Value	Enumerated Type
1	alive
2	not-alive

pnniCode An identified reason for Miscellaneous Reasons in PNNI Configuration. Valid range is a number between 1 and 20. See table below for a mapping between numbers and their enumerated type.

Table A-32. PNNI Codes

Number Value	Enumerated Type
1	pnniInvEndSysPortId
2	pnniNodeAdmStatNotUp
3	pnniProtLnkStatDown
4	pnniProtLnkStatUpNotAdv
5	pnniProtLinkStatUpAdv
6	pnniIntfAdmStatUp
7	pnniNodeNotCfg
8	pnniRtAddrAddedByIlmi
9	pnniRtAddrDelByIlmi
10	pnniLvlMismatchInNodeId
11	pnniLvlMismatchInPGId
12	pnniATMAddrInvInNodeId
13	pnniATMAddrInvInPGId
14	pnniIntfAdmStatNotDel
15	pnniNodeAdmStatUp
16	pnniNodeRowStatNotActive
17	pnniNewRtAddrAdded
18	pnniRtAddrMod
19	pnniAdvtNodeIdNotMine
20	pnniFeatureNotSupported

portFailureReasonCode

Identification of cause for failure in changing the parameters of a port. Valid range is either the number 1 or 2. See table below for a mapping between numbers and their enumerated type.

Table A-33. Port Failure Reason Codes

Number Value	Enumerated Type
1	insufficientModuleBandwidth
2	localLoopNotAllowedWhenInAPS

portId

Port ID used for identification in traps. Number value is interpreted as a port of the form, SSPP, where SS is the module slot and PP is the port number.

powerSupplyReason Code

Identification for change in status of a power supply. Valid range is a number between 1 and 8. See table below for a mapping between numbers and their enumerated type.

Table A-34. Power Supply Reason Codes

Number Value	Enumerated Type
1	overload
2	overloadCleared
3	plus5vFailed
4	plus5vCleared
5	plus120vFailed
6	plus120vCleared
7	minus48vFailed
8	minus48vCleared

primarySoftware Version

Software version running on primary CPU.

pvcFailureReasonCode

An identified reason why an ATM PVC connection request failed. Valid range is a number between 1 and 218. See table below for a mapping between numbers and their enumerated type.

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
1	vpiVciUnavailableA2B
2	vpiVciUnavailableB2A
3	bandwidthUnavailableA2B
4	bandwidthUnavailableB2A
5	qosUnavailableA2B
6	qosUnavailableB2A
7	internalResourceUnavailable
8	cantUseSignalingChnlIgrsA2B

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
9	cantUseSignalingChnlEgrsA2B
10	cantUseSignalingChnlIgrsB2A
11	cantUseSignalingChnlEgrsB2A
12	cantUseManagementChnlIgrsA2B
13	cantUseManagementChnlEgrsA2B
14	cantUseManagementChnlIgrsB2A
15	cantUseManagementChnlEgrsB2A
16	vcLessThanVcMinIgrsA2B
17	vcLessThanVcMinEgrsA2B
18	vcLessThanVcMinIgrsB2A
19	vcLessThanVcMinEgrsB2A
20	vcGreaterThanVcMaxIgrsA2B
21	vcGreaterThanVcMaxEgrsA2B
22	vcGreaterThanVcMaxIgrsB2A
23	vcGreaterThanVcMaxEgrsB2A
24	vpLessThanVpMinIgrsA2B
25	vpLessThanVpMinEgrsA2B
26	vpLessThanVpMinIgrsB2A
27	vpLessThanVpMinEgrsB2A
28	vpGreaterThanVpMaxIgrsA2B
29	vpGreaterThanVpMaxEgrsA2B
30	vpGreaterThanVpMaxIgrsB2A
31	vpGreaterThanVpMaxEgrsB2A
32	vpGreaterThanVpMaxIispIgrsA2B
33	vpGreaterThanVpMaxIispEgrsA2B
34	vpGreaterThanVpMaxIispIgrsB2A
35	vpGreaterThanVpMaxIispEgrsB2A
36	rsvdChnlRangeIgrsA2B
37	rsvdChnlRangeEgrsA2B
38	rsvdChnlRangeIgrsB2A
39	rsvdChnlRangeEgrsB2A
40	internalSrvcTypeUnavailableA2B
41	internalSrvcTypeUnavailableB2A
42	unrecognizableBindTypeEgrsA2B
43	unrecognizableBindTypeEgrsB2A
44	callWithoutConnections
45	callDataStructuresUnavailable

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
46	cnctnDataStructuresUnavailable
47	nullTrafficParametersRejectedA2B
48	nullTrafficParametersRejectedB2A
49	vpiWithinSvcRangeIgrsA2B
50	vpiWithinSvcRangeEgrsA2B
51	vpiWithinSvcRangeIgrsB2A
52	vpiWithinSvcRangeEgrsB2A
53	vpiInReservedListA2B
54	vpiInReservedListB2A
55	vpiInPvcListA2B
56	vpiInPvcListB2A
57	vpiInReleasedListA2B
58	vpiInReleasedListB2A
59	vciIsNotNullInVpcIgrsA2B
60	vciIsNotNullInVpcEgrsA2B
61	vciIsNotNullInVpcIgrsB2A
62	vciIsNotNullInVpcEgrsB2A
63	vpiInVpcReservedListA2B
64	vpiInVpcReservedListB2A
65	vpiVciInReservedListA2B
66	vpiVciInReservedListB2A
67	vpiInVpcPvcListA2B
68	vpiInVpcPvcListB2A
69	vpiVciInPvcListA2B
70	vpiVciInPvcListB2A
71	vpiInVpcReleasedListA2B
72	vpiInVpcReleasedListB2A
73	vpiVciInReleasedListA2B
74	vpiVciInReleasedListB2A
75	illegalMulticaseIdA2B
76	illegalMulticaseIdB2A
77	unsupportedConnectionA2B
78	unsupportedConnectionB2A
79	connectionsUnavailableInModuleA2B
80	connectionsUnavailableInModuleB2A
81	scrBandwidthUnavailableIgrsA2B
82	scrBandwidthUnavailableEgrsA2B

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
83	scrBandwidthUnavailableIgrsB2A
84	scrBandwidthUnavailableEgrsB2A
85	pcrBandwidthUnavailableIgrsA2B
86	pcrBandwidthUnavailableEgrsA2B
87	pcrBandwidthUnavailableIgrsB2A
88	pcrBandwidthUnavailableEgrsB2A
89	vpiVciWithinSvcRangeIgrsA2B
90	vpiVciWithinSvcRangeEgrsA2B
91	vpiVciWithinSvcRangeIgrsB2A
92	vpiVciWithinSvcRangeEgrsB2A
93	multicastDataStructuresUnavailable
94	semaphoreTimeout
95	dlciFoundInReservedList
96	dlciFoundInPvcList
97	dlciFoundInReleasedList
98	invalidDlci
99	slotA-OutOfRange
100	portA-OutOfRange
101	channelA-OutOfRange
102	moduleA-Uninitialized
103	physicalPortA-Uninitialized
104	channelA-NotBound
105	moduleA-UnrecognizablePortType
106	slotB-OutOfRange
107	portB-OutOfRange
108	channelB-OutOfRange
109	moduleB-Uninitialized
110	physicalPortB-Uninitialized
111	channelB-NotBound
112	moduleB-UnrecognizablePortType
113	interfaceA-NotAtm
114	interfaceB-NotAtm
115	unrecognizableServiceTypeA2B
116	unrecognizableServiceTypeB2A
117	unrecognizableSarTypeA2B
118	unrecognizableSarTypeB2A
119	interfaceA-NotCircuitEmulation

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
120	interfaceB-NotCircuitEmulation
121	unrecognizableSilenceDetectionMode
122	unrecognizableEchoCancellationMode
123	unrecognizableVoiceCompressionMode
124	interfaceA-NotVbr
125	interfaceB-NotVbr
126	interfaceA-NotFrameRelay
127	interfaceB-NotFrameRelay
128	interfaceA-InHdlcPvcList
129	interfaceA-InHdlcReleasedList
130	interfaceA-InHdlcReservedList
131	interfaceA-InTerminalEmulationPvcList
132	interfaceA-InTerminalEmulationReleasedList
133	interfaceA-InTerminalEmulationReservedList
134	interfaceA-InCircuitEmulationPvcList
135	interfaceA-InCircuitEmulationReleasedList
136	interfaceA-InCircuitEmulationReservedList
137	notNullVpcInNoisyLinkA2BIgrs
138	notNullVpcInNoisyLinkA2BEgrs
139	invalidVccInNoisyLinkA2BIgrs
140	invalidVccInNoisyLinkA2BEgrs
141	unsupportedFrwdErrCorrectValueA2B
142	interfaceB-InHdlcPvcList
143	interfaceB-InHdlcReleasedList
144	interfaceB-InHdlcReservedList
145	interfaceB-InTerminalEmulationPvcList
146	interfaceB-InTerminalEmulationReleasedList
147	interfaceB-InTerminalEmulationReservedList
148	interfaceB-InCircuitEmulationPvcList
149	interfaceB-InCircuitEmulationReleasedList
150	interfaceB-InCircuitEmulationReservedList
151	notNullVpcInNoisyLinkB2AIgrs
152	notNullVpcInNoisyLinkB2AEgrs
153	invalidVccInNoisyLinkB2AIgrs
154	invalidVccInNoisyLinkB2AEgrs
155	unsupportedFrwdErrCorrectValueB2A
156	interfaceInUse

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
157	unsupportedFrwdErrCorrectSettings
158	unsupportedFlowSettings
159	frwdErrCorrectResourceInternalError
160	unsupportedConnection
161	ipDestAddrSubnetAInReservedList
162	ipDestAddrSubnetAInPvcList
163	ipDestAddrSubnetAInReleasedList
164	ipDestAddrSubnetBInReservedList
165	ipDestAddrSubnetBInPvcList
166	ipDestAddrSubnetBInReleasedList
167	notCpuIpInterfaceA
168	ipResourceUnavailable
169	fecAutoInSimplexNotValid
170	fecResourceUnavailable
171	notBridgeInterfaceA
172	notBridgeInterfaceB
173	invalidBridgePortA2B
174	invalidBridgePortB2A
175	interfaceAInBridgePvcList
176	interfaceBInBridgePvcList
177	interfaceAInBridgeReleasedList
178	interfaceBInBridgeReleasedList
179	interfaceAInBridgeReservedList
180	interfaceBInBridgeReservedList
181	invalidDlciA
182	invalidDlciB
183	unrecognizableServiceType
184	moduleAMcstNotSupported
185	moduleBMcstNotSupported
186	moduleAMultiPortMcstNotSupported
187	moduleBMultiPortMcstNotSupported
188	bcBeCirCannotBeNullA2B
189	bcBeCirCannotBeNullB2A
190	bcBeOrCirValTooHiA2B
191	bcBeOrCirValTooHiB2A
192	bcNotValidA2B
193	bcNotValidB2A

Table A-35. PVC Failure Reason Codes

Number Value	Enumerated Type
194	beNotValidA2B
195	beNotValidB2A
196	bcOrCirNotValidA2B
197	bcOrCirNotValidB2A
198	iWF-NotSupportedModuleA
199	iWF-NotSupportedModuleB
200	invalidMaxFrSizeA2B
201	invalidMaxFrSizeB2A
202	invalidSARType
203	unrecognizableSilenceDetectionModeA2B
204	unrecognizableEchoCancellationModeA2B
205	unrecognizableVoiceCompressionModeA2B
206	unrecognizableCallingToneDetectionA2B
207	unrecognizableCodingTranslationA2B
208	unrecognizableSilenceDetectionModeB2A
209	unrecognizableEchoCancellationModeB2A
210	unrecognizableVoiceCompressionModeB2A
211	unrecognizableCallingToneDetectionB2A
212	unrecognizableCodingTranslationB2A
213	dspUnsupportedForMultiCastConns
214	dspResourceUnavailable
215	destOrSrcCannotBeDSPCard
216	internalDSPResourceError
217	echoCancellationOnlySupportedForDuplex
218	cirEmCirEm-ThruPutMismatch

remoteRebootReason Code

The result of a remote reboot request. Valid range is a number between 1 and 46. See table below for a mapping between numbers and their enumerated type.

Table A-36. Remote Reboot Reason Codes

Number Value	Enumerated Type
1	ioCard1Reboot-OK
2	ioCard2Reboot-OK
3	ioCard3Reboot-OK
4	ioCard4Reboot-OK
5	ioCard5Reboot-OK
6	ioCard6Reboot-OK

Table A-36. Remote Reboot Reason Codes

Number Value	Enumerated Type
7	ioCard7Reboot-OK
8	ioCard8Reboot-OK
9	ioCard9Reboot-OK
10	ioCard10Reboot-OK
11	ioCard11Reboot-OK
12	ioCard12Reboot-OK
13	ioCard13Reboot-OK
14	ioCard14Reboot-OK
15	ioCard15Reboot-OK
16	ioCard16Reboot-OK
17	ioCard1Reboot-NoCardInSlot
18	ioCard2Reboot-NoCardInSlot
19	ioCard3Reboot-NoCardInSlot
20	ioCard4Reboot-NoCardInSlot
21	ioCard5Reboot-NoCardInSlot
22	ioCard6Reboot-NoCardInSlot
23	ioCard7Reboot-NoCardInSlot
24	ioCard8Reboot-NoCardInSlot
25	ioCard9Reboot-NoCardInSlot
26	ioCard10Reboot-NoCardInSlot
27	ioCard11Reboot-NoCardInSlot
28	ioCard12Reboot-NoCardInSlot
29	ioCard13Reboot-NoCardInSlot
30	ioCard14Reboot-NoCardInSlot
31	ioCard15Reboot-NoCardInSlot
32	ioCard16Reboot-NoCardInSlot
33	allIOCardReboot-OK
34	allIOCardReboot-NoIOCards
35	chassisReboot-Proceeding
36	backupCpuReboot-Proceeding
37	backupCpuReboot-NoBackup
38	primaryCpuReboot-Proceeding
39	primaryCpuSwitchover-Proceeding
40	primaryCpuSwitchover-NoBackup
41	chassisReboot-Fail-VersionControlInProgress
42	backupCpuReboot-Fail-VersionControlIn Progress

Table A-36. Remote Reboot Reason Codes

Number Value	Enumerated Type
43	primaryCpuReboot-Fail-VersionControlIn Progress
44	primaryCpuSwitchover-Fail-VersionControlIn Progress
45	primaryCpuSwitchover-Fail-BkCPUDataBase NotNew
46	primaryCpuSwitchover-Fail-BkCPUBuildNot-Good

removeConfigFiles Used to indicate the status of a remove configuration files request. Valid range is a number between 1 and 4. See table below for a mapping between numbers and their enumerated type.

Table A-37. Remove Configuration Files Codes

Number Value	Enumerated Type
1	from-PrimaryCPU
2	from-BackupCPU
3	chassisReboot
4	failed-VersionControlInProgress

routeSrvStatus Return codes for basic route server task operations not related to any specific VPN or IP/Connection operation. Valid range is a number between 1 and 4. See table below for a mapping between numbers and their enumerated type.

Table A-38. Route Server Status Codes

Number Value	Enumerated Type
1	rsCardOK
2	rsModInitFail
3	rsIntfInitFail
4	rsPortInitFail

routingStatus Success: Routing Data is Available. Failure: Reply from RS Card timed-out. Valid range is a number between 1 and 2. See table below for a mapping between numbers and their enumerated type.

Table A-39. Routing Status Codes

Number Value	Enumerated Type
1	success
2	failure

saveConfiguration ReasonCode

The result of a save configuration request. Valid range is a number between 1 and 14. See table below for a mapping between numbers and their enumerated type.

Table A-40. Save Configuration Reason Codes

Number Value	Enumerated Type
1	equipment-OK
2	equipment-Fail-VersionControlInProgress
3	equipment-Fail
4	connections-OK
5	connections-Fail-VersionControlInProgress
6	connections-Fail
7	routing-OK
8	routing-Fail-VersionControlInProgress
9	routing-Fail
10	all-OK
11	all-Fail-VersionControlInProgress
12	all-Fail
13	fileTransferFailed
14	fileTransferCompleted

spvcConfigFailureCode

Identification of cause for failure while configuring/modifying SPVC parameters.

- noSpvcConfigured: The endpoint has not been configured as SPVC, so SPVC parameters can't be modified.
- spvcAlreadyConfigured: SPVC is already configured, so it can't be configured again as SPVC endpoint.
- noInterfaceConfigured: There is no interface configured.
- interafceNotConfiguredAsRequired: While configuring it as SPVC endpoint, this interface is not as desired (e.g., it is not CE, while trying to configure CES SPVC).
- notActiveSpvc: This endpoint is "Passive" SPVC endpoint, so SPVC paramerers can't be modified.

Valid range is a number between 1 and 20. See table below for a mapping between numbers and their enumerated type.

Table A-41. SPVC Configuration Failure Codes

Number Value	Enumerated Type
1	noSpvcConfigured
2	spvcAlreadyConfigured
3	noInterfaceConfigured
4	interfaceNotConfiguredAsRequired
6	notActiveSpvc

Number Value	Enumerated Type
7	slotA-OutofRange
8	portA-OutofRange
9	channelA-OutofRange
10	vpiVciWithInSvcRange
11	retryIntervalExceedsTheLimit
12	interfaceNotConfiguredAsCE
13	interfaceNotConfiguredAsVbr
14	interfaceNotConfiguredAsAtm
15	noAddressConfiguredOnTheInterface
16	localAddressNotValid
17	vpiVciUnavailable
18	pvcAlreadySetupOnVpiVci
19	pvcAlreadySetupOnInterface
20	retryIntervalTooSmall

statRtStatus

Return codes for Route Server module static route condititions. Valid range is a number between 1 and 18. See table below for a mapping between numbers and their enumerated type.

Table A-42. Static Route Codes

Number Value	Enumerated Type
1	statRtOk
2	statRtIntFailure
3	statRtMany
4	statRtSlot
5	statRtBadId
6	statRtBadState
7	statRtBadTimer
8	statRtExists
9	statRtCantFind
10	statRtDelInProgress
11	statRtLockedIdle
12	statRtBadNetMask
13	statRtCorrelation
14	statRtShutting
15	statRtDisabled
16	statRtBadMetric
17	statRtBadIPAddr
18	intfRtExists

stratumMode

Current status of the primary Stratum 3–4 module. Valid range is a number between 1 and 4. See table below for a mapping between numbers and their enumerated type.

Table A-43. Stratum 3–4 Module Mode Codes

Number Value	Enumerated Type
1	synchronized3
2	synchronized4
3	holdover
4	freerun

subChanStatus

Return codes for route server sub channel connections operations. Valid range is a number between 1 and 19. See table below for a mapping between numbers and their enumerated type.

Table A-44. Subchannel Status Codes

Number Value	Enumerated Type
1	scOK
2	scIntFailure
3	scTooMany
4	scBadSlot
5	scBadId
6	scBadState
7	scBadTimerVal
8	scExists
9	scCantFind
10	scDelInProgress
12	scLockedIdle
13	scSameVc
14	scFailedSetup
15	scShutting
16	scDisabled
17	scSetupErr
18	scRemvErr
19	scBadPortNo

swtchNodeIndx

Switch Node Index for PNNI.

timingReasonCode

Indicator of type of relationship violated. Valid range is a number between 1 and 2. See table below for a mapping between numbers and their enumerated type.

Table A-45. Timing Reason Codes

Number Value	Enumerated Type
1	invalidForwardDelay-MaxAge
2	invalidHelloTime-MaxAge

upgradeSwCopyStatus Current status of the ftp software upgrade download. Valid range is a number between 1 and 5. See table below for a mapping between numbers and their enumerated type.

Table A-46. Upgrade Software Copy Status Codes

Number Value	Enumerated Type
1	noActivity
2	working
3	doneSuccessfully
4	doneWithError
5	aborted

upgradeSwErrorStatus The result of the finish of the FTP software upgrade download. Set to a value 3-23 if upgradeSwCopyStatus is doneWithError. Set to none if upgradeSwCopyStatus is doneSuccessfully. Set to userAbort if upgradeSwCopyStatus is aborted. Valid range is a number between 1 and 23. See table below for a mapping between numbers and their enumerated type.

Table A-47. Upgrade Software Error Status Codes

Number Value	Enumerated Type
1	none
2	userAbort
3	invalidIpAddress
4	invalidAccountName
5	invalidAccountPassword
6	invalidCdromFile
7	libraryCRCFail
8	unableToOpenLibraryFile
9	unableToLoadLibraryModule
10	unableToFindTaskSymbolName
11	failureInSpawningTask
12	failureInCreatingMsgQ
13	failureInCopyingDataFiles
14	failureToRemoveNextTree
15	unableToMakeNextTree
16	unableToOpenFile

Table A-47. Upgrade Software Error Status Codes

Number Value	Enumerated Type
17	unableToMakeFtpConnection
18	unableToWriteFile
19	unableToCompleteFtp
20	fileCRCFail
21	unableToWritePackageList
22	taskSuspendOrDead
23	unabletoUpdateBackup

vbrAtmPvcVccIfA Interface index for side A, the variable bit rate side, of a variable bit rate-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

vbrAtmPvcVccIfB Interface index for side B, the ATM side, of a variable bit rate-to-ATM PVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

vbrAtmPvcVccVciB VCI value for side B, the ATM side, of a variable bit rate-to-ATM PVC VCC connection. Valid range is a number between 0 and 65535.

vbrAtmPvcVccVpiB VPI value for side B, the ATM side, of a variable bit rate-to-ATM PVC VCC connection. Valid range is a number between 0 and 4095.

vbrAtmSpvcVccIfA Interface index for side A, the variable bit rate side, of a variable bit rate-to-ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

vbrAtmSpvcVccIfB Interface index for side B, the ATM side, of a variable bit rate-to-ATM SPVC VCC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

vbrAtmSpvcVccVciB VCI value for side B, the ATM side, of a variable bit rate-to-ATM SPVC VCC connection. Valid range is a number between 0 and 65535.

vbrAtmSpvcVccVpiB VPI value for side B, the ATM side, of a variable bit rate-to-ATM SPVC VCC connection. Valid range is a number between 0 and 4095.

vbrVbrPvcIfA Interface index for side A of a variable bit rate-to-variable bit rate PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

vbrVbrPvcIfB

Interface index for side B of a variable bit rate-to-variable bit rate PVC connection. Number value is interpreted as an interface of the form, SSPPCCC, where SS is the module slot, PP is the port number, and CCC is the channel number.

versionConfiguration ReasonCode

Valid range is a number between 1 and 20. See the table below for a mapping between numbers and their enumerated type.

Table A-48. Version Configuration Reason Codes

Number Value	Enumerated Type
1	upgrade-Start
2	upgrade-Completed
3	upgrade-Fail
4	downgrade-Start
5	downgrade-Completed
6	downgrade-Fail
7	upgrade-Fail-NoVersion
8	upgrade-Fail-VersionControlInProgress
9	downgradeFail-NoVersion
10	downgrade-Fail-VersionControlInProgress
11	upgrade-InProgress
12	downgrade-InProgress
13	upgrade-sanityCheck-InProgress
14	downgrade-sanityCheck-InProgress
15	upgrade-sanityCheck-Completed
16	downgrade-sanityCheck-Completed
17	upgrade-Fail-SanityCheckFail
18	downgrade-Fail-SanityCheckFail
19	upgrade-Fail-BkCPUFailedToRespond
20	downgrade-Fail-BkCPUFailedToRespond

viprIntfId

A unique ID for the Interface in a router instance.

viprRouteId

The unique ID to the routing table entry.

viprRouterId

A unique ID for the Router Instance in a router module.

viprSlot

The slot number of the Route Server module (SS).

viprSubChnlId

A unique ID for the subchannel in the interface.

vpnTrapStatus

Return codes for Route Server module virtual private network (VPN) level operations. Valid range is a number between 1 and 16. See table below for a mapping between numbers and their enumerated type.

Table A-49. VPN Trap Status Codes

Number Value	Enumerated Type
1	vpnAddOk
2	vpnInternalFailure
3	vpnTooMany
4	vpnBadSlot
5	vpnBadId
6	vpnBadState
7	vpnBadTimerVal
8	vpnAlreadyExists
9	vpnCantLocate
10	vpnDelInProgress
11	vpnLockedIdle
12	vpnGeneralFailure
13	vpnNotAllowed
14	vpnShutting
15	vpnDisabled
16	vpnModifyOk

B Pin Configurations

Overview of This Appendix

This appendix describes the pinout configurations for the connectors on the PSAX 20 common equipment components. It also describes the pinout configurations on the PSAX 20 input/output and server components. Use the following information to connect correctly configured cables to the PSAX 20 system.

Configuration for the Power Supply Connector

AC Power Supply Connector

The configuration of the connector pins for the 110 V ac Power Supply component on the PSAX 20 chassis faceplate is shown in Figure B-1.

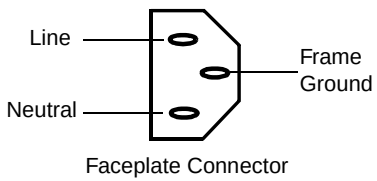

Figure B-1. Pin Configuration for the Connector on the 110 V ac Power Supply Component

Table B-1 describes the pin configuration for the connectors on the 110 V ac Power Supply component.

Table B-1. Pin Descriptions for the Connector on the 110 V ac Power Supply Component

Pin	Description
Line	Accepts the appropriate phased voltage.
Frame-Ground	Provides the frame ground for the PSAX 20 chassis. A 2 K ohm resistance separates the frame ground and the logical ground for all circuits in the PSAX 20 chassis, and on the I/O and server modules.
Neutral	In conjunction with the line pin, provides the reference voltage.

Configuration for the CPU Connectors

Two different interfaces are available for direct access to the CPU component. You can use the console serial interface or the Ethernet interface to connect to the terminal emulator for configuring and managing the PSAX 20 system.

Console Serial Interface

The serial port console interface of the PSAX 20 chassis faceplate accepts an RJ-11 connector. The faceplate connector accommodates the standard RJ-11 interface; however, due to differences among manufacturers of connectors, be sure to check your cable and connector to determine what type you have. DB9 connectors are available with different wire-coloring schemes. If you are using the serial port of a personal computer (PC) or workstation as the console, use a standard DB9 female connector with an attached RJ-11 connector. Be sure to use the correct type of cable to ensure proper operation. Table B-2 and Table B-3 describe the pin configuration for DB9 connectors with two different wire coloring schemes.

Table B-2. Pin Descriptions for the Serial Interface DB9 Connector with Black/Red/Green Wires

Pin	Description
2	Black = RX (receive)
3	Red = TX (transmit)
5	Green = Ground

Table B-3. Pin Descriptions for the Serial Interface DB9 Connector with Yellow/Green/Red Wires

Pin	Description
2	Yellow = RX (receive)
3	Green = TX (transmit)
5	Red = Ground

The SUN Microsystems workstation (as well as other types of workstations) can also be used to connect to the console serial port. If you are using the serial port of a SUN workstation as the console, use a DB25 male connector. Table B-4 describes the pin configuration for the DB25 connector.

Table B-4. Pin Descriptions for the Serial Interface DB25 Connector

Pin	Description
2	Red = TX (transmit)
3	Black = RX (receive)
7	Green = Ground

Ethernet 10Base-T Interface

The PSAX 20 chassis faceplate also accommodates the Ethernet interface using standard RJ-45 pin assignments. Figure B-2 shows the pin locations for the RJ-45 connector for the 10Base-T connector on the faceplates.

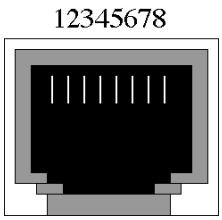

Figure B-2. Pin Locations on the RJ-45 Connector

Table B-5 describes the pin configuration for the RJ-45 faceplate connector.

Table B-5. Pin Descriptions for the RJ-45 Connector for the CPU Ethernet Interface

Pin	Description
1	TD+ (transmit to UTP wire)
2	TD– (transmit to UTP wire)
3	RD+ (receive from UTP wire)
4	Not used by 10Base-T
5	Not used by 10Base-T
6	RD– (receive from UTP wire)
7	Not used by 10Base-T
8	Not used by 10Base-T

Configuration for the DS1/T1 Interface Cable Connector

This section describes the pinout configuration on the T1 component. A T1 interface using an RJ-45 connector provides the connectivity on the T1 component. See Table B-6 for descriptions of the RJ-45 connector pins.

Table B-6. Pin Descriptions for the RJ-45 Connector on the DS1/T1 Interface on the PSAX 20 Chassis Faceplate

Pin	Description
1	Rx Ring
2	Rx Tip

Table B-6. Pin Descriptions for the RJ-45 Connector on the DS1/T1 Interface on the PSAX 20 Chassis Faceplate

Pin	Description
3	Not used
4	Tx Ring
5	Tx Tip
6	Frame Ground
7	Not used
8	Not used

C Configuring In-Band Management

Setting Up In-Band Management Configuration

Three types of in-band management configurations are available:

- Direct connection configuration—Connects the network management system (NMS) machine, usually a SUN workstation, to a PacketStar™ PSAX Multiservice Access Concentrator system through an OC-3c interface. This configuration requires that the NMS machine have an FORE card.
- Routed connection configuration—Connects a PSAX Multiservice Access Concentrator system through another Access Concentrator system, which is acting as a main router. The "main router" Access Concentrator system is connected to the NMS machine through an Ethernet connection. The "main router" is connected to an "intermediate router" Access Concentrator system, or an "end system" Access Concentrator system through ATM connections. In this configuration, ATM connections are made to the nearest hop in the tree structure.
- Hybrid connection configuration—Connects the "main router" Access Concentrator system directly to the "end system" Access Concentrator system through ATM connections. These ATM connections can be tunneled through a number of switches to reach the "end system" Access Concentrator system. The "main router" Access Concentrator system is connected to the NMS machine through an Ethernet connection.

The guidelines for setting up an in-band management network for each of these configurations are provided in the following sections.

Using the Direct Connection Configuration

The default gateway through the in-band network can be configured on all Access Concentrators with the IP address of the NMS machine, or network router, if used in place of an NMS station (see Figure C-1).

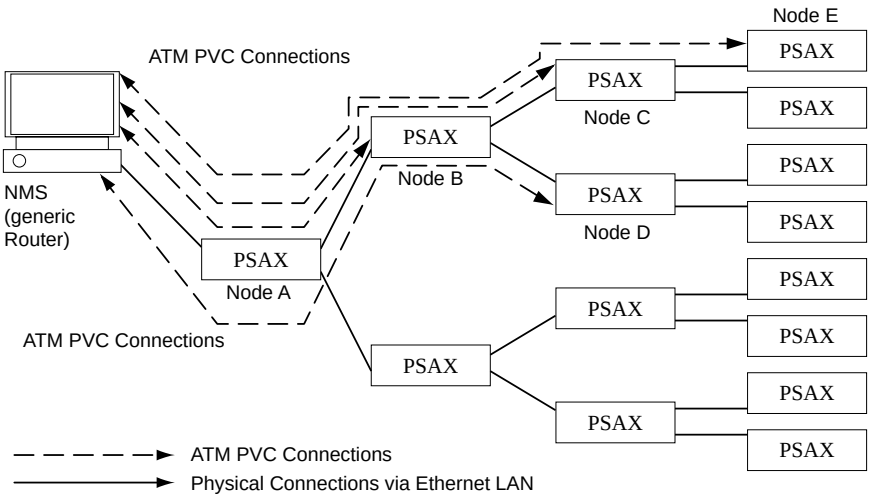

Figure C-1. Direct Connection Configuration

The tasks for setting up a direct connection configuration are the following:

1. Setting configuration values for the FORE card on the SUN workstation (see the procedure immediately below, "Setting Up the FORE Card on the SUN Workstation")
2. Setting up ATM ARP entries for the end of the ATM connection at the SUN workstation (see the procedure, also below)

Setting Up the FORE Card on the SUN Workstation

Begin

On the SUN workstation, assign the FORE card interface an IP address that is on a different network than the IP address for the Ethernet interface of the SUN workstation. Perform the steps in the following procedure to set up the FORE card on the SUN workstation:

1 On the SUN workstation, log in and type **root**.

2 To configure the FORE card, type the following command:

ifconfig fa0 *<forecard_Ip_Address>* **netmask** *<Netmask>* **broadcast** *<Bcast_address>* **mtu** *<Mtu_Size>* **up**

where,

forecard_Ip_Address = the IP address of the FORE card (for example, 136.242.140.222)

Netmask = the <IP subnet mask> (for example, 255.255.255.0)

Bcast_address = the IP address of the broadcast <server> (for example, 136.242.140.255)

Mtu_Size = <maximum transfer unit size [packet size]> (for example, 9180—refer to RFC 1577)

3 To test whether the FORE card has been configured correctly, type the following command:

ifconfig fa0

<Consult your FORE user's manual for additional instructions on the many variables you may encounter beyond this point.>

End

ATM ARP table entries should be created on the SUN machine. Each entry specifies the remote PSAX system in-band management IP address (primary) and the corresponding ATM connection (VCC: VPC) that is connected to the remote PSAX system. Add a PVC connection on the FORE card to the in-band management port on the PSAX system. Set up the following PVC connections:

Setting Up ATM ARP Table Entries

Begin

1 Type the following command:

Atmarp -s *<Remote_Ip>* **fa0** *<VPI> <VCI> <AAL>* **llc**

Atmarp -l fa0 <*VPI*> <*VCI*> <*AAL*> llc

Where Remote_Ip = (IP Address of the in-band connection on the CPU CARD)

Example:

Local IP = 136.242.140.223 (Primary IP Address of Node A)

VPI= 0

VCI= 300

AAL= 5

and

Remote IP = 136.242.140.225 (Primary IP Address of Node B)

VPI= 0

VCI= 302

AAL= 5

Check whether the connections have been configured by using the command **atmarp -a**

2. All the remote PSAX systems' in-band interface IP addresses may or may not be in the same subnet as that of the FORE card's IP address.
3. If the remote PSAX systems' in-band interface IP address is not in the same subnet as that of the FORE card's IP address, then a route entry should be added on the SUN machine for the remote PSAX systems' subnet, using the FORE card interface as the gateway.
4. On the PSAX system, the in-band management interface (primary) should be assigned an IP address that lies in a different network than that of its Ethernet interface.
5. The in-band connection from each of the remote PSAX systems is a direct connection to the SUN machine's FORE card interface IP address. (Here a direct connection implies that it should not be IP routed through a CPU module. It should be an ATM connection, which may be tunneled through a number of switches.)
6. If the ATM end points are connected to a Cisco router instead of a SUN machine, then the remote PSAX system can be configured with a default gateway address, which should be the same as the in-band connection end point's IP address (that is, the Cisco router's address).
7. The gateway IP address should be either an Ethernet subnet or an in-band management subnet. The gateway IP address should not be the same as the in-band IP address.
8. If the gateway IP address is in the in-band management subnet, then there should be an in-band connection to that address.
9. If a traffic-shaping OC-3 card is used, the recommended values for in-band connection are Peak Rate: 2000 cps; Sustained Rate: 1000 cps; MBS: 10000 cells.

End

Using the Routed Connection Configuration

No default gateway through an in-band network should be configured on any of the PSAX systems.

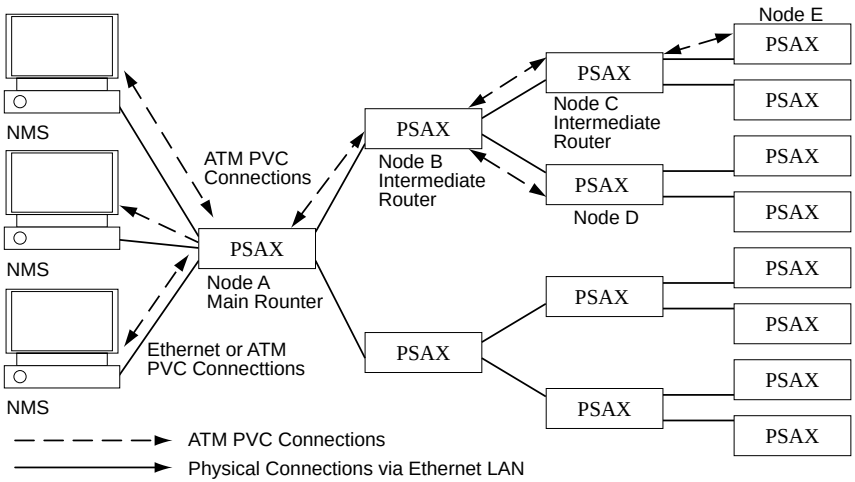

Figure C-2. Routed Connection Configuration

Perform the steps in the following procedure to configure the routed connection.

Steps for Setting Connections for a Routed Connection Configuration

Begin

1 A Routed Connection Configuration consists of a SUN (or PC) host connected through Ethernet to the router PSAX system. The router PSAX system has direct or routed in-band connections to the remote PSAX system. Log in as root on the SUN machine and add a routing table entry using the "route add" command:

route add net < *In-band network address*> <*PSAX IP address on Ethernet*> <*metric*>

where in-band network address = 20.0.0.0

PSAX IP address on Ethernet = {Check Site Specific Configuration -> Site Specific Configuration -> IP Address on the main router PSAX system- node A}

metric = 10

2 In this configuration, one or more PSAX systems can act as routers to channel traffic to different subnets. There are two type of router PSAX system connections. The first type is the main router connected directly to the NMS stations (either through Ethernet or OC3-ATM connection), and the second type is the intermediate router PSAX system. The main router PSAX system has only one type of connection: downstream connections to an intermediate router PSAX system or an end system

PSAX system. The intermediate router PSAX system has two types of in-band connections: upstream connections to a router PSAX system and downstream connections to either the router PSAX system or the end system PSAX system. This helps to form a simple tree structure (see Figure C-2 on page C-5).

3. On the PSAX system, the in-band management interface (primary) should be assigned an IP address that should be on a different network than that of its Ethernet interface.
4. Also, for all the PSAX system models (except the main router PSAX system), the Ethernet interface IP network should be different from the SUN machine's Ethernet interface IP network.
5. All of the NMS stations should be in the one IP network, but can be in different subnets connected to the main router PSAX system by an Ethernet or OC3-ATM connection.
6. All the end system and router PSAX system in-band interface IP addresses should be in the same IP network. They can have different masks (that is, the PSAX system downstream can have a mask wider in ones than that of the parent node). This allows multiple connections to be set to end system PSAX system that are in the same in-band subnet. Routing to intermediate PSAX systems is done based on the subnet mask. The subnetwork address provided in the connection table and routing to the end system PSAX system is based on the host address of the end system configured in the connection table. Routing to the NMS stations is based on the mask and network address to the NMS stations configured in the connection table. (With this configuration, an upstream connection should be made only to the NMS network).
7. The tree structure is based on subnet routing, where connections to each subtree lie in one subnet and the connections to a downstream subtree are configured with in-band subnetwork addresses and a mask larger (wider in ones) than the parent subtree. (See the example configuration in the next section).
8. The downstream connections to intermediate routers should be configured with the subnetwork address of the subtree and a mask larger (wider in ones) than that of the parent connections.
9. The upstream connection should only be to the NMS stations' network address with an appropriate mask.
10. On the host (SUN or PC) machine, an IP routing table entry should be added. This entry should be a network-specific routing table entry, with the in-band network address of each of the remote PSAX systems and the main router PSAX system Ethernet interface IP address as the gateway. The metric should be set to the depth of the tree (or default 10).
11. The default gateway should not be configured with an IP address within the in-band network.

End

Setting PVC Connections for Routed Connection Configuration

Assume that the VPI:VCI for the connection between node A and B is VPIab: VCIab, etc. Also assume that the Ethernet IP addresses of all nodes except node A do not lie in the NMS station's network address range.

Perform the steps in the following procedure to set PVC connections for a routed connection.

Steps to Setting PVC Connections for Routed Connection Configuration

Begin

1. Configure the primary IP address for in-band management on the CPU module of the main router PSAX system (Node A) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.001

Primary IP Mask: 255.000.000.000

The connection downstream from Node A to subtrees should have a mask greater than 255.0.0.0 if they go to network 20.0.0.0. For example, mask 255.255.0.0 is assigned for downstream connection.

2. Configure the primary and backup IP addresses for in-band management on the CPU module of the intermediate router PSAX system (Node B) using the console interface:

Example:

Primary IP Address:020.001.001.002

Primary IP Mask: 255.255.000.000

Connections downstream from Node B to the subtrees should have a mask greater than for the connection downstream on parent Node A (255.255.0.0) if they go to network 20.0.0.0. For example, mask 255.255.255.0 is assigned for downstream connection.

3. Configure the primary IP Address for in-band management on the CPU module of main router PSAX system (Node C) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.003

Primary IP Mask: 255.255.255.000

Connections downstream from Node C to subtrees will go directly to end-system PSAX systems and should have mask greater than or equal to that for connections on parent Node B (255.255.255.0) if they go to network 20.0.0.0. For example, mask 255.255.255.0 is assigned for downstream connections

4 Configure the primary IP Address for in-band management on the CPU module of main router PSAX system (Node D) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.002.001

Primary IP Mask: 255.255.255.000

5 Configure the primary IP Address for in-band management on the CPU module of the main router PSAX system (Node E) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.004

Primary IP Mask: 255.255.255.000

6 Configure the primary IP address for in-band management on the CPU module of the main router PSAX system (Node X) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.002.001.001

Primary IP Mask: 255.255.000.000

7 Configure the primary IP Address for in-band management on the CPU module of the main router PSAX system (Node Y) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.002.001.002

Primary IP Mask: 255.255.255.000

8 Configure the primary IP Address for in-band management on the CPU module of main router PSAX system (Node Z) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.002.002.001

Primary IP Mask: 255.255.255.000

9 Set up in-band management connections on the CPU module of Node A to DS3:

For setting up an in-band connection from the DS3 card to the CPU module, configure the DS3 card and put it into service. Then, using the console interface **[Connection Configuration]-> [In-Band Management IP PVC] -> [Add Connection]** screen, configure the PVC to the FORECARD.

Example:

Slot<Slot> VPI:VPIabIP Address: 020.001.000.000

Port1 VCI:VCIabIP Mask: 255.255.000.000

Channel 1

Slot<Slot> VPI: VPIaxIP Address: 020.002.000.000

Port1 VCI: VCIaxIP Mask: 255.255.000.000

Channel 1

10 Set up in-band management connections on the CPU module of Node B:

Example:

Slot<Slot> VPI: VPIabIP Address: <NMS net. addr>

Port1 VCI: VCIabIP Mask: <NMS net. mask>

Channel 1

Slot<Slot> VPI: VPIbcIP Address: 020.001.001.000

Port1 VCI: VCIbcIP Mask: 255.255.255.000

Channel 1

Slot<Slot> VPI: VPIbdIP Address: 020.001.002.000

Port1 VCI: VCIbdIP Mask: 255.255.255.000

Channel 1

11 Set up in-band management connections on the CPU module of Node C:

Example:

Slot<Slot> VPI: VPIbcIP Address: <NMS net. addr>

Port1 VCI: VCIbcIP Mask: <NMS net. mask>

Channel 1

Slot<Slot> VPI: VPIceIP Address: 020.001.001.003

Port1 VCI: VCIceIP Mask: 255.255.255.000

Channel 1

Slot<Slot> VPI: VPIcfIP Address: 020.001.001.004

Port1 VCI: VCIcfIP Mask: 255.255.255.000

Channel 1

12 Set up in-band managment connections on the CPU module of Node E:

Example:

Slot<Slot> VPI: VPIceIP Address: <NMS net. addr>

Port1 VCI: VCIceIP Mask: <NMS net. mask>

Channel 1

13 Verify that a routing table entry from the SUN machine's network to network 20.0.0.0 exists on the SUN machine using the "netstat -nr" command.

14 Use ping, telnet, rlogin and ftp from the SUN machine to nodes A, B, C, E and F to test the TCP/IP connectivity.

End

Using the Hybrid Connection Configuration

The main router PSAX system (Node A) has two or more connections to remote PSAX systems that are in the same in-band subnet as the Node A PSAX system.

Default gateways through in-band connections can be configured on all remote PSAX systems (that is, all PSAX systems except Node A) with the IP address of Node A's in-band interface. In this case, in-band connections on remote PSAX systems should be configured with Node A's in-band IP address and a default gateway should be set to Node A's in-band IP address.

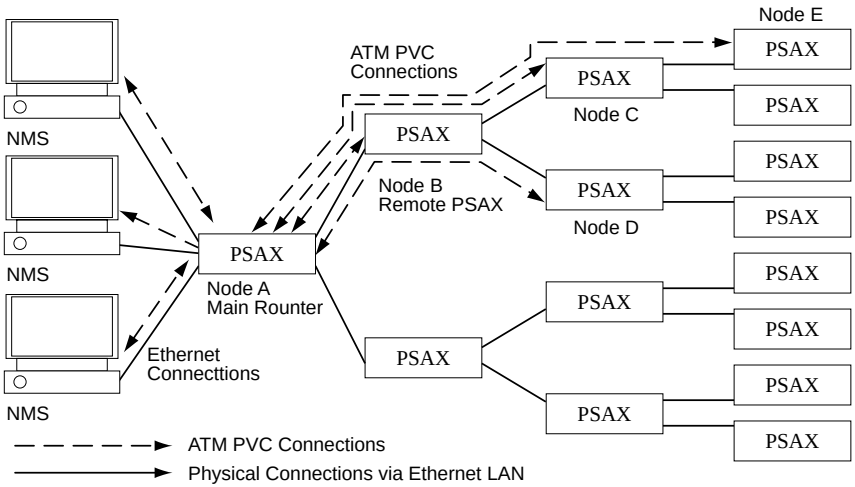

Figure C-3. Hybrid Connection Configuration

Perform the steps in the following procedure to configure a hybrid connection.

Steps to Setting Connections for Hybrid Connection Configuration

Begin

1. In the hybrid connection type, Ethernet to in-band network routing as well as ATM channel tunneling is used. Log in as root on the SUN machine and add a routing table entry using "route add" command:

route add net < *In-Band network address*> <*PSAX IP address on Ethernet*> <*metric*>

where the in-band network address = 20.0.0.0

PSAX IP address on Ethernet = {Check Site Specific Configuration -> Site Specific Configuration -> IP AddrPSAX systemess on the main router PSAX system [node A]}

metric = 10

2. In this configuration, only one PSAX system can act as the router to channel traffic from Ethernet to the in-band network. This is the main router PSAX system. The main router PSAX system has direct ATM connections to all remote PSAX systems. (These connections may be tunneled through a number of switches.)

3. On the main router PSAX system, the in-band management interface (primary) should be assigned an IP address that is on a different network than that of its Ethernet interface.

4 For all the PSAX systems except the main router PSAX system, the Ethernet interface IP network should be different from the SUN machine's Ethernet interface IP network.

5 All of the NMS stations should be in the one IP network, but can be in different subnets connected to the main router PSAX system via Ethernet or OC3-ATM connections.

6 All the end system and router PSAX system in-band interface IP addresses may or may not be in the same IP network. For each different IP network, a route should be configured on each of the NMS station (SUN machine) to use the main router PSAX system as gateway to that network. (The metric should be set to 2).

7 The default gateway can be configured on the remote PSAX system to use the main router PSAX system as a gateway.

8 The main router PSAX system should be configured with in-band connections to each of the remote PSAX systems.

9 The remote PSAX system should have only one connection to the NMS station's network and the appropriate mask if the main router PSAX system is not used as default gateway by the remote PSAX system.

10 If the main router PSAX system is used as a default gateway by the remote PSAX system, then the remote PSAX system should have only one in-band connection to the main router PSAX system, the in-band IP address.

End

Setting PVC Connections for Hybrid Connection Configuration

Assume that the VPI: VCI for connection between node A and B is VPIab: VCIab and so on. Also assume that the Ethernet IP address of all nodes, except node A, do not lie in the NMS stations' network address range.

Steps to Setting PVC Connections for Hybrid Connection Configuration

Begin

Either work from the console or the *AQueView* screen. *AQueview* directions are in the *AQueView* guide.

Perform the steps in the following procedure to set PVC connections for hybrid connection.

1 Configure the primary IP address for in-band management on the CPU module of the main router PSAX system (Node A) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.001

Primary IP Mask: 255.000.000.000

2 Configure the primary and backup IP Address for in-band management on the CPU module of the intermediate router PSAX system (Node B) using the console interface:

Example:

Primary IP Address: 020.001.001.2

Primary IP Mask: 255.000.000.000

3 Configure the primary IP address for in-band management on the CPU module of the main router PSAX system (Node C) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.003

Primary IP Mask: 255.000.000.000

4 Configure the primary IP Address for in-band management on the CPU module of main router PSAX system (Node D) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.004

Primary IP Mask: 255.000.000.000

5 Configure the primary IP address for in-band management on the CPU module of main router PSAX system (Node E) using the console interface:

Use **[Site Specific Configuration]->[In-Band Management]** menu.

Example:

Primary IP Address: 020.001.001.005

Primary IP Mask: 255.000.000.000

6 Set up in-band management connections on the CPU module of Node A to a remote PSAX system:

For setting up an in-band connection from the DS3 card to the CPU module, configure the DS3 card and put it into service. Then using the console interface **[Connection Configuration]-> [In-Band Management IP PVC] -> [Add Connection]** screen, configure the PVC to the FORECARD.

Example:

Slot<Slot>VPI: VPIabIP Address: 020.001.001.002

Port1 VCI: VCIabIP Mask: 255.000.000.000

Channel 1

Slot<Slot>VPI: VPIacIP Address: 020.001.001.003

Port1 VCI: VCIacIP Mask: 255.000.000.000

Channel 1

Slot<Slot>VPI: VPIadIP Address: 020.001.001.004

Port1 VCI: VCIadIP Mask: 255.000.000.000

Channel 1

Slot<Slot>VPI: VPIaeIP Address: 020.001.001.005

Port1 VCI: VCIaeIP Mask: 255.000.000.000

Channel 1

7 Set up in-band management connections on the CPU module of each of the Nodes B,C,D,and E:

Example:

Node B

Slot<Slot>VPI: VPIabIP Address: <NMS net. addr>

Port1 VCI: VCIabIP Mask: <NMS net. mask>

Channel 1

Node C

Slot<Slot>VPI: VPIacIP Address: <NMS net. addr>

Port1 VCI: VCIacIP Mask: <NMS net. mask>

Channel 1

Node D

Slot<Slot>VPI: VPIadIP Address: <NMS net. addr >

Port1 VCI: VCIadIP Mask: <NMS net. mask>

Channel 1

Node E

Slot<Slot>VPI: VPIaeIP Address: <NMS net. addr>

Port1 VCI: VCIaeIP Mask: <NMS net. mask>

Channel 1

8 Verify that a routing table entry from the SUN machine's network to network 20.0.0.0 exists on the SUN machine using the **netstat -nr** command:

9 Use ping, telnet, rlogin and ftp from the SUN machine to nodes A, B, C, E and F to test the TCP/IP connectivity.

End

D ATM Traffic Descriptors

Overview of This Appendix

This appendix describes how each traffic descriptor affects the ATM cell streams under different traffic conditions. When you create a PVC, you can select one of several traffic descriptors. The traffic descriptor specifies which traffic parameters are used for traffic control. It also determines the number and type of cells that are admitted into a congested queue, and whether high-priority cells are tagged as low-priority cells when traffic exceeds the traffic parameter thresholds.

Connections Supporting Traffic Descriptors

The traffic descriptors used in the *PacketStar* Access Concentrator system software are selected on the user interface windows for the following types of connections:

- ATM-to-ATM VCC PVC connection
- ATM-to-ATM VPC PVC connection
- Bridge-to-ATM VCC PVC connection
- Circuit Emulation-to-ATM VCC PVC connection
- Frame Relay-to-ATM VCC PVC connection
- In-band ATM PVC connection
- VBR-to-ATM VCC PVC connection

Traffic Descriptors Supported

The traffic descriptors available for these connections types are as follows (the values as they appear on the window are shown in parentheses):

- Best effort (Best-effort)

  This traffic descriptor allows the system to attempt to send all cells in a "best effort" fashion, without specifying traffic parameters, similar to the *AQueMan* algorithm. The Access Concentrator might drop some or all cells during congestion.

- Best effort with tagging (Best-effort-tag)

  This traffic descriptor allows the system to tag all CLP=0 (high priority) cells to change them to CLP=1 (low priority) cells, and then attempt to send all cells in a "best effort" fashion, without specifying any other traffic parameters, similar to the *AQueMan* algorithm. The network might drop some or all cells during congestion.

- One bucket, with no tagging for cells with both CLP bit=0 and CLP bit=1 (1B-NT-0+1)

  This traffic descriptor uses the parameters one bucket, no tagging, cell loss priority (CLP)=0+1 cells (high and low priority). The Access Concentrator ignores the CLP bit value and drops all cells violating the value set for the peak cell rate (PCR).

- Two buckets, with no tagging for cells with both CLP bit=0 and CLP bit=1 (2B-NT-0+1-0+1)

  This traffic descriptor uses the parameters two buckets, no tagging, CLP=0+1 cells (high and low priority) for bucket 1, and CLP=0+1 cells (high and low priority) for bucket 2. The Access Concentrator ignores the CLP bit value for cells passing into bucket 1 and drops all cells violating the value set for the PCR. The remainder of the cells are passed to bucket 2. The Access Concentrator ignores the CLP bit value for cells passing into bucket 2, and drops all cells violating the value set for the sustainable cell rate (SCR).

- Two buckets, with no tagging for cells with both CLP bit=0+1 and CLP bit=0 (2B-NT-0+1-0)

  This traffic descriptor uses the parameters two buckets, no tagging, CLP=0+1 cells (high and low priority) for bucket 1, and CLP=0 cells (high priority) for bucket 2. For bucket 1, the Access Concentrator ignores the CLP bit value for cells passing into bucket 1 and drops all cells violating the value set for the PCR. For bucket 2, the system takes one of the following actions:

  ~ When the connection is configured for variable bit rate (VBR) traffic, the Access Concentrator drops all CLP=0 cells violating the value set for the SCR in bucket 2.

  ~ When the connection is configured for constant bit rate (CBR) traffic, the Access Concentrator drops all CLP=0 cells violating the value set for the PCR in bucket 2.

- Two buckets, for cells with CLP bit=0 and CLP bit=0 (2B-NT-0+1-0)

  This traffic descriptor uses the parameters two buckets, tagging, CLP=0+1 cells (high and low priority) for bucket 1, and CLP=0 cells (high priority) for bucket 2. For bucket 1, the Access Concentrator ignores the CLP bit value for cells passing into bucket 1 and drops all cells violating the value set for the PCR. For bucket 2, the system takes one of the following actions:

  ~ When the connection is configured for variable bit rate (VBR) traffic, the Access Concentrator tags all CLP=0 cells violating the value set for the SCR to CLP=1 in bucket 2.

  ~ When the connection is configured for constant bit rate (CBR) traffic, the Access Concentrator tags all CLP=0 cells violating the value set for the PCR to CLP=1 in bucket 2.

  The network then might drop some or all cells during congestion.

E Reference Tables

Overview of This Appendix

This appendix contains reference tables which will be helpful to you in many situations. The information is organized as follows.

- QoS Information Tables
- Compliance Matrix
- Alarm Status Tables
- Connection Type by Interface Type Table
- Interface Type by Module Table

QoS Information Tables

Table E-1 details the Access Concentrator system support of defined ATM quality of service (QoS) classes.

Table E-1. Access Concentrator System-Supported Service Classes

ATM Service Class	Description
Constant Bit Rate (CBR)	Service that operates on a connection basis and offers consistent delay predictability; used for applications such as circuit emulation, voice, and video.
Variable Bit Rate—Real Time (VBR-RT)	Service that operates on a connection basis and offers very low delay variance but requires access to a variable amount of network bandwidth; used for such applications as packet video and voice.

Table E-1. Access Concentrator System-Supported Service Classes

ATM Service Class	Description
Variable Bit Rate—Nonreal Time (VBR-NRT)	Service that operates on both a connection and connectionless basis and allows delay variance between the delivery of cells; used for data applications that have potentially bursty traffic characteristics, including LAN interconnect, CAD/CAM, and multimedia. This class can be used to support SMDS (switched multimegabit data service).
Unspecified Bit Rate (UBR)	Service that operates on a connection basis and allows for raw cell or best-effort transport by the network. In this service, cells are transported by the network whenever bandwidth is available and traffic is presented by the user. Data using UBR service is more apt to be discarded during peak traffic times in deference to data using other classes of service.

Table E-2 illustrates the attributes of the classes of service supported by the Access Concentrator system software.

Table E-2. Class of Service Descriptions

	Constant Bit Rate (CBR)	Real Time (VBR-RT)	Nonreal Time (VBR-NRT)	Unspecified Bit Rate (UBR)
QoS Class	Class 1	Class 2	Classes 3, 4	Class 5
Applications	Voice and video	Packet video and voice	Data	
Bit Rate	Constant	Variable		
Timing Required Source/ Destination	Required		Not required	
Service Examples	Private line	Compressed voice	Frame relay, Switched multimedia data service	Raw cell, Ethernet
AAL	1	2	3/4 and 5	3/4 and 5

The following two tables illustrate how ATM classes of service map to internal priority levels to structure the *AQueMan*™ algorithm. Table E-3 identifies the cell-loss and cell-delay tolerance of each service class. Table E-4 on page -3 lists the class-of-service choices available when configuring PVC connections on an Access Concentrator system and shows service level examples for each PVC connection type.

The examples are intended simply as illustrations and will need fine tuning based on the network applications supported by the Access Concentrator

system. The flexibility of the Access Concentrator systems allows the user to tailor the system based on the required service applications and the selection of the appropriate priority levels.

Table E-3. Cell-Loss and Cell-Delay Characteristics of ATM Service Classes

ATM Classes of Service	QoS Class Supported by AC Systems	Cell Loss Tolerance	Cell Delay Tolerance	Internal Priority
Constant Bit Rate (CBR)	Class 1	High	Very Low	CBR-1
	Class 1	High	Very Low	CBR-2
	Class 1	High	Low	CBR-3
	Class 1	High	Low	CBR-4
Variable Bit Rate (VBR)	Class 2	Very Low	Very Low	VBR-1
	Class 2	Low	Low	VBR-2
Variable Bit Rate, Real Time (VBR-RT)	Class 2	Low	Low	VBR-3
Variable Bit Rate, Nonreal Time (VBR-NRT)	Classes 3, 4	Low	Medium	VBR-4
	Classes 3, 4	Low	High	VBR-5
Unspecified Bit Rate (UBR)	Class 5	Very High	Very High	VBR-6

Table E-4. Mapping ATM Service Classes to Access Concentrator Systems Priority Levels

ATM Classes of Service	Internal Priority	PVC Connection Configuration Selections	Service Examples
Constant Bit Rate (CBR)	CBR-1	CBR1	911 calls
	CBR-2	CBR2	Preferred customers
	CBR-3	CBR3	Standard
	CBR-4	CBR4	Cellular
Variable Bit Rate (VBR)	VBR-1	VBR-express	Network management
Variable Bit Rate	VBR-2	VBR-RT1	Real-time videos
Real Time (VBR-RT)	VBR-3	VBR-RT2	MPEG1-2/JPEG
Variable Bit Rate	VBR-4	VBR-NRT1	FR data
Nonreal Time (VBR-NRT)	VBR-5	VBR-NRT2	FTP/e-mail transfer
Unspecified Bit Rate (UBR)	VBR-6	UBR	IP data

Compliance Matrix

The following table contains compliance specifications for the Access Concentrator systems, and the I/O and server modules as described in Table E-5.

Table E-5. Compliance Specifications

Name	Partial Title	Notes
ITU-T E.164	Overall Network Operation, telephone service, service operation, and human factors: Operation, numbering, routing and mobile services International operation- Numbering plan of the international telephone service	
ITU-T G.164	Transmission Systems and Media Apparatus Associated with Long-Distances Telephone Circuits and Other Terminal Equipments: Echo Suppressors	Fax/modem detection
ITU-T G.165	General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers	Echo cancellation (general)
ITU-T G.702	General Aspects of Digital Transmission Systems— Terminal Equipments: Digital Hierarchy Bit Rates	
ITU-T G.703	Physical/Electrical Characteristics of Hierarchical Digital Interfaces	
ITU-T G.704	Synchronous frame structures used at 1544, 6312, 2048, 8488 and 44 736 Kbit/s hierarchical levels	Comply for 1.544 Mbps, 2.048 Mbps, 44.736 Mbps. Includes channel-associated signaling (CAS) ABCD in-band signaling
ITU-T G.706	Frame alignment and cyclic redundancy check (CGC) procedures relating to basic frame structures defined in Recommendation G.704	
ITU-T G.707	Transmission Systems and Media—Digital transmission systems— Terminal equipments— General: Network node interface for the synchronous digital hierarchy (SDH)	
ITU-T G.711	General Aspects of Digital Transmission Systems Terminal Equipments: Pulse Code Modulation (PCM) of Voice Frequencies	64 Kbps fax encoding

Table E-5. Compliance Specifications

Name	Partial Title	Notes
ITU-T G.726	General Aspects of Digital Transmission Systems Terminal Equipments: 40, 32, 24, 16 Kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)	Voice compression (16, 24, 32, 40 Kbps) and tandem encoding
ITU-T G.729	General Aspects of Digital Transmission Systems: Coding of Speech at 8 Kbit/s Using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP)	Annex A: Voice compression (8 Kbps), Annex B: Silence suppression
ITU-T G.732	General Aspects of Digital Transmission Systems Terminal Equipments: Characteristics of Primary PCM Multiplex Equipment Operating at 2048 Kbit/s	
ITU-T G.736	General Aspects of Digital Transmission: Characteristics of a Synchronous Digital Multiplex Equipment Operating at 2048 kbits/sec	
ITU-T G.751	Digital multiplex equipments operating at the third order bit rate of 34 368 kbit/s and the fourth order bit rate of 139 264 kbit/s and using positive justification	
ITU-T G.783	Transmission Systems and Media, Digital Systems and Networks— Digital Transmission Systems—Terminal Equipments—Principal Characteristics of Multiplexing Equipment for the Synchronous Digital Hierarchy: Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks	
ITU-T G.804	ATM cell mapping into Plesiochronous Digital Hierarchy (PDH)	
ITU-T G.823	The control of jitter and wander within digital networks which are based on the 2048 Kbit/s hierarchy	
ITU-T G.832	Transmission Systems and Media, Digital Systems and Networks— Digital transmission systems—Digital networks— Network capabilities and functions: Transport of SDH Elements on PDH Networks—Frame and Multiplexing Structures	Includes Multiplex Section Protection (MSP)
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy	Intra-office and short haul supported (not long haul).

Table E-5. Compliance Specifications

Name	Partial Title	Notes
ITU-T I.121	Integrated Services Digital Network (ISDN) General Structure and Service Capabilities: Broadband Aspects of ISDN	
ITU-T I.150	B-ISDN ATM Functional characteristics	
ITU-T I.233	Frame Mode Bearer Services	
ITU-T I.321	Integrated Services Digital Network (ISDN) Overall Network Aspects and Functions, ISDN User-Network Interfaces: B-ISDN Protocol Reference Model and its Application	
ITU-T I.356	B-ISDN ATM layer cell transfer performance	No ABR
ITU-T I.361	B-ISDN ATM Layer Specification	
ITU-T I.363	B-ISDN ATM Adaptation Layer specification	Only AAL1, AAL2, and AAL5 are supported
ITU-T I.363.1	B-ISDN ATM Adaptation Layer specification: Type 1 AAL	
ITU-T I.363.2	B-ISDN ATM Adaptation Layer specification: Type 2 AAL	Multiplexing support
ITU-T I.363.5	B-ISDN ATM Adaptation Layer specification: Type 5 AAL	
ITU-T I.366.1	Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL type 2	
ITU-T I.370	Congestion Management for ISDN Frame Relay Bearing Service	Enhanced DS1 and Enhanced E1 modules
ITU-T I.371	Traffic control and congestion control in B-ISDN	No ABR
ITU-T I.372	Integrated Services Digital Network (ISDN) Overall Network Aspects and Functions: Frame Relaying Bearer Service Network-to-Network Interface Requirements	
ITU-T I.413	Integrated Services Digital Network (ISDN) User-Network Interfaces: B-ISDN User-Network Interface	
ITU-T I.431	Integrated Services Digital Network (ISDN) User-Network Interfaces: Primary Rate User-Network Interface—Layer 1 Specification	
ITU-T I.432	B-ISDN User-Network Interface—Physical layer specification	Includes scrambling, header error control (HEC) processing, cell delineation

Table E-5. Compliance Specifications

Name	Partial Title	Notes
ITU-T I.610	B-ISDN operation and maintenance principles and functions	OAM F4/F5 processing (remote defect indication [RDI] and alarm indication signal [AIS])
ITU-T Q.922 Annex A	Digital Subscriber Signaling System No.1 (DSS 1) Data Link Layer: ISDN Data Link Layer Specification for Frame Mode Bearer Services	
ITU-T Q.931	Switching and Signaling - Digital subscriber Signalling System No. 1 - Network layer: Digital Subscriber Signaling System No. 1 (DSS 1) - ISDN User-Network Interface Layer 3 Specification for Basic Call Control	• AAL1 Trunking CCS (Q.931) • AAL1 Trunking CCS (Q.931/QSIG), AAL1 Trunking CAS • AAL2 Trunking CCS (Q.931)
ITU-T Q.933 Annex A	Digital Subscriber Signaling System No. 1—Integrated Services Digital Network (ISDN) Digital Subscriber Signaling System No. 1 (DSS 1)—Signaling Specifications for Frame Mode Switched and Permanent Virtual Connection Control and Status Monitoring	
ITU-T Q.2931	B-ISDN Application protocols for access signalling—Broadband Integrated Services Digital Network (B-ISDN)— Digital Subscriber Signalling System No. 2 (DSS 2)—User Network Interface (UNI) Layer 3 Specification For Basic Call/Connection Control	
ITU-T Q.2971	B-ISDN—DSS 2—User-network interface layer 3 specification for point-to-multipoint call/connection control	
V.35	Defines signaling for data rates greater than 19.2 Kbps for a trunk interface between network access device and a packet network	Multi-Serial module
X.21 bis	Interface between Data Terminal equipment and data circuit-terminating equipment for synchronous operation on public data networks	Multi-Serial module
X.144	User information transfer performance parameters for data networks providing international frame relay PVC service	
af-ilmi-0065.000	Integrated Logical Management Interface (ILMI)	

Table E-5. Compliance Specifications

Name	Partial Title	Notes
af-phy-0086.000	Inverse Multiplexing over ATM (IMA)	Up to 3 groups, with up to six circuits per group
af-pnni-0026.000	Interim Inter-Switch Signaling Protocol (IISP)	
af-pnni-0055.000	Private Network-Network Interface (PNNI)	Annex G, mandatory requirements; Annex C, Soft permanent virtual circuits (SPVCs) for circuit emulation, frame relay, and terminal emulation
af-uni-0010.001	User-Network Interface (UNI) 3.0	
af-uni-0010.002	User-Network Interface (UNI) 3.1	
af-vtoa-0078.000	Circuit Emulation Service 2.0	Includes 56 (DS1), Nx64 (DS1, E1)
af-vtoa-0085.000	(DBCES) Dynamic Bandwith Utilization in 64 Kbps Time Slot Trunking Over ATM—Using Circuit Emulation Service (CES)	• AAL1 Trunking CCS (Q.931) • AAL1 Trunking CCS (Q.931/QSIG), AAL1 Trunking CAS
af-vtoa-0089.000	ATM Trunking Using AAL1 for Narrow Band Services V1.0	AAL2 Trunking
af-vtoa-0119.000	Low Speed Circuit Emulation Service	
IEEE 802.1d	MAC Bridges	Spanning Tree Protocol
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications	Ethernet module
IETF RFC 1157	Simple Network Management Protocol (SNMP) Version 1.0	
IETF RFC 1483	Multi-Protocol Encapsulation and Layer 2 Bridging Service	Ethernet module
IETF RFC 1490	Multiprotocol Interconnect over Frame Relay	Route Server module
GR-63-CORE	Network Equipment Building Standards (NEBS): Physical Protection	
GR-1089-CORE	Electromagnetic Compatibility and Electrical Safety—Generic Criteria for Network Telecommunications Equipment	NEBS
ANSI T1.101	Telecommunications - Synchronization Interface Standard Stratum synchronization	

Table E-5. Compliance Specifications

Name	Partial Title	Notes
RS-232	Electrical, mechanical,and functional standards for communication between computers, terminals and modems	Multi-serial module
RS-449	Faster version of RS-232-C; capable of longer cable runs	Multi-serial module, High Speed module
RS-530	Defines mechanical/electrical interfaces between DTEs and DCEs that transmit serial binary data	Multi-serial module, High Speed module
FRF.1.1	User-to-Network (UNI) Implementation Agreement	
FRF.2.1	Frame Relay Network-to-Network (NNI) Implementation Agreement LMI services between two NNI services	link management interface (LMI) services between two network-network interface (NNI) services
FRF.5	Frame Relay ATM/PVC Network Internetworking Implementation Agreement	
FRF.8	Frame Relay ATM/PVC Service Internetworking Implementation Agreement	
others	EN50082-1, EN55022, EN60950, EN61000-3-2, EN61000-4-5, EN61000-4-6, CSA-C22.2 (No 950-95), IEC950, TS001, AS3548, VCCI (Class 2), ICES-003 (Industry Canada), CISPR22 (with Nordic variations), Class A FCC Part 15, FCC Part 68, 3rd Edition UL	

Alarm Status Table

The Alarm Status field on the Equipment Configuration window displays the current status of all *PacketStar* I/O, server , and common equipment module in your PSAX Access Concentrator system. The alarm status descriptions are provided in Table E-6.

Table E-6. Alarm Status Descriptions for PSAX Access Concentrator Modules

Number	Alarm Status	Module Type Affected	Description
1	NoAlarm/CardPresent	I/O	No module is inserted in the chassis.
2	WrongCardType	I/O	One type of module was configured in this slot in the chassis, but a different module now occupies this slot.
3	LineFailed	All	The line has failed.

Table E-6. Alarm Status Descriptions for PSAX Access Concentrator Modules

Number	Alarm Status	Module Type Affected	Description
4	CardRemoved	All	A module has been configured and then removed.
5	ReferenceClockFailed	Stratum	The timing reference clock has failed.
6	CompositeClockFailed	Stratum	The timing composite clock has failed.
7	Overload	Power Supply	The Power Supply is operating under an overload condition.
8	Plus5vFailed	Power Supply	The 5 V Power Supply has failed.
9	Plus120vFailed	Power Supply	The 120 V ac Power Supply has failed.
10	Minus48vFailed	Power Supply	The -48 V dc Power Supply has failed.
11	UnknownAlarm	I/O	The reason for failure is not known.
12	CompleteClockFailed	Stratum	The timing complete clock has failed.
13	BackplaneCircuitryFailed	All	The chassis backplane circuit board is not operating.
14	PowerFailed	Power Supply	Power failed

Connection Type by Interface Type Table

Table E-7. Interface Types by Connection Types

Interface / Connection	ATM IISP (Network/User)	ATM IMA	ATM PNNI 1.0	ATM UNI 3.0/3.1/4.0	Bridge	Circuit Emulation	Dynamic Bandwidth Circuit Emulation	Frame Relay (UNI, NNI)	HDLC Pass-through	PRI ISDN (Network/User)	Terminal Emulation
AAL-2 Trunking connection	X		X	X		X					
ATM-to-ATM virtual channel connection (VCC) PVC connection	X		X	X							

Table E-7. Interface Types by Connection Types

Interface / Connection	ATM IISP (Network/User)	ATM IMA	ATM PNNI 1.0	ATM UNI 3.0/3.1/4.0	Bridge	Circuit Emulation	Dynamic Bandwidth Circuit Emulation	Frame Relay (UNI, NNI)	HDLC Pass-through	PRI ISDN (Network/ User)	Terminal Emulation
ATM-to-ATM virtual path connection (VPC) PVC connection	X	X	X	X							
Bridge-to-ATM VCC PVC connection	X	X	X	X	X						
Bridge-to-bridge PVC connection					X						
Circuit emulation-to ATM VCC PVC connection	X	X	X	X		X	X				
Circuit emulation-to circuit emulation PVC connection						X	X				
Frame relay-to-ATM VCC PVC connection	X	X	X	X				X			
Frame relay-to-frame relay PVC connection								X			
In-band management ATM PVC connection	X	X	X	X							
Variable bit rate (VBR)-to-ATM VCC PVC connection	X	X	X	X					X		X
VBR-to-VBR PVC connection	X	X	X	X					X		X

Table E-7. Interface Types by Connection Types

Interface / Connection	ATM IISP (Network/User)	ATM IMA	ATM PNNI 1.0	ATM UNI 3.0/3.1/4.0	Bridge	Circuit Emulation	Dynamic Bandwidth Circuit Emulation	Frame Relay (UNI, NNI)	HDLC Pass-through	PRI ISDN (Network/ User)	Terminal Emulation
ATM-to-ATM IISP constant bit rate (CBR) SVC connection	X		X	X		X	X				
ATM-to-ATM IISP VBR SVC connection	X		X	X							
ATM-to-ATM VCC SPVC connection	X	X	X	X							X
Circuit emulation-to-ATM VCC SPVC connection	X	X	X	X		X	X				
Frame relay-ATM VCC SPVC connection	X	X	X	X				X			
VBR-to-ATM VCC SPVC connection	X	X	X	X							X

Interface Type by Module Table

Table E-8 shows the available interface types for each *PacketStar*™ I/O module in the Access Concentrator system. This table does not include other *PacketStar*™ modules that are not I/O modules, which include: the Alarm

module, the DSP2A/B/C Voice Server modules, the Route Server module, and the Tones and Announcements Server module.

Table E-8. Interface Types by I/O Module Types

Module	ATM IISP (Network/User)	ATM IMA	ATM PNNI 1.0	ATM UNI 3.0/3.1	Bridge	Circuit Emulation	Dynamic Bandwidth Circuit Emulation	Frame Relay (UNI, NNI)	HDLC Pass-through	PRI ISDN (Network/ User)	Terminal Emulation
Channelized DS3 (multi-function)	X		X	X		X		X	X	X	
Channelized STS-1e (T1) (multi-function)	X		X	X		X		X	X	X	
DS1 IMA	X	X	X								
DS3 ATM	X		X	X							
DS3 Frame Relay								X			
DS3 IMA	X	X	X	X							
E1 IMA	X	X	X								
E3 ATM	X		X	X							
Enhanced DS1 (multi-function)	X		X	X		X	X	X	X	X	
Enhanced E1(multi-function)	X		X	X		X		X	X	X	
Ethernet					X						
High-Density E1 (21-port)	X		X	X		X		X	X	X	
High Speed	X			X		X (port 2 only)					
Medium-Density DS1 (12-port)	X		X	X		X		X	X	X	
Multi-Serial				X		X		X	X		X
OC-3c (six types): MMAQ, MMTS, SMAQ, SMTS, MM 1+1 APS, SM 1+1 APS	X		X	X							

Table E-8. Interface Types by I/O Module Types

Module	ATM IISP (Network/User)	ATM IMA	ATM PNNI 1.0	ATM UNI 3.0/3.1	Bridge	Circuit Emulation	Dynamic Bandwidth Circuit Emulation	Frame Relay (UNI, NNI)	HDLC Pass-through	PRI ISDN (Network/ User)	Terminal Emulation
STM-1 (six types): MMAQ, MMTS, SMAQ, SMTS, MM 1+1 MSP, SM 1+1 MSP	X		X	X							
Voice 2-Wire Office						X					
Voice 2-Wire Station						X					

Index

A

accessing a PSAX device
  using a serial port interface 3-9
  using an Ethernet interface connection on a LAN 3-10
  using in-band management 3-10
Adaptive Queue Management (AQueMan) 3-2
analog 3-64
ATM interface management entities (IME) 3-2
ATM interface management information base (MIB) 3-2
ATM Routing Properties 4-12

B

Bridge management 3-20

C

Caller ID frequency shift keying 3-72
capabilities
  system 3-1
CBR voice traffic 3-58
cell test diagnostics
  running 5-5
channel-associated signalling (CAS) 3-56, 3-60
Comfort noise 3-73
connection gateway application programming interface 3-2
connection types
  ATM IISP CBR E-12
  ATM IISP VBR E-12
  ATM-to-ATM VCC E-10, E-11
  bridge-to-ATM VCC E-11
  bridge-to-bridge E-11
  circuit emulation-to-ATM VCC E-11
  circuit emulation-to-circuit emulation E-11
  frame relay-to-ATM VCC E-11
  frame relay-to-frame relay E-11
  VBR-to-ATM VCC E-11
  VBR-to-VBR E-11
Connector Type
  DS1 IMA Module 3-47
  DS3 ATM Module 3-48, 3-51
  DS3 Frame Relay Module 3-49, 3-52
  E3 ATM Module 3-54
  Ethernet Module 3-58
  High Speed Module 3-59
  Multi-Serial Module 3-63
cyclic redundancy check multi-frequency (CRC-mf) 3-57, 3-61

D

Data Transmission Rate
  High Speed Module 3-59
  Multi-Serial Module 3-64
Digital Signal Level 3 (DS3) 3-48, 3-51
DS0s 3-56
dual-homed permanent virtual circuit (DHPVC) 3-2, 3-12
Dual-tone multifrequency 3-73

E

Ethernet interfaces 3-58
Ethernet MIBs 3-20

F

Facsimile/modem call sequence detection 3-73
Filtering 3-20
flash signalling 3-72

H

HDLC data links 3-56

I

IMA groups 3-53
in-band management 4-24
In-Band Management Configuration Data 4-30
integrated local management interface (ILMI) 3-2
Interfaces
    High Speed Module
        Parallel Port 3-59
        Serial Port 3-59
    Multi-Serial Module 3-64
Inverse multiplexing over ATM (IMA) 3-2

L

LANET protocol 3-58
LED indicators 3-56, 3-58
Limitless ATM Network (LANET) 3-2
Line Rate
    DS1 IMA Module 3-47
    DS3 ATM Module 3-48, 3-51
    DS3 Frame Relay Module 3-48, 3-51
    E3 ATM Module 3-53
    Enhanced E1 Module 3-56
    High-Speed Module 3-58
    Multi-Serial Module 3-61
    OC-3c Modules 3-65
    STM-1 Modules 3-67
line rate 3-59
logging on the PSAX system 4-1

M

MAC layer data 3-20
media access control (MAC) layer 3-58
MIB, object definitions A-43
MIB, see management information base A-43
Mu-law/A-law pulse code modulation 3-73

N

Near-end echo cancellation 3-73

O

OAM
    performing tests 5-26, 5-28
operations and maintenance (OAM) 3-3

P

passwords
    changing 4-7
Performance 3-20
permanent virtual circuit (PVC) 3-65
PNNI
    link table 4-62
    map link table 4-58
    neighbor peer table 4-68
private network-network interface (PNNI) 3-2
private-line automatic ring-down (PLAR) 3-65
Protocols
    DS1 IMA Module 3-47, 3-50
    High Speed Module 3-59
    Multi-Serial Module 3-64

R

rebooting system components 5-9
removing configuration files 5-11

S

Silence Detection 3-73
Simple Network Management Protocol (SNMP) 3-2, 3-75, A-1
soft permanent virtual circuit (SPVC) 3-2
Spanning Tree Algorithm and Protocol 3-20
structured circuit emulation service 3-56, 3-59
switched virtual circuits (SVC) 3-2

T

TCP Server Configuration Data 4-17
TIA/EIA-464-B Requirements for Private Branch Exchange (PBX) Switching Equipment 3-72
time-division multiplex (TDM) 3-56
trap messages, see Simple Network Management Protocol (SNMP) A-1

U

Using System Diagnostics 5-1

V

VBR data traffic 3-58
virtual port 3-58
virtual private networks 3-74
Voice compression 3-73

Printed in the USA.
Doc. No.: 255-700-020
Part No.: 20M2A6303A1

Printed on paper with 100%
total recycled content.
Please recycle.

Lucent Technologies
Bell Labs Innovations