8260 Nways Multiprotocol Switching Hub
8285 Nways ATM Workgroup Switch

ATM Control Point Version 3 User's Guide

SA33-0452-00

8260 Nways Multiprotocol Switching Hub
8285 Nways ATM Workgroup Switch

ATM Control Point Version 3 User's Guide

SA33-0452-00

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page xi.

First Edition (March 1997)

The information contained in this manual is subject to change from time to time. Any such changes will be reported in subsequent revisions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

IBM France
Centre d'Etudes et Recherches
Service 0798 - BP 79
06610 La Gaude
France

- FAX: (33) (0)4.93.24.77.97
- E-mail: FRIBMQF5 at IBMMAIL
- IBM Internal Use: LGERCF AT LGEPROFS
- Internet: rcf_lagaude@vnet.ibm.com

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Corporation, IBM Director of Licensing, 500 Columbus Avenue, Thornwood, New York 10594, U.S.A.

Product Page/Warranties

The following paragraph does not apply to the United Kingdom or to any country where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

Industry Standards Reflected in This Product

The *ATM Control Point and Switch* complies with the following ATM standards:

- ATM User-Network Interface (UNI) Specifications V3.0 and V3.1, ATM Forum
- ATM Interim Inter-Switch Signalling (IISP), ATM Forum
- ATM Public Network-to-Network Interface (PNNI) Phase 1, ATM Forum
- LAN Emulation over ATM Specifications V1.0, ATM Forum
- Q.2110 Service Specific Connection-Oriented Protocol (SSCOP), ITU, March 17, 1994
- Q.2130 Service Specific Coordination Function (SSCF) for support of signaling at the user-network interface, March 17, 1994.

The ATM Control Point and Switch (A-CPSW) module is designed according to the specifications of the following industry standards as understood and interpreted by IBM as of September 1994:

- RFC854 - TELNET protocol
- RFC1350 - Trivial File Transfer Protocol (TFTP)
- RFC1577 - Classical IP and ARP (Address Resolution Protocol) over ATM
- SNMP:
  - RFC1155 - Structure and Identification of Management Information (SMI) for TCP/IP based Internet.
  - RFC1156 - Management Information Base (MIB) for network management of TCP/IP based Internets (MIB-I)
  - RFC1157 - Simple Network Management Protocol (SNMP)
  - RFC1212 - Concise MIB definitions
  - RFC1213 - Management Information Base (MIB) for network management of TCP/IP based Internets (MIB-II)
  - RFC1215 - Convention for defining traps for use with SNMP.

Trademarks and Service Marks

The following terms, denoted by an asterisk (*) in this publication, are trademarks or service marks of the IBM Corporation in the United States or other countries:

AIX
IBM
NetView for AIX
Nways
RISC System/6000
Turboways

About this Book

This book presents information on Version 3 of the ATM Control Point, for use in the IBM 8260 Nways ATM Control Point and Switch Module and 8285 Nways ATM Workgroup Switch.

The ATM commands that you enter at the console to manage the ATM subsystem are described in detail in the *IBM 8260 Nways Multiprotocol Switching Hub*, *IBM 8285 Nways ATM Workgroup Switch*, *ATM Control Point Version 3 Command Reference Guide*, SA33-0453.

Who Should Use this Book

This book is intended for the following people at your site:

- ATM network administrator
- ATM network operator.

How to Use this Book

This book contains seven chapters and two appendixes:

Chapter 1, "Introducing the ATM Control Point Version 3" on page 1 gives an overview of the main functions of the A-CPSW module.

Chapter 2, "ATM Campus Networks" on page 7 describes the components of an ATM Campus Network.

Chapter 3, "Configuring Basic Parameters" on page 15 describes how to configure basic control point parameters.

Chapter 4, "Configuring Network Access Security" on page 17 describes how to enable and configure network access control to prevent unauthorized access to your ATM network.

Chapter 5, "Configuring PNNI Parameters" on page 33 describes how to configure the PNNI system.

Chapter 6, "Configuring Ports and Media Modules" on page 53 describes how to configure ports and media modules.

Chapter 7, "Troubleshooting" on page 63 describes how to diagnose and solve problems associated with the operation of the Control Point Version 3 and ATM subsystem in the 8260/8285

Appendix A, "Error and Information Codes" on page 85 describes the return codes displayed for the Q.2931 protocol and Maintenance mode.

Appendix B, "ATM Address Formats" on page 89 describes the ATM addressing formats.

"Glossary" on page 93 describes the terms and abbreviations used in this manual.

“Bibliography” on page 103 lists the publications that provide additional information regarding the functions and technology of the *ATM Control Point and Switch*.

“Index” on page 105 lists the concepts, terms, and tasks described in this manual and the page numbers on which you can find the information.

Prerequisite Knowledge

To understand the information presented in this book, you should be familiar with:

- Features and characteristics of the IBM 8260 Nways Multiprotocol Switching Hub and *IBM 8285 Nways ATM Workgroup Switch*, as described in *IBM 8260 Nways Multiprotocol Switching Hub Product Description*, GA33-0315. *IBM 8285 Nways ATM Workgroup Switch, Installation and User's Guide*, SA33-0381.
- Features and characteristics of the ATM control Point and Switch Module, as described in *IBM 8260 Nways Multiprotocol Switching Hub Product ATM Control Point and Switch Module Installation and User's Guide*, SA33-0326.
- Principles of Asynchronous Transfer Mode (ATM) technology
- ATM Forum UNI Specification V3.0 and V3.1.
- ATM Forum LAN Emulation Specification V1.0.
- ATM Forum P-NNI Specification V1.0.

Where to Find More Information

The publications for the A-CPSW module and associated product documentation are listed in the “Bibliography” on page 103.

World Wide Web
You can access the latest news and information about IBM network products, customer service and support, and microcode upgrades via the Internet, at the URL:

`http://www.networking.ibm.com`

Terms Used in This Book

The term *Control Point* refers to the ATM Control Point Version 3, located in either the IBM 8260 Nways ATM Control Point and Switch Module or 8285 Nways ATM Workgroup Switch.

The term *Command Reference Guide* refers to the *IBM 8260 Nways Multiprotocol Switching Hub, IBM 8285 Nways ATM Workgroup Switch, Control Point Version 3, Command Reference Guide*, SA33-0453.

Chapter 1. Introducing the ATM Control Point Version 3

This chapter describes the following new functions available with Version 3 of the ATM Control Point, for use in the IBM 8260 hub and 8285 ATM Workgroup switch.

- Implementation of PNNI

  PNNI (private network-to-network interface) automates connections links between ATM switches and improves network performance. With the PNNI protocol, you can let the network determine the optimal route between connections, or you can set weights on the ATM links to favor some lines over others. The PNNI protocol improves LAN emulation network reliability and simplifies its setup.

- Extended ATM connections.

  The Control Point Version 3 supports an extended set of ATM connections, including:

  - Switched (SVC) and permanent (PVC)
  - Point-to-point and point-to-multipoint
  - Reserved Bandwidth (CBR, rt VBR, nrt VBR, minimum cell rate of ABR) and best-effort (UBR).

- Network security access function

  The Control Point Version 3 provides network security by allowing you to control which ATM addresses are allowed access. Unauthorized address registration attempts are rejected.

PNNI Control Point Characteristics

The PNNI control point imbedded in each 8260 switch provides advanced standard-compliant ATM signalling and routing, and has the following characteristics:

Control Plane

- UNI
  - Support of ATM signalling (SVC point-to-point and point-to-multipoint) according to ATM Forum V3.0 and V3.1 specifications.
  - Support of permanent connections (PVC point-to-point and point-to-multipoint). The setting of PVCs is supported in accordance with PNNI Phase 1 Specification (soft-PVC), ATM Forum.
  - Support of internetworking between V3.0 and V3.1 end-systems.
- NNI
  - Support of Interim Inter-Switch Signalling (IISP) according to ATM Forum specifications.
  - Support of Private NNI (P-NNI Phase 1) according to ATM Forum specifications.
  - Support of path selection. Depending on network constraints, connection types and network operator wishes, either precomputed or on-demand paths, and either widest or shortest paths can be selected.
  - Crankback extension. Call rerouting is extended on IISP links.
- VP Tunneling
  - Support of interconnection of ATM campus switches over an ATM WAN providing Permanent Virtual Paths (PVPs). The signalling channel is transparently passed to the WAN.
  - Support of VP multiplexor
  - Support of multiple VPs of differing types (UNI, IISP, PNNI) on the same physical interface.
- Link redundancy
  - Supported on physical and VP tunnel interfaces regardless of interface type (UNI, IISP, or PNNI). Application examples:

    UNI: High throughput required by video servers
    IISP: Redundant attachment to multiple switches of the ATM backbone
    PNNI: High throughput and redundancy required at the ATM campus backbone level
  - Link selection can be based on a load balancing algorithm according to the 'Administrative Weight' defined on the links.
  - Automatic Call Setup rerouting on the next best-fit link in case of failure on the selected link.

- Link Sharing Control
  - Allow the network administrator to limit the proportion of link bandwidth (or VP tunnel) that can be reserved by reserved bandwidth connections (CBR, rt VBR, nrt VBR, UBR, and ABR). This is supported on all interface types (UNI, IISP, PNNI).
- Switch Access
  - Support of Classical IP over ATM (CIP, RFC 1577) for switch management and services.
  - Support of Ethernet and Token-Ring LAN Emulation Client (LEC) for switch management and services.
- LAN Emulations Servers (LES)
  - Support of LES and Broadcast Unknown Server (BUS) functions for Ethernet and Token-Ring.

Management Plane

- Network Management
  - ILMI support (3.0, 3.1) for Plug-and-Play operations on both physical and VP links on all interface types (UNI, IISP, PNNI).

  Extension (ILMI 4.0) to support registration of Anycast and Group addresses.
  - SNMP support (Get, Getnext, Set, and Traps)
  - MIB 2 support
  - IETF AToMIB
  - ATM Forum PNNI MIB (partial menu)
- Box services
  - Command line interface
    - Local console
    - Remote access via Telnet with inband (IP over ATM, IP over LAN emulation) or out-of-band (IP over SLIP).
  - Code and hardware picocode upgrade via TFTP (inband or out-of-band)
    - Redundant code and picocode image to resist download failures
  - Troubleshooting support
    - Trace services
    - Dump services
    - Error logging in non-volatile storage
    - Transfer of trace, dump, and error logs using TFTP (inband or out-of-band)
  - Configuration services
    - Management of configuration parameters in non-volatile storage
    - Upload and download of configuration (for same microcode version) via TFTP (inband and out-of-band)

  - Box survey
    - Module monitoring and failure handling
  - Switch redundancy
    - Automatic configuration synchronization
    - Monitoring and automatic takeover in case of active switch failure.

User Plane (Hardware)

- ATM layer switching
- Support of reserved bandwidth connections
- Support of UBR and ABR connections
- Support of frame discard.

Extended Connections

The Control Point Version 3 supports an extended set of ATM connections, including:

- Switched (SVC) and permanent (PVC)
- Point-to-point and point-to-multipoint
- Reserved Bandwidth (CBR, real time VBR, non-real time VBR, minimum cell rate of ABR) and best-effort (UBR).

Table 1. ATM Connections Supported by ATM Control Point Version 3

Type of Virtual Connection	Connection Type	Connection Class	Connection Mode
Virtual Path Connection (VP)	Permanent	Reserved Bandwidth and Best-effort	Point-to-point and point-to-multipoint
Virtual Channel Connection (VC)	Switched	Reserved Bandwidth and Best-effort	Point-to-point and point-to-multipoint
Virtual Channel Connection (VC)	Permanent	Reserved Bandwidth and Best-effort	Point-to-point and point-to-multipoint

Network Access Protection

Access to the 8260 ATM network is provided for all types of ATM applications, regardless of whether the ATM device is running LAN Emulation, Classical IP, or Native ATM.

When an ATM station connects to the ATM switch, it registers its ATM address through ILMI to the connecting ATM switch. The ATM switch can be configured to verify either the End System Identifier (ESI) or the full ATM address; the latter applies, for instance, when dealing with anycast or group addresses. The network administrator can configure one or several addresses (up to 16) for a given port. Addresses can also be configured at the switch level if needed, allowing the mobility of ATM devices on all ports of a given switch.

To simplify the definition of access control tables, an autolearn mode exists where the ATM switch automatically learns the ATM addresses and stores them into an access control address table. Where several ATM addresses are allowed per port, the number of addresses learned can be defined by the administrator.

Default parameters can be to ensure that when a new module is installed, its ports are automatically protected.

The access control address table is a file that is automatically downloaded from a TFTP file server after a reset (when security is enabled). This file can be updated by the administrator, either via the terminal dialog, or by downloading the file manually and editing it. When access control is enabled, the Control Point checks whether the registering address is present in its access control table.

If the registering address is not in the access control address table, the ATM switch will disable the port and report an SNMP trap; a report of the last violations can be consulted by the network administrator.

Chapter 2. ATM Campus Networks

Overview

The purpose of an ATM network is to set up connections between ATM user devices, the two end points of a connection.

IBM ATM subsystems can be interconnected in order to build a local, privately owned and administered ATM network called an **ATM Campus Network**.

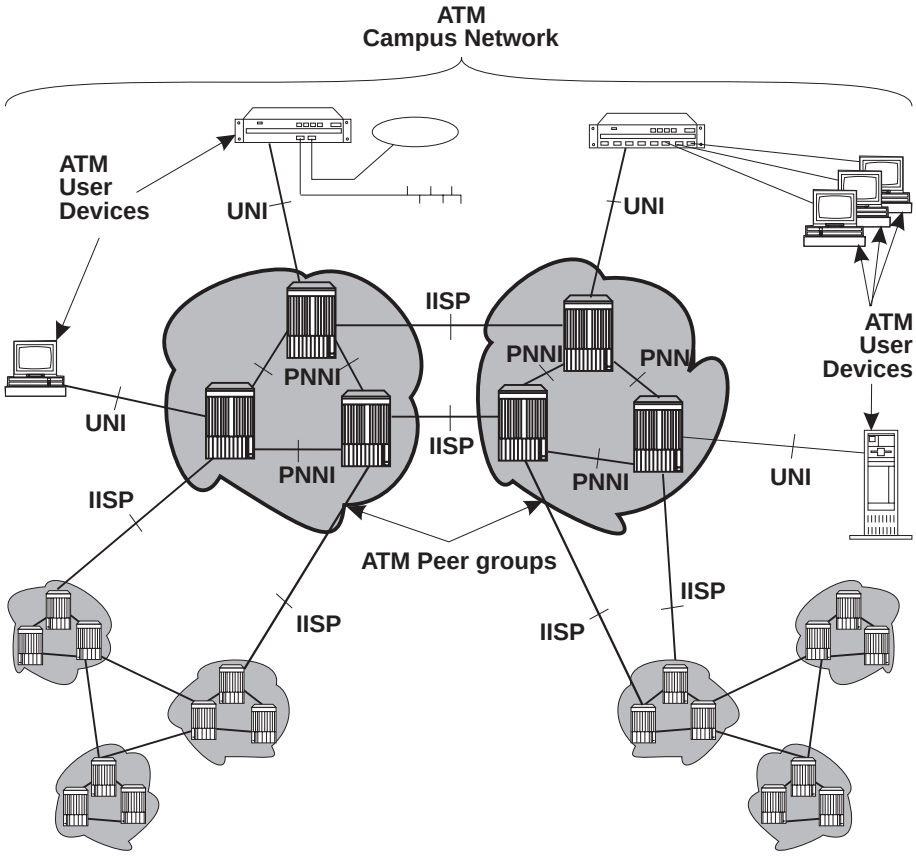

Figure 1. Components of an ATM Campus Network

Network Components

The terms used to describe the components of an ATM Campus Network are defined here:

ATM Campus Network One or more interconnected ATM peer groups.

This set of peer groups is controlled by one administrative domain and a single private owner using one network access protocol (UNI).

ATM Peer Group One or more ATM switches interconnected by PNNI interfaces, and sharing the same peer group identifier.

ATM User Device An end system that encapsulates data into ATM cells and forwards them to the ATM subsystem across a UNI interface. Examples of ATM user devices are:

- Servers and workstations equipped with ATM adapters
- ATM concentrators or workstations equipped with ATM adapters
- Routers with ATM adapters
- LAN ATM bridges.

The control point passes the network prefix of an ATM address to attached end systems using the Interim Local Management Interface (ILMI) protocol.

Network Interfaces

The following protocols are defined in ATM standards for use across the interfaces connecting the components of an ATM campus network:

UNI Defines the interface between an ATM user device (such as a terminal, router, bridge, server, workstation, or concentrator equipped with an ATM adapter) and the ATM network. The ATM subsystem supports the private UNI defined by the ATM Forum UNI Specification V3.0 and V3.1.

IISP Defines the interface between two ATM switches belonging to different ATM routing domains. In the current release, IISP switches are used to interconnect PNNI peer groups.

Operator intervention is required in order to define the addresses reachable over IISP links.

You can define multiple IISP connections between two different peer groups.

PNNI Defines the interface between ATM switches in the same peer group. Version 3 of the PNNI control point supports a single level of hierarchy, therefore PNNI links can be used in the same peer group only.

The PNNI interface supports networking functions without the need of operator intervention, such as routing, node failure and node recovery, backup, and topology management.

You can define multiple PNNI connections between two ATM switches.

Public UNI ILMI is not supported.

VP tunnels can be defined on such a port, and signalling can be supported through the VP.

VOID ILMI is not supported.

VP tunnels can be defined on such a port, and signalling can be supported through the VP.

The PNNI Network

PNNI is a network system for supporting ATM routing and path selection. It selects the best path that interconnects two end systems or a group of end systems. It is structured as a hierarchy of successive higher entities called *levels*. The Control Point maps these levels into nodes. For example, when a switch Control point is running three levels, the first level is executed in the PNNI's **node_0** subsystem, the next level is running in the **node_1** subsystem, and so on.

Version 3 of the PNNI control point operates a single level only, the sole active subsystem being that of **node_0**.

Peer Groups

A peer group is a group of switches having a common identifier, called the *peer group id*. This peer group id is based on a specified length of a private ATM address, based either on the switch's own ATM address or explicitly entered. All switches must share the same peer group id (both length and content, to be included in the peer group.

Summary Addresses

In PNNI, reachability is the advertising of end system addresses throughout a peer group for the purpose of setting up connections between end systems. Reachability in PNNI routing is simplified by the capability of having groups of addresses with a common prefix to be represented by that prefix. Such a prefix is called a *summary address*. PNNI generates a default summary address to provide reachability to all end systems attached to the switch whose addresses share the switch's 13 byte ATM address prefix, that is, whose addresses are generated by the ILMI address notification protocol. Additional non-default summary addresses can be configured to provide reachability for address groups that do not share their switch's 13 byte ATM address prefix.

PNNI also supports path selection to end systems that lie outside a peer group, that is, end systems that are connected to a peer group via non-PNNI links (typically IISP links).

Every switch Control Point feeds end system addresses (that do not share the switch's 13 byte address prefix) to its PNNI subsystem which represents them by corresponding summary addresses if these are already configured. The absence of a configured summary address does not impair the reachability of end system addresses that would otherwise be represented by that summary address: it simply increases the reachability overhead for these addresses. Consequently, the removal of a configured summary address does not impair the reachability of end systems that were previously represented by the summary address: it simply increases PNNI's reachability overhead.

Configuring a new summary address can affect the functioning of previously configured summary addresses.

PNNI Routing

IBM's PNNI supports three types of path selection:

- Constant Bit Rate (CBR), real time Variable Bit Rate (rt VBR), and non-real time Variable Bit Rate (nrt VBR).

  Routing is done on demand:

  – Calls not satisfying the Generic Call Admission Control (GCAC) are pruned.

  – A shortest path is computed based on the Administrative Weight.

- Available Bit Rate (ABR)

  There are two types of ABR path selection, precomputed and on-demand:

  – With precomputed path selection, the specific route is obtained via table look-ups, resulting in fast connection setup.

  – With on-demand path selection, more optimization for the individual routes is possible, but connection setup is slower.

  Note: When MCR=0, the ABR is treated the same as UBR.

- Unspecified Bit Rate (UBR).

  There are two types of UBR path selection, widest path and shortest path:

  – The widest path approach finds the least loaded path in terms of bandwidth regardless of the number of hops required to reach the destination. This approach balances the load on the paths through a network in the absence of critical constraints within that network.

  – The shortest path approach follows a three step algorithm.

    1. In the first step, path selection is based on the administrative weight.
    2. In the second step, paths with minimal hop count to the destination are selected.
    3. In the third step, the widest path approach is applied to the previously selected group of shortest paths to select the final route.

    The shortest path approach is favored when the network contains critical restraints such as links (vcis, vpis) and/or switches that tend to become traffic bottlenecks. The drawback of the shortest path approach, is its reduced load balancing capability.

Virtual Path Connections

When an 8260/8285 is physically attached to a Wide Area Network (WAN), and VP tunnelling is provided, the device attached at the other side of the WAN appears as an adjacent device for the local switch.

Creating VPCs allows to extend the connectivity of the 8260/8285, and to have several VP tunnels on a unique physical interface.

Each VPC can be of UNI, PNNI or IISP type and ensures the same functionality as a physical interface. This means that ILMI, signalling and routing may be provided per logical interface, i.e. VPC.

VPCs may be created on VOID or Public-UNI physical links, and a maximum of 64 is allowed per switch.

Figure 2 shows an example of these VPC links.

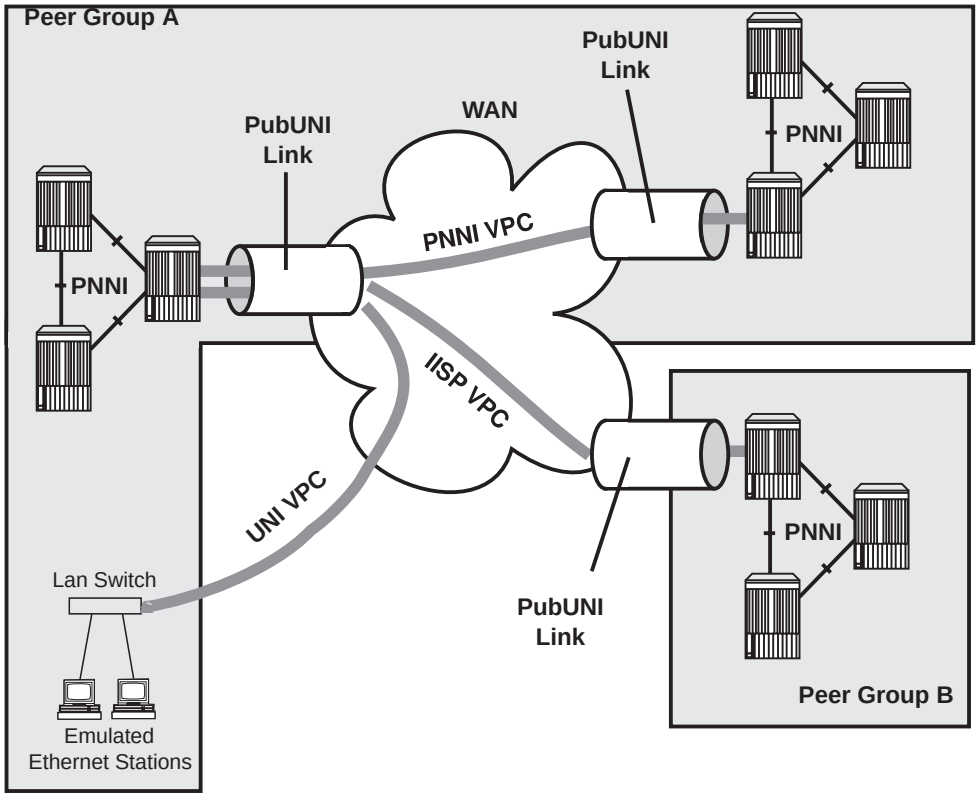

Figure 2. UNI, IISP, and PNNI VPC Links

Permanent Virtual Connections

A PVC is a permanent connection established by a network administrator between two end-points pertaining to the network, as opposed to an SVC, which is a connection established dynamically on an end-user station request, and between two end-user devices.

A PVC is established between 2 (more if multicast) end-points pertaining to the network, with specific traffic characteristics (best effort, reserved bandwidth...).

There are two types of PVC:

- point-to-point, which has one source end-point and one target end point
- point-to-multipoint, which has one source end-point, and several target end-points. Each additional end-point is called a party or a branch of the multicast tree. The traffic characteristics are common for all the parties of a PVC.

The two end-points of a PVC may be on the same 8260/8285, or on different 8260/8285s. In the latter case, the path may be selected either by the routing protocol (PNNI, for example) or by creating several PVCs in each 8260/8285 until the final end point is reached.

PVCs are created, and deleted, via the terminal dialog. Between these 2 events, the PVC is active, unless a network failure occurs. If this happens, up to 20 attempts (with 15 second intervals are made to re-establish the connection.

PVC's are automatically established when an 8260/8285 is reset or powered on.

A PVC is automatically saved after it has been activated successfully.

The 8260/8285 supports a maximum of 100 PVCs.

Chapter 3. Configuring Basic Parameters

This chapter describes:

- How to configure the ATM switch address
- How to configure the operating mode (8260 only).

Configuring the ATM Switch Address

Note: Configuring the ATM switch address will cause a reset of the ATM system. If you have made any other configuration changes, and not saved them, save them now or they will be lost.

When a PNNI switch is powered on for the first time, it automatically loads a default configuration, including a default ATM address. If you have multiple switches in your network, the default ATM address must be reconfigured so that each switch has a unique address. This reconfiguration is achieved by issuing the following command:

```
8260ATM> set pnni node_0 atm_address: 39.99.99.99.99.99.99.00.00.99.99.01.01.99.
99.99.99.99.99.01
```

where `39.99.99.99.99.99.99.00.00.99.99.01.01.99.99.99.99.99.99.01` is an example of a 20 byte hex address entry.

PNNI responds by displaying a short description of your next entry alternatives. If setting the address is the only reconfiguration action, you issue the COMMIT PNNI command to activate the new configuration. If you wish to modify the address further, you reissue the SET PNNI NODE_0 ATM_ADDRESS command before issuing the COMMIT PNNI command. The COMMIT PNNI command causes the address to be saved in the NVS Configuration repository and then resets the Control Point.

In the default PNNI configuration, the address of all switches that are to form one peer group must have one common 96 bit (12 byte) prefix. This prefix is called the **peer group id** and defines the set of switches that together form one peer group.

As the default length for the peer group id is 12 bytes, the 13th byte of the ATM address can be used to uniquely identify a switch within a peer group.

A simple way to configure a collection of interconnected switches into one peer group is to issue the SET PNNI NODE_0 ATM_ADDRESS command for each switch whereby all addresses have a common 96 bit prefix.

Configuring the Operating Mode (8260 only)

PNNI and LES/BUS are exclusive operating modes, they cannot both operate at the same time. You must configure the operating mode of the ATM Control Point to run one or the other (by default, the ATM Control Point is configured to run PNNI).

LES Operating Mode: To set the operating mode for LESs, enter the following command:

```
8260ATM> set device config_functions les_without_nni_pnni
```

As LES/BUS and PNNI configurations are exclusive, you will be given the following message:

```
This call will reset the ATM subsystem and at least one potential or
existing NNI or PNNI port will turn to disabled UNI.
Are you sure? (Y/N)
8260ATM>
```

Enter `Y` to continue, or `N` to cancel the call.

PNNI Operating Mode: To set the operating mode for PNNI, enter the following command:

```
8260ATM> set device config_functions nni_pnni_without_les
```

As PNNI and LES/BUS configurations are exclusive, you will be given the following message:

```
This call will stop all LESs and reset the ATM subsystem.
Are you sure? (Y/N)
8260ATM>
```

Enter `Y` to continue, or `N` to cancel the call.

Chapter 4. Configuring Network Access Security

The purpose of access security is to validate physical access to the ATM network.

When an ATM station connects to the ATM switch, it registers its ATM address through ILMI to the connecting ATM switch. When network security access is enabled, the ATM address is validated (based on the ILMI protocol, and using either the End System Identifier (ESI) or the full ATM address), to determine if network access is granted. Stations that do not have ILMI must have their address defined via the SET REACHABLE_ADDRESS command (see “Configuring Reachable Addresses” on page 55.)

Security can be implemented either globally (on all detected ports) or on an individual port basis.

The network access security system maintains a table of ATM addresses that are allowed access (either at the switch or port level). If the registering address is not in the table, the ATM switch will disable the port and report an SNMP trap. The last violation for each port can be displayed by the network administrator. A maximum of 512 addresses can be maintained in the address table.

The access control address table is a file stored on a dedicated TFTP server. When security is enabled, the file is automatically downloaded whenever the 8260/8285 is powered on or reset. The network administrator can use the ATM Control Point console, accessible either via the RS-232 interface or via Telnet, to modify the security settings (the Administrator password is required).

In addition to maintaining address tables, the following functions are also available:

- Autolearn Function
- Default Values
- Violation notification

Autolearn Function

To simplify the definition of addresses, an autolearn mode exists where the ATM switch automatically learns the ATM addresses that register through ILMI and stores them into the access control address table.

The autolearn function is enabled by specifying the number of addresses per port to be learnt. If 0 is specified, autolearning is disabled. When autolearn is enabled:

- Each time a new address is learnt, the number of addresses that can be learnt is decreased by 1. Once the value reaches 0, no further learning can take place.
- Each ATM address learnt for the port is automatically added to the list of authorized addresses for this port.

An MSS server can work with more than 16 internal addresses. When this is the case, it is advised that you disable security on the port connected to the MSS server.

Default Values

Because ATM ports may be dynamically added to a switch (when new modules are inserted), you can set default parameters that can be applied to newly detected ports.

Unless specified otherwise, the default settings are:

1. security: disabled
2. autolearn: 0 (not active)
3. notification: disabled.

See “Setting Default Values” on page 24.

Violation Notification

When the security trap is enabled, an SNMP trap is sent to the network management station each time a security violation occurs. The SNMP trap contains:

- The date and time of the violation
- The data that failed the security check (such as ATM address)
- The interface where the violation occurred.

Configuration Control Mechanism

The access control system is created from:

- A file containing the access control address table downloaded from the network access control server. Each 8260/8285 has its own unique file.
- Access control parameters stored in non-volatile storage (NVRAM) in each 8260/8285.

Figure 3 shows the components of the access control system and how they are handled when a RESET or SAVE action is performed.

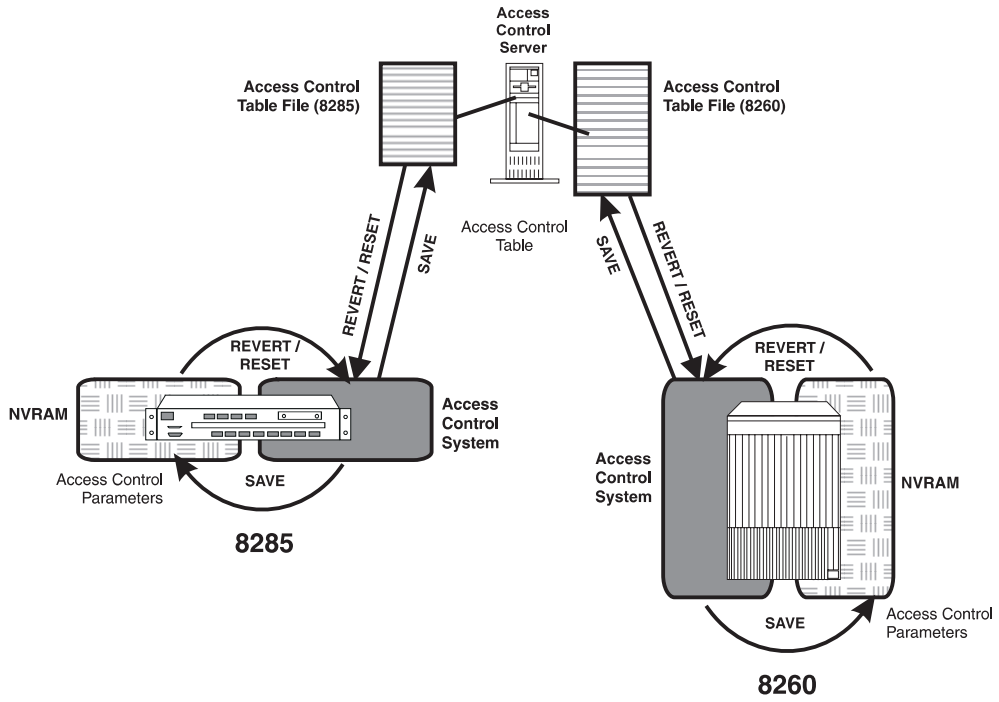

Figure 3. Access Control Configuration Mechanism

Notes:

1. If global security is disabled when a reset if performed, the access control address table is not downloaded from the server. If no addresses have been entered via the terminal dialog, when the SAVE SECURITY command (or SAVE ALL command) is issued, the access control address table is not uploaded to the server. If changes have been made to the access control address table, then the new table will be uploaded, overwriting the previous table.
2. If the TFTP server that contains the access control address table is connected via a UNI link, you must ensure that the port to which it is connected has security disabled. Otherwise, the access control address table cannot be downloaded from the server.

3. If the automatic download fails after a reset, the operation is retried until successful. During this time, registration attempts are rejected, but the ports remain enabled to allow for reconnection attempts. You may choose to disable security and allow connections to proceed while you manually check the download mechanism via the DOWNLOAD command. Once the operation is successful, you can re-enable security and reset the system.
4. The Access Control Server should be placed as close to the 8260/8285(s) as possible, to reduce the possibility of connection failures.

Enabling or Disabling Security

You can enable or disable security either globally (on all detected ports in the 8260/8285) or on selected ports only. To enable security on selected ports, security must be enabled globally.

These settings only apply to ports currently detected. Ports newly detected have security enabled or disabled depending on the default mode setting (see “Setting the Security Mode Default” on page 24.)

Enabling Security

If you only wish to have security on a few selected ports, the easiest way to do this is:

1. Set the default security mode to NO_SECURITY.
2. Set the security mode on.
3. Enable security on the required ports only.

Conversely, if you wish to have security on all or most ports, the easiest way to do this is:

1. Set the default security mode to ACCESS_CONTROL
2. Set the security mode on.
3. Disable security on the ports for which security is not required.

To enable security globally, you enter the following command:

```
8260ATM> set security mode access_control
```

Note: If the access control server or an ARP server is connected via a UNI link, you must ensure that the port to which it is connected has security disabled. Otherwise, the server(s) will not be able to connect to the 8260/8285 after a reset.

To enable security on a specific port, you enter the following command:

```
8260ATM> set security port <slot.port> mode access_control
```

Disabling Security

To disable security globally, you enter the following command:

```
8260ATM> set security mode no_security
```

To disable security on a specific port, you enter the following command:

```
8260ATM> set security port <slot.port> no_security
```

Configuring TFTP Parameters

In order to upload and download the access control address table from the TFTP server (either automatically by the access control system during save and reset operations or manually), you must:

1. Define the TFTP server that retains the access control address table (use the SET SECURITY TFTP_SERVER_IP_ADDRESS command)
2. Set the TFTP file name (use the SET SECURITY TFTP_FILE_NAME command).

Setting the Autolearn Values

You can configure the autolearn function to learn up to 16 ATM addresses per port at a time. You can disable the autolearn function by specifying that no addresses may be learned.

To set the value, enter the following command:

```
8260ATM> set security port <slot.port> autolearn <value>
```

where <value> specifies the number of ATM addresses that can be learned. By entering a value of 0, you disable the autolearn function (no addresses may be learned).

Enabling and Disabling Traps

You can enable or disable traps on selected ports by entering the following command:

```
8260ATM> set security port <slot.port> trap enable|disable
```

Setting Default Values

You can set default values that will be automatically applied to any new ports detected after the values have been set (for example, after a new module has been inserted in the hub).

You can set default parameters to :

- Specify if security is to be enabled or not on the port
- Specify the number of addresses that can be automatically learned for the port
- Specify if is an SNMP trap is sent to the network management station when a security violation occurs.

Setting the Security Mode Default

To automatically enable or disable security for newly detected ports, enter the following command:

```
8260ATM> set security default mode access_control|no_security
```

Setting the Trap Mode default

To set the default for whether SNMP traps are sent to the network manager station when security violations are detected, enter the following command:

```
8260ATM> set security default trap enable|disable
```

Setting the Autolearn Default

To specify if the autolearn function is to be effected for newly detected ports, and if so, the number of addresses to be learned, enter the following command:

```
8260ATM> set security default autolearn <value>
```

where <value> specifies the number of ATM addresses that can be learned. A value of 0 indicates that autolearning will be disabled.

If you only wish to have the autolearn function in effect on a few selected ports, the easiest way to do this is:

1. Set the default autolearn setting to 0 (disabled)
2. Enable autolearn on the required ports only.

Conversely, if you wish to have autolearn on all or most ports, the easiest way to do this is:

1. Set the default autolearn setting to a value other than 0
2. Set the default autolearn value to 0 on the ports that you do not wish to have the autolearn function active.

Specifying ATM Addresses to be Accepted

The ATM address can be validated on either the full ATM address (19 bytes) or just the ESI portion (bytes 14 through 19) of the address, and can be set at either the hub or individual port level.

To set the validation to be done on the network prefix, enter the following command:

```
8260ATM> set security atm_address <value> any|<slot.port>
```

where `any` specifies that the address is to be accepted for all ports in the hub, and `<slot.port>` can be used to specify a single port.

To set the validation to be done on the ESI, enter the following command:

```
8260ATM> set security esi_address <value> any|<slot.port>
```

where `any` specifies that the address is to be accepted for all ports in the hub, and `<slot.port>` can be used to specify a single port.

Note: You should not have both a full ATM address and ESI address authorized for the same range (either any port or a specific port) when the full ATM address contains the same ESI address as the ESI address specified by the SET SECURITY ESI_ADDRESS command. This may cause a rejection of one of the addresses.

Removing ATM Addresses

You can remove either a single ATM address or all ATM addresses from the list of authorized addresses by entering the following command:

```
8260ATM> clear security atm_address all|<index>
```

where `<index>` denotes the index entry of the address, as displayed by the SHOW SECURITY ATM_ADDRESS command.

Displaying Security Information

You can display the following information:

- The current security mode (enabled or disabled)
- The current defaults set
- The ATM addresses authorized for access (at the hub or port level)
- Specific port information, such as:
  - Whether security is enabled or not
  - The number of ATM address that can be learned
  - Whether traps are enabled or not.
- The last security violations.

Current Security Mode

To display if the security system is active, enter the following command:

```
8260ATM> show security mode
```

Current Default Settings

To display the current default settings that will be applied to all newly detected ports, enter the following command:

```
8260ATM> show security default
```

ATM Addresses Defined

To display the ATM addresses that have been granted access, enter the following command:

```
8260ATM> show security atm_address all|any|<slot.port>
```

where:

`all` is used to display information on all ports in an 8260/8285

`any` is used to display the addresses that have been authorized on any port in the 8260/8285

`<slot.port>` is used to display information on a specific port only.

Note that the resulting display will show all addresses defined, (both ESI and ATM addresses).

If it appears that there is a mismatch between the addresses displayed and the addresses in the access control address table on the server, this may due to an address incorrectly entered in the file (only valid entries are downloaded). To check this, edit the access control address table on the TFTP server and check for errors.

Port Settings

To display information for ports, enter the following command:

```
8260ATM> show security port all|<slot.port>
```

where:

`all` is used to display information on all ports in a hub, and

`<slot.port>` is used to display information on a specific port only.

The resulting display will show:

- If security is enabled
- How many further addresses can be automatically learned
- Whether SNMP traps are enabled.

Security Violations

To display information regarding the last security violation, enter the following command:

```
8260ATM> show security last_violation all|<slot.port>
```

where `all` is used to display information on all ports in a hub, and `<slot.port>` is used to display information on a specific port only.

The resulting display will show:

- The slot and port where the violation occurred
- The ATM address that was rejected
- Date and time of the violation

TFTP Settings

To display the current TFTP settings, enter the following command:

```
8260ATM> show security tftp
```

The resulting display will show:

- TFTP Server IP address
- TFTP file name
- Result of the last transfer.

Saving Security Settings

Once changes have been made to the security settings (either through the terminal dialog or via the autolearn function) you must save them. If not, the changes will be lost at the next reset.

If changes have been made to the access control address table, before saving the settings you must configure the TFTP settings (see page “Configuring TFTP Parameters” on page 23).

The security settings are saved by entering the following command:

```
8260ATM> save security
```

This will save the parameter settings to NVRAM and automatically upload the access control address table to the server (if the access control address table has been changed).

Reverting Security Changes

If after making changes to the security configuration, you decide that you do not wish to retain them, you can restore the previously saved values.

Before you can restore the values, you must configure the TFTP settings (see page “Configuring TFTP Parameters” on page 23).

The security settings are restored by entering the following command:

```
8260ATM> revert security
```

This will automatically retrieve the parameter settings from NVRAM and download the access control address table from the server.

Note: This will cause a reset of the ATM system.

Manually Uploading and Downloading the Access Control Address Table

You can manually upload and download the access control address table, via TFTP. This can be useful to:

- Test the TFTP connection between the server and the 8260/8285.
- To upload the current access control address table from the 8260/8285 without causing a reset (the file must be write-accessible on the server).
- To check for errors if there appears to be a mismatch between the addresses displayed by the SHOW SECURITY ATM_ADDRESS command and the addresses manually entered in the access control address table.
- As a means of manually entering, updating, or removing ATM addresses. Once you have made your changes, you can download the access control address table from the TFTP server and display its contents using the SHOW SECURITY ATM_ADDRESS command (regardless of whether security is enabled or not). If security is enabled, the new access control address table will automatically come into effect.

Uploading the Access Control Address Table

To manually upload the access control address table, enter the following commands:

1. SET TFTP SERVER_IP_ADDRESS (to define where the file is to be stored on the server)
2. SET TFTP FILE_NAME (to define the path name for the file on the server)
3. SET TFTP FILE_TYPE SECURITY
4. UPLOAD (to upload the file).

Downloading the Access Control Address Table

To manually download the access control address table, enter the following commands:

1. SET TFTP SERVER_IP_ADDRESS (to define the server where the file is stored)
2. SET TFTP FILE_NAME (to define the path name of the file on the server)
3. SET TFTP FILE_TYPE SECURITY
4. DOWNLOAD (to download the file).

Updating the Access Control Address Table

If you are intending to enter all the ATM addresses to be authorized directly in the access control address table on the server (as opposed to using the terminal dialog or autolearn function), you may find it helpful to first enter one address through the terminal dialog, which can then be used as a base for your other addresses. If you choose to do this, then after entering the address, the access control address table must be uploaded to the server. This can be done either by entering the SAVE SECURITY command, or manually uploading the file as described in “Uploading the Access Control Address Table.”

The access control address table file contains four fields:

- ATM address field, which contains the address to be authorized
- ATM mask field, which determines if the full address (19 bytes) or the ESI part of the address (bytes 14 through 19) are to be used for validation purposes.
- The slot and port fields, which are to specify a particular port for which the address is authorized.

The following example shows a typical address table:

```
---- ATM address to be authorized ---- ---- address bytes to be checked ----- slot/port

00000000000000000000000000010203040501 0000000000000000000000000fffffffffff 01 01
00000000000000000000000000010203040502 0000000000000000000000000fffffffffff 01 02
00000000000000000000000000010203040503 0000000000000000000000000fffffffffff 02 04
39020304050607080910111213141516171819 ffffffffffffffffffffffffffffffffffff 00 00
```

Figure 4. Example Address Table

Note that the value `00 00` has been displayed for `slot/port` in line 4. This means that the address is authorized for ANY port.

To enter a new address, perform the following steps:

1. Enter the address to be authorized (in hex). If you only want the ESI part of the address to be validated, enter `00` for the first 13 bytes.
2. Enter the corresponding mask to be used. If the full address is to be validated, enter `ff` for all 19 bytes. If only the ESI part of the address is to be validated, enter `00` for the first 13 bytes.
3. Enter the port(s) for which the address is to be authorized. You can enter a specific port (slot and port must be specified), or, if the address is to be authorized for ALL ports, you can specify `00 00`.

   You cannot specify the same address (either full or ESI) for multiple ports.

The changed access control address table will come into effect either

- Automatically at the next reset of the ATM Control Point (providing security is enabled at the time).
- Immediately if the access control address table is downloaded to the 8260/8285 and security is currently active.

If security is current disabled, you can still download the access control address table and check that your changes are valid by entering the SHOW SECURITY ATM_ADDRESS command (invalid address settings will not be downloaded and therefore will not be displayed).

Chapter 5. Configuring PNNI Parameters

The chapter describes how PNNI configuration changes are managed, and how they are made.

Important (8260 only): PNNI and LES/BUS are exclusive. They cannot both operate at the same time. You must define the operating mode of the ATM Control Point to run PNNI only, in which case the LES will be stopped and the hub reset. See “Configuring the Operating Mode (8260 only)” on page 16 on how to configure the ATM Control Point to run PNNI.

Configuration Control Mechanism

Unlike other configuration parameters, which are implemented as soon as the SET command is issued, PNNI stores the new parameter values until instructed to implement them.

A default configuration is provided with the ATM Control Point Version 3, and activated when is powered on or reset. All configurable parameter values for this configuration are stored in a non-volatile storage (NVS) area called the *NVS Configuration* repository. These parameters are copied into the *Active Configuration* repository when the 8260/8285 is powered on (and every time the ATM subsystem is reset) and used by the active PNNI system.

A *Future Configuration* repository is provided that allows you to enter changes to the current configuration. These changes are kept in memory until you instruct PNNI to implement them.

PNNI only accepts parameter changes if the parameter value lies within the correct range and is consistent with all the other, already configured parameter values. PNNI thus assures that the new configuration will be consistent.

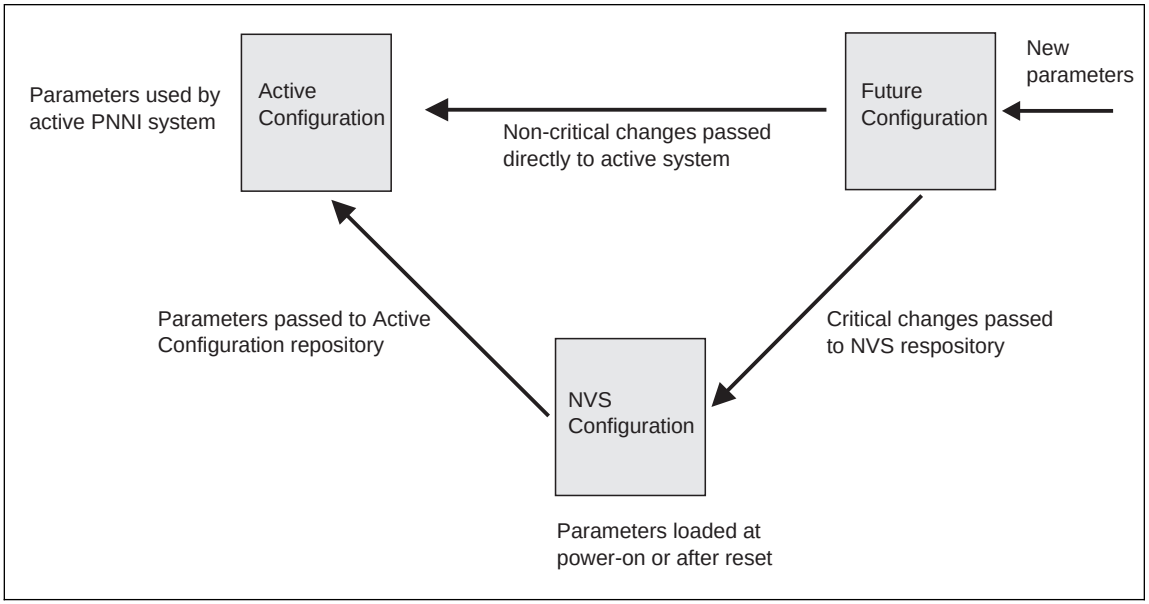

Figure 5. PNNI Configuration Update Mechanism

Once you have set all the parameters you wish to configure, you issue an instruction for them to be implemented.

What happens next depends on whether the configuration changes are deemed to be critical or not. Critical settings are deemed those that, when reconfigured, affect PNNI to such an extent that the ATM subsystem must be restarted (such as ATM address, for example).

Critical Changes

1. PNNI gives an informative warning that the changes made are critical and asks you if you wish to continue.

   If you decide not to continue, the parameter values are retained in the Future Configuration repository.

2. If you decide to proceed, PNNI copies the parameters from the Future Configuration repository into the NVS Configuration repository, before issuing a reset of the switch's ATM subsystem This ensures that the new parameters are automatically reinstalled after subsequent reset or power on actions.
3. The reset action re-initializes PNNI by loading the Active Configuration repository from the NVS repository.
4. The PNNI system is activated with the reconfigured parameters.

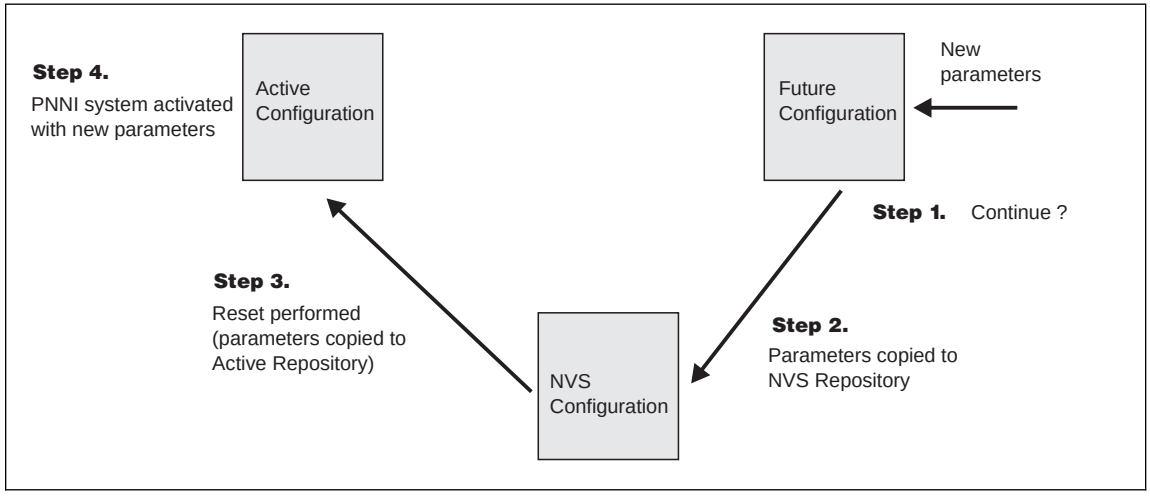

Figure 6. PNNI Configuration Update (Critical)

Non-Critical Changes

1. The changed parameters are copied to the Active Configuration repository.
2. The PNNI system continues running, using the new parameters.
3. If you decide that the configuration changes that you have made should be maintained indefinitely, you can save the Active Configuration to the NVS Configuration. This ensures that the current Active Configuration (now with the new parameters) is automatically reinstalled after subsequent reset or power on actions.
4. If you decide that the configuration changes that you have made should be removed, you can instruct PNNI to replace the new parameters with the previous values (from the last save). This does not cause a reset, and the PNNI system continues running.

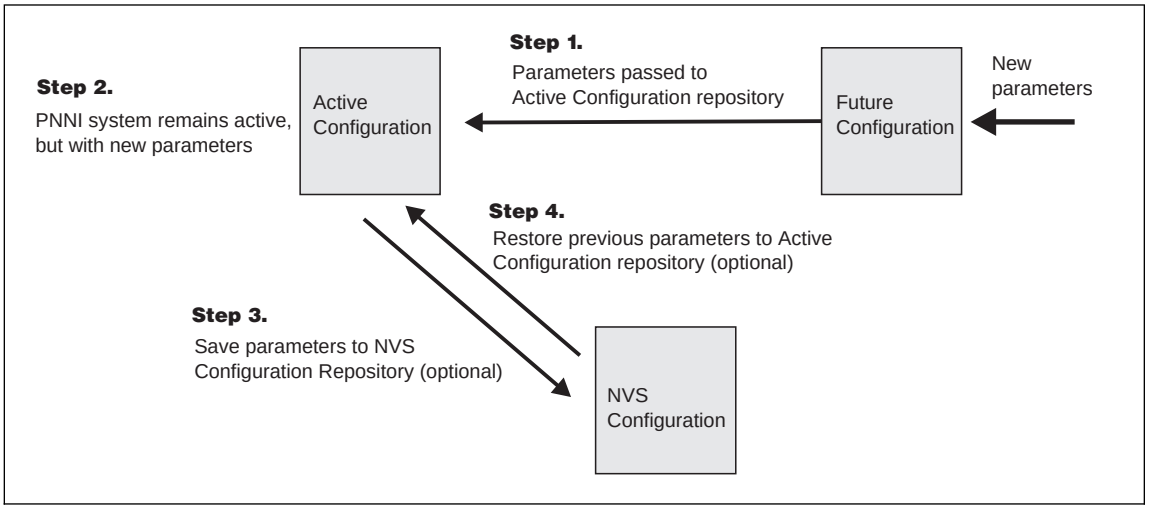

Figure 7. PNNI Configuration Update (Non-critical)

Working with PNNI Configuration Settings

This section describes the various PNNI parameters, what the default values are, and how to change them.

Default Parameter Settings

The default parameter values are shown in Table 2.

Table 2. Default PNNI Parameters

Parameter	Default Setting
ATM address	39.99.99.99.99.99.99.00.00.99.99.01.01.99.99.99.99.99.99.00
Level Identifier (bits)	96
Peer Group Id	39.99.99.99.99.99.99.00.00.99.99.01
Internal Summary Address	39.99.99.99.99.99.00.00.99.99.01.01
External Summary Address	none
Path Selection	ABR = precomputed UBR = widest path

Changing Parameter Values

Changes to the configuration parameters are made via the following command:

```
8260ATM> set pnni
```

See further sections in this chapter which describe the full command syntax and individual parameter values.

Applying Configuration Changes

Once you have set all the parameters you wish to configure, you issue the following command:

```
8260ATM> commit pnni
```

- If the configuration changes affect critical settings, that is settings that will cause the ATM subsystem to be reset, PNNI gives an informative warning, and provides you with the option to proceed or cancel the update.

  If you decide not to proceed with the update, you can restore the parameter values in the Future Configuration to those of the active system (see “Restoring the Future Configuration” on page 39.). Alternatively, you may change the parameter values (with the SET PNNI command) before re-issuing the COMMIT PNNI command.

- If the changes are not critical, PNNI will remain active with the new parameters.

  Note: If you wish to retain these new parameter settings, you should save them to the NVS Configuration repository. Otherwise, the next time that the ATM subsystem is reset, the new values will be lost. See “Saving the Active Configuration.”

  If you decide to discard the new parameters, you can return to the previous settings (provided they have been saved). See “Restoring the Active Configuration” on page 39.

Saving the Active Configuration

The Active Configuration need only be saved when non-critical changes have been made, and you wish the changes to be retained when the ATM subsystem is reset. This is because when critical changes are detected when the COMMIT PNNI command is issued, the new parameters are automatically saved before the ATM subsystem is reset.

If you decide that the configuration changes that you have made (and implemented via a non-critical commit) should be maintained indefinitely, you can save the Active Configuration to the NVS Configuration by issuing the following command:

```
8260ATM> save pnni
```

This ensures that any changes made to the active configuration as a result of a non-critical commit are reinstalled after a reset or power on action.

Restoring the Active Configuration

If you have changed your active PNNI configuration with the SET PNNI and COMMIT commands, you can remove the newly changed parameter values by issuing the command:

```
8260ATM> revert pnni
```

Note: This applies only when a non-critical commit has been issued. If the commit was critical, then the NVS Configuration repository will have been overwritten by the parameter values in the Future configuration repository.

Restoring the Future Configuration

If you have decided not to proceed with a critical commit, or you wish to remove parameter changes made but not yet committed, you can restore the Future Configuration with the values contained in the Active Configuration by issuing the command:

```
8260ATM> uncommit pnni
```

Viewing Configuration Settings

To display the parameters in the Future Configuration issue the command:

```
8260ATM> show future_pnni node_0
```

To display the Active Configuration parameters , enter the following command:

```
8260ATM> show pnni node_0
```

Note: After a COMMIT PNNI command has been issued, the Active and Future Configuration will show the same information.

To display whether the active configuration is saved or not, and whether there is a pending commit or not, enter the following command:

```
8260ATM> show pnni configuration_state
```

Configuring the ATM Switch Address

When a PNNI switch is powered on for the first time, it automatically loads a default configuration (see 37.) As this default configuration also includes a default ATM address, the address must be reconfigured so that the switch has a unique address. This reconfiguration is achieved by issuing the following command:

```
8260ATM> set pnni node_0 atm_address: <address>
```

where <address> is the desired ATM address.

PNNI responds by displaying a short description of your next entry alternatives. If setting the address is the only reconfiguration action, you issue the COMMIT PNNI command to activate the new configuration. If you wish to modify the address further, you reissue the SET PNNI NODE_0 ATM_ADDRESS command before issuing the COMMIT PNNI command (which causes the address to be saved in the NVS Configuration repository before the Control Point is reset).

Example: The following example sets the ATM address to 39.10.20.30.40.50.60.70.80.90.A0.B0.C0.D0.E0.20.11.12.13.14:

```
8260ATM> set pnni node_0 atm_address: 39.10.20.30.40.50.60.70.80.90.A0.B0.C0.D0.
E0.20.11.12.13.14
```

Note: In the default PNNI configuration, the address of all switches that are to form a peer group must have a common 96 bit (12 byte) prefix. This prefix is called the **peer group id** and defines the set of switches that together form one peer group. A simple way to configure a collection of interconnected switches into one peer group is to issue the SET PNNI NODE_0 ATM ADDRESS command for each switch whereby all addresses have a common 96 bit prefix.

Configuring Peer Group Identifiers

Peer group identifiers are private ATM address prefixes that define the set of switches that together form one peer group.

All switches that are to form a peer group must have the same Peer Group Identifier (both length and content must be the same).

The length, in bits, of the peer group identifier is called the *level identifier*, and governs the length of the address that must be matched. The level identifier can be set to any length from 0 bits through 104 bits, although normally less than 104 bits are used, as shown in Figure 8

The address itself can be based either on the switch's ATM address or explicitly defined.

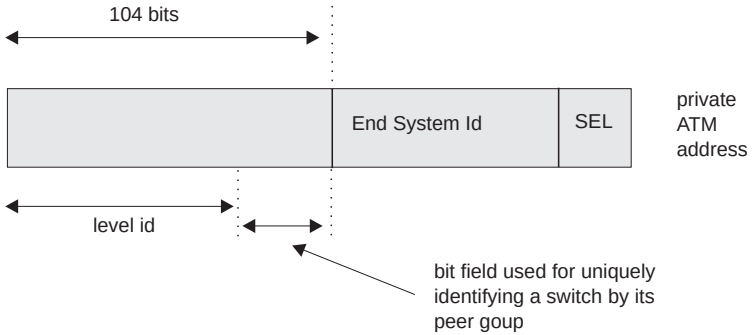

Figure 8. Level ID Perspective of a Switch ATM Address

If the full 104 bits are used, then the address bits positioned between the level id and End System Id disappear.

In the default PNNI configuration, the peer group identifier is derived from the first 12 bytes of the switch's address.

How you configure the peer group identifier depends on whether you use the switch's ATM address or not. Both scenarios are covered in the next sections.

Using the Switch's ATM Address

If the peer group identifier is to be based on the switch's ATM address, then you only have to specify the portion, or length, of the address that must be matched by other switches in order for them to belong to the peer group.

The default length, 96 bits, may be changed by entering the following command:

```
8260ATM> set pnni node_0 level_identifier: <n>
```

where <n> can vary from 0 to 104 bits). This causes PNNI to select the first n bits of the switch's address as the new peer group id.

If you change the level identifier in one switch (and by doing so the peer group id), you must also make the same change at any other switches belonging to the peer group.

Note: When the peer group identifier is based on the switch's ATM address, a change to that ATM address can cause the peer group identifier to change (if the change part of the address falls within the length specified by the level identifier).

Explicitly Entering a Peer Group ID

To explicitly define a peer group id, you must specify both the length and content. For example, if you enter:

```
8260ATM> set pnni node_0 peer_group_id: 51 47.a5.32.4e.b7.48.19
8260ATM> commit pnni
```

then the node_0 takes the peer group id from the first 51 bits of the entered string 47.a5.32.4e.b7.48.19 and 51 is the new level id. This action results in the peer group id being different from the switch's 51 bit ATM address.

Note: The entered peer group id value must conform to the prefix of the private ATM address. PNNI applies address checking to entered peer group ids.

This operation removes the restraint that the address of every switch in a peer group has to have a common prefix of level id length. One peer group id, common to the network, can be entered at each switch, thereby making the network operation independent of whether the switch addresses have a common prefix or not.

Once you have explicitly defined a peer group id, you cannot modify the length of it by entering the SET PNNI NODE_0 LEVEL_IDENTIFIER command. This will cause the peer group id to be determined from the switch's ATM address. To change the length of an explicitly defined peer group id, you must re-enter the SET PNNI NODE_0 PEER_GROUP_ID command.

Configuring Summary Addresses

In PNNI, reachability is the advertising of end system addresses throughout a peer group for the purpose of setting up connections between end systems. Reachability in PNNI routing is simplified by the capability of having groups of addresses with a common prefix to be represented by that prefix. Such a prefix is called a *summary address*. PNNI generates a default summary address to provide reachability to all end systems attached to the switch whose addresses share the switch's 13 byte ATM address prefix, that is, whose addresses are generated by the ILMI address notification protocol. Additional non-default summary addresses can be configured to provide reachability for address groups that do not share their switch's 13 byte ATM address prefix. For example, entering:

```
8260ATM> set pnni node_0 summary_addr internal: 30 39.22.ee.99
```

will cause all end systems directly attached to the switch via UNIs whose addresses begin with the first 30 bits of the string 39.22.ee.99 to be represented in the peer group by the just entered summary address. PNNI stores a summary address without using it if no end system address prefixes match that address.

PNNI uses a longest matching prefix criterion, so no two summary addresses within a PNNI network should have the same value unless they represent the same set of addresses. Furthermore, summary addresses should be configured as long as possible to enhance longest matching prefix selection.

PNNI also supports path selection to end systems that lie outside a peer group, that is, end systems that are connected to a peer group via non-PNNI links (typically IISP links). For example, at a switch belonging to a peer group the command:

```
8260ATM> set pnni node_0 summary_addr exterior 28 45.22.ee.99
```

then all end system addresses, reachable from that switch, that have a prefix the same as the first 28 bits of the string 45.22.ee.99 and lie outside the peer group, will be represented in the peer group by the entered summary address.

To ascertain the number of existing summary addresses, and the remaining number that can be set, enter the following command:

```
8260ATM> show pnni summary_address
```

The resulting display also includes an index number for each summary address set. This index number can be used to delete a summary address, when used in the following command:

```
8260ATM> clear pnni summary_addr <n>
```

where <n> is the index number displayed by the SHOW PNNI SUMMARY_ADDRESS command.

Every control point feeds end system addresses (that do not share the switch's 13 byte address prefix) to its PNNI subsystem which represents them by corresponding summary addresses if these are already configured.

Configuring a new summary address can affect the functioning of previously configured summary addresses. In the following example, assume that you have configured an external summary address 39.aa.bb, and that you have also set the following reachable external addresses:

- 39.aa.bb.cc.45.63...
- 39.aa.bb.cc.64.32...
- 39.aa.bb.cc.46.39...

then all 3 external addresses will automatically be represented in PNNI by the address prefix 39.aa.bb of the configured summary address. If you now set a second external summary address to 39.aa.bb.cc then PNNI will automatically migrate the three external addresses to the new summary address. The result is that the three addresses are now represented by the new summary address prefix 39.aa.bb.cc and the old summary address 39.aa.bb is unused although it remains stored in PNNI. The reason for this is that all address to summary address associations are computed on the basis of longest matching prefix and 39.aa.bb.cc is a longer match than 39.aa.bb. You could reactivate the summary address 39.aa.bb by setting the following group of external reachable addresses:

- 39.aa.bb.ff.45.63...
- 39.aa.bb.ff.64.32...

which cannot be represented by the address prefix 39.aa.bb.cc.

Configuring PNNI Path Selection

IBM's PNNI supports three types of path selection, for the following classes of traffic:

- Constant Bit Rate (CBR), real time Variable Bit Rate (rt VBR), and non-real time Available Bit Rate (nrt VBR)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

Constant Bit Rate and Variable Bit Rate (CBR, rt VBR, and nrt VBR)

Routing is done on demand, corresponding to the demand appearing when processing a call from the network (this is automatic and requires no configuration action from the ATM console):

- Calls not satisfying the Generic Call Admission Control (GCAC) are pruned.
- A shortest path is computed based on the Adminisitrative Weight.

Available Bit Rate

IBM's PNNI Path Selection supports Available Bit Rate (ABR) calls in two ways, precomputed and on-demand:

- Paths are precomputed and specific route is obtained via table look-ups, resulting in fast connection setup.
- Paths are computed on-demand, resulting in slower connection setups, but with more optimization for the individual routes.

The default configured setting is for paths to be precomputed, and can be changed to on-demand by entering the following command:

```
8260ATM> set pnni path_selection abr: on_demand_path
```

The setting can be changed back to precomputed by entering the following command:

```
8260ATM> set pnni path_selection abr: precomputed_path
```

Unspecified Bit Rate

IBM's PNNI Path Selection supports Unspecified Bit Rate (UBR) in two ways, shortest path and widest path:

- The shortest path approach follows a two step algorithm. In step one, paths with minimal hop count to the destination are selected. In the second step, the widest path approach is applied to the previously selected group of shortest paths to select the final route. This approach is favored when the network contains critical restraints such as links (VCIs, VPIs) and/or switches that tend to become traffic bottlenecks. The drawback of the shortest path approach, is its reduced load balancing capability.
- The widest path approach finds the least loaded path in terms of bandwidth regardless of the number of hops required to reach the destination. This approach balances the load on the paths through a network in the absence of critical constraints within that network.

The default configured setting is the widest path approach, and this can be changed to shortest path by entering the following command:

```
8260ATM> set pnni path_selection ubr: shortest_path
```

The setting can be changed back to widest path by entering the following command:

```
8260ATM> set pnni path_selection ubr: widest_path
```

To display the current route modes, enter the following command:

```
8260ATM> show pnni path_selection
```

Note: Reserved Bandwidth (VBR, CBR) and point-to-multipoint calls are processed as on-demand, shortest path.

Displaying PNNI Information

This section details how to display information about the PNNI system.

There are two types of information that can be displayed:

- Information relating to the Active and Future Configurations:
  - Node_0 information (ATM address, level identifier, and peer group id)
  - Path selection settings
  - Summary addresses.
- Information relating to the PNNI system itself:
  - Configuration status
  - Peer group members
  - Neighbors
  - PTSEs

Displaying Node_0 Information

The following parameters can be displayed for node_0:

- ATM address
- Level identifier
- Peer Group Id

To display the node_0 parameters for the Active configuration, enter the following command:

```
8260ATM> show pnni node_0
```

To display the node_0 parameters for the Future configuration, enter the following command:

```
8260ATM> show future_pnni node_0
```

Path Selection Settings

To display whether paths are set to be precomputed or set up on demand, enter one of the following commands.

For the Active configuration, enter the following command :

```
8260ATM> show pnni path_selection
```

For the Future configuration, enter the following command :

```
8260ATM> show future_pnni path_selection
```

Summary Addresses

To display the summary addresses already in effect (in the Active system), enter the following command :

```
8260ATM> show pnni summary_address
```

To display the summary addresses set in the Future configuration, enter the following command :

```
8260ATM> show future_pnni summary_address
```

The resulting display also includes an index number for each summary address set. This index number can be used to delete a summary address, when used in the following command:

```
8260ATM> clear pnni summary_addr <n>
```

where <n> is the index number of the address to be deleted.

Configuration State

To display the configuration state, enter the following command :

```
8260ATM> show pnni configuration_state
```

This displays whether the active configuration is saved or not, and whether a there is a pending commit.

Peer Group Members

```
8260ATM> show pnni node_0 peer_group_members
```

Neighbor Node Ids

To obtain a list of neighbor node ids enter the following command:

```
8260ATM> show pnni neighbor
```

Node ids are 22 byte identifiers that characterize a PNNI node. Neighbor nodes are nodes directly connected via one or more links to the node being referenced.

PTSEs

Key entities in PNNI are PNNI Topology State Elements (PTSEs). PTSEs are a collection of PNNI information that is flooded to all logical nodes within a peer group. Each node_0 creates its own PTSEs called *self originated* PTSEs, of which there are 6 types:

- Nodal State Parameter (NSP)
- Nodal Information Group (NIG)
- Internal Reachability (IR)
- External Reachability (ER)
- Horizontal Link (HL)
- Up Link (UL).

Summary information about these PTSEs can be obtained by issuing the following command:

```
8260ATM> show pnni ptse self_originated all
```

This lists the number of existing PTSEs of each type. If the summary shows the presence of, for example, 3 HL PTSEs, you can use a positive integer, smaller or equal to 3, to retrieve detailed information about the respectively indexed HL PTSE. Say, for example, you wish to inspect the second PTSE, then you would enter the following command:

```
8260ATM> show pnni ptse self_originated horizontal_link 2
```

The general structure of the command applies to all other PTSE types, you simply replace `horizontal_link` by `nodal_information_group`, `internal_reachability`, `external reachability`, `nodal_state_parameters`, or `up_link`.

Additionally, you can also display the PTSE's Resource Availability Information Groups (RAIGS) by including the parameter `with_raigs`. For example:

```
8260ATM> show pnni ptse self_originated horizontal_link 2 with_raigs
```

You can also limit the PTSE summary information displayed to only one type of self originated PTSE. For example, entering:

```
8260ATM> show pnni ptse self_originated horizontal_link
```

will display summary information about HL PTSEs only.

Self originated PTSEs are flooded to all other switches in the ATM PNNI network so that the database of any one switch contains copies of PTSEs issued by all other switches. These PTSEs can also be displayed. By entering the `show pnni peer_group_members`, you can obtain the index entry identifying the node id (which identifies the switch) whose PTSEs you want to display. If, for example, the index entry is 3, you would enter the following command:

```
8260ATM> show pnni ptse 3
```

to obtain summary information about all PTSE types issued by the respective node. Then you could display that node's second HL PTSE (assuming it exists), by entering the following command:

```
8260ATM> show pnni ptse 3 horizontal_link 2
```

and `with_raig` could be added, if required.

You can also limit the displayed PTSE summary information to one PTSE type. For example, entering the following command:

```
8260ATM> show pnni ptse 3 horizontal_link
```

will limit the summary to HL PTSEs issued by the switch whose node id corresponds to index 3. Remember that you obtain the node id to index mapping by entering a `show pnni peer_group_members` command.

Chapter 6. Configuring Ports and Media Modules

This chapter describes:

- How to enable ports and interfaces
- How to set up Virtual Path Channels (VPCs)
- How to configure reachable addresses
- How to set up permanent virtual connections (PVCs)
- The different ways of connecting switches
- How to allow or disallow duplicate ATM address registration.

Enabling ATM Ports and Interfaces

Before you can use the devices attached to the ATM media ports, you must enable each port and configure the type of interface used by the port to receive and transmit ATM data. For example, to enable port 2 of a module in slot 1 as a UNI port:

```
8260ATM> set port 1.2 enable uni
```

Note that you can specify multiple ports on the same module within the same command, for example `set port 1.2 3 5 4 7 enable uni` would enable ports 2, 3, 4, 5, and 7.

You can set a port to any of the ATM interfaces:

- User-to-Network (UNI)
- Public User-to-Network (public_UNI)
- Interim Inter-Switch Signalling (IISP)
- Private Network-to-Network (PNNI)
- VOID

See “Network Interfaces” on page 9 for more information on ATM network interfaces.

Note: To enable the ports, the module must be connected to the network. See the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide* for details on the SET MODULE CONNECTED command.

Setting Up Virtual Path Channels (VPCs)

VPC links can only be defined for VOID or Public UNI ports, and may be of UNI, IISP, or PNNI types.

UNI is used to connect user devices (such as Ethernet stations).

PNNI is used to connect switches within the same peer group, via a WAN.

IISP is used to connect switches in different peer groups, via a WAN.

Figure 2 on page 12 shows an example of these VPC links.

Virtual path channels (VPCs) are created via the SET VPC_LINK command. See the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide* for details.

Configuring Reachable Addresses

When VPC links (on Public UNI or VOID ports) are defined to connect to switches or workstations that do not support ILMI address registration, you also need to specify the address of the switch to be reached. To do this, you enter the SET REACHABLE_ADDRESS command.

If several reachable addresses share the same network prefix, they should be entered as a PNNI summary address to reduce PNNI traffic. See 43 for details on configuring summary addresses.

Setting Up Permanent Virtual Connections (PVCs)

PVCs can be set up to connect two end-points, local and remote. The local endpoint is a port in the local 8260/8285 and the remote endpoint can either be another port on the same 8260/8285 or on a remote 8260/8285

If the remote endpoint is located on a remote 8260/8285 you must define the ATM address of that 8260/8285.

For each PVC connection you can specify whether a reserved bandwidth is to be allocated.

The valid settings (shown as the number of bits used) for Virtual Path Identifiers (VPIs) and Virtual Channel Identifiers (VCIs) are as follows:

- **For 25Mbps ports:**

VPI	VCI
0	0-12
1 or 2	0-10
3 or 4	0-8

- **For all other ports:**

VPI	VCI
0	0-14
1, 2, 3, or 4	0-10
5 or 6	0-8

You can also specify if frame discard is to operational or not.

See the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide* for details on the SET PVC and SET PARTY PVC commands.

Connecting Switches

Switches can be connected either directly, through cabling, or indirectly via a WAN. Figure 1 on page 7 shows an example of the different types of connection.

Connecting Switches Directly

When connecting two switches directly you must:

- If the switches belong to the same peer group:
  1. Define the two connecting ports as PNNI links
  2. Ensure that the peer group id of both switches match (and are less than 104 bits in length). See "Configuring Peer Group Identifiers" on page 41 for more information.
- If the switches do not belong to the same peer group:
  1. Define the two connecting ports as IISP links

Example: The following example shows how to connect two switches in different PNNI peer groups.

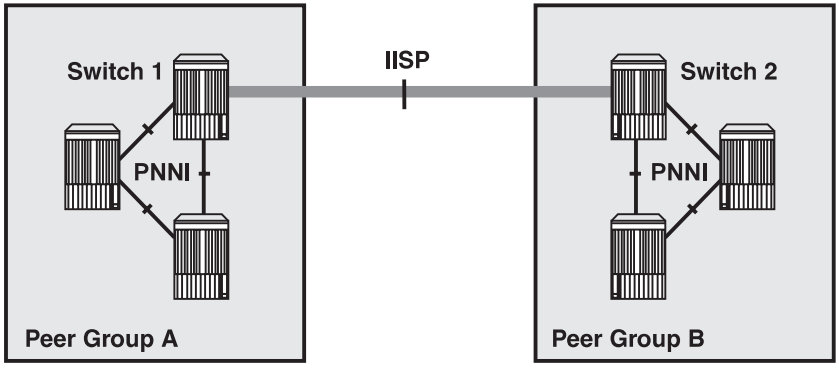

Figure 9. Connecting Switches in Different Peer Groups

This example shows how to connect Switch 1 in Peer Group A to Switch 2 in Peer Group B (using slot 6 port 1, of Switch A and slot 4 port 2 of switch B).

Assuming the network prefix of switch 1 in peer group A is 39.99.99.99.99.99.99.00.00.99.99.01, and the network prefix of switch 2 in peer group B is 39.99.99.99.99.99.99.00.00.99.99.02, then:

1. On switch A, you would enter the commands:

```
8260ATM> set port 6.1 enable iisp user
8260ATM> set reachable_address 6.1 96 39.99.99.99.99.99.99.00.00.99.99.02
```

2. On switch B, enter the commands:

```
8260ATM> set port 4.2 enable iisp network
8260ATM> set reachable_address 4.2 96 39.99.99.99.99.99.99.00.00.99.99.01
```

This is using the default VPI=0. If the VPI is not 0, you must define the VP at the end of the set reachable address, and set the port signalling version accordingly.

Connecting Switches via VPCs Over VOID or Public UNI Interfaces

1. In cases where it is not appropriate for an IISP link to use the default VPI (VPI=0), then the solution to interconnect switches is to define the port as a VOID port and set up a VP link with VPI=x.
2. VP tunneling over a WAN. Very often when a link crosses a WAN the service provider will not allow the use of VPI=0 because it is used for internal WAN traffic. Consequently, the private organization must use another VPI than the default. In addition, at both ends of the WAN, the VPI could be different, as shown in Figure 10.

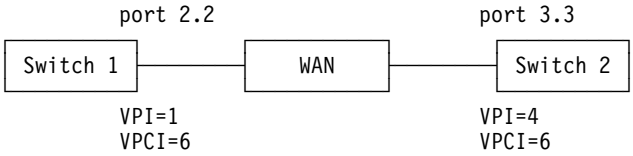

Figure 10. VP Tunneling Over a WAN

If Switch 1 and Switch 2 are part of th same PNNI peer group they will still be able to communicate thanks to the definition of the same Virtual Path Channel Identifier (VPCI) at both ends, achieved by entering the following commands:

```
8260ATM> set port 2.2 enable public_uni
8260ATM> set vpc_link 2.2 1 enable pnni bandwidth:155000 vpci:6
8260ATM> set port 3.3 enable public_uni
8260ATM> set vpc_link 3.3 4 enable pnni bandwidth:155000 vpci:6
8260ATM>
```

Connecting Switches via a WAN

When connecting two switches via a WAN you must:

- Define the two connecting ports as either Public UNI or VOID links.
- Define, via the SET VPC_LINK command, a VPC link between the ports, of type:
  - PNNI if the switches belong to the same peer group
  - IISP if the switches belong to different peer groups
- If the VPC link is type IISP, define, via the SET REACHABLE_ADDRESS command, the address that is to reached over link (at both ends). At the other switch, enter the reachable address of your switch.
- If the two switches are to belong to the same PNNI peer group, ensure that the peer group id of both switches match (and are less than 104 bits in length). See “Configuring Peer Group Identifiers” on page 41 for more information.

Allowing Duplicate ATM Addresses

Depending on network configuration and requirements, you can configure the ATM control point to allow or disallow the acceptance of duplicate ATM addresses registered from ILMI.

Disallowing duplicate addresses may, for example, be useful for backup servers.

Allowing duplicate addresses may be useful for load balancing between switches.

To specify whether duplicate addresses are allowed or disallowed, you enter the following command:

```
8260ATM> set device duplicate_atm_addresses allowed|disallowed
```

Chapter 7. Troubleshooting

This chapter describes how to diagnose and solve problems associated with the operation of Version 3 of the ATM Control Point.

The following problems are detailed in this chapter:

USA and Canada: If the problem is not resolved after following the troubleshooting procedures outlined in this chapter, call toll-free 800-IBM-SERV for IBM support.

Diagnosing Problems with ATM Ports

If all ATM modules are operational (`connected`, `hardware okay`, and `normal` displayed with SHOW MODULE VERBOSE), the cause of the problem may be due to an inoperable ATM port. To see if the ATM ports on a given module are functioning correctly, use the SHOW MODULE and SHOW PORT commands to display port status. Any of the following types of port status may appear:

-
- DOWN: Bad FPGA level
- DOWN: Module not operational
- DOWN: Hardware error
- DOWN: No activity
- DOWN: Inconsistency in bandwidth
- DOWN: Internal error
- DOWN: Invalid VPI-VCI range
- DOWN: Connection limit reached
- DOWN: Duplicate VPC
- DOWN: VPC limit reached
- DOWN: Signalling version missing
- DOWN: Not in service
- DOWN: Error detected
- UP: No address registration

The problem associated with each port status (except for Up contacted) and the action to take to solve it are described below. If, after trying to solve the problem, the status of ATM media ports does not change to `UP`, perform the Wrap test as described in the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide*. If you find that the module is faulty, replace it. For assistance, contact your IBM service representative.

Status: Down: Bad FPGA level

Explanation: The FPGA of the media module is not compatible with the FPGA of the ATM Control Point. Check the prerequisites in the Release Notes.

Steps to Take:

1. Upgrade the FPGA of the media module.

Status: Down: Module not operational

Explanation: The module cannot be made operational.

Steps to Take:

1. Use the SHOW MODULE VERBOSE command to display more information.
2. Check that the module is correctly installed.
3. Check that the module is connected to the network (use the SET MODULE CONNECTED command).
4. Check that the module is receiving power (use the SHOW HUB command with the 8260).
5. Check that the FPGA level of the module is supported.
6. If the problem persists, replace the ATM media module.

Status: Down: Hardware error

Explanation: The microcode encountered an error when setting the hardware.

Steps to Take:

1. If the problem persists after a reset, move the module to another slot.
2. If the problem persists, replace the ATM media module.

Status: Down: No activity

Explanation: No physical layer activity is detected (either there is no cable/fiber attached, or there is no signal on the Receive cable/fiber.

Steps to Take:

1. See if the port is enabled by entering the SHOW PORT command.
2. If the port is not enabled, use the SET PORT command to set the `mode` parameter to `enable`.
3. If the port is enabled, make sure that the remote device is operational and that its adapter is securely plugged in.
4. Make sure that the fiber/cable is securely plugged on the 8260/8285.
5. Enter the WRAP command to perform a wrap test.
6. If the wrap test result is `K0`, the problem is associated with the 8260/8285.
7. For SC-type connectors, check that the receive and transmit cables/fibers are not swapped.
8. For 25Mbps PNNI ports, make sure that the cables used to interconnect 8260/8285 switches are swapping the receive and transmit signals.

Status: Down: Inconsistency in bandwidth

Explanation: The bandwidth specifications are different at each end of a connection.

Steps to Take:

1. Use the SHOW PORT command to display the bandwidth specifications for each port.
2. Use the SET PORT command to ensure that the values match.

Status: Down: Internal error

Explanation: An internal error is detected on the port.

Steps to Take:

1. Reset the ATM media module using the RESET MODULE command.
2. If the problem persists, replace the ATM media module.

Status: Down: Invalid VPI-VCI range

Explanation: The VPI-VCI range entered for a given port is invalid.

Steps to Take:

1. Make sure that the range specified for the port is valid, and that the same range is applied at the other end of the connection. See “Setting Up Permanent Virtual Connections (PVCs)” on page 56 for valid settings.

Status: Down: Connection limit reached

Explanation: The maximum number of connections (including point-to-point and point-to-multipoint) allowed has been reached, either at the port level or module level. The maximum number allowed is 4064.

Status: Down: Duplicate VPC

Explanation: When a port is enabled, it is enabled with its associated vpi. The vpi is already in use for this port.

Steps to Take:

1. Delete the existing VPC is not required, and disable/enable the port.
2. Disable the port, then re-enable it with a different vpi value.

Status: Down: VPC limit reached

Explanation: The maximum number of VPCs (64) has been reached.

Steps to Take:

1. Delete an existing VPC to allow the creation of a new one.

Status: Down: Signalling version missing

Explanation: The signalling version must be specified if the interface does not support ILMI. The signalling version was not specified for a UNI or IISP port or VPCs.

Steps to Take:

1. Disable the port
2. Redefine the port specifying the signalling version for the attached device
3. Re-enable the port.

Status: Down: Not In Service (UNI port)

Explanation: Physical layer activity is detected (there is a receive signal on the Receive fiber/cable) but the remote device is not responding to ILMI polling.

Steps to Take:

1. Check that the remote device is operational and that its adapter is securely plugged in.
2. Make sure that the fiber/cable is securely plugged on the hub.
3. Enter the WRAP command to perform a wrap test.
4. If the wrap test result is K0, the problem is associated with the hub.
5. The peer device does not support ILMI. Change the UNI port configuration to suppress ILMI.
6. A PVC with VPI=0 is or was defined on that port. Release the PVC and disable/enable the port.
7. The transmit wire/fiber of the cable is defective. Replace the cable.
8. Some devices have restricted IMLI implementation and cannot access address registration if an LECS is defined in the 8260.

   Check that you have an LECS address configured in your 8260 with the command SHOW LAN_EMUL CONFIGURATION_SERVER command. If there should not be any LECS address defined, clear it with the CLEAR LAN_EMUL CONFIGURATION_SERVER ALL command.
9. Take traces from both the hub and the remote device for an IBM service engineer.

Status: Down: Not in Service (PNNI Port)

Steps to Take:

1. Use the command SHOW PORT slot.port VERBOSE command to determine the problem.
2. Check that the remote device is operational and that its adapter is securely plugged in.
3. Make sure that the fiber/cable is securely plugged on the hub.
4. Enter the WRAP command to perform a wrap test.
5. If the wrap test result is K0, the problem is associated with the hub.
6. The peer device does not support ILMI. Change the UNI port configuration to suppress ILMI.
7. A PVC with VPI=0 is or was defined on that port. Release the PVC and disable/enable the port.
8. The transmit wire/fiber of the cable is defective. Replace the cable.
9. Take traces from both the hub and the remote device for an IBM service engineer.

Status: Down: Error detected

Explanation: This indicates an ILMI protocol error. This status may be a result of a security violation on the port.

Steps to Take:

1. Enter the SHOW SECURITY PORT command to check that security is enabled for this port.
2. Enter the SHOW SECURITY LAST_VIOLATION command to check if an address registration has been rejected on the port.
3. Check that the attached device supports ILMI.
4. Perform a wrap test to check the connection to the attached device.
5. Re-enable the port.

Status: UP: No Address Registration

Explanation: ILMI is up but the connecting device does not accept address registration.

Problems with ATM Ports Attached to ATM Devices

After you attach ATM devices to ATM media ports, the status of the ports may still not change to `UP` (ready for ATM traffic). To diagnose this type of problem, follow these steps:

1. Use the SHOW PORT VERBOSE command (described in the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide*) to display the status of each port.
2. If the status of a PNNI or UNI port is `DOWN: NOT IN SERVICE`:
   - Refer to “Diagnosing Problems with ATM Ports” on page 64.
   - Make sure that the attached ATM device is operating properly (for example, the daemon is running).
   - Check the ATM address registration as described in “Checking ATM Address Registration” on page 69 (UNI ports only).
   - Perform the the Wrap test as described in the WRAP EXTERNAL command in the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide* If the test results show that the port status is `KO`, replace the module.
3. If the status of a port is `DOWN: NO ACTIVITY` and if a Turboways* 155Mbps/100Mbps/25Mbps workstation is attached to the port, make sure that the device is correctly installed:
   - Refer to “Diagnosing Problems with ATM Ports” on page 64.
   - Make sure that the adapter is securely plugged into the port.
   - Make sure that the cable is securely plugged into the adapter.
   - Make sure that the device driver is correctly installed by de-installing it and re-installing a new one.
4. If the status of a UNI port is `UP: NO ADDRESS REGISTRATION`, make sure that the ATM address of the attached device supports ATM address registration.

Checking ATM Address Registration

If you suspect that a problem is due to faulty ATM address registration between a switch and an attached ATM device, follow these steps:

1. Enter the SHOW PORT command to make sure that the ATM media port is configured with a UNI interface. If not, enter the SET PORT command and specify `uni` for the interface parameter.
2. Check that the port status shows `UP` (not `UP: NO ADDRESS REGISTRATION`, which would indicate an ILMI protocol error). ATM address registration can only occur when ILMI is up.
3. Make sure that the attached device supports the ATM network prefix used by the switch.
4. Make sure that the device supports ATM address registration. To check whether the device registered its ATM address, use the command SHOW REACHABLE_ADDRESS (with the `DYNAMIC` parameter). Make sure that the reachable address is also shown as active.
5. Make sure that the device is not using a protocol for ATM address registration that is incompatible with the protocol used by the switch.
6. Contact your IBM service representative.

Problems with Normal ATM Operation

The problems in this phase occur after ATM traffic is started in the network between ATM devices attached to ATM media ports. The ATM port status is UP.

Important: Problems in the normal operation of your ATM network may occur when the maximum number of virtual connections (VCs) allowed on a switch or an individual ATM media module is exceeded. The maximum number of virtual connections supported (in a burst) is as follows:

- **6144** per switch
- **4064** per ATM media module (with up to 4064 VCs per ATM media port).

In normal operation 95% of the above figures should be considered as the maximum.

You should also be aware of the following maximums:

- 128 reachable addresses per switch
- 127 point-to-multipoint connections per switch
- 100 PVCs per switch
- 512 ESIs per switch
- 180Mbps reservable bandwidth per module (for IISP and PNNI).

You should ensure that the ports and both ends of a connection are using the same VPI/VCI settings. See “Setting Up Permanent Virtual Connections (PVCs)” on page 56 for valid settings.

If you cannot solve the problem after performing the troubleshooting operations described in this section, contact your IBM service representative.

8260/8285 Cannot PING the ARP Servers and Vice-versa

Use the SHOW DEVICE command and look at the Q2931 cause code:

Cause Code: 31

Explanation: The IP address of the switch is not in the same IP subnet as the ARP server.

Steps to Take:

1. Change the IP address or IP subnet mask of the 8260/8285.

Cause Code: 1

Explanation: A wrong ARP server address was entered with the SET DEVICE ARP_SERVER command, or the status of the port of the ARP server is `DOWN: NOT IN SERVICE` or `DOWN: NO ACTIVITY`.

Steps to Take:

1. Check that the status of the port attached to the ARP server is `UP`, then check that the ATM address shown by the ARP server is exactly the same as the one entered in the 8260/8285 (by entering the SHOW DEVICE command).

Cause Code: 3

Steps to Take: If the ARP server is in the same peer group (PNNI links):

1. A PNNI port has not enough bandwidth. Having several PNNI ports on the module may reach the bandwidth limit.

   Spread the ports over several modules.

2. A connection has failed. Action to take varies according to the type of connection that has failed.

If you cannot solve the problem, take a PNNI dump (with the DUMP PNNI topology_data_base command), and contact your IBM representative.

Cause Code: 3

Steps to Take: If the ARP-server is in another peer group (IISP links):

1. The IISP network-side/user-side definition rules have not been applied.

   Check that one side of the link is defined as user, and that the other side is defined as network.

2. No VPC link has been defined for the port.

   Define the link, using the SET VPC_LINK command.

3. The peer logical links do not match (bad vpi match, bad cluster match, bad bandwidth match).

   Check that the logical links on both sides match, and if necessary, clear those logical links are re-define them.

4. No reachable address has been defined, if the 8260/8285 and the ARP-server are in different ATM peer groups.

   Define the reachable address using the SET REACHABLE_ADDRESS command.

5. A reachable address was badly configured.

   Check the reachable addresses, using the SHOW REACHABLE_ADDRESS command.

6. The VP-tunnel is defective.

   Ask your VP-tunnel provider to test it.

8260/8285 LEC Cannot Register to the LES/BUS

Use the SHOW DEVICE command and look at the `subnet lan emulation` status message:

Abnormal Termination: LES connection cleared. ATM Forum cause xx:

The LEC automatically tries to reconnect to the LES/BUS when the connection is lost. It will try to reconnect every 5 seconds, 5 times, and thereafter every 1 minute.

Cause Code: 1

Explanation: A wrong LES address was entered using the SET DEVICE LAN_EMULATION_CLIENT command (`les_atm_address` parameter), or the port attached to the LES is not in service.

Steps to Take:

1. Check is the port status is `UP` (via the SHOW PORT command), then check that the LES ATM address is exactly the same as the one entered in the 8260/8285.

Cause Code: 3

Steps to Take:

- If the LE server is in the same peer group (PNNI links):
  1. A PNNI port has not enough bandwidth. Having several PNNI ports on the module may reach the bandwidth limit. Spread the PNNI ports over several modules.
  2. The ATM address of an 8260/8285 located on the PING path has been changed.

     Disable the PNNI link and re-enable it.

  If the above does not solve the problem, take a PNNI dump (with the DUMP PNNI command), and contact your IBM representative.
- If the LE server is in another peer group (IISP links):
  1. The IISP network-side/user-side definition rules have not been applied.

     Check that one side of the link is defined as user, and that the other side is defined as network.

     Check that the same signalling stack (3.0 or 3.1) is used at each end of the link.
  2. No logical-link has been defined for the port.

     Define the logical link, using the SET REACHABLE_ADDRESS command.
  3. The peer logical links do not match (bad vpi, peer group id, or bandwidth match).

     Check that the reachable addresses on both sides correspond, and if necessary, re-define them.
  4. The VPI number does not match.

     Correct the VPI number using the SET PORT command.
  5. The VP-tunnel is defective.

     Ask your VP-tunnel provider to test it.

Cause Codes: 16/31

Explanation: The connection has been voluntarily rejected the LE server. The reason depends on LE server implementation.

Cause Codes: 18/102

Explanation: The LE server is present, but not started.

Cause Code: 47

Explanation: There may be a lack of resources on the LE server side preventing connection to it.

ATM/LAN Bridge is De-registered from 8260/8285 LES

The ATM/LAN bridge cannot support a bigger frame size than 1516, but the 8260/8285 LES has a larger size defined.

Perform the following:

1. Stop the LES (with the SET LAN_EMUL_SERVER STOP command).
2. Restart the LES, specifying a maximum frame size of 1516 (with the SET LAN_EMUL_SERVER START command). See the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide* for details.

ATM Forum LAN Emulation Ethernet and TCP/IP (DOS, OS/2) Not Working

Default parameters of DOS TCP/IP and 8260/8285 Ethernet LEC do not match; a DOS TCP/IP station cannot ping an 8260/8285.

The 8260/8285 TCP/IP LEC is Ethernet 802.3 by default (with version v1.0.0). The IBM TCP/IP drivers for DOS and OS/2 are configured for DIX (Ethernet v2) by default. As a result, the TCP/IP IBM stations configured with the default parameters will not be able to ping the 8260/8285

Perform either of the following:

1. Change the TCP/IP frame type to 802.3 on the TCP/IP stations, using the CUSTOM.EXE ('Advanced Configuration') for DOS TCP/IP, or the TCPIPCFG.EXE for OS/2 TCP/IP 2.0.
2. Keep the TCP/IP frame type of DIX and change the 8260/8285 LEC Ethernet type to DIX, using the command SET DEVICE LAN_EMULATION_CLIENT ETH_TYPE DIX.

DOS TCP/IP Installation TIPS

To install the TW25 adapter for TCP/IP:

1. Install the TW25 drivers for 802.3 from the TW25 disks.
2. Install TCP/IP with the NODIS interface.
3. Append the NDIS.DDI file with the TW25 information. For example, `copy c:/tcpdos/etc/ndis.ddi + a:/eth/at25led.ddi c:/tcpdos/etc/ndis.ddi`
4. Run CUSTOM.EXE. The ATM adapter will now appear in the drop-down box.
5. Do not allow the CUSTOM.EXE to overwrite the PROTMAN or AT25LED lines.
6. The CUSTOM.EXE will now complete. The PROTOCOL.INI in the AT25LEI directory will be the one TCPDOS appends with its stanza.

Problems in an IBM Proprietary LAN Emulation Environment

LES Monitor Statistics: Default Vccs counter oscillating, too few registered workstations.

Explanation: The workstation knows its ATM address, but that address has been de-registered at the Switch/Control-point level. This happens when the workstation is behind a concentrator (8282) that has been disconnected from the switch for a short time.

Steps to Take:

1. Wait a few minutes for the new registration to take place.

Note: You can check whether the station is registered in the 8260/8285 by using the command SHOW REACHABLE_ADDRESS.

ATM Control Point and Switch Module Problems (8260 only)

Standby ATM Control Point and Switch Does Not Mirror Active ATM Control Point and Switch (8260 only)

Explanation: In normal operation, the standby ATM Control Point and Switch should continually mirror any changes made to the active ATM Control Point and Switch.

If this is not being done, this is because the microcode versions are not the same on both ATM Control Point and Switch modules.

Steps to Take: There are two cases to consider:

1. The active ATM Control Point and Switch is at an older level than the standby ATM Control Point and Switch

   Perform the following steps:

   a. Download inband the new microcode from a TFTP server, by following the installation instructions associated with the new microcode.

   b. At maintenance time, swap the microcode on the active ATM Control Point and Switch.

2. The active A-CPSW is at an newer level than the standby ATM Control Point and Switch:

   Perform the following steps:

   a. On the standby ATM Control Point and Switch, force the maintenance mode (by issuing the command MAINTAIN force).

   b. On the standby ATM Control Point and Switch download out-of-band the microcode (providing the out-of-band download is allowed in the installation instructions).

   c. If the out-of-band download is NOT allowed, you need to plan a maintenance period (of at least one hour) where you will:

      - Manually copy the TCP/IP and port configuration of the active ATM Control Point and Switch to the standby ATM Control Point and Switch.
      - Remove the active ATM Control Point and Switch from the hub.
      - Enter the right TFTP parameters on the remaining ATM Control Point and Switch, in order to download the new microcode.
      - Download the new microcode.
      - Swap the microcode.
      - Remove the ATM Control Point and Switch module from the hub (non are installed now).
      - Reinsert the original A-CPSW module.
      - Reinstall the second A-CPSW module, which will copy all the configuration parameters of the active one.

Some Modules not Managed by ATM Control Point and Switch in Slots 11 and 12

Explanation: This problem can become apparent when an active ATM Control Point and Switch in slots 9 and 10 fails, and the standby ATM Control Point and Switch (in slots 11 & 12) becomes active.

Only modules with an FPGA level of 8 or above can be managed by an ATM Control Point and Switch module in slots 11 & 12.

Steps to Take: To resolve this, you must upgrade the modules to the following levels:

A4-FB100 8

A4-SC100 8

A2-MB155 81

There are two ways to achieve this:

1. Download from Internet the file `atmmedia.zip` from the following URL:

   A4-FB100 `http://www.networking.ibm.com/826/8265004.html`

   A4-SC100 `http://www.networking.ibm.com/826/8265104.html`

   A2-MB155 `http://www.networking.ibm.com/826/8265002.html`

2. Order Field B/M 51H4282, EC E28134 (no charge).

ATM Connection Problems

No Connection between Two Switches in the Same Peer Group

Steps to Take:

1. Use the SHOW PORT VERBOSE command to:
   - Make sure that the ATM media port at each end of the connection is configured with a PNNI interface. If not, use the SET PORT command and specify `PNNI` as the interface parameter.
   - Make sure that the status of each port is `UP`. If not, follow the procedure described in “Problems with ATM Ports Attached to ATM Devices” on page 68.
2. Make sure that the bandwidth specified is the same at both ends of the trunk.

   If you have not specified a bandwidth, make sure that the bandwidth of of the module is exceeded.
3. Contact your IBM service representative.

No Connection Between Two ATM Switches in Different Peer Groups

Steps to Take:

1. Use the SHOW PORT command to:
   - Make sure that the ATM media port at each end of the connection is configured with an IISP interface. If not, use the SET PORT command and specify `IISP` as the interface parameter.
   - Make sure that the status of each port is `UP`. If not, follow the procedure described in “Problems with ATM Ports Attached to ATM Devices” on page 68.
2. Use the SHOW REACHABLE_ADDRESS command to:
   - Make sure that the ATM address of each hub is configured with a reachable address of the other one.
3. Use the SHOW PORT command to make sure that the VPI of the ATM media ports on each boundary hub are correctly configured.
4. If the connection is over a VP service provider, refer to your contract with the VP service provider to make sure that certain settings (for example, VP identifier) are correct.
5. Contact your IBM service representative.

Cannot create a PVC between two 8260/8285s located in different peer groups.

Explanation:

- This is normal. The 8260/8285 does not allow the creation of PVCs over network-to-network (IISP) links.
- You have created two different PVCs, each one ending at the IISP port.

  Note: Make sure that the VPI used by the PVC on the IISP port corresponds to the one of the logical link defined on that port.

Problems of ATM connections/performance through a WAN (VP tunnel).

Steps to Take:

1. Check the Switch configurations at both sides:
   - check that the VPI corresponds to the VPI provided by your network provider.
   - check that the bandwidth is lower or equal to the Maximum Peak Rate negotiated with your network provider.

   The actual bandwidth used by your media modules is the maximum one (155 Mbps for an A2-MB155 module, 100 Mbps for an A4-FB100 module etc.), even if a lower value is specified with the SET PORT command.
   - check that one IISP port on one side is defined as 'network' and that the IISP port on the other side is defined as 'user'.
   - if you are using singlemode A2-MB155 modules, you probably have to define the clocking as external, using the SET PORT command (the clock is usually provided by the WAN). In addition, to specify the type of network (SONET or SDH) at the end of the SET PORT command.
2. If the previous steps did not help, then you require an ATM Analyzer for the following tests:
   - Hardware wrap test through the WAN up to the media module, install the ATM Analyzer at one side of the WAN, and the 8260/8285 at the other. Disable your IISP port, and enter the command WRAP slot.port REPLY_MODE ENABLE. Your port is now redirecting Received Cells to the transmit side. Now, from the ATM Analyzer, generate traffic on the VCI=5, and compare the outgoing cells with the incoming cells. If some cells are lost or corrupted, contact your public network provider. When you are finished, enter the command WRAP slot.port REPLY_MODE DISABLE.
   - Hardware wrap test through the WAN up to the media module, install the ATM Analyzer at one side of the WAN, and the 8260/8285 at the other. Enable your port, and create a PVC from the VCI=x to a VCI=y on the same port, using the command SET PVC. Check that the PVC is active using the command SHOW PVC ALL. Now, from your ATM Analyzer, generate traffic on the VCI=x, and compare it with the received cells on the VCI=y. If some cells are lost or corrupted, contact your IBM representative.

Bad Communication Between 8260/8285 and 25Mbps Adapters

The port is either `NOT-IN-SERVICE`**, or is** `UP` **but some cells are lost.**

Explanation: The flow control on all 25Mbps adapters attached to the 8260/8285 must be disabled. This flow control (of OAM F4 cells) is not supported on the 8260/8285, whereas it is supported on the ATM concentrator 8282.

Steps to Take: Disable the flow control on the 25Mbps adapters. Refer to the documentation associated with the adapter.

Network Access Security Problems

All ATM Registration Attempts Rejected

Steps to Take: The action to take depends on whether the ports are disabled or not after the registration rejection.

1. Ports are disabled (Status = DOWN: ERROR DETECTED)

   Check that the addresses authorized have been correctly entered (SHOW SECURITY ATM_ADDRESS command).

2. Ports are enabled

   The problem is due to an empty address table. Check that the TFTP download of the address was successful (see “No ATM Addresses Displayed”)

Some ATM Registration Attempts Rejected

Steps to Take:

1. The problem may be due to addresses incorrectly entered in the access control address table. Check the file contents.
2. Check that both full ATM address and ESI address (with the same ESI address) have not been defined for the same setting (either specific port or any port). Remove one of the entries if this is the case.

No ATM Addresses Displayed

Explanation: No addresses are displayed when you enter the SHOW SECURITY ATM_ADDRESS command.

Steps to Take:

1. Security may have been de-activated at the time of the last reset (the address tables will not have been downloaded).

   You can recover the tables by setting security on (SET SECURITY MODE ACCESS_CONTROL) and performing a reset.

2. The TFTP download operation failed after the last reset.

   Check the result of the TFTP download by entering the SHOW SECURITY TFTP command. Usually, if the download fails, the operation is retried until successful or deactivated by setting security off (SET SECURITY MODE NO_SECURITY). If the retry is successful, the download will be automatically performed. If you disable security, the download operation is stopped and you should manually test the TFTP link by manually downloading the address table (see page 31). Once the link is operational, perform a reset to download the address tables.

   The TFTP error may be due to a file access problem on the TFTP server. Check that access is allowed.

Address Cannot be Set: Limit Reached

Explanation: A maximum of 512 addresses may be set. Once the limit is reached, you must remove some addresses before adding others.

Steps to Take: See page 26 for information on how to remove addresses.

Further Assistance

For further assistance with a troubleshooting problem, call your IBM representative, providing as much of the following information as possible:

- The name of the ‘failing part’ or ‘possible failing part’, if indicated in the troubleshooting procedure
- Types and slot numbers of all modules installed in the 8260/8285.
- Output of the following commands:
  - SHOW DEVICE
  - SHOW HUB (8260 only)
  - SHOW LAN_EMUL_SERVERS
  - SHOW LAN_EMUL CONFIGURATION_SERVER
  - SHOW MODULE ALL VERBOSE
  - SHOW PORT ALL
  - SHOW PNNI
  - SHOW PVC
  - SHOW REACHABLE_ADDRESSES
  - SHOW SECURITY
  - SHOW VPC_LINK
- Type and characteristics of each ATM device attached to the 8260/8285.
- On/Off condition and color of the all ATM Port LEDs and 8260/8285 Status LEDs.
- Last ATM commands entered from the local console
- Error log information uploaded to the host by entering the UPLOAD command
- Trace information uploaded to the host by entering the UPLOAD command
- Dump information uploaded to the host by entering the UPLOAD command
- Q.2931 error code for the clear cause in the SVC.
- The following information from Campus Manager - ATM Version 2 (if installed):
  - SVC list for this interface (Interface panel)
  - Call logging list for this node (Node panel)
  - Interface information listed in the configuration panel for this node (Node panel)
  - Registered address list associated with this interface (Interface panel).

Notes:

1. In order to record trace information, perform dumps, and upload the error log, you must use a TFTP file server reachable from the 8260/8285.
2. For information on how to record trace information, see “TRACE Information” on page 83.
3. For more information on the UPLOAD command, see the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide*.

TRACE Information

In order to record trace information, follow these steps:

1. Use a TFTP file server reachable from the 8260/8285.
2. Reproduce the problem and activate the trace facility by entering `SET TRACE MAIN_TRACE ON`.
3. If requested by the service representative, start a specific trace or enter SET TRACE ALL ON to trace all activities.
4. Stop the trace by entering the SET TRACE MAIN_TRACE OFF command.

Note: The TRACE may degrade system performance while active.

For more information on the SET TRACE command and types of trace available, see the *IBM 8260/8285 ATM Control Point Version 3 Command Reference Guide*.

Appendix A. Error and Information Codes

This appendix contains explanations of the error and information codes displayed for the Q.2931 protocol, the IBM LAN Emulation Server error codes, and the codes issued from Maintenance Mode.

Q.2931 Error Codes for Clear Causes

Table 3 lists the error codes from the Q.2931 protocol for clear causes generated by 8260/8285s and other ATM devices in an 8260/8285-based ATM network. For a detailed explanation of each cause, see the *ATM User-Network Interface Specification - Version 3.0 and Version 3.1*.

The decimal and hexadecimal values of the codes are both given below. The terminal dialog issues the codes in hexadecimal format.

Table 3 (Page 1 of 2). Q.2931 Error Codes for Clear Causes in 8260/8285-based ATM Networks

Error Code (decimal)	Error Code (hex)	Meaning of Clear Cause
1*	0x01*	ATM address not defined/assigned.
2	0x02	There is no route to the transit network.
3*	0x03*	There is no route to the destination.
10*	0x0A*	VPI/VCI is unacceptable.
16	0x10	Normal clearing (UNI 3.1)
17	0x11	User is busy.
18*	0x12*	No user is responding.
21	0x15	Call has been rejected.
22	0x16	ATM address has changed.
27*	0x1B*	Destination is out of order.
28	0x1C	Invalid ATM address format (address incomplete).
30*	0x1E*	Response to STATUS ENQUIRY.
31*	0x1F*	Normal, unspecified (UNI 3.0)
35*	0x23*	Requested VPI/VCI is unavailable.
36	0x24	VPI/VCI assignment failed (on user side) (UNI 3.1).
37	0x25	User cell rate not available (UNI 3.1).
38*	0x26*	Network is out of order.
41*	0x29*	Temporary failure.
43	0x2B	Access information has been discarded.
45*	0x2D*	No VPI/VCI is available.
47*	0x2F*	Resource is unavailable, unspecified.
49*	0x31*	Quality of Service is unavailable.
51*	0x33*	User cell rate is not available (UNI 3.0).
57	0x39	Bearer capability is not authorized.
58	0x3A	Bearer capability is not available.
63*	0x3F*	Service or option is not available, unspecified.
65	0x41	Bearer capability is not implemented.

Table 3 (Page 2 of 2). Q.2931 Error Codes for Clear Causes in 8260/8285-based ATM Networks

Error Code (decimal)	Error Code (hex)	Meaning of Clear Cause
73*	0x49*	Unsupported combination of traffic parameters.
81*	0x51*	Invalid call reference value.
82	0x52	Identified channel does not exist.
88	0x58	Incompatible destination.
89*	0x59*	Invalid end-point reference.
91	0x5B	Invalid transit network selection.
92*	0x5C*	Too many pending add-party requirements.
93*	0x5D*	AAL parameters cannot be supported.
96*	0x60*	Mandatory information element is missing.
97*	0x61*	Message type does not exist or is not implemented.
99*	0x63*	Information element does not exist or is not implemented.
100*	0x64*	Invalid information element contents.
101*	0x65*	Message is not compatible with call state.
102*	0x66*	Expiry of recovery on timer.
104*	0x68*	Incorrect message length.
111*	0x6F*	Protocol error, unspecified.

Note: Q.2931 codes generated by the 8260/8285 are shown with an asterisk (*).

IBM LAN Emulation Server Error Codes

Table 4. IBM LAN Emulation Server Error Codes

Error Code	Meaning
1	Network cause
2	Internal cause
3	Memory exhausted
4	Network is down

Maintenance Codes

The following table explains the prompts that can be displayed in Maintenance Mode.

Table 5. Maintenance Codes and Meanings

Code	Meaning
>>0020>>	The NVRAM diagnostics failed, the battery may be low.
>>0021>>	Bad checksum, the loading or de-compression of the operational code failed.
>>0022>>	8260 only. After 3 retries, the switch FPGAs did not initialize properly.
>>0023>>	8285 only. After 3 retries, the base FPGAs did not initialize properly.
>>0030>>	The initialization or the diagnostics failed for the switch, the SPU (Switch Processing Unit), or the serial link.
>>0031>>	The ATM wrap test from the control point to the switch failed.
>>0032>> >>0033>> >>0034>>	The initialization of the operational code was halted due to insufficient memory.
>>0035>>	8285 only. FAT and other signals tested failed with wrap expansion plug.
>>0036>>	8285 only. After 3 retries, the base FPGAs did not initialize properly.
>>0040>>	8260 only. Active to backup CPSW polling does not work, SPI serial link may fail.
>>0050>>	8260 only. No FPGA picocode level (active or backup) in the A-CPSW module matches the active microcode level, and the backup microcode of the A-CPSW module is either unavailable or identical to the active one.
>>0051>>	The SWAP of the ATM control point FPGA picocode terminated in error.
>>0052>>	A connected ATM media module has no FPGA picocode matching the A-CPSW microcode level. This is a normal condition for the first A-CPSW of a redundant 8260 during the automatic migration process to level B50. It makes the second A-CPSW active, allowing the upgrade of the rest of the 8260. Once the whole 8260 is upgraded, the A-CPSW displaying >>0052>> becomes either active or standby at the next reset.
>>00BA>>	Maintenance mode is running with the backup daemon.

Appendix B. ATM Address Formats

The 8260/8285 ATM subsystem supports the addressing scheme defined by the ATM Forum for addressing end-points in private ATM networks. The scheme is modeled after the format of the OSI Network Service Access Point (NSAP) as specified in ISO-8348 (CCITT X.213).

As shown in Figure 11, the ATM Control Point supports the three initial domain identifier (IDI) formats specified by the ATM Forum:

- DCC (Data Country Code)
- E.164 (Specific Integrated Service Digital Network Number).
- ICD (International Code Designator)

Each of the three ATM address formats is 20 bytes long and consists of two main parts:

- Network Prefix (13 bytes)
- End System Part (7 bytes).

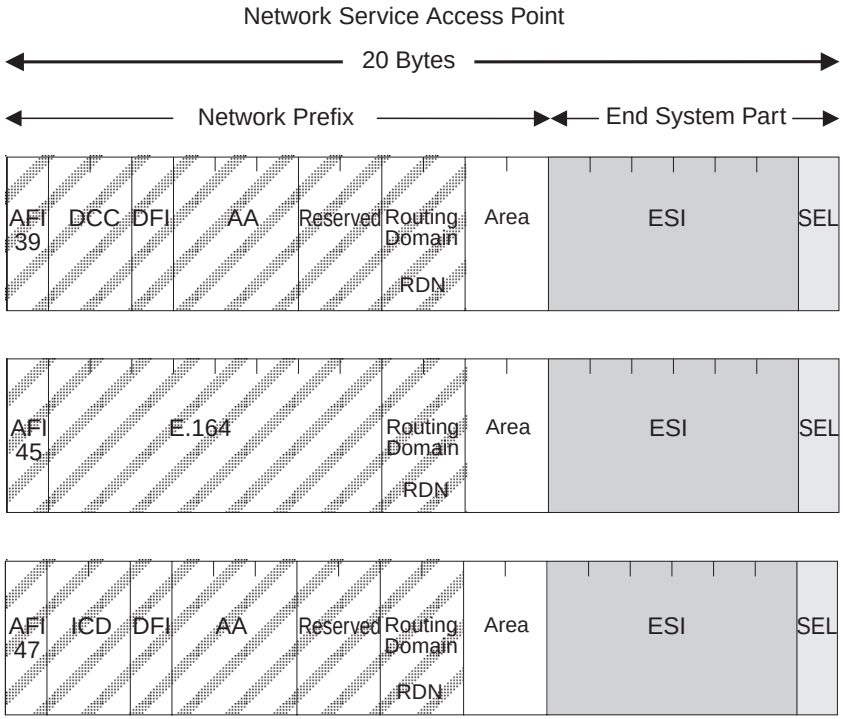

Figure 11. NSAP Address Formats Supported in the 8260/8285 ATM Subsystem

Network Prefix

The fields that make up the Network Prefix part of an ATM address include:

AFI The one-byte AFI identifies the authority allocating the portion of the address that follows. It defines the structure of the NSAP format. The AFI values accepted by the 8260 ATM subsystem are as follows:

- 39 (ATM format of the Domain-Specific Part)
- 45 (ATM format of the E.164 Initial Domain Identifier)
- 47 (ATM format of the International Code Designator).

DCC Data Country Code (2 bytes)

Specifies the country in which the address is registered. The codes are given in ISO-3166.

This value is handled as a bit mask and is not checked by the ATM subsystem.

DFI Domain-specific Format Identifier (1 byte)

Specifies the structure, semantics, and administrative requirements for the remainder of the address.

This value is handled as a bit mask and is not checked by the ATM subsystem.

AA Administrative Authority (3 bytes)

Identifies the organizational entity that allocates addresses for the remainder of the domain-specific part.

This value is handled as a bit mask and is not checked by the ATM subsystem.

E.164 E.164 IDI (8 bytes)

Specifies the international addressing format used by B-ISDN public transport providers and is up to 15 digits long (BCD syntax). This field is padded with leading '0000' semi-bytes to reach the maximum length. A closing semi-byte '1111' is used to obtain an integral number of bytes.

This code is handled as a bit mask and is not checked by the ATM subsystem.

ICD International Code Designator (2 bytes)

Identifies an international organization. Values and codes (BCD syntax) are assigned by the ISO-6523 registration authority.

This code is handled as a bit mask and is not checked by the ATM subsystem.

Reserved 2 bytes set to binary zero.

RDN Routing Domain Number (2 bytes)

Specifies a domain that is unique within one of the following:

E.164
DCC/DFI/AA
ICD/DFI/AA

and that allows for the same addressing scheme and administrative authority to be used.

Area Area (2 bytes)

Specifies an area unique within a routing domain for the purpose of hierarchical routing and efficient use of resources based on topological significance.

In an 8260/8285 ATM subsystem, this value consists of two 1-byte subfields, that can be used either:

- to uniquely identify switches within a peer group
- as part of the peer group identifier

End System Part

The fields that make up the End System part of an ATM address are:

ESI End System Identifier (6 bytes)

Identifies an end system unique within an area or within any larger addressing structure such as the IEEE MAC address space. Not used for routing within the ATM network.

SEL SELector (1 byte)

Has local significance only within the end system.

Glossary

This glossary defines terms and abbreviations used in this manual. It includes terms and definitions from the *IBM Dictionary of Computing* (New York; McGraw-Hill, Inc., 1994).

(A) Identifies definitions from the *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018.

(E) Identifies definitions from the *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronics Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, DC 20006.

(I) Identifies definitions from the *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1).

(T) Identifies definitions from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1.

The following cross-references are used in this glossary:

Contrast with
This refers to a term that has an opposed or substantively different meaning.

See
This refers the reader to multiple-word terms in which this term appears.

See also
This refers the reader to terms that have a related, but not synonymous, meaning.

Synonym for
This indicates that the term has the same meaning as a preferred term, which is defined in the glossary.

If you do not find the term you are looking for, refer to the index or to the *IBM Dictionary of Computing*.

A

ABR. Available bit rate.

ACR. Allowed cell rate.

active. (1) Able to communicate on the network. A token-ring network adapter is active if it is able to transmit and receive on the network. (2) Operational. (3) Pertaining to a node or device that is connected or is available for connection to another node or device. (4) Currently transmitting or receiving.

adapter. In a LAN, within a communicating device, a circuit card that, with its associated software and/or microcode, enables the device to communicate over the network.

address. (1) In data communication, the IEEE-assigned unique code or the unique locally administered code assigned to each device or workstation connected to a network. (2) To refer to a device or an item of data by its address (A).

Address Resolution Protocol (ARP). A protocol for converting a higher level protocol address (for example, an IP address) into a physical network address (for example, an ATM address).

AFI. Authority and Format Identifier (1 byte) in an ATM address.

AIX. Advanced Interactive Executive. The AIX operating system is IBM's implementation of the UNIX operating system.

alert. (1) For IBM LAN management products, a notification indicating a possible security violation, a persistent error condition, or an interruption or potential interruption in the flow of data around the network. (2) In SNA, a record sent to a system problem management focal point to communicate the existence of an alert condition. (3) In the NetView for AIX program, a high-priority event that warrants immediate attention. This database record is generated for certain event types that are defined by user-constructed filters.

allowed cell rate (ACR). An ABR service parameter. ACR is the current rate, in cells/sec at which a source is allowed to send data.

American National Standard Code for Information Interchange (ASCII). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphics characters. (A)

ARP. Address Resolution Protocol.

ASCII. American National Standard Code for Information Interchange.

Asynchronous Transfer Mode (ATM). A transfer mode in which the information is organized into cells. It is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.

ATM. Asynchronous Transfer Mode.

ATM campus network. A union of privately-owned ATM subsystems interconnected by network node interfaces (PNNIs). See also *private network node interface (PNNI)*.

ATM device. An end system that encapsulates data into ATM cells and forwards them to the ATM subsystem in the 8260/8285 across an UNI interface.

ATM subnetwork. A set of ATM subsystems interconnected by ATM interfaces (UNI, IISP, PNNI).

ATM subsystem. The ATM components in an ATM switch.

attach. To make a device a part of a network logically. Contrast with *connect*, which implies physically connecting a device to a network.

Authority and Format Identifier. One byte in an ATM address.

available bit rate (ABR). ABR is an ATM layer service category for which the limiting ATM layer transfer characteristics provided by the network may change subsequent to connection establishment. A flow control mechanism is specified which supports several types of feedback to control the source rate in response to changing ATM layer transfer characteristics.

B

bandwidth. The bandwidth of a link designates the information-carrying capacity of the link and is related to the maximum bit rate that a link can support.

BER. Bit Error Rate.

bit error rate (BER). The ratio of the number of bits experiencing error on a telecommunications link divided by the number of bits sent over the link.

bits per second (bps). The rate at which bits are transmitted per second. Contrast with *baud*.

bridge. (1) An attaching device that connects two LAN segments to allow the transfer of information from one LAN segment to the other. A bridge may attach the LAN segments directly by network adapters and software in a single device, or may connect network adapters in two separate devices through software and use of a telecommunications link between the two adapters. (2) A functional unit that connects two LANs that use the same logical link control (LLC) procedures but may use the same or different medium access control (MAC) procedures. (T) Contrast with *gateway* and *router*.

broadband. A frequency band divisible into several narrower bands so that different kinds of transmissions such as voice, video, and data transmission can occur at the same time. Synonymous with *wideband*.

broadcast. Simultaneous transmission of data to more than one destination.

BUS. Broadcast and Unknown Server.

byte. (1) A string that consists of a number of bits, treated as a unit, and representing a character. (T) (2) A binary character operated upon as a unit and usually shorter than a computer word. (A) (3) A string that consists of a particular number of bits, usually 8, that is treated as a unit, and that represents a character. (4) A group of 8 adjacent binary digits that represent one extended binary-coded decimal interchange code (EBCDIC) character.

C

CBR. Constant Bit Rate.

CCITT. Comité Consultatif International Télégraphique et Téléphonique. The International Telegraph and Telephone Consultative Committee.

cell loss ratio (CLR). CLR is a negociated QoS parameter and acceptable values are network-specific. The objective is to minimize CLR provided the end-system adapts the traffic to changing ATM layer transfer characteristics. The CLR is defined for a connection as Cells Lost/total Transmitted Cells. The CLR parameter is the value of CLR that the network agrees to offer as an objective over the lifetime of the connection. It is expressed as an order of magnitude, having a range of 10-1 to 10-15, and unspecified.

CLP. Cell Loss Priority.

CLR. Cell Loss Ratio.

configuration. (1) The arrangement of a computer system or network as defined by the nature, number, and chief characteristics of its functional units. More specifically, the term may refer to a hardware configuration or a software configuration. (I) (A) (2) The devices and programs that make up a system, subsystem, or network.

connect. In a LAN, to physically join a cable from a station to an access unit or network connection point. Contrast with *attach*.

connection. (1) In data communication, an association established between functional units for conveying information. (I) (A) (2) In Open Systems Interconnection architecture, an association established by a given layer between two or more entities of the next higher layer for the purpose of data transfer. (T) (3) In SNA, the network path that links two logical units (LUs) in different nodes to enable them to establish communications. (4) The path between two protocol functions, usually located in different machines, that provides reliable data delivery service. (5) A logical association between a call participant (party) and a switch. A party's connection represents that party's participation in a telephone call.

crankback. A mechanism for partially releasing a connection setup in progress which has encountered a failure. This mechanism allows PNNI to perform alternate routing.

customer-replaceable unit (CRU). An assembly or part that a customer can replace in its entirety when any of its components fail. Contrast with *field replaceable unit (FRU)*.

D

data communication. (1) Transfer of information between functional units by means of data transmission according to a protocol. (T) (2) The transmission, reception, and validation of data. (A)

data transfer rate. The average number of bits, characters, or blocks per unit of time passing between equipment in a data-transmission system. (I) The rate is expressed in bits, characters, or blocks per second, minute, or hour.

data transmission. The conveying of data from one place for reception elsewhere by telecommunication means. (I)

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

destination. Any point or location, such as a node, station, or particular terminal, to which information is to be sent.

device. (1) A mechanical, electrical, or electronic contrivance with a specific purpose. (2) An input/output unit such as a terminal, display, or printer.

diagnostics. Modules or tests used by computer users and service personnel to diagnose hardware problems.

DMM. Distributed Management Module.

dump. (1) To record, at a particular instant, the contents of all or part of one storage device in another storage device. Dumping is usually for the purpose of debugging. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

E

EIA. Electronic Industries Association.

EEPROM. Electrically Erasable Programmable Read-Only Memory.

electrically erasable programmable read-only memory (EEPROM). A PROM that can be erased by a special process and reused. (T)

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

Ethernet. A local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission.

external reachable address. An address that can be reached through a PNNI routing domain, but which is not located in that PNNI routing domain.

F

FCC. Federal Communications Commission (USA).

field. On a data medium or a storage medium, a specified area used for a particular category of data; for example, a group of character positions used to enter or display wage rates on a panel. (T)

file. A named set of records stored or processed as a unit. (T)

G

gateway. A device and its associated software that interconnect networks or systems of different architectures. The connection is usually made above the reference model network layer. For example, a gateway allows LANs access to System/370 host computers. Contrast with *bridge* and *router*.

H

hardware. Physical equipment as opposed to programs, procedures, rules, and associated documentation. (I) (A)

header. The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

host computer. (1) The primary or controlling computer in a multi-computer installation or network. (2) In a network, a processing unit in which resides a network access method. Synonymous with *host processor*.

I

ILMI. Interim Local Management Interface.

InARP. Inverse Address Resolution Protocol.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

internal reachable address. An address of a destination that is directly attached to the logical node advertising the address.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Protocol (IP). (1) A protocol that routes data through a network or interconnected networks. IP acts as an interface between the higher logical layers and the physical network. This protocol, however, does not provide error recovery, flow control, or guarantee the

reliability of the physical network. IP is a connectionless protocol. (2) A protocol used to route data from its source to its destination in an Internet environment.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

Inverse Address Resolution Protocol (InARP). A protocol for converting a physical network address (for example, an ATM address) into a higher level protocol address (for example, an IP address).

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comment (RFC) 791. It is usually represented in dotted decimal notation.

K

Kbps. Kilobits per second.

kilobit (Kb). (1) For processor storage, real and virtual storage, and channel volume, 2^{10} or 1024 bits. (2) For disk storage capacity and communications volume, 1000 bits.

kilobyte (KB). (1) For processor storage, real and virtual storage, and channel volume, 2^{10} or 1024 bytes. (2) For disk storage capacity and communications volume, 1000 bytes.

L

LAN. Local area network.

LE. LAN Emulation.

LAN emulation. A set of services, functional groups and protocols which provide for the emulation of LANs utilizing ATM as a backbone to allow connectivity among LAN and ATM attached end stations.

LEC. LAN Emulation Client.

LAN emulation client (LEC). The entity in end systems which performs data forwarding, address resolution, and other control functions.

LECS. LAN Emulation Configuration Server.

LAN emulation configuration server (LECS). This implements the policy controlled assignment of individual LE clients to different emulated LANs by providing the LES ATM addresses.

LED. Light-emitting diode.

LES. LAN Emulation Server.

LAN emulation server (LES). This implements the control coordination function for the emulated LAN, examples are enabling a LEC to join an emulated LAN, resolving MAC to ATM addresses.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

M

MAN. Metropolitan area network.

Management Information Base (MIB). A tree-like data structure for the definition and use of information.

Mb. Megabit; 1 048 576 bits.

Mbps. One million bits per second.

MB. Megabyte; 1 048 576 bytes.

megabyte. (1) For processor storage and real and virtual memory, 2^{20} or 1 048 576 bytes. (2) For disk storage capacity and transmission rates, 1 000 000 bytes.

MIB. Management Information Base.

multipoint-to-multipoint connection. A collection of associated ATM VC or VP links, and their associated nodes, with the following properties:

1. All nodes in the connection, called end-points, serve as a root node in a point-to-multipoint connection to all the remaining end-points.
2. Each of the end-points on the connection can send information without additional (i.e. higher layer) information.

N

neighbor node. A node that is directly connected to a particular node via a logical link.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) An arrangement of nodes and connecting branches. Connections are made between data stations. (T)

network administrator. A person who manages the use and maintenance of a network.

network node interface (NNI). The interface between two network nodes.

NNI. Network node interface.

node. A generic term applying to an active element in an ATM network (station or concentrator).

NSAP. Network Service Access Point.

NVRAM. Non-volatile Random Access Memory. See *random access memory (RAM)*

O

output device. A device in a data processing system by which data can be received from the system. (I) (A) Synonymous with *output unit*.

output unit. Synonym for *output device*.

P

Packet Internet Groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

parameter. (1) A variable that is given a constant value for a specified application and that may denote the application. (I) (A) (2) An item in a menu or for which the user specifies a value or for which the system provides a value when the menu is interpreted. (3) Data passed between programs or procedures.

path. (1) In a network, any route between any two nodes. (T) (2) The route traversed by the information exchanged between two attaching devices in a network.

peer group. A set of logical nodes which are group for purposes of creating a routing hierarchy. PTSEs are exchanged among all members of the group.

peer group identifier. A string of bits that is used to unambiguously identify a peer group.

peer group leader. A node which has been elected to perform some of the functions associated with a logical group node.

peer group level indicator. The number of significant bits in the peer group identifier of a particular peer group. group.

permanent virtual connection (PVC). (1) In X.25 and frame-relay communications, a virtual connection that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual connection (SVC)*. (2) The logical connection between two frame-relay terminating equipment stations, either directly or through one or more frame-relay frame handlers. A PVC consists of one or more PVC segments.

PING. Packet Internet Groper.

PNNI. Private-Network-Network-Interface. A routing information protocol that enables extremely scalable, full function, dynamic multi-vendor ATM switches to be integrated in the same network.

PNNI routing domain. A group of topologically contiguous systems which are running one instance of PNNI routing.

PNNI topology state element (PTSE). A collection of PNNI information that is flooded among all logical nodes within a peer group.

point-to-multipoint connection. A collection of associated ATM VC or VP links, with associated end-point nodes, with the following properties:

1. One ATM link, called the root link, serves as the root in a simple tree topology. When the root node sends information, all of the remaining nodes on the connection, called leaf nodes, receive copies of the information.
2. Each of the leaf nodes on the connection can send information directly to the root node. The root node cannot distinguish which leaf node is sending information without additional (higher layer) information.
3. The leaf nodes cannot communicate directly to each other with this connection type.

point-to-point connection.. A connection with only two end-points.

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket*. (3) A PHY entity and a PMD entity in a node, together creating a PHY/PMD pair, that may connect to the fiber media and provide one end of a physical connection with another node.

protocol. (1) A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (I) (2) In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. (3) A specification for the format and relative timing of information exchanged between communicating parties.

PTSE. PNNI Topology State Element.

PVC. Permanent virtual connection.

Q

QOS. Quality of service

quality of service (QOS). A set of communication characteristics required by an application. Each QOS defines a specific transmission priority, level of route reliability, and security level. Each QOS also defines whether the sessions are interactive.

R

RAIG. Resource Availability Information Group

RAM. Random access memory.

random access memory (RAM). A computer's or adapter's volatile storage area into which data may be entered and retrieved in a non-sequential manner.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Contrast with *local*.

request for comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

resource availability information group (RAIG). The RAIG contains information that is used to attach values of topology state parameters to nodes, links, and reachable addresses. The topology state parameters are maximum cell rate, available cell rate, administrative weight, and cell delay variation.

RFC. Request for Comments.

router. An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway*.

routing. (1) The assignment of the path by which a message will reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by the parameters carried in the message unit, such as the destination network address in a transmission header.

RS-232. In data communications, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

S

server. (1) A device, program, or code module on a network dedicated to providing a specific service to a network. (2) On a LAN, a data station that provides facilities to other data stations. Examples are a file server, print server, and mail server.

session. The period of time during which a user of a terminal can communicate with an interactive system, usually, elapsed time between logon and logoff.

signaling. Establishment of an ATM connection from a call set up by an end device.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SLIP. Serial Line Internet Protocol.

SNMP. Simple network management protocol.

station. (1) A communication device attached to a network. The term most often used in LANs is an *attaching device* or *workstation*. (2) An input or output point of a system that uses telecommunication facilities. (3) An addressable node on an FDDI network capable of transmitting, repeating, and receiving information. A station has exactly one SMT, at least one MAC, at least one PHY, and at least one PMD.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension of the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnetwork. (1) A group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

summary address. An address prefix that tells a node how to summarize reachability information.

SVC. Switched virtual connection.

T

TCP/IP. Transmission Control Protocol/Internet Protocol

Telnet. In TCP/IP, an application protocol that allows a user at one site to access a remote system as if the user's display station were locally attached. Telnet uses the Transmission Control Protocol as the underlying protocol.

TFTP. Trivial File Transfer Protocol.

token ring. A network with a ring topology that passes tokens from one attaching device (node) to another. A node that is ready to send can capture a token and insert data for transmission.

topology. The physical or logical arrangement of nodes in a computer network. Examples include ring topology and bus topology.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) A record of the frames and bytes transmitted on a network.

Transmission Control Protocol (TCP). A communications protocol used in the Internet. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmit. (1) The action of a station in generating a token, frame, or other symbol sequence and placing it on the outgoing medium. (2) The action of a station that consists of generating a frame, token, or control sequence, and placing it on the medium to the next station.

trap. Trajectory analysis program.

trunk. A physical topology, either open or closed, employing two optical fiber signal paths, one in each direction (that is, counter-rotating), forming a sequence of peer connections between FDDI nodes. When the trunk forms a closed loop it is sometimes called a trunk ring.

U

UBR. Unspecified Bit Rate.

unspecified bit rate (UBR). UBR is an ATM service category which does not specify traffic related service guarantees. Specifically, UBR does not include the notion of a per-connection negotiated bandwidth. No numerical commitments are made with respect to the cell loss ratio experienced by a UBR connection, or as to the cell transfer delay experienced by cells on the connection.

UNI. User-network interface.

user-network interface (UNI). Physical and logical definition of the interface between an ATM user device and the ATM network.

V

variable. (1) In computer programming, a character or group of characters that refers to a value and, in the execution of a computer program, corresponds to an address. (2) A quantity that can assume any of a given set of values. (A)

variable bit rate (VBR). An ATM service category which supports variable bit rate data traffic with average and peak traffic parameters.

VBR. Variable Bit Rate.

VCC. Virtual Channel Connection.

VCI. Virtual Channel Identifier

virtual path connection (VPC). A concatenation of VPLs between Virtual Path Terminators (VPTs). VPCs are unidirectional.

virtual path connection identifier (VPCI). Identifies an end-to-end virtual path. Allows the creation of a relationship between the VPIs used at both ends of a connection.

virtual path identifier (VPI). An eight bit field in the ATM cell header which indicates the virtual path over which the cell should be routed.

VPC. Virtual Path Connection.

VPCI. Virtual Path Connection Identifier.

VPI. Virtual Path Identifier.

W

WAN. Wide area network.

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN).*

workstation. (1) A functional unit at which a user works. A workstation often has some processing capability. (T) (2) One or more programmable or non-programmable devices that allow a user to do work. (3) A terminal or microcomputer, usually one that is connected to a mainframe or to a network, at which a user can perform applications.

Bibliography

For additional information on the functions and technology in the *ATM Control Point and Switch*, please refer to the following documents:

IBM 8260 Nways Mulitprotocol Switching Hub, IBM 8285 Nways ATM Workgroup Switch, Control Point Version 3, Command Reference Guide, SA33-0453.

IBM 8260 Nways Multiprotocol Switching Hub, Installation and Operation Guide, SA33-0251.

IBM 8260 Nways Multiprotocol Switching Hub, ATM Control Point and Switch Module, Installation and User's Guide, SA33-0326.

IBM 8285 Nways ATM Workgroup Switch, Installation and User's Guide, SA33-0381.

IBM 8260 Nways Multiprotocol Switching Hub, Distributed Management Module Commands Guide, SA33-0275.

IBM 8260 Nways Multiprotocol Switching Hub, Distributed Management Module User's Guide, SA33-0259.

Case, J., Fedor, M., Scoffstall, M., and Davin, J., *The Simple Network Management Protocol*, University of Tennessee at Knoxville, Performance Systems International and the MIT Laboratory for Computer Science, May 1990.

De Prycker, M., *Asynchronous Transfer Mode – Solution for Broadband ISDN*, Ellis Horwood, 1991.

Handel, R. and Huber, M.N., *Integrated Broadband Networks – An Introduction to ATM-Based Networks*, Addison-Wesley, 1991.

The ATM Forum:

- *UNI Specification – Version 3.0 and Version 3.1*.
- *P-NNI Specification Version 1.0*.
- *ILMI Specification Version 4.0*.
- *UNI Traffic Management Version 4.0*.

Index

T

U

V

Readers' Comments — We'd Like to Hear from You

8260 Nways Multiprotocol Switching Hub
8285 Nways ATM Workgroup Switch
ATM Control Point Version 3
User's Guide

Publication No. SA33-0452-00

Please send us your comments concerning this book. We will greatly appreciate them and will consider them for later releases of the present book.

If you prefer sending comments by FAX or electronically, use:

- FAX: 33 4 93 24 77 97
- E-mail: FRIBMQF5 at IBMMAIL
- IBM Internal Use: LGERCF at LGEPROFS
- Internet: rcf_lagaude@vnet.ibm.com

In advance, thank you.

Your comments:

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SA33-0452-00

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM France
Centre d'Etudes et Recherches
Service 0798 - BP 79
06610 La Gaude
France

Fold and Tape | **Please do not staple** | Fold and Tape

SA33-0452-00

Cut or Fold
Along Line

Printed in U.S.A.

SA33-0452-00