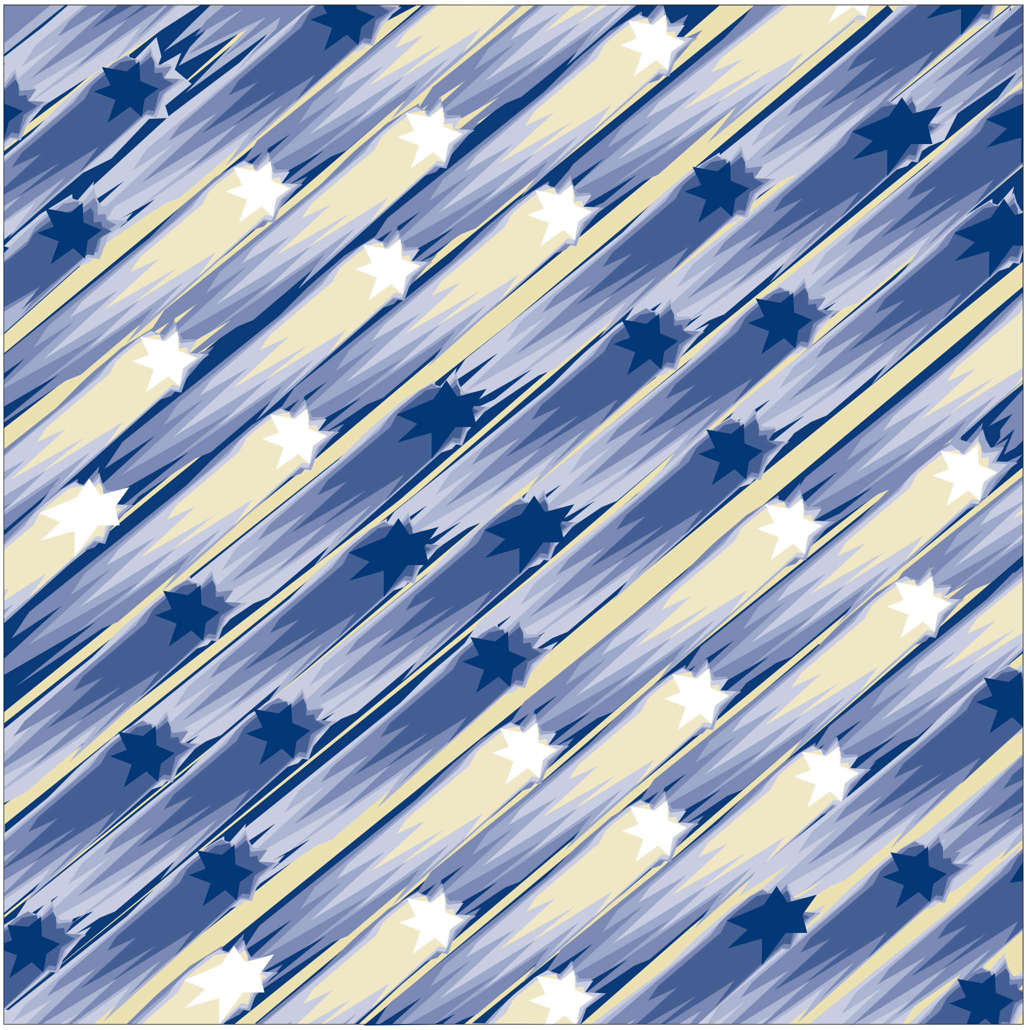
8265 Nways ATM Switch

User's Guide



SA33-0456-01

8265 Nways ATM Switch

User's Guide

SA33-0456-01

Note!

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

Second Edition (January 1998)

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

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 IBM 8265 Nways ATM Switch complies with the following ATM standards:

- ATM User-Network Interface (UNI) Specifications V3.0, V3.1, and V4.0 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.

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
NetView for AIX
RISC System/6000
IBM
Nways
Turboways

About this Book

This book descibes how to use the IBM 8265 Nways ATM Switch.

The ATM commands that you enter at the console to manage the ATM subsystem are described in detail in the *IBM 8265 Nways ATM Switch Command Reference Guide*, SA33-0458.

Who Should Use this Book

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

- ATM network administrator
- ATM network operator.

Prerequisite Knowledge

To understand the information presented in this

- Features and characteristics of the IBM 8265 Nways ATM Switch as described in *IBM 8265 Nways ATM Switch Product Description*, GA33-0449.
- Principles of Asynchronous Transfer Mode (ATM) technology
- ATM Forum UNI Specification Versions 3.0, 3.1, and 4.0.
- ATM Forum LAN Emulation Specification Version 1.0.
- ATM Forum P-NNI Specification Version 1.0.

Where to Find More Information

The publications for the CPSW module and associated product documentation are listed in the “Bibliography” on page 171.

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 located in the IBM 8265 Nways ATM Switch Control Point and Switch Module.

The term *Command Reference Guide* refers to the *IBM 8265 Nways ATM Switch Command Reference Guide*, SA33-0458.

Part 1. Configuring Your ATM Network

Chapter 1. Overview

ATM Networks

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**.

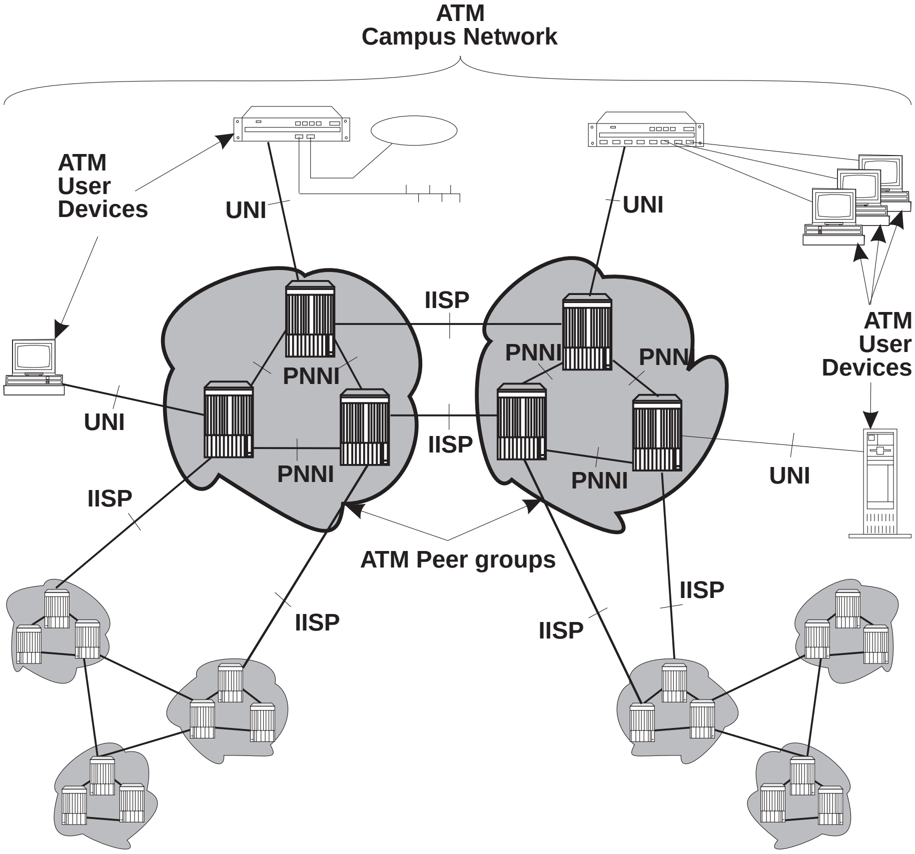


Figure 1. Components of an ATM Campus Network

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 Specifications V3.0, V3.1 and V4.0.

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.

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.

AUTO The interface is automatically set according to that of the incoming signal, as detected by ILMI.

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.

The 8265 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 8265 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 8265, 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 512 is allowed per switch.

Figure 2 shows an example of these VPC links.

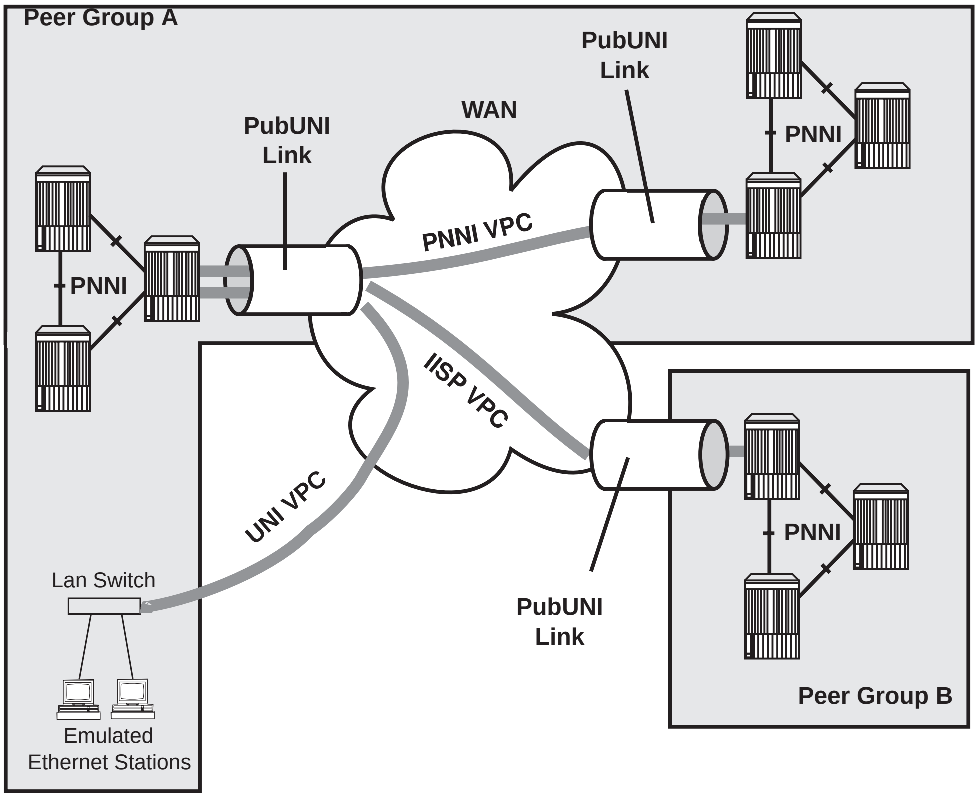


Figure 2. UNI, IISP, and PNNI VPC Links

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 8265, or on different 8265s. In the latter case, the path may be selected either by the routing protocol (PNNI, for example) or by creating several PVCs in each 8265 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 8265 is reset or powered on.

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

The 8265 supports a maximum of 512 PVCs.

Chapter 2. Setting-Up and Using a Configuration Console

This chapter describes:

- How to enter commands and get help on the CPSW configuration console
- How to set up the CPSW configuration console in Normal (ASCII) mode
- How to set up the CPSW configuration console via a SLIP protocol connection
- How to access the CPSW from a remote console via TELNET
- How to reconfigure configuration console settings.

Overview

The commands for configuring the CPSW are entered using a configuration console (ASCII terminal or workstation) connected to the console port. The console can communicate in one of two ways:

Normal (ASCII) mode

In normal mode, commands are entered directly from the configuration console.

See “Setting Up a Configuration Console in Normal (ASCII) Mode” on page 12 for instructions on connecting a configuration console to the CPSW in Normal mode.

SLIP mode

In SLIP mode, commands are entered via a TELNET session between an IP workstation and the CPSW.

If your workstation supports TFTP, it can also be used as a TFTP server to perform DOWNLOAD and UPLOAD operations between your workstation and the 8265. (See “Upload and Download Operations” on page 119.)

Note: If no activity takes place for a period of 20 minutes, the console is automatically returned to normal mode.

This method requires an initial connection in Normal mode to set up the IP addresses and change the port protocol.

See “Setting Up a Configuration Console in SLIP Mode” on page 13 for instructions on connecting a configuration console to the CPSW in SLIP mode.

After the switch has been initially configured, it is also possible to configure and manage the switch:

- From a remote TELNET sessions, as described in “TELNET Sessions Via a Remote Switch or Workstation” on page 18.
- Using an SNMP management application.

Before You Start

The following section describes keystrokes and the command syntax to use to enter commands from a configuration console. For a complete description of all configuration commands, see the *IBM 8265 Command Reference Guide*.

Entering Commands

By entering commands at the prompt on the configuration console attached to the CPSW console, you can configure various functions of the 8265. The management prompt appears as follows:

```
8265ATM>
```

Commands are not case-sensitive. The system interprets `ABC` (uppercase) the same as `abc` (lowercase).

The values you enter for certain command **parameters** are, however, case-sensitive and must be typed exactly as shown in the *IBM 8265 Command Reference Guide*. For example, if you enter `RWTRAP` and `rwtrap` for the `com_name` parameter in two separate SET COMMUNITY commands, you will create two different community names.

Keyboard Functions

When entering commands the following keyboard functions are available:

Keystroke	**Function**
BS or Backspace	Moves the cursor one space backward and deletes the character.
Enter	Runs the command or prompts you to enter missing parameters.
Space bar	Types the complete command.
Ctrl + C	Cancels the command that is currently running and returns you to a blank command line.
Ctrl + R	Retypes the last command you entered on the command line.
Ctrl + L	Types the currently edited command on the next line.
?	Displays a list of available commands.

Getting Help

To list the available commands, which vary according to whether you logged on with the user or administrator password, type`?`on the command line and press Enter.

```
8265ATM> ?
```

To list the possible keywords that follow a command, you can enter the first word of the command, followed by `?`. For example, to see what commands start with the word `SAVE`, you would enter:

```
8265ATM> save ?
```

Example Screens Shown in This Book

The example screen displays shown in this book are correct at the time of publication of this guide. Actual displays may vary due to improvements in code or configuration options.

Command Completion

The command line accepts abbreviated command input with a facility called **command completion**. Command completion lets you enter a command and its parameters by typing the minimum number of characters to uniquely identify the command or a parameter.

For example, to enter the SAVE command, you only need to type `SA` and press the space bar:

```
8265ATM> sa
```

The system automatically fills in the rest of the command:

```
8265ATM> save
```

To enter a parameter, such as `COMMUNITY`, with the SAVE command, you can type the first few letters (for example, `COMM`) and press the space bar:

```
8265ATM> save comm
```

The rest of the parameter is automatically entered:

```
8265ATM> save community
```

If you enter an insufficient number of letters (for example, only `S` or `C`) for the system to determine the command or parameter (for example, `Set`, `Show`, `Save` and so on), the word is not completed and you are prompted to enter the rest of the command. The system also prompts you if you forget to enter a mandatory parameter.

Setting Up a Configuration Console in Normal (ASCII) Mode

The following procedure sets up the configuration console in Normal mode and logs you on as the system administrator with full access to all 8265 commands:

1. Connect an ASCII-type terminal to the RS-232 console port on the front panel of the CPSW module.
2. In the terminal's user guide, locate the procedure for setting parameters for baud rate, data bits, parity, and stop bits.
3. Configure these configuration console settings to the values used by the CPSW so that the configuration console and the CPSW can communicate. The factory-set default settings for the CPSW are as follows:

Baud rate	9600
Data bits	8
Parity	None
Stop bits	1

4. Press Enter. The following message is displayed:

   ```
   ATM Switch/Control Module
   (c) Copyright IBM Corp. 1994, 1997. All rights reserved.

   Password:
   ```

5. Enter the Administrator password (factory default is 8265).

You can now proceed to configure the 8265, as described in Chapter 3, "Configuring Basic Parameters" on page 23.

Setting Up a Configuration Console in SLIP Mode

The procedure that follows sets up the configuration console in SLIP mode and logs you on as the system administrator with full access to all commands.

Note: A typical workstation includes two serial ports (COM1, COM2):

- One dedicated to an ASCII-terminal emulator,
- The other dedicated to an IP stack and supported via the SLIP protocol.

Both ports are needed for this procedure.

1. Connect your workstation to the RS-232 console port on the front panel of the CPSW module from the ‘ASCII-terminal’ serial port.
2. Configure the terminal in Normal mode and logon as administrator as described in “Setting Up a Configuration Console in Normal (ASCII) Mode” on page 12.
3. If a data transmission rate **other than 9600** is required, use the SET TERMINAL BAUD command to configure a data transmission rate.

```
8265ATM> set terminal baud 19200
```

4. Set the local IP address (8265) and remote IP address (workstation) for the SLIP protocol using the SET TERMINAL SLIP_ADDRESSES command.

```
8265ATM> set terminal slip_addresses
Enter local ip address : 9.100.86.139
Enter remote ip address : 9.100.86.138
8265ATM>
```

5. Switch the configuration console port operating mode to SLIP using the SET TERMINAL CONSOLE_PORT_PROTOCOL command.

```
8265ATM> set terminal console_port_protocol slip
```

6. Unplug the cable from the ‘ASCII-terminal’ serial port and plug it into the ‘IP-stack’ serial port of your workstation.
7. Configure the IP stack SLIP with the IP address of the 8265 and verify the CPSW-to-workstation connectivity by issuing a PING request.

```
C:\ ping 9.100.86.139
```

8. Start a TELNET session to the CPSW.

```
C:\  telnet 9.100.86.139
```

9. Logon as administrator (factory default password is 8265). The Welcome screen is displayed:

```
Password:

Welcome to system administrator service on 8265.
8265ATM>
```

You can now proceed to configure the 8265, as described in Chapter 3, “Configuring Basic Parameters” on page 23.

Returning to Normal Mode

To switch the configuration console port back to Normal mode, use the SET TERMINAL CONSOLE_PORT_PROTOCOL command.

```
8265ATM> set terminal console_port_protocol normal
```

Note: A CPSW module RESET restores the configuration console port to NORMAL operating mode.

SLIP Support

The SLIP function is supported on:

- TCP/IP for AIX version 3.2.5
- TCP/IP V2.1.2 for IBM DOS V7 (no TFTP support)
- TCP/IP V2.0 for OS/2 V3 (WARP)
- ChameleonNFS V4.0 for Windows

Using TCP/IP for AIX version 3.2.5

1. Enter `smitty mkinet`
2. Enter `serial line INTERNET Network Interface`
3. Configure the local and remote IP addresses
4. The mask is not required
5. Do not fill in the baud rate and the dial string
6. PING the IP address of the remote 8265.

Using TCP/IP V2.1.2 for IBM DOS V7 (no TFTP support)

1. Use `Custom` command, then SLIP interface
2. Select `SL0` and enable the interface
3. Select COM1 and 9600 modem speed
4. Configure the local and remote IP addresses
5. The mask is not required
6. PING the IP address of the remote 8265.

Using TCP/IP V2.0 for OS/2 V3 (WARP)

1. Configure the SLIP connection using the TCPIPCFG icon then SLIP.
2. Enable the SLIP interface on the correct COMM port.
3. Keep VJ compression **off** and use 1000 as MTU size.
4. Configure the local and remote IP addresses.
5. The mask is not required.
6. Configure FTFP server using TCPIPCFG icon thru *AUTOSTART*. This is required in the FTFP server for CPSW download and upload operations.
7. Set terminal speed with the `mode com1` command.
8. PING the IP address of the remote CPSW.

Using ChameleonNFS V4.0 or V4.1 for Windows

1. Configure the SLIP connection using the Custom icon under ChameleonNFS.
2. Select COM1 and no flow control PORT option.
3. Do not select a modem under the Modem option.
4. Configure the local and remote IP addresses.
5. The mask is not required.
6. Enter the appropriate hostname in the **services/host** table.
7. Use the TELNET icon under ChameleonNFS to connect to terminal dialog via VT220 emulation.

Configuring the CPSW Ethernet Port

To use the Ethernet port on a CPSW module, you must first configure the following:

- The Internet Protocol (IP) address
- The subnet mask used for your class of Internet device.
- The Ethernet MAC address. A burned-in address (BIA) is supplied with each CPSW module (displayed via the SHOW INVENTORY VERBOSE command). You can redefine this address with a locally administered address (LAA). Once an LAA has been assigned, you can always return to the BIA, by entering a MAC address of 000000000000.

Setting the IP Address and Subnet Mask

The IP address and subnet mask for the Ethernet port can be configured when in either Adminstrator or Maintenance Mode.

Administrator Mode: When in Adminstrator mode, the IP address and subnet mask can be configured in one command, SET DEVICE IP_ADDRESS.

The following example defines the Ethernet port IP address as 9.100.109.25 and the subnet mask as ff.ff.ff.00:

```
8265ATM> set device ip_address eth 9.100.109.25 ff.ff.ff.00
```

Maintenance Mode: When in Maintenance mode, the IP address and subnet mask are configured by two separate commands, SET IP_ADDRESS and SET SUBNET_MASK.

The following example defines the Ethernet port IP address as 9.100.109.25:

```
8265ATM> set ip_address 9.100.109.25
```

The following example defines the subnet mask ff.ff.ff.00:

```
8265ATM> set subnet_mask ff.ff.ff.00
```

Setting the Ethernet MAC Address

The Ethernet port MAC address can be configured when in either Adminstrator or Maintenance Mode.

Administrator Mode: The MAC address is configured using the SET DEVICE ETHERNET_MAC_ADDRESS command.

The following example configures the Ethernet port with a MAC address of 0E0000020304:

```
8265ATM> set device ethernet_mac_address 0E0000020304
```

Maintenance Mode: The MAC address is configured using the SET MAC_ADDRESS command.

The following example configures the Ethernet port with a MAC address of 0E0000020304:

```
8265ATM> set mac_address 0E-00-00-02-03-04
```

TELNET Sessions Via a Remote Switch or Workstation

The CPSW’s remote login feature allows you to log on to an 8265 from a remote configuration console or network workstation that supports the TELNET protocol.

You can remotely log on to only one 8265 at a time.

Minimum Local Configuration

Before you can log on to the 8265 from a remote switch, you must perform a minimum configuration using a configuration console (in either Normal or SLIP mode). The minimum configuration that is required depends on the type of subnetwork you will use for the TELNET session:

Classical IP

- Set the ATM address of the 8265
- Enable the port that connects to the ARP server
- Get the ATM address of the ARP server
- Set the ARP server ATM address in the 8265
- Set the IP address of the 8265
- Enable the port that will be used for the TELNET session.

LAN Emulation

- Set the ATM address of the 8265
- Start the LEC.

These steps are described in Chapter 4, “Configuring SNMP and LANE Parameters” on page 37.

Logon Procedure

You specify the 8265 by entering its IP address with the TELNET command:

```
C:\  telnet 123.94.202.9
```

Once you are connected to the remote switch, you must log on by entering the correct password. Afterwards all the commands you enter are run on the remote module as if entered from a local 8265 session.

To log off from a TELNET session, enter the LOGOUT command. The LOGOUT command disconnects the TELNET connection and reconnects you to the local 8265 accessed through your configuration console. The following message is displayed with the local management prompt:

```
ATM2 logout

Bye

Remote session completed
C:\
```

Figure 3 shows an example of a remote login. Note that once you are connected to 8265 A, you can remotely log on and manage the CPSW modules in either 8265 B or 8265 C.

Note: The TELNET protocol is not routable.

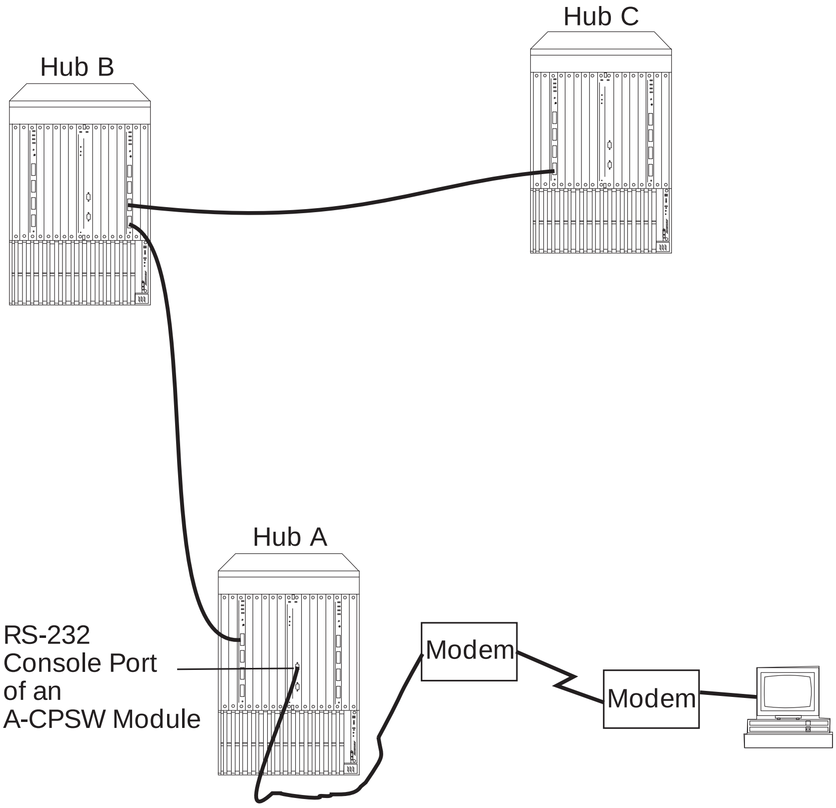


Figure 3. Working in Remote CPSW Sessions

You can set a timeout period for a remote CPSW by entering the SET TERMINAL TIMEOUT command. When this value is exceeded, the system automatically logs you off the remote 8265 session and returns you to your local session.

Although any unsaved configuration changes are still active, they will be lost the next time you reset or reboot the remote 8265. To save these changes, you must re-establish the remote session and enter the SAVE command.

Accessing the 8265 via the Internet

The 8265 has an integrated web server that enables you to access the 8265 via the Internet. The web server has the following features:

- Graphical view of the 8265 chassis, ATM modules, and ATM interfaces, with easy navigation.
- TELNET link to the Control Point.
- Direct navigation to integrated web servers on attached devices.
- Basic configuration functions (isolate and connect modules, enable and disable ATM interfaces).
- Debugging facilities (set up traces, display the error log, display connection table).
- Basic SHOW functions.

The web server has been optimized for the following environments:

- 16 to 256 colors
- a web browser that supports tables and timed-page refresh.

Recommended Web Browser Configuration

In order to ensure that all displays are current, it is recommended that your web browser be configured as follows:

- Disk cache set to zero
- Memory cache set to zero
- Document verification set to "every time".

Accessing the 8265

In order to access the web server, the Control Point must be configured as described in “Minimum Local Configuration” on page 18.

To access the 8265, simply provide your web browser with the IP address of the Control Point. Enter `http://` followed by the IP address.

Note: Default port 80 is used by the server.

You will be prompted to enter a user name and password. The user name is always "ADMIN", and the password is the current Administrator password (defined with the "SET DEVICE" command).

Reconfiguring 8265 Configuration Console Settings

Carry out the procedures in this section only if you need to connect another device (besides the CPSW configuration console) to the CPSW module, and if the other device runs at a slower baud rate, uses a different parity, or has a different data bit value than the CPSW module's pre-configured factory settings.

For example, if you want to connect a 4800 baud modem to the CPSW module to remotely manage the 8265 you must change the factory-set default baud rate from 9600 to 4800. To do so, you would enter the following command:

```
8265ATM> set terminal baud 4800
```

See the *IBM 8265 Command Reference Guide* for information on the SET TERMINAL commands that allow you to reconfigure configuration console settings.

Saving Reconfigured Configuration Console Settings

After you use the SET TERMINAL command to reset the baud rate, the parity, or the data bit value, the change is activated immediately and you lose communication with the configuration console. The new configuration console setting is not, however, permanently saved.

In order to save the configuration console parameters that you reconfigure with the SET command, you must connect the new configuration console to the 8265, log on, and enter the SAVE TERMINAL command. Once saved in this way, the new configuration console settings remain stored in memory after you log off and in case of a power failure.

For more information on how to reconfigure and save configuration console settings, see the sections describing the SET TERMINAL commands in the *IBM 8265 Command Reference Guide*.

Automatic Modem Hangup

If you use a modem to connect to the CPSW, you can use the SET TERMINAL HANGUP command to automatically hang up the modem connection when you log off the CPSW. If you do not hang up the modem connection, an unauthorized user can pick up your open session and work in it.

The following command shows what to enter to automatically hang up the modem after you log off the CPSW. The command is set by default to `disable` so that the modem does not automatically hang up.

```
8265ATM> set terminal hangup enable
```

Chapter 3. Configuring Basic Parameters

This chapter describes:

- How to configure the ATM switch address
- How to configure CPSW module parameters.

Note: You must been logged in as Administrator in order to configure the 8265. The factory default password is 8265.

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 an 8265 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 SET PNNI NODE_0 ATM_ADDRESS command, followed by the desired ATM address.

The following example sets the ATM address to 39.99.99.99.99.99.99.00.00.99.99.01.01.99.99.99.99.99.99.01.

```
8265ATM> set pnni node_0 atm_address: 9.99.99.99.99.99.99.00.00.99.99.01.01.99.
99.99.99.99.99.01
```

Once you have entered the ATM address, you can do any of the following:

- Issue the COMMIT PNNI command. This saves the ATM address entered and resets the ATM control point.
- Issue the SAVE PNNI command. This saves the ATM address entered. The ATM address will applied at the next reset.
- Issue the UNCOMMIT PNNI command. This removes the ATM address that you have entered (the previous ATM address remains).
- Issue the SHOW FUTURE_PNNI NODE_0 to display the ATM address that you have just entered. Do this if you think you may have made an error when entering the address.
- Reissue the SET PNNI NODE_0 ATM_ADDRESS command to change the ATM address again.

To display the current ATM address, enter the SHOW PNNI NODE_0 command.

If you have the PNNI control point code installed, refer to Chapter 6, “Configuring PNNI Parameters” on page 55 for more information.

Configuring CPSW Module Parameters

This section describes the commands needed to configure the CPSW module.

Before beginning the procedures listed below, make sure that:

1. You have installed the CPSW module correctly (see the *IBM 8265 Installation Guide*, SA33-0441.)
2. You have set up a configuration console and logged on as administrator (see Chapter 2, “Setting-Up and Using a Configuration Console” on page 9).

Configuration Summary

To configure the CPSW, follow the steps listed below. Each of these steps are described in a subsequent section of this chapter.

1. Set the CPSW user and administrator passwords.
2. Set the node clock.
3. Set the local CPSW parameters such as:
    - Switch name
    - Service contact information
    - Console prompt
    - Console timeout
4. Define the ATM address of the CPSW. This resets the ATM subsystem.
5. Optionally enable the sending of alert messages to an SNMP workstation or the local console.

For a detailed description of each CPSW configuration command, see the *IBM 8265 Command Reference Guide*.

Setting CPSW Passwords

It is necessary to set two levels of CPSW passwords:

- **Administrator** password that provides access to **all** CPSW commands with read-write (configuration) access (factory default is 8265).

  When logged in with the administrator password, you can place the 8265 in Maintenance Mode (see page 34).

- **User** password that provides access to a **subset** of CPSW commands including most SHOW commands, PING and TELNET (factory default is a null string).

See the *IBM 8265 Command Reference Guide* for more information on access to CPSW commands.

Administrator Password:

1. At the console prompt, type the SET DEVICE PASSWORD ADMINISTRATOR command:

   ```
   8265ATM> set device password administrator
   ```

   Then press Enter.

2. In the next three fields displayed, enter your current password and the new password (up to fifteen characters) twice as shown below. For security purposes, the values you enter are not displayed on the screen.

   ```
   Enter current administrator password: {old password}
   New password:                         {new password}
   Re-enter password:                    {new password}
   ```

   Then press Enter. You are prompted when your password is accepted:

   ```
   Password changed.
   ```

3. To save your new password, type the SAVE DEVICE or the SAVE ALL command:

   ```
   8265ATM> save device
   ```

   Then press Enter.

You will need to enter the new administrator password the next time you log on to the CPSW. Note that you have only ten seconds to enter a password when the Password prompt is displayed. If you do not enter a password, a Timeout message is displayed. To re-display the Password prompt and start again, press Enter.

User Password:

1. Log on to CPSW using the administrator password.
2. At the management prompt, type the SET DEVICE PASSWORD USER command:

   ```
   8265ATM> set device password user
   ```

   Then press Enter.
3. In the next three fields displayed, enter the administrator password and the new user password (up to fifteen characters) twice as shown here:

   ```
   Enter current administrator password: {admin password}
   New password:                         {new user password}
   Re-enter password:                    {new user password}
   ```

   Then press Enter. You are prompted when the password is accepted:

   ```
   Password changed.
   ```

4. To save your new user password, type the SAVE DEVICE or the SAVE ALL command:

   ```
   8265ATM> save device
   ```

   Then press Enter.

Setting the Node Clock

You need to set the CPSW's 24-hour node clock only once, when you install the CPSW. When you set the node clock, you establish a starting time, date, and day.

- To set the node clock, enter the SET CLOCK command and specify the time and date parameters. Then press Enter.

For example, the following command sets the node clock to 4:44 p.m. on March 20, 1997:

```
8265ATM> set clock 16:44 1997/03/20
```

The CPSW node clock uses its own battery and functions even when the CPSW fails to operate.

Setting Local CPSW Parameters

The CPSW is preconfigured with default settings that may need to be changed before you can use the switch. To modify these parameters, you must log on using the system administrator password. Then use the SET command to change the values for any of the following:

- Switch name
- Service contact information
- Console prompt
- Console timeout value.

A brief description of each parameter is given in the following sections. For more detailed information, see the *IBM 8265 Command Reference Guide*.

Switch Name:

In order to simplify the command parameters you need to enter to perform certain ATM tasks, you can assign a unique name to each 8265. You can then use this name instead of the IP address to identify the 8265.

To set a unique name for the 8265, enter the SET DEVICE NAME command and press Enter.

```
8265ATM> set device name [8265 name]
```

Service Contact Information:

After installing the 8265 and logging on to the CPSW, you should enter the location details and the name of the appropriate person to contact in case of a failure in the ATM subsystem or with the 8265.

To do so, enter the following commands:

- SET DEVICE LOCATION to specify where the 8265 is installed
- SET DEVICE CONTACT to specify the name of the service personnel to contact.

Console Prompt:

IBM also recommends that you customize the prompt used by each CPSW console. This helps you to easily recognize the CPSW to which you are connected when you are logged on to a remote switch.

The default prompt is:

```
8265ATM>
```

Suggestion: To make it easier to recognize the CPSW by its command prompt, set the prompt to the name of the CPSW used in the SET DEVICE NAME command. See the *IBM 8265 Command Reference Guide* for more information.

To customize the CPSW management prompt, use the SET TERMINAL PROMPT command.

```
8265ATM>set terminal prompt ATM2
ATM2>
```

Console Timeout: The TERMINAL TIMEOUT parameter is a safety precaution that lets you specify how long you can remain logged on to the CPSW console without entering any data from the keyboard. This prevents unauthorized users from accessing the CPSW if you forget to log off the system. If no keystroke is entered for the time period specified by SET TERMINAL TIMEOUT, the system automatically logs you off.

The default value for SET TERMINAL TIMEOUT is `0`. This means that no timeout period is set and that you cannot be automatically logged off from the system.

To specify a timeout value (in minutes), use the SET TERMINAL TIMEOUT command.

```
8265ATM>set terminal timeout 2
```

Configuring the ATM Switch Address

Note: Configuring the ATM switch address will cause a reset of the CPSW module. 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:

```
8265ATM> 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.

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 before the Control Point is reset.

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.**

Using Alert Messages

You can configure the CPSW to issue alert messages when certain system events are detected. These alerts can be sent to the configured trap receiver (for example, an SNMP workstation) and/or to the local configuration console.

Types of Alerts

There are three types of alerts:

- Hello alerts
- Authentication alerts
- Change alerts.

A **Hello** alert is sent when:

- The ATM subsytem is reset in one of the following ways:
  - Entering the BOOT command
  - Pressing the ATM Reset button
  - Entering the RESET command
  - Powering off and powering on the 8265.
- A LAN Emulation Client becomes active.
- Any of the following parameters are changed:
  - An agent's IP address (using the SET DEVICE IP_ADDRESS or SET DEVICE LAN_EMULATION_CLIENT command)
  - An agent's subnetwork mask (using the SET DEVICE IP_ADDRESS or SET DEVICE LAN_EMULATION_CLIENT command)
  - ATM address of the ARP server (using the SET DEVICE ARP_SERVER command)
  - IP address of the default gateway (using the SET DEVICE DEFAULT_GATEWAY command).

A Hello alert is sent either once a minute until an SNMP request is received or once a minute for up to 4 hours and 15 minutes. It then shuts off and no Hello alert is sent for 6 hours. After 6 hours have elapsed, Hello alerts are sent again for up to 4 hours and 15 minutes.

An **Authentication** alert is sent when an unauthorized user tries to access the 8265 and the IP address or community name is not valid for the attempted read or write operation.

A **Change** alert is sent when any of the following chqnges are made:

- An ATM media module is isolated or reconnected
- An ATM media module port is enabled or disabled
- Time and date used on the ATM subsystem are reconfigured
- Name, location, or service contact information for the CPSW module are reset.

Configuring Alerts

Alerts are configured via the SET ALERT command. You can configure each type of alert (Hello, Authentication, and Change) to be trapped and sent to the trap receiver (via the TRAP parameter), and/or displayed at the local configuration console (via the DISPLAY parameter).

Examples: The following example shows how to configure a Hello alert to be sent to the trap receiver and local configuration console only:

```
8265ATM> set alert hello trap display
```

The following example shows how to configure a Change alert to be sent to the trap receiver only:

```
8265ATM> set alert change trap nodisplay
```

The following example shows how to configure an Authentication alert to be sent to the local configuration console only:

```
8265ATM> set alert authentication notrap display
```

By default, all alerts are set to NOTRAP and NODISPLAY.

Current alert settings can be displayed via the SHOW ALERT command.

Q.2931 Branches and Parties

According to your networking needs, you can configure the amount of Q.2931 branches and parties available. Five types of configuration are available:

config_1 providing at least 32000 branches and 2 parties

config_2 providing at least 30000 branches and 2000 parties

config_3 providing at least 28000 branches and 4000 parties

config_4 providing at least 26000 branches and 6000 parties

config_5 providing at least 24000 branches and 8000 parties

The above configurations guarantee the `minimum` number of branches and parties possible. The 8265 will optimize the configuration based on these values, the maximum number of branches and parties possible will be determined by available system resources.

To configure the 8265 to use one of the above configurations, you enter the SET DEVICE_CONFIG_FUNCTIONS GSMP:OFF command, followed by the required configuration (config_1, for example).

To display the current configuration, enter the SHOW DEVICE command.

Using Maintenance Mode

Some operations (such as downloading out-of-band) can only be done when the 8265 is in Maintenance mode.

This mode is entered when the MAINTAIN command is issued when logged in with Administrator mode (from a local session via the RS-232 console port).

When the command is issued, the CPSW is reset. You should stop all traffic before issuing the command.

Changes made during the Administrator mode session should be saved prior to issuing the MAINTAIN command, or they will be lost. If you have made changes, but do not wish to keep them, you need to issued the comand MAINTAIN FORCE to enter Maintenance mode.

When Maintenance mode is active, the ATM prompt appears as >> and the System Status LCD on the CPSW module displays the message: "MAINTENANCE MODE ENTERED UPON USER REQUEST".

Table 1 provides a summary of the commands available in Maintenance mode. For details of each command, refer to the *IBM 8265 Command Reference Guide*.

Table 1. Maintenance Mode Command Summary

Command	Description
BOOT	Activates the new software stored in the flash EEPROM, ends Maintenance mode, and starts a new CPSW session.
CLEAR ALL	Deletes all stored information, such as configuration, error log, and restart counters.
CLEAR CONFIGURATION	Erases the customization of a CPSW module.
DOWNLOAD OUT_OF_BAND	Downloads new CPSW module software.
SET DEFAULT_GATEWAY	Assigns the IP address of the router that will be used to receive IP packets from, and forward IP packets to, stations that are not connected to the 8265.
SET IP_ADDRESS	Assigns an IP address to the Ethernet port on the CPSW module.
SET MAC_ADDRESS	Assigns a MAC address to the Ethernet port on the CPSW.
SET ROLE	Selects (in a redundant CPSW configuration) which CPSW module is primary and which is secondary.
SET SUBNET_MASK	Assigns a subnetwork mask to the Ethernet port on the CPSW module.
SHOW ERRORS	Displays the errors recorded during the last execution of the DOWNLOAD OUT_OF_BAND command.
SHOW FLASH	Displays a summary of the microcode stored in the flash memory, including: • Which of the two flash EEPROMs is the active one • Which versions of microcode are present (boot and operational).
SHOW RAM	Displays the amount of Random Access Memory (RAM) installed.
SHOW ROLE	Displays the role (primary or secondary) of the local CPSW.
SWAP ACTIVE	Activates the backup flash EEPROM without resetting the CPSW.
USE BAUD	Changes the baud rate of the configuration console connection while in Maintenance mode (9600 bps or 19200 bps).

Leaving Maintenance Mode

You exit Maintenance mode by:

- Entering the BOOT command. This resets the ATM subsystem. The MAINTENANCE MODE display on the CPSW module System Status LCD switches off.
- Entering the DOWNLOAD OUT_OF_BAND BOOT command. This operation loads the new boot program and executes it immediately.

Chapter 4. Configuring SNMP and LANE Parameters

Carry out the procedures in this section only if you want to manage your ATM subsystem from an SNMP workstation.

If you want to manage the ATM subsystem from an SNMP workstation, you may access the 8265 through either a Classical IP subnetwork or a LAN Emulation subnetwork.

The steps required to set the SNMP parameters depend on the type of subnetwork you will use:

Classical IP over ATM subnetwork (IP)

- Set Set IP Address and Subnetwork Mask
- Set Default Gateway
- Set ARP server
- Set Community Table
- Set Alerts

LAN Emulation over ATM subnetwork (LE)

- Set LAN Emulation Client parameters (including IP Address and Subnetwork Mask)
- Set Default Gateway
- Set Community Table
- Set Alerts

These steps are described in the following sections.

Note: Although it is expensive, nothing prevents you from using both subnetworks at the same time, each subnetwork being independent from the other (no communication between them). In the latter case an ARP server and an 802.3 LES are required. A single subnetwork must be chosen for the Default Gateway.

IP Address and Subnetwork Mask (IP only)

In order for SNMP to run properly, every device in the network must have a unique IP address and subnetwork mask. In a classical IP subnetwork, you must use the SET DEVICE IP_ADDRESS command to assign a unique IP address and subnetwork mask to the CPSW.

For example, the following command sets a unique IP address for a Classical IP over ATM subnetwork on the CPSW and a subnetwork mask for an ATM class C device:

```
8265ATM> set device ip_address atm 195.44.45.48 FF.FF.FF.00
```

The subnetwork mask is specific for each type of Internet class. In general, the subnetwork mask is the group of common characters in the left part of the IP address. (These characters are also called the network ID.) The host address is the group of unique characters to the right of the IP address.

The following command sets the subnetwork mask for an ATM class B device:

```
8265ATM> set device ip_address atm 195.44.45.48 FF.FF.00.00
```

Using Host Names

You can also assign host names to each device with an IP address. This allows you to assign meaningful, easy to remember names to devices.

For example, an 8265 located in Laboratory C with an IP address of 9.100.109.203 could be called LabC. This can be set using the SET HOST command as shown in the following example:

```
8265ATM>set host LabC 9.100.109.203
```

Host names assigned to devices are displayed using the SHOW HOST command.

LAN Emulation Client (LE only)

In order for SNMP to run properly, every device in the network must have a unique IP address and subnetwork mask. In a LAN emulation subnetwork, you must use the SET DEVICE LAN_EMULATION_CLIENT command to assign a unique IP address and subnetwork mask to the CPSW.

To configure the LEC, use the SET DEVICE LAN_EMULATION_CLIENT with the following parameters:

- LAN type (Ethernet or Token-Ring)
- IP address
- Subnetwork Mask
- Individual MAC address
- Associated LES/LECS ATM address

Notes:

1. The LEC may be Ethernet or Token-Ring. If Ethernet, then you must specify the Ethernet type (either DIX or 802.3.) It is possible to specify one Ethernet and one Token-Ring LEC simultaneously.
2. If two LECs are configured, they must have different IP addresses, even if they are connected to different LESs.
3. The MAC address must be in a 802.3 format. Local and universal administrated MAC addresses are supported.
4. The associated LES ATM address is the address of a LES monitoring the emulated LAN. The LES must be a LE Forum compliant LES, connected to an 8265 switch or 8285 ATM Workgroup Switch.
5. The maximum frame size and emulated LAN name are provided by the associated LES.
6. The SET DEVICE LAN_EMULATION_CLIENT command automatically starts the LEC.
7. No command to stop the LEC is available.

For example, to configure an Ethernet LEC with IP address 9.100.20.55:

```
8265ATM>set device lan_emulation_client eth eth_type DIX ip_address 9.100.20.55

Client starting.
8265ATM>
```

After the `eth` parameter, the other parameters may be entered in any order.

The first time the SET DEVICE LAN_EMULATION_CLIENT command is used, you must configure all parameters before saving the configuration settings (no default values are provided). Once the configuration settings have been saved, it is possible to change only one parameter at a time using the SET DEVICE LAN_EMULATION_CLIENT command.

Default Gateway (IP & LE)

The default gateway is the IP address of the gateway that will receive and forward packets whose addresses are unknown to the ATM subnetwork. The default gateway is useful when sending CPSW alert packets to a management workstation that is on a different network and is accessible via a router.

For example, the following command defines the gateway with the address `195.44.45.26` as the default gateway:

```
8265ATM> set device default_gateway 195.44.45.26
```

ARP Server (IP only)

The ARP (Address Resolution Protocol) server is used in a classical IP over ATM network to map IP addresses to ATM addresses. This is necessary to permit communication between an ATM network and SNMP stations in a Classical IP subnetwork.

The following command defines the ATM address for an ARP server:

```
8265ATM> set device arp_server 39.11.FF.22.99.99.99.00.00.00.00.01.49.11.11.11.
11.11.11.49
```

Community Table (IP & LE)

The Community table defines which SNMP stations in the network can access information from the CPSW, and which station(s) will receive a trap from the CPSW when an error is detected.

To create an entry in the Community table, you use the SET COMMUNITY command. For example, the following command specifies that a community name called ATMMGMT with an IP address of 195.44.45.244 has read-write access to the CPSW:

```
8265ATM> set community ATMMGMT 195.44.45.244 read_write
```

The community name parameter is case-sensitive. Be sure, therefore, to enter the community name in uppercase or lowercase letters exactly as you want it to appear. To display a list of existing community names, use the SHOW COMMUNITY command.

Alerts (IP & LE)

To enable or disable the function for sending alerts via SNMP traps to the CPSW local console and network management stations, you use the SET ALERT command. See the *IBM 8265 Command Reference Guide* for information on the different types of alerts you can enable and disable with this command.

For example, the following command enables an alert to be sent when a configuration change is made:

```
8265ATM> set alert change trap
```

Setting Up a LAN Emulation Client

To configure the LEC, use the SET DEVICE LAN_EMULATION_CLIENT command with the following parameters:

- LAN type
- IP address
- Subnetwork mask
- LES ATM address, LECS ATM address or nothing (if using the default well-known address or using a locally administered LECS set via the SET LAN_EMUL CONFIGURATION_SERVER command.)
- Individual MAC address.

The following choices are offered:

1. LES ATM address definition.

To define the LES ATM address for a LEC, you issue the following command:

```
8265ATM> SET DEVICE LAN_EMULATION_CLIENT (tr/eth) NO_LECS_WITH_LES les_atm_address
```

2. LECS ATM address definition.

To define the LECS ATM address for a LEC, you issue the following command:

```
8265ATM> SET DEVICE LAN_EMULATION_CLIENT (tr/eth) NO_LES_WITH_LECS les_atm_address
```

3. No specific LES or LECS definition.

The default value for the NO_LECS_WITH_LES or NO_LES_WITH_LECS keywords are NONE. For example:

```
8265ATM> SET DEVICE LAN_EMULATION_CLIENT (tr/eth) NO_LES_WITH_LECS NONE
```

Notes:

1. You should start the LES (whether internal or external) before you configure the LEC, in order to get its ATM address (via the SHOW LAN_EMUL SERVERS command).
2. The maximum frame size and emulated LAN name are provided by the associated LES.
3. The SET DEVICE LAN_EMULATION_CLIENT command automatically starts the LEC.

LECS ATM Address

Some Lan Emulation Clients (LECs) determine the ATM address of their associated LES from the LAN Emulation Configuration Server (LECS). The CPSW supports these LECs with three separate methods for establishing a connection to the LECS:

- ILMI MIB
- LECS Well Known Address
- Fixed PVC (0.17).

ILMI MIB

The LEC can get the unicast ATM address by doing a GETNEXT on the variable atmSrvcRegATMAddress in the ILMI MIB.

For LECs that use this method of addressing, you must define the LECS ATM address in each ATM switch that deals with these LECs. You define the LECS ATM address with the SET LAN_EMUL CONFIGURATION_SERVER command.

```
8265ATM> set lan_emul configuration_server 39.99.99.99.99.99.99.00.00.99.99.01.
84.0C.11.80.95.4F.13.00
```

You may define several ATM addresses. at any given time.

LECS Well Known Address

The LEC can directly call on one of two LEC Well Known Addresses, which are:

```
47.00.79.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01.00
and
C5.00.79.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01.00
```

Note: In order to use this method, the LEC must be able to make calls to the WKA. If the LECS does not support calls to the WKA, you must use another addressing method.

Fixed PVC (0.17)

If the LEC requires a connection via fixed PVC, you must use the command SET PVC to define a PVC for virtual connection on the LEC side with vpi.vci equal to 0.17. When defining a PVC for virtual channel connection (VCC), the range of allowed VCI values includes the value 17.

The following example defines a PVC on the LEC side with vpi-vci equal to 0.17 going to the LECS side:

```
8265ATM> set pvc 1.2 1 2.3 5 channel_point_to_point 0.17 0.33 best_effort
```

Checking the Configuration

To check the configuration of the LECS addresses, enter the following command:

```
8265ATM> show lan_emul configuration_server
```

Chapter 5. 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 media module 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:

```
8265ATM> 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
- AUTO.

See “Network Interfaces” on page 4 for more information on ATM network interfaces.

Note: To enable the ports, the module must be connected to the network. See the *IBM 8265 Command Reference Guide* for details on the SET MODULE CONNECTED command.

Enabling PNNI Ports on 8260 Modules

The number of PNNI ports that can be enabled on 8260 modules is restricted. The sum total bandwidth of the ports cannot exceed 212 Mbps. For example

- If you have a 4-port 100 Mbps module, you can only enable two of the ports (200 Mbps bandwidth).
- If you have a 12-port 25 Mbps module, you can enable up to 8 of the ports (200 Mbps).

Setting Up Virtual Path Channels (VPCs)

VPC links can only be defined for Public UNI, VOID, and AUTO interfaces, 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 7 shows an example of these VPC links.

Virtual path channels (VPCs) are created via the SET VPC_LINK command. See the *IBM 8265 Command Reference Guide* for details.

Traffic Shaping

Note: This function is only available on 1–port 622 Mbps and 4–port 155 Mbps modules.

When setting up a VPC, you can specify the traffic type provided by the WAN. To do this, you enter the VPC_SERVICE_CATEGORY paramter on the SET VPC_LINK command, giving one of the following two values:

CBR This activates traffic shaping and the type of traffic allowed can be specified with the VPC_SERVICE_CATEGORY parameter (see below).

UBR Traffic shaping is inactive and only Unspecified Bit Rate (UBR) traffic is allowed through this VPC.

When traffic shaping is active (when the parameter CBR is given to the VPC_SERVICE_CATEGORY parameter of the SET VPC_LINK command) you can define which traffic types can be chosen by connections established on this VPC. The possible traffic types are Available Bit Rate (ABR), Constant Bit Rate (CBR), Unspecified Bit Rate (UBR), and Variable Bit Rate (VBR), and you can specify the following:

- CBR VBR only
- ABR only
- UBR only
- CBR VBR, and ABR
- CBR VBR, and UBR
- ABR and UBR
- CBR VBR, ABR, and UBR.

See the *IBM 8265 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 you define an IISP port, check that no VPI is defined in your reachable address.

If you define a VOID or Public UNI port with a VPC link of type IISP, check that the VPI of the VPC link is defined in your reachable address.

If several reachable addresses share the same network prefix, they should be entered as a PNNI summary address to reduce PNNI traffic. See 64 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 8265 and the remote endpoint can either be another port on the same 8265 or on a remote 8265

If the remote endpoint is located on a remote 8265 you must define the ATM address of that 8265.

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 25 Mbps 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

See the *IBM 8265 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 3 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 62 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.

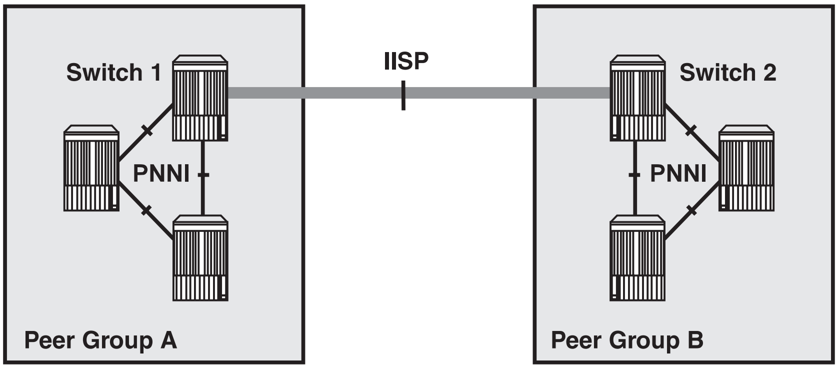


Figure 4. Connecting Switches in Different Peer Groups

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 1 and slot 4 port 2 of Switch 2).

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 1, you would enter the commands:

```
8265ATM> set port 6.1 enable iisp user
8265ATM> set reachable_address 6.1 96 39.99.99.99.99.99.99.00.00.99.99.02
```

2. On Switch 2, enter the commands:

```
8265ATM> set port 4.2 enable iisp network
8265ATM> 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 5 on page 52.

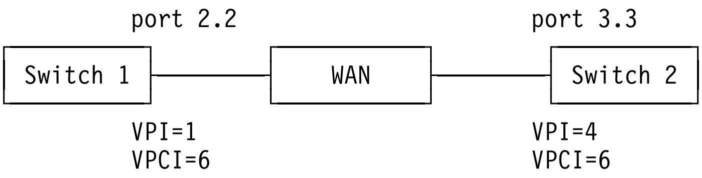


Figure 5. VP Tunneling Over a WAN

If Switch 1 and Switch 2 are part of the 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:

```
8265ATM> set port 2.2 enable public_uni
8265ATM> set vpc_link 2.2 1 enable pnni bandwidth:155000 vpci:6
8265ATM> set port 3.3 enable public_uni
8265ATM> set vpc_link 3.3 4 enable pnni bandwidth:155000 vpci:6
8265ATM>
```

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 be 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 62 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:

```
8265ATM> set device duplicate_atm_addresses allowed|disallowed
```

Enabling Port Mirroring

Note: The Port Mirroring function requires Release 2 or higher of the Control Point code.

The Port Mirroring function duplicates and redirects traffic to any desired port. A Traffic Analyzer can then be connected to this port. Multiple mirrored ports can be active at the same time.

When a port mirroring is active all other ports on the module used for mirroring are disabled.

Port mirroring is enabled using the SNOOP_ENABLE command.

The following example mirrors port 3 of the module in slot 4 to port 1 of the module in slot 2:

```
8265ATM> snoop_enable 4.3 2.1
```

All other ports on the module in slot 2 are disabled.

To disable port mirroring, enter the SNOOP_DISABLE command for the port that is being used for mirroring. For example, to cancel the port mirroring just set up in the earlier example, you would enter:

```
8265ATM> snoop_disable 2.1
```

All ports on the module in slot 2 can now be enabled, if so desired.

Chapter 6. Configuring PNNI Parameters

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

Note: You must have PNNI control point code is order to use the functions described in this chapter.

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 PNNI Control Point code, 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 8265 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.

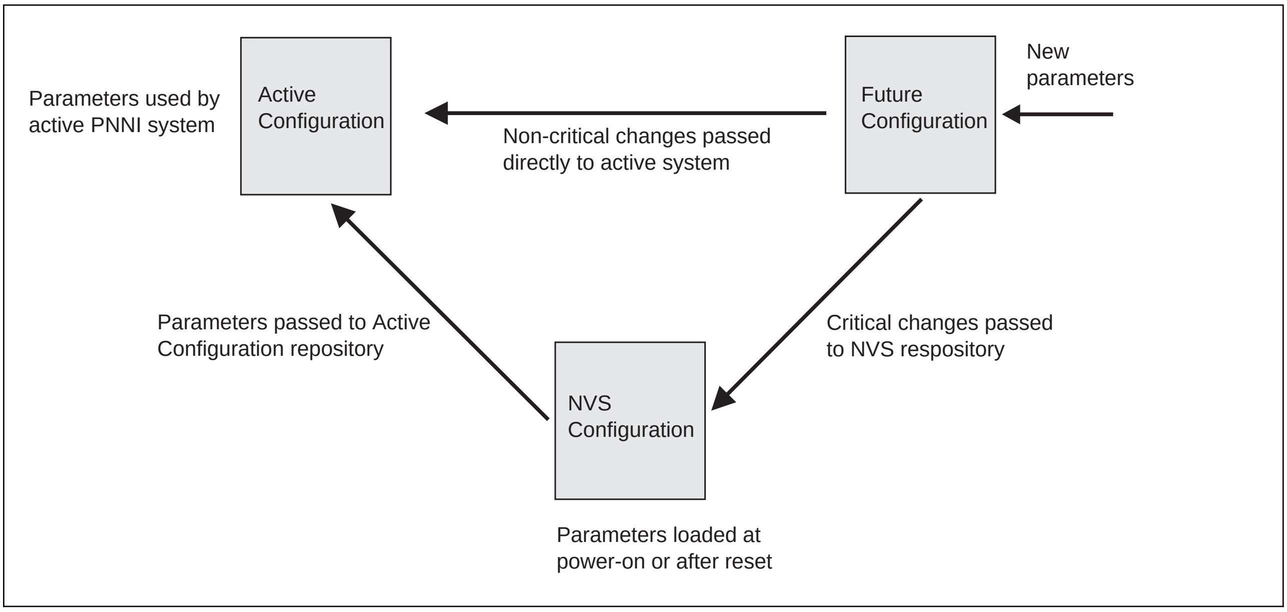

Parameters used by active PNNI system
Active Configuration
Non-critical changes passed directly to active system
Future Configuration
New parameters
Parameters passed to Active Configuration repository
Critical changes passed to NVS respository
NVS Configuration
Parameters loaded at power-on or after reset

Figure 6. 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.

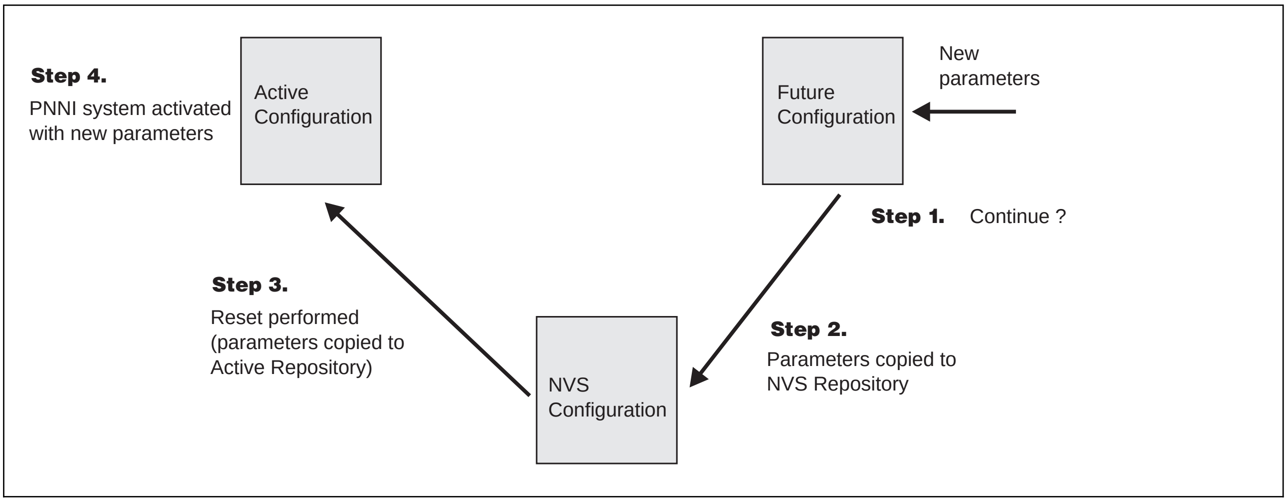

Step 4.
PNNI system activated with new parameters
Active Configuration
Future Configuration
New parameters
Step 1. Continue ?
Step 3.
Reset performed (parameters copied to Active Repository)
NVS Configuration
Step 2.
Parameters copied to NVS Repository

Figure 7. 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.

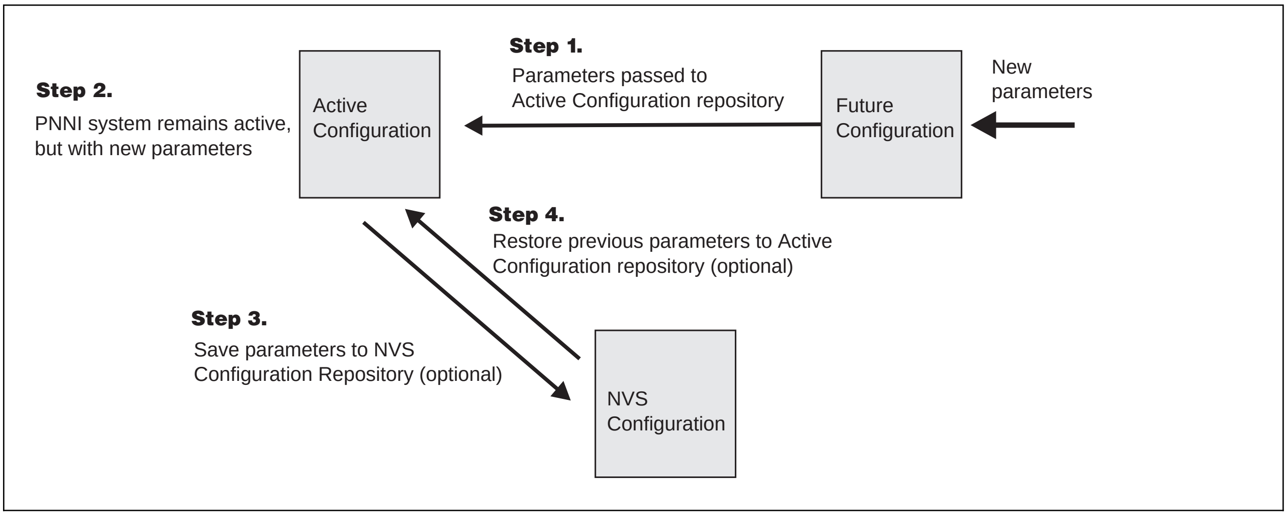

Step 1.
Parameters passed to Active Configuration repository
Step 2.
PNNI system remains active, but with new parameters
Active Configuration
Future Configuration
New parameters
Step 4.
Restore previous parameters to Active Configuration repository (optional)
Step 3.
Save parameters to NVS Configuration Repository (optional)
NVS Configuration

Figure 8. 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:

```
8265ATM> 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:

```
8265ATM> 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 59.). 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” on page 59.

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 59.

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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> uncommit pnni
```

Viewing Configuration Settings

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

```
8265ATM> show future_pnni node_0
```

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

```
8265ATM> 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:

```
8265ATM> 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 58.) 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:

```
8265ATM> 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`:

```
8265ATM> 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 9

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

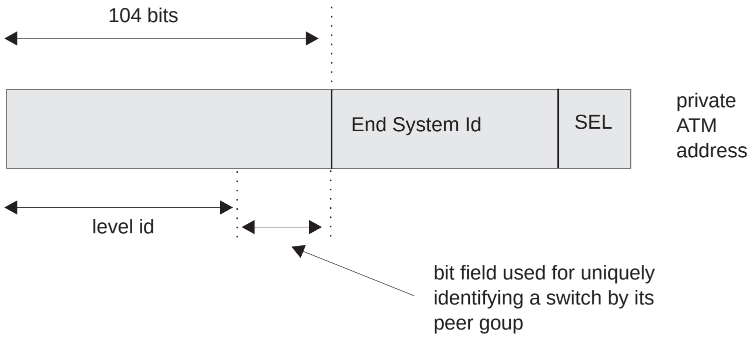


Figure 9. Level ID Perspective of a Switch ATM Address

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:

```
8265ATM> 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:

```
8265ATM> set pnni node_0 peer_group_id: 51 47.a5.32.4e.b7.48.19
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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. This is the path with the smallest sum of adminisitrative weights. If more than one path is found with the same sum of administrative weights, the path with the highest available bandwidth is chosen.

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. The path is computed according to the "widest path" criterion.
- Paths are computed on-demand, resulting in slower connection setups, but with more optimization for the individual routes. The path is computed according to the "shortest path" criterion, based on administrative weights.

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

```
8265ATM> set pnni path_selection abr: on_demand_path
```

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

```
8265ATM> 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.

Regardless of the criterion used, UBR path computation is always done in precomputed mode.

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

```
8265ATM> set pnni path_selection ubr: shortest_path
```

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

```
8265ATM> set pnni path_selection ubr: widest_path
```

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

```
8265ATM> show pnni path_selection
```

Note: Point-to-multipoint calls are processed as on-demand, shortest path.

Using the Crankback Function

The crankback function enables the PNNI control point to automatically establish an alternate link to a target device when a failure occurs on the current route.

To enable or disable the crankback function, you enter the SET PNNI CRANKBACK ON or SET PNNI CRANKBACK OFF command.

The follow example shows how to enable the crankback function.

```
8265ATM> set pnni crankback on
```

You can display whether the crankback function is enabled or not by entering the SHOW PNNI CRANKBACK command.

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:

```
8265ATM> show pnni node_0
```

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

```
8265ATM> 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 :

```
8265ATM> show pnni path_selection
```

For the Future configuration, enter the following command :

```
8265ATM> show future_pnni path_selection
```

Summary Addresses

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

```
8265ATM> show pnni summary_address
```

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

```
8265ATM> 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:

```
8265ATM> 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 :

```
8265ATM> 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

```
8265ATM> show pnni node_0 peer_group_members
```

Neighbor Node Ids

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

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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:

```
8265ATM> 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 7. Configuring Network Access Security

This chapter describes

- How Network Access Security operates
- How to configure the Netwqork Access Security system
- How to display current security settings. 8265.

Introduction

Access to the 8265 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. 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 49.)

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 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 trapping
- Violation logging.

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: disabled
3. violation trapping: disabled
4. violation logging: disabled.

To change the default values, see “Setting Default Values” on page 81.

Violation Trapping

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.

Violation Logging

When violation logging is enabled, the last 64 security violations are stored in a log. The contents of this log can be displayed at the terminal, or uploaded to a server via TFTP.

This information allows a network operator to rapidly help a user determine the reason why network access was denied.

Violation logging can be enabled either for all ports, or individual ports.

Enabling or Disabling Security

You can enable or disable security either globally (on all detected ports in the 8265) 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 “Security Mode Default” on page 81.)

Enabling Security

To enable security globally, you enter the following command:

```
8265ATM> 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 8265 after a reset.

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

```
8265ATM> set security port <slot.port> mode access_control
```

where `<slot.port>` specifies the slot where the module is installed and the port on the module.

Tips:

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

1. SET SECURITY MODE NO_SECURITY (to stop the security system - only required if the system is active)
2. SET SECURITY DEFAULT MODE NO_SECURITY (to disable security on all ports newly detected after security is activated)
3. SET SECURITY MODE ACCESS_CONTROL (to start the access security system)
4. SET SECURITY PORT (slot.port) MODE ACCESS_CONTROL (to enable security on the required ports).

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

1. SET SECURITY MODE NO_SECURITY (to stop the security system - only required if the system is active)
2. SET SECURITY DEFAULT MODE ACCESS_CONTROL (to enable security on all ports newly detected when security is activated)
3. SET SECURITY MODE ACCESS_CONTROL (to start the access security system)
4. SET SECURITY PORT (slot.port) MODE NO_SECURITY (to disable security on the ports for which security is not required).

Disabling Security

To disable security globally, you enter the following command:

```
8265ATM> set security mode no_security
```

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

```
8265ATM> set security port <slot.port> no_security
```

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 for a particular port by specifying that no addresses may be learned.

The autolearn function can be enabled or disabled either for all ports or for specific ports.

To enable or disable the autolearn function for all ports, enter the following command:

```
8265ATM> set security autolearn enable|disable
```

To set a value for a given port, enter the following command:

```
8265ATM> set security port <slot.port> autolearn <value>
```

where `<slot.port>` specifies the slot where the module is installed and the port on the module, and `<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 Violation Traps

You can enable or disable traps on either all ports or selected ports.

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

```
8265ATM> set security trap access_violation|nothing
```

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

```
8265ATM> set security port <slot.port> trap enable|disable
```

where `<slot.port>` specifies the slot where the module is installed and the port on the module.

Enabling and Disabling Violation Logging

You can enable or disable the logging of security violations either on all ports or specific ports.

You enable or disable logging on all ports by entering the following command:

```
8265ATM> set security log nothing|access_violation
```

You enable or disable logging on specific ports by entering the following command:

```
8265ATM> set security port <slot.port> log enable|disable
```

where `<slot.port>` specifies the slot where the module is installed and the port on the module.

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 8265).

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
- Specify if security violations are to be logged.

Security Mode Default

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

```
8265ATM> set security default mode access_control|no_security
```

Violation Trapping 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:

```
8265ATM> set security default trap enable|disable
```

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:

```
8265ATM> 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.

Violation Logging Default

To enable or disable the logging of security violations on all newly detected ports, enter the following command:

```
8265ATM> set security default log enable|disable
```

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 8265 or individual port level.

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

```
8265ATM> set security atm_address <value> any|<slot.port>
```

where `any` specifies that the address is to be accepted for all ports in the 8265, 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:

```
8265ATM> set security esi_address <value> any|<slot.port>
```

where `any` specifies that the address is to be accepted for all ports in the 8265, 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:

```
8265ATM> 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 global settings
- The current default settings
- The ATM addresses authorized for access (at the 8265 or port level)
- The contents of the security violation log
- 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.
  - Whether security voilations are logged or not.
- The last security violations (at the 8265 or port level)

Current Global Settings

To display the global settings currently in effect, enter the following command:

```
8265ATM> show security control
```

The resulting display will show if the following are enabled or disabled:

- Security
- Autolearn function
- SNMP Traps
- Violation logging.

Current Default Settings

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

```
8265ATM> show security default
```

The resulting display will show the default settings for:

- Security
- Autolearn function
- SNMP Traps
- Violation logging.

ATM Addresses Defined

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

```
8265ATM> show security atm_address all|any|<slot.port>
```

where:

`all` is used to display information on all ports in an 8265

`any` is used to display the addresses that have been authorized on any port in the 8265

`<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:

```
8265ATM> show security port all|<slot.port>
```

where:

`all` is used to display information on all ports in an 8265, 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
- Whether security violation logging is enabled.

Security Violations

There are two ways of displaying security violations:

- By displaying the security violation log. This log contains the last 64 violations detected on the 8265.
- By displaying the last violation that occured, either on all ports or on a specific port.

Displaying the Violation Log:

To display information regarding the last 64 security violations, enter the following command:

```
8265ATM> show security violation_log
```

Note: Violation logging must be enabled. See “Enabling and Disabling Violation Logging” on page 80. 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.

Displaying the Last Violation:

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

```
8265ATM> show security last_violation all|<slot.port>
```

where `all` is used to display the last violation on all ports in the 8265, and `<slot.port>` is used to display the latest violation 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.

Clearing the Violation Log:

You can clear the contents of the violation log be entering the following command:

```
8265ATM> clear security violation_log
```

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.

The security settings are saved by entering the following command:

```
8265ATM> save security
```

This will save the parameter settings to NVRAM.

Reverting Security Changes

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

The security settings are restored by entering the following command:

```
8265ATM> revert security
```

This will automatically reset the ATM subsystem and retrieve the security parameter settings from NVRAM.

Uploading and Downloading the Access Control Address Table

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

- 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_CONFIG
4. UPLOAD (to upload the file).

Downloading the Access Control Address Table

To 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_CONFIG
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. Once you have done this, upload the access control address table to the server 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 00000000000000000000000000ffffffffffff 01 01
00000000000000000000000000010203040502 00000000000000000000000000ffffffffffff 01 02
00000000000000000000000000010203040503 00000000000000000000000000ffffffffffff 02 04
39020304050607080910111213141516171819 ffffffffffffffffffffffffffffffffffffff 00 00
```

Figure 10. 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 immediately if the access control address table is downloaded to the 8265 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).

Uploading the Violation Log

The security violation log can be uploaded, via TFTP, to a server.

To upload the log, 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_LOG
4. UPLOAD (to upload the file).

Part 2. Managing the 8265

Chapter 8. Management Commands

This chapter describes the commands used to display information about the 8265 and it s components.

Commands are shown to:

- Displaying information about the 8265, including backplane information, number and status of installed power supplies, operating temperature, and status of the cooling fans.
- Displaying power system information, include the power mode (fault tolerant or non-fault tolerant), slot information, and the 8265 power budget. For more detailed discussion of the power management commands, refer to Chapter 9, “Managing the Power Subsystem” on page 103.
- Displaying information about installed modules.
- How to reset the 8265 and installed modules.

The *IBM 8265 Command Reference Guide*, SA33-0458 provides details of all 8265 commands.

Displaying 8265 Information

Enter the SHOW HUB command to display basic information about 8265 operating conditions, including temperature and power supply conditions.

The following 8265 information is provided by the SHOW HUB command:

- Type - indicates that this is a specific model of a 8265
- Backplane - indicates the type and revision level of all installed backplanes
- Power supply - indicated if a power supply is present in the slot, its normal or faulty status, and its model number
- Fan - indicates the status of each 8265 fan
- Temperature - indicates 8265 temperature at three locations.

To display 8265 information and operating conditions, use the following command syntax:

```
SHOW HUB
```

The following example shows typical output from the SHOW HUB command:

```
8265ATM> show hub

 Hub Information:
     Hub Type: 8265_S17

 Backplane Information:
     Backplane Type                             Revision
     --------------                             --------
     Load-Sharing Power Distribution Board      0
     SwitchChannel Backplane                    0

 Power Supply Information:

     Power Supply  Status       Model Number
     ------------  ------       -----------
      1            OKAY         8265PS-HO
      2            OKAY         8265PS-HO
      3            OKAY         8265PS-HO
      4            NORMAL       8265PS-HO

 Temperature Information:
     Probe         Location         Temperature
     -----         --------         -----------
      1            FAN_1            29 Degrees Celsius
      2            FAN_2            29 Degrees Celsius
      3            FAN_3            29 Degrees Celsius

 Fan Information:
      Fan           Status
      ---           ------
       1            OKAY
       2            OKAY
       3            OKAY

8265ATM>
```

Displaying the Power System

To display the power mode, slot power information, and power budget information for the 8265 and all installed 8265 modules, use the following command syntax:

```
SHOW POWER ALL
```

The following example shows typical output from the SHOW POWER ALL command:

```
8265ATM> show power all

                Power Management Information
                ----------------------------
 Hub Power Modes:

         Fault_Tolerant Mode:       NON_FAULT_TOLERANT
         Fault_Tolerant Status:     NON_FAULT_TOLERANT

 Slot Power Information:

 Slot     Class          Admin Status       Operating Status
 ----     -----          ------------       ----------------
 1        9              ENABLE             ENABLED
 3        4              ENABLE             ENABLED
 5        4              ENABLE             ENABLED
 6        5              ENABLE             ENABLED
 9        8              ENABLE             ENABLED
14        7              ENABLE             ENABLED


 Hub Power Budget :

 Voltage Type Voltage Level Watts Capacity Watts Available Watts Consumed
 ------------ ------------- -------------- --------------- --------------
 +5V            5.128         366.00         225.00         141.00
 -5V           -5.058          25.50          22.25           3.25
 +12V          11.803          81.00          27.50          53.50
 -12V         -11.993          30.50          30.25           0.25
 +2V            2.125          14.20          10.10           4.10
8265ATM>
```

In the example above:

- 8265 modules are installed in slots 1, 3, 5, 6, 9, and 14.
- Power is enabled to all occupied slots.
- Power mode and power budget information is displayed.

Displaying 8265 Module Information

Show the Inventory of Modules

Use the following SHOW INVENTORY commands to display information about the installed modules:

- SHOW INVENTORY NO_VERBOSE
- SHOW INVENTORY VERBOSE.

When you enter SHOW INVENTORY NO_VERBOSE, the following information is displayed for installed modules:

- 8265 identification information:
- Hardware version number of the 8265
- Serial number of the 8265
- Vendor name
- Date of manufacture
- Slot numbers and slot contents per slot (slots 1 through 19, inclusive)
- Model number, hardware version number, serial number, and vendor name for each installed module
- Date of manufacture for each installed module.

When you enter SHOW INVENTORY VERBOSE, the following additional information is shown for installed 8265 modules:

- Operational software version number
- Boot software version number
- Burned in addresses for the Ethernet port and LAN emulation.

Show Inventory No_Verbose:

To display basic inventory information for the 8265, use the following command syntax:

```
SHOW INVENTORY NO_VERBOSE
```

The following example shows typical output from the SHOW INVENTORY NO_VERBOSE command:

```
8265ATM> show inventory no_verbose


Hub/                   Hardware
Slot  Module           Version  Serial #         Vendor           Date
----- ---------------  -------- ---------------- ---------------- ------
HUB   8265-S17         A        L9915            IBM              970708

01.01 53-58G9611FC5004 C38844   VIM R034         IBM              960531
09.01 93076H8108FC6501 E95775   16               IBM              970820
09.02 93002L2428FC6501 E95775   24               IBM              970820
18.01 8000-RCTL        R        1002442          IBM              970620

8265ATM>
```

Show Inventory Verbose:

To display more detailed inventory information for the 8265, use the following command syntax:

```
SHOW INVENTORY VERBOSE
```

Note: In the following screen output display, information for slots 11 through 15 is not shown (a vertical row of dots below the information given for slot 10 indicates a break in output display continuity).

The following example shows typical output from the SHOW INVENTORY VERBOSE command:

```
Hub/                 Hardware
Slot  Module          Version  Serial #         Vendor           Date
----- --------------- -------- ---------------- ---------------- ------
HUB   8265-S17        A        H5876            IBM              970708

      Type:      58G5801          Number of slots:  17
      Note Pad:
      LAN Emulation Token Ring BIA:0006291f1234
      LAN Emulation Ethernet BIA  :000629771234
      Ethernet Port BIA           :000629779234

01.01 53-58G9611FC5004 C38844   VIM R034         IBM              960531

      Note Pad: OK for combo
      Hardware Features  0X020202020
      Operational Version: n/a        Boot Version: n/a

09.01 93076H8108FC6501 E95775   16               IBM              970820

      Note Pad: 13J8704 8265 Switch Card
      Hardware Features  0X020202020
      Operational Version: d3.02.9    Boot Version: e3.02.9

09.02 93002L2428FC6501 E95775   24               IBM              970820

      Note Pad: 13J8704 8265 Control Point Card
      Hardware Features  0X020202020
      Operational Version: n/a        Boot Version: n/a

18.01 8000-RCTL        A        1002442          IBM              970620

      Note Pad: 0
      Hardware Features  0X020202020
      Operational Version: b1.14.0    Boot Version: v1.01

8265ATM>
```

Displaying Module Details

Enter the SHOW MODULE command to display information for a module installed in a specified slot, or to display information for all modules and submodules installed in the 8265.

The following SHOW commands are available:

- SHOW MODULE
- SHOW MODULE ALL
- SHOW MODULE VERBOSE

Show Module:

To display basic information for a module installed in a specified slot, use the following command syntax:

```
SHOW MODULE
```

In the following example, the SHOW MODULE command is used to display basic information for a controller module installed in slot 18.

```
8265ATM> show module 18

Slot  Install Connect Operation General Information
----------------------------------------------------------------
18    Y       N       Y         Active Controller Module

8265ATM>
```

Show Module All:

To display basic information for all modules installed use the following command syntax:

```
SHOW MODULE ALL
```

In the following example, SHOW MODULE ALL is used to display the following information for all installed modules:

- Slot location
- Module name
- Module version number
- Network assignment
- General information.

```
8265ATM> show module all

 Slot Install Connect Operation General Information
 --------------------------------------------------------------------------------
  1       Y        n        n     8265 ATM WAN 2 Module
  2       n        n        n     -
  3       n        n        n     -
  4       Y        Y        Y     8265 ATM 4-ports 155 Mbps Module
  5       n        n        n     -
  6       n        n        n     -
  7       n        n        n     -
  8       n        n        n     -
  9       Y        Y        Y     8265 ATM Control Point and Switch Module:Active
 10       Y        n        n     <extension>
 11       n        n        n     -
 12       n        n        n     -
 13       Y        n        n     8265 ATM 622 Mbps Module
 14       Y        n        n     8265 ATM 4-ports 155 Mbps Module
 15       Y        n        n     8265 ATM 622 Mbps Module
 16       n        n        n     -
 17       n        n        n     -
 18       Y        n        Y     Active Controller Module
 19       n        n        n     -

8265ATM>
```

Show Module Verbose:

To display detailed information about a module installed in a specified slot, use the following command syntax:

```
SHOW MODULE {slot} VERBOSE
```

In the following example, SHOW MODULE VERBOSE is entered to display detailed information for a 4-port 155 Mbps module installed in slot 1:

```
8265ATM> show module 1 verbose


 Slot  Install  Connect  Operation  General Information
 ----  -------  -------  ---------  -----------------------------
  1        Y        Y         Y      8265 ATM 4-ports 155 Mbps Module

 status: connected / hardware OK
         enable / normal

 P/N: 58G9878  EC level: D55931 Manufacture: VIME
 Operational FPGA version : 6
      Backup FPGA version : 6


      Type  Mode      Status
 ------------------------------------------------------------------------
  1.01:PNNI enabled   UP
  1.02:VOID enabled   no activity
  1.03:UNI  enabled   UP
  1.04:UNI  disabled

8265ATM>
```

Resetting Components

Enter the RESET command to reset either individual media modules or the 8265 chassis and all installed modules. The following RESET commands are available:

- RESET MODULE
- RESET HUB
- RESET ATM SUBSYSTEM.

Resetting Modules

Use the RESET MODULE command to perform a hardware reset of a specific installed media module (not controller or CPSW modules). Use this command only if a module is not functioning properly.

The 8265 contains 19 slots (including controllers), numbered sequentially from left (#1) to right (#19). The 8265 resets the module in the specified slot to its last-saved configuration.

To reset a media module, use the following command syntax:

```
RESET MODULE {slot}
```

In the following example, RESET MODULE initiates a hardware reset of the module installed in slot 16:

```
8265ATM> reset module 16

Reset started.
8265ATM>
```

Resetting the 8265

Use the RESET HUB command to reboot all installed modules and the 8265 itself, including the active controller module. RESET HUB performs a hardware reset of the 8265 and all installed modules. Diagnostic routines execute (if enabled) and traffic forwarding may be briefly interrupted. Once the 8265 reset is complete, you must log back in to the CPSW before you can enter any other commands.

Note: You must save or revert unsaved changes before RESET HUB executes.

To reboot the 8265 and all installed modules, use the following command syntax:

```
RESET HUB
```

In the following example, RESET HUB reboots the 8265 and all installed modules:

```
8265ATM> reset hub
8265ATM>
ATM Control Point and Switch Module
Copyright IBM Corp. 1997.

8265ATM>
```

Resetting the ATM Subsystem

Resetting the ATM susbsytem is similar to resetting the 8265, but the reset is achieved more quickly as the Controller modules are not reset.

The following example shows the RESET ATM_SUBSYSTEM command in use:

```
8265ATM> reset atm_subsystem

This will reset the atm subsystem.  Are you sure (Y/N) ? Y
Copyright IBM Corp. 1997.

Password:
```

Chapter 9. Managing the Power Subsystem

This chapter descibes:

- How to display the 8265 power budget, and increase the budget if neccessary.
- How to establish fault-tolerance in the power subsystem.
- The sequence that the 8265 powers up slots, and how to change the sequence.
- How the 8265 manages power deficits.
- How to enable and disable power to individual slots.

Budgeting Power

Before install a new 8265 module in the switch, you should establish that there is sufficient power available for it to operate. The SHOW POWER BUDGET command displays current switch power conditions that help you decide if there is sufficient power available to power up and operate the new module.

When the controller module powers up an 8265 module, the controller module adjusts the available power budget to reflect the power consumption of the newly powered-up module. The controller module then powers up remaining modules (by power class and slot location) to the limit of the unallocated power budget.

By maintaining an accurate power budget, the controller module can determine:

- Which installed modules to power up
- Which installed modules (if any) to power down to bring module power consumption under budget
- Which installed modules to place in power pending state due to a lack of sufficient unallocated power budget to power them up.

This section describes:

- Determining the Power Budget
- Increasing the Unallocated Power Budget.

Determining Switch Power Budget

To ensure optimal power fault-tolerance, determine the current power budget for the switch as follows:

1. Enter the SHOW POWER BUDGET command at the terminal prompt. The SHOW POWER BUDGET command shows the amount of power currently available for modules:

   - Total power installed
   - Amount of power consumed
   - Amount of power available.

   Compare this information with the power requirements for each module installed.

   Refer to the *Planning and Site Preparation Guide* to determine your module power requirements. Take into account any modules you plan to install, as well as those already installed.

   Note: Power supply output values displayed by the SHOW POWER BUDGET command have been rounded down. Therefore, these values may not precisely match those provided in the documentation shipped with each module.

2. Examine the output of the SHOW POWER BUDGET command. If necessary, add another power supply to your switch.

Displaying the Power Budget:

To display power budget information, use the following command syntax:

```
SHOW POWER BUDGET
```

This command shows you how power output is distributed among all installed load-sharing power supplies. This information helps you to determine if power is sufficient to permit the addition of modules, and to avoid an unintentional loss of power fault-tolerance (if currently in effect).

When you enter SHOW POWER BUDGET command, the following information is displayed.

```
8265ATM> show power budget

                     Power Management Information
                     ----------------------------
8265 Power Budget :

Voltage Type Voltage Level Watts Capacity Watts Available Watts Consumed
------------ ------------- -------------- --------------- --------------
     +5V        5.094         366.00         225.00           141.00
     -5V       -5.058          25.50          22.25             3.25
    +12V       11.083          81.00          27.50            53.50
    -12V      -11.993          30.50          30.25             0.25
     +2V        2.125          14.20          10.10             4.10

8265ATM>
```

If you have a mixture of 415 Watt and 295 Watt power supplies in your 8265 and fault-tolerant mode is enabled, a warning message is displayed to inform you that the 415 Watt power supplies are being treated as having 295 Watts.

Note: This condition is a result of a physical limitation on the lower output power supply. The lower output power supply (295 Watt) cannot back up a higher output power supply (415 Watt).

Increasing the Unallocated Power Budget

This section describes actions you can take to increase the unallocated power budget whenever you need more power for installed modules, or to power up newly installed modules.

To increase the unallocated power budget:

- Add one or more power supplies.
- If the 8265 is running in power fault-tolerant mode, change the power mode to power non-fault-tolerant (load sharing) to make reserve power available to all installed modules.
- As a last resort, manually power down selected low power class media modules until you have enough power.

Establishing Power Fault-Tolerance

Operate the switch in power fault-tolerant mode to ensure that at least one supply's worth of power is available to replace power lost when and if a single power supply fails.

To set the switch to power fault-tolerant mode or power non-fault-tolerant mode enter the SET POWER MODE command at the terminal prompt.

When you attempt to set the switch to power fault-tolerant mode, the active controller module determines if there is sufficient unallocated power budget available to place one power supply's worth of power in reserve.

- If there is sufficient unallocated power budget, the switch sets to power fault-tolerant mode.
- If there is insufficient unallocated power budget, the switch remains in power non-fault-tolerant mode.

CAUTION:
The 8265 may reset unpredictably when in power fault-tolerant mode if there is insufficient power in reserve when a power supply failure occurs.

Displaying Current Power Mode

To display which of two power modes is currently in effect (power fault-tolerant mode or power non-fault-tolerant mode), use the following command syntax:

```
SHOW POWER MODE
```

When you enter SHOW POWER MODE command while the 8265 is running in power non-fault-tolerant mode, the following information is displayed:

```
8265ATM> show power mode

                     Power Management Information
                     ----------------------------
 Hub Power Modes:

        Fault-Tolerant Mode:         NON_FAULT_TOLERANT

8265ATM>
```

When you enter SHOW POWER MODE command while the 8265 is running in power fault-tolerant mode, the following information is displayed:

```
8265ATM> show power mode

                     Power Management Information
                     ----------------------------
 Hub Power Modes:

        Fault-Tolerant Mode:         FAULT_TOLERANT
        Fault-Tolerant Status:       FAULT_TOLERANT

8265ATM>
```

Changing the Power Mode

The 8265 uses load-sharing power supplies that support two power modes.

- Power fault-tolerant mode - this mode can be established only if there is at least one power supply's worth of power more than what is needed to meet the current power requirements of all installed modules.

  When the 8265 is running in power fault-tolerant mode, one power supply's worth of power is always kept in reserve. If a power supply fails, reserve power becomes available and the 8265 continues to operate.

- Power non-fault-tolerant mode - when in this mode, the full power output of all installed power supplies is available to run the 8265 and installed modules.

Note: 8265 modules are automatically power-managed by the controller module.

Use the SET POWER MODE to choose between normal and fault-tolerant power supply operation using the 8265 intelligent power management system.

For example:

- Each power supply (415 Watt power supply) provides approximately 300 Watts at +5 Volts
- You have three power supplies available (which gives you 900 Watts of +5 Volts)

In this example, non-fault tolerant mode allows you to use 900 Watts. Fault-tolerant mode allows you to use 600 Watts, reserving 300 Watts to use in the event of a power supply failure.

Note: Regardless of the power mode setting, the power load being used is shared across all installed power supplies.

To set the power mode to fault-tolerant mode or power non-fault-tolerant mode, use the following command syntax:

```
SET POWER MODE {fault_tolerant}

SET POWER MODE {non_fault_tolerant}
```

In the following example, the power mode is set to power fault-tolerant mode:

```
8265ATM> set power mode fault_tolerant
       Power mode set to FAULT_TOLERANT

8265ATM>
```

Note: Fault-Tolerant Mode indicates the power mode you set. Fault-Tolerant Status indicates the mode currently in effect. A power supply failure, or the installation of an additional power supply exemplify conditions that may cause the Fault-Tolerant Status to change to the power mode you previously set.

8265 Module Power Up Strategy

This section describes:

- Default 8265 Module Power Up Strategy
- How to Specify 8265 Module Power Up Order.

Default Power Up Strategy

The controller module determines how much power an 8265 module requires before it permits the module to power up.

The controller module employs the following powerup strategy:

- Current unallocated power budget must be sufficient to power up this module.
- Media modules power up, in order, from slot 1 to slot 17.
- Media modules that have the highest power class setting power up first.
- Media modules continue to power up based on power class settings (from highest to lowest). This process continues until the limit of the power budget is reached.
- If two or more media modules have the same power class setting, they power up, in order, from slot 1 to slot 17.

Note: Power-on occurs in this manner only if the installed do not configure from saved power management configuration data stored in their NVRAM. For more details, refer to Chapter 4 the section titled Saved Power Management Configurations.

Specifying Power Up Order

To specify the order in which 8265 modules power up, you change their power class settings.

To change the power class setting for a module:

1. Enter the SET POWER SLOT {slot} CLASS command, giving the new class value.
2. Press Enter.

For further information, see the 8265 Command Reference Guide.

Power Class Settings

A power class setting is a definable value ranging from 1 through 10 (10 is the highest possible power class setting). You can define the power class setting for any installed media module to make one module more important or less important than another.

The controller module uses default and user-defined power class settings to make power management decisions. For example, power class settings are used to determine the order in which media modules power up and power down under certain power deficit and overheat conditions.

This section describes:

- Displaying the Current Slot Status
- Using the Default Power Class Setting
- Setting Power Class Manually
- Power Class 10 Warnings.

Displaying the Current Slot Status

To display the slot number, power class setting, administrative status (slot power enabled or disabled), and module operating status of a module installed in a specified slot, use the following command syntax:

```
SHOW POWER SLOT {slot}
```

The following examples show the typical display when you enter the SHOW POWER SLOT command for a module installed in slot 1:

```
8265ATM> show power slot 1

               Power Management Information
               ----------------------------
Slot Power Information:

Slot     Class          Admin Status       Operating Status
----     -----          ------------       ----------------
1        9              ENABLE             ENABLED
8265ATM>
```

Using the Default Power Class Setting

Each media module is shipped with a default power class setting of 3.

Assign a higher power class setting to any media module connected to critical network resources.

Setting Power Class Manually

To set the power class for a module in a specified slot:

1. Enter the SET POWER SLOT {slot} CLASS command, giving the new class value.
2. Press Enter.

Note: Even though it has a power class setting, a controller module cannot be power managed. A controller module always draws power when inserted in the switch, and cannot be powered down using a terminal command.

Set Power Slot {slot} Class:

Use the SET POWER SLOT {slot} CLASS command to determine the order in which modules power down if there is inadequate power to run the system. Modules with the lowest priority power down first.

The active controller module uses media module power class settings to decide:

- Which modules should be powered down following a power supply failure.
- Which modules should be powered down because of an overheat condition.

Power class settings range from 10 (highest) to 1 (lowest). The default power class setting for all media modules is 3.

Notes:

1. Modules set to power class 10 do not power down automatically under any circumstances.
2. You cannot change the default power class setting for installed controller modules.

To set the power class for a media module, use the following command syntax:

```
SET POWER SLOT {slot} CLASS
```

In the following example, SET POWER SLOT CLASS is used to set the power class for a media module installed in slot 1 to power class 7:

```
8265ATM> set power slot 1 class
Enter class: 7

Slot 01 power class is set to 07.
8265ATM>
```

Power Class 10 Warnings:

A media module assigned a power class setting of 10 cannot be automatically powered down by installed controller modules.

- If a power supply failure causes a power deficit, a media module assigned a power class setting of 10 continues to run until you order it to shut down. Under some conditions (such as an extended overheat condition), switch or module hardware damage may result.
- To ensure that the controller module is able to automatically make all power management decisions without waiting for user intervention, do not assign a power class setting of 10 to any media module unless absolutely necessary.

8265 Module Power-Down Response

This section describes how Intelligent Power Management responds to power deficits caused by selected abnormal operating conditions.

Correcting a Power Deficit

To correct a power deficit, the controller module must reduce the power consumption of all installed modules. The controller module can only reduce power consumption by:

- Disabling power fault-tolerant mode (if in effect) to make reserve power available to installed modules.
- Selectively powering down media modules to return power to the budget.

If the controller module is unable to respond to a power deficit (for example, due to a power failure), the switch resets. Under these conditions, powerup (recovery) occurs when the 8265 reboots.

For more information, refer to the section titled Power Supply Failure later in this chapter.

Powering Up With Insufficient Power:

If there is insufficient power to power up, the controller module will automatically place modules in power pending state until there is enough power to enable them.

Power Supply Failure:

Intelligent Power Management response to a power supply failure is determined by the current power mode:

- If a power supply fails while the switch is running in power fault-tolerant mode:
  - The controller module responds by disabling power fault-tolerant mode. If the power budget deficit remains in effect after power fault-tolerant mode has been disabled, media modules selectively power down based on power class settings and relative slot locations until the power budget deficit is corrected.
  - Once the power budget deficit is corrected and there is again enough power to re-establish power fault-tolerant mode, power fault-tolerant mode is automatically re-enabled.

  Note: When a power deficit occurs while the 8265 is running in power fault-tolerant mode, the controller module does not shut down media modules to reduce the power budget.

- If a power supply fails while the 8265 is running in power non-fault-tolerant mode (the default mode), the controller module may selectively shut down media modules in an attempt to bring module power consumption under budget.

The media module power-down sequence is as follows:

- The modules power down, in order, from slot 17 to slot 1, starting with modules having the lowest power class setting.
- If two or more modules have the same power class, they power down from slot 17 to slot 1.
- Modules continue to be powered down until total power consumption is at or below budget.

You can specify the order in which media modules power down when a power supply failure occurs by changing the module power class settings (SET POWER SLOT {slot} command).

For more information, refer to the section titled Specifying Power Up Order earlier in this chapter and the 8265 Command Reference Guide

For information concerning 8265 module power-down due to an overheat condition, see “Overheating” on page 115.

Chapter 10. Managing the Intelligent Cooling Subsystem

The Intelligent Cooling Subsystem in the 8265 helps prevent:

- Damage to the switch and all installed modules
- Loss of configuration information

The default temperature threshold is the maximum internal switch temperature for normal switch operation.

- The allowable ambient temperature operating range is 0 °C to 40 °C (32 °F to 104 °F).
- An overheat condition exists when internal switch temperature exceeds the default temperature threshold.
- The default internal operating temperature threshold for the switch is 60 °C (140 °F) or higher.

This chapter describes:

- Operating temperature and fan status indicators
- Overheat conditions and recovery actions
- The automatic 8265 module power-down strategy.

Operating Temperature and FAN Status Indicators

The controller modules in the 8265 are equipped with LEDs that illuminate when the operating temperature is exceeded or a fan unit fails.

These indicators work on the active controller only, as the standby controller does not monitor 8265 operating conditions.

Operating Temperature Indicators

The Temp LED on the active controller module blinks to warn you of an internal overheat condition.

When switch internal operating temperature rises above the temperature threshold, the following occurs:

1. A built-in temperature sensor detects the rise in switch internal operating temperature.
2. The Temp LED on the active controller module blinks.
3. The active controller module sends an alert to the system administrator.

The overheat indication stops when switch internal operating temperature falls below the temperature threshold for at least 15 minutes. Correct the overheat condition promptly to avoid possible hardware damage (only the active controller module indicators report switch operating conditions.)

Table 3 on page 114 describes controller module LEDs associated with switch internal operating temperature.

Table 3. Active Controller LEDs

LED	LED State	Indicates
Temp	On	Temperature is normal.
	Off	Temperature is normal, or the Temp LED is faulty.
	Blinking	Temperature is higher than the allowable limit.
Fan (1 - 3)	On	Fan is present and operating.
	Off	Fan is not installed or Fan LED is faulty.
	Blinking	Fan unit is malfunctioning or not operational.
Power Supply (1-4)	On	Power supply present and OK.
	Off	Power supply not installed, or Power Supply LED is faulty.
	Blinking	Power supply present, but faulty.

Fan Status Indicators

Fan status indicators (LEDs) on the active controller module will illuminate when a fan unit fails. The 8265 can temporarily run with two functioning fans.

Because the switch can run on just two fans, the warning provided by the FAN status LEDs allows you adequate time to replace a faulty fan at your convenience.

Note: Operate the switch with all fans running.

Automatic 8265 Module Power-Down

The Intelligent Cooling Subsystem operates as follows:

1. The active controller module continually monitors the temperature sensor located behind each fan unit, providing an accurate measurement of internal switch temperature.
2. An overheat condition may cause the active controller module to power down selected media modules. This condition continues until the cause of the overheat condition is corrected and normal switch internal operating temperature is restored.

   The order in which media modules power down is determined by:

   - Individual module power class settings
   - Relative slot location of each installed module

For more information, refer to “8265 Module Power-Down Response” on page 111.

Overheating

This section describes:

- Overheat Conditions
- Overheat Management Areas
- Power-Down Strategy
- Recovery Strategy.

Overheat Conditions

An overheat condition exists when one of the 8265 temperature sensors detects an operating temperature that exceeds a pre-defined threshold. The allowed ambient temperature operating range is 0 °C to 40 °C. The default threshold setting is fixed at an upper limit of 60 °C (140 °F) to prevent module damage.

An overheat condition may be caused by cooling loss or excessively high ambient (room) air temperature.

The Temp LED on the active controller module blinks to warn you in the case of internal overheat condition.

The following occurs during an overheat condition:

1. If an SNMP agent is present in the 8265, power management informs the SNMP agent of the overheat condition.
2. A 1-minute delay is provided, during which external management entities are notified of the overheat condition.
3. Approximately 1 minute later, the controller module applies a power down strategy to media modules installed in the overheat management area where the overheat condition was detected.
4. The overheat indication ends when the 8265 internal operating temperature falls below the temperature threshold and stays there for 15 minutes.

The controller module does not power down media modules occupying slots outside affected overheat management areas. This overheat power-down strategy is based on the power class setting and slot location of each media module.

Overheat Management Areas

The overheat power-down strategy is based on three temperature sensors in the 8265, one per installed fan unit, that effectively divides the module payload area of the 8265 into three overlapping overheat management areas.

Each overheat management area comprises 8 payload slots. The overlap reflects the overlapping cooling effects of adjacent fan units (the 8265 can run with a minimum of two fan units installed, but three are recommended).

The overheat management areas divide the payload slots as follows:

- Slots 1 through 8 (overheat management area 1)
- Slots 6 through 13 (overheat management area 2)
- Slots 10 through 17. (overheat management area 3).

Power-Down Strategy

The media module overheat power-down strategy is as follows:

- When any 8265 temperature sensor detects an internal operating temperature of 45 °C or higher, power management issues warning traps that tell the user an overheat condition may soon exist. The system generates warning traps every 30 seconds (approximate) at this point.
- When the internal operating temperature reaches 60 °C (140 °F), power management power-disables selected media modules installed within each affected overheat management area to reduce the 5 Volt power consumption by at least 50 Watts.

  Selected media modules in affected overheat management areas power-down, in order, starting with modules having the lowest power class setting.

  This reduction of power consumption should provide a 2 °C drop in temperature at the temperature sensor for that overheat management area. A single temperature sensor is located at the back of each exhaust fan. The system generates overheat traps every 10 seconds (approximately).
- If two or more media modules in an affected overheat management area have the same power class, they power down from highest slot to lowest slot.
- Media modules continue to power down until all media modules in the affected overheat management area have powered down. Modules with a power class setting of 10 continue to run.
- 8265 temperature is allowed to stabilize for 15 minutes before further action is taken.
- If the temperature is not at or below the established overheat threshold after 15 minutes, all modules in the affected overheat management area (or areas) are powered down. Modules in affected overheat management areas do not power up again until you correct the overheat condition.

Recovery Strategy

Overheat recovery occurs when the temperature sensor that detected an overheat condition reports that the internal temperature is now at or below the overheat threshold.

Once overheat recovery is initiated, modules that were powered down to alleviate the overheat condition power up to the limit of the current power budget.

The controller module performs the recovery powerup as follows:

- Modules power up, in order, from the lowest slot in the affected overheat management area to the highest slot in the affected overheat management area.
- Modules with the highest power class setting power up first. If two or more modules have the same power class setting, they power up from the lowest slot in the affected overheat management area to the highest slot in the affected overheat management area.

Saved Power Management Configurations

The active controller module stores:

- Saved power management configuration data for all installed modules in on-board NVRAM
- Unmanaged power allocation data describing the type (per voltage) and the amount of power (Watts) available to installed modules.

When the 8265 powers up following a reset:

- The controller module uses saved power management configuration data to verify that power configurations for installed modules precisely match those in effect prior to the reset.
- If necessary, the controller module uses the saved data to restore lost module power configurations.

The controller module saves the power management configuration data shown in Table 4.

Table 4. Saved Power Management Configuration Data

Data Type	Description
Unmanaged power allocation	Power available to modules after all installed modules have powered up.
Slot profile	Identifies the module installed in a given slot as a CPWS module or a media module. In addition, empty slots are identified.
Slot power state	Power state for each installed module (enabled, disabled, or pending).
Slot power class	Power class setting for each installed module.
Power mode	Power mode for the switch prior to a switch reset (power fault-tolerant mode or power non-fault-tolerant mode).

As the switch powers up following a reset, the controller module compares the saved slot profile data with current slot profile data, in each successive slot.

- If the saved slot profile data for all slots matches the current slot profile data, all modules then configure to saved power management configuration data.
- If a current slot profile does not match the saved profile for a given slot, the following applies:
  - Modules power up based on power class setting and relative slot location.

  See above, "8265 Module Power Class Settings" for more information.
- If a current slot profile does not match the saved profile for a given slot, the following applies:
  - The controller module powers up modules based on power class setting and relative slot location to the limit of the current power budget.

Note: If a power supply fails while the switch is rebooting, saved power management configuration data (for example, the number of installed and functioning power supplies) does not accurately describe switch conditions following the reboot. Under these circumstances, total power required by modules may be more power than the power available after the reboot.

Chapter 11. Updating Microcode and Picocode

Receiving Code Updates

New versions of code for 8265 modules that are already in operation are available via the Internet, at the following URL:

```
http://www.networking.ibm.com/8265/8265fix.html
```

This is the '8265 Microcde Upgrades' home page. From here, you can select the right 8265 module.

Automatic Notification of Updates

To automatically receive notification when microcode updates are available, register your e-mail address at the follwoing URL:

```
http://www.networking.ibm.com/8265/8265reg.html
```

Upload and Download Operations

The hardware microcode for your CPSW and media modules can be upgraded by inband operations. The software microcode for your CPSW and media modules can be upgraded by out-of-band operations. Data such as error logs, traces, and dumps can also be uploaded to the host. These operations are shown in Figure 11.

For more information on the commands used to start these operations, see the *IBM 8265 Command Reference Guide*.

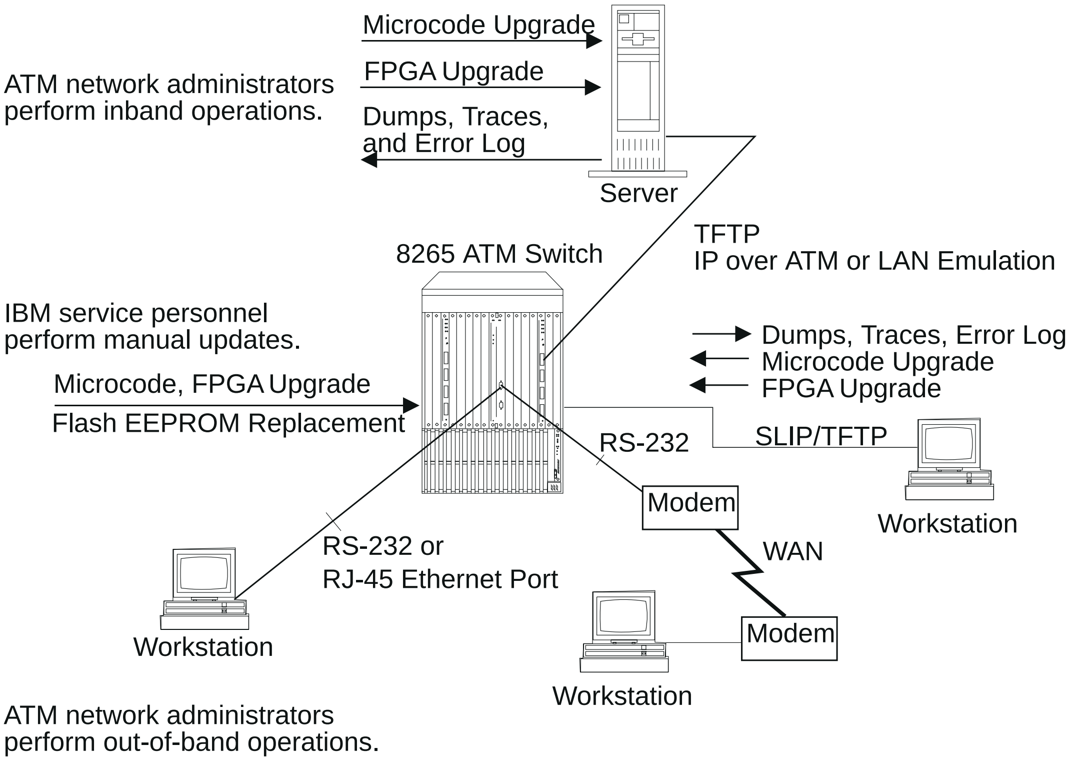


Figure 11. Upgrade Operations for ATM Microcode

Inband Operations

To upgrade ATM microcode, ATM network administrators perform inband operations from a server connected to an 8265, using a workstation connected to the CPSW module as the CPSW console. After locating the directory where the microcode updates are stored, log on using the administrator password and perform one of the following operations:

- Upgrade CPSW microcode.
- Upgrade hardware picocode in the Field Programmable Gate Array (FPGA) of the CPSW and media modules.

Upgrading CPSW Microcode: To upgrade CPSW microcode, enter the following CPSW commands:

1. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode is stored)
2. SET TFTP FILE_NAME (to define the path name of the file on the server)
3. SET TFTP FILE_TYPE (to specify boot or operational microcode)
4. DOWNLOAD INBAND (to load the CPSW microcode).
5. SWAP MICROCODE (to reboot the CPSW module with the new code).

Upgrading FPGA Picocode in ATM Modules: To upgrade hardware picocode in the FPGA of CPSW and media modules, enter the following commands at the directory prompt:

1. SET TFTP SERVER_IP_ADDRESS (to define the server where the picocode is stored)
2. SET TFTP FILE_NAME (to define the file on the server)
3. SET TFTP FILE_TYPE (to specify FPGA)
4. SET TFTP TARGET_MODULE (to specify the slot number of the CPSW or media module)
5. DOWNLOAD INBAND (to load new hardware picocode)
6. SWAP FPGA_PICOCODE (to change the picocode in the CPSW or media module). If the swap is for a CPSW module, this causes an automatic reset of the ATM subsystem.

Uploading Dumps: To upload a dump to the host, enter the following CPSW commands at the directory prompt:

1. DUMP PNNI topology_data_base (to take a dump of the topology of the network)
2. SET TFTP SERVER_IP_ADDRESS (to define the server connected to the CPSW module)
3. SET TFTP FILE_NAME (to define the path name of the file on the host)
4. SET TFTP FILE_TYPE (to specify a dump)
5. UPLOAD INBAND (to upload the dump).

Uploading Traces: To upload a trace log to the host, enter the following CPSW commands at the directory prompt:

1. SET TRACE MAIN_TRACE ON (to enable recording)
2. SET TRACE `name` ON (to specify the trace to record) where `name` should be the name of the of trace (enter SET TRACE ? to display options) or ALL.
3. SET TRACE `name` OFF (to disable selected trace or all)
4. SET TRACE MAIN_TRACE OFF (to disable recording)
5. SET TFTP SERVER_IP_ADDRESS (to define the server connected to the CPSW module)
6. SET TFTP FILE_NAME (to define the path name of the file on the host)
7. SET TFTP FILE_TYPE MAIN_TRACE
8. UPLOAD INBAND (to upload the trace).

Uploading the Error Log: To upload the error log to the host, enter the following CPSW commands at the directory prompt:

1. SET TFTP SERVER_IP_ADDRESS (to define the server connected to the CPSW module)
2. SET TFTP FILE_NAME (to define the path name of the file on the host)
3. SET TFTP FILE_TYPE (to specify the error log)
4. UPLOAD INBAND (to upload the error log).

Manual Operations

To upgrade ATM microcode and picocode, IBM service personnel can perform manual upgrades (such as replacing the flash EEPROM) by following these steps:

1. Removing an ATM module and upgrading the microcode manually.
2. Replacing the flash EEPROM in the module and then re-inserting the module in the 8265.
3. Entering the RESET ATM_SUBSYSTEM command to reboot all ATM modules.

Out-of-band Operations

ATM network administrators can upgrade CPSW microcode (but not media modules) using an out-of-band operation with an RS-232 plug. To do this, you must attach a workstation with an emulated VT100 protocol to the CPSW module.

After locating the directory where the microcode updates are stored, use the workstation as the CPSW console. Log on using the administrator password and enter the following commands:

1. MAINTAIN (to activate Maintenance mode)
2. DOWNLOAD OUT_OF_BAND (to specify boot or operational code and to load it in the flash EEPROM of the CPSW module).

   Start the file transfer in the workstation using the Xmodem protocol. The transfer takes approximately 6 minutes for the boot code, 22 minutes for the operational code, at 9600 bps (the time is halved if the transfer is done at 19200 bps).

   If you enter DOWNLOAD OUT_OF_BAND BOOT, you automatically quit Maintenance mode and activate the new BOOT microcode.
3. BOOT (to restore normal operation), if you did not enter DOWNLOAD OUT_OF_BAND BOOT in Step 2.

Downloading Software to Controller Modules

Future enhancements to controller module functionality may make it necessary to download a new revision of the software. This section describes:

- Guidelines
- How to download boot and operational microcode
- The Download Status Display.

Guidelines

The following guidelines explain the differences when downloading code when one or two controller modules are installed.

Downloading When Two Controller Modules Installed:

In an 8265 containing with two controller modules installed, always perform the download in this order:

1. Perform a download to the standby controller module.
2. Perform a download to the active controller module.

When you download to the standby controller module first:

- The standby controller module remains in standby mode and causes no disruption to 8265 operation.
- The active controller module reboots, and then loses active controller module status to the standby controller module. The active controller module reboots and briefly disrupts 8265 operation.

  A download to the active controller module first would cause two disruptions to 8265 operation. Because it causes two disruptions (one more than necessary), this approach to download is feasible but not recommended.

When you download to the active controller module first:

- The active controller module reboots and loses active controller module status (the standby controller module becomes the "new" active controller module, and the "old" active controller module becomes the standby controller module).

  This is the first disruption to 8265 operation.
- A second disruption to 8265 operation occurs when you download to the 'new' active controller module that was previously the standby controller module (a second reboot and swap of active controller module status takes place).

Downloading When One Controller Module Installed:

In an 8265 containing only one installed controller module, the system recognizes the single installed controller module as the active controller module.

When you download software when there is just one controller module installed, keep in mind the following:

- Power management functionality is inactive while a download is in progress, and until the download completes.
- If a power failure occurs while download is in progress, the system may not be able to recover and the controller module to which you are downloading may fail.
  - Upon power recovery, replace the failed controller module and re-initiate the download to the replacement controller module.
  - Next (optionally), reinsert the original controller module (the one that failed during the first download) and re-initiate download to the original controller module while the active controller module is present and functioning.

  The original controller module powers up as the standby controller module.

Upgrading Controller Module Boot Microcode

To upgrade the controller module boot microcode, enter the following commands:

1. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode is stored)
2. SET TFTP FILE_NAME (to define the path name of the file on the server)
3. SET TFTP FILE_TYPE CONTROLLER_BOOT (to specify boot microcode)
4. DOWNLOAD INBAND (to load the microcode).

Upgrading Controller Module Operational Microcode

To upgrade the controller module operational microcode, enter the following commands:

1. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode is stored)
2. SET TFTP FILE_NAME (to define the path name of the file on the server)
3. SET TFTP FILE_TYPE CONTROLLER_OPERATION (to specify operational microcode)
4. DOWNLOAD INBAND (to load the microcode).

Download Status Display

As you perform a download to the controller module, the controller module front panel indicates download status.

- The TEMP LED lights and remains lit until the download completes. If a download attempt is unsuccessful, the STBY and ACTIVE LEDs on the controller module light and remain lit until you re-initiate the download.

Part 3. Appendixes

Appendix A. Troubleshooting

This appendix describes how to diagnose and solve problems associated with the operation of the 8265.

The following problems are detailed in this appendix:

Problem	Refer to:
Power Supply Problems	Page 128
Management Console Problems	Page 129
Control Point and Switch Module Problems	Page 131
Hardware Problems	Page 133
ATM Network Problems	Page 137
ATM Connection Problems	Page 139
LAN Emulation Problems	Page 141
Network Security Problems	Page 149
Administration Problems	Page 150

"Getting Further Assistance" on page 153 explains the information to collect should you require additional help in solving a problem.

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

Troubleshooting Prerequisites

This section describes the troubleshooting operations for problems if the CPSW Active LED fails to come on after you switch on the 8265 (if diagnostics are enabled the LED should come on after approximately 7 seconds, if diagnostics are disabled the LED should come on immediately.)

In order to determine the cause of a problem with CPSW and media modules after switching on the 8265:

- The correct microcode must be installed.
- CPSW LEDs must be functioning properly.
- CPSW and media modules must be plugged into the 8265.

To ensure that these conditions are satisfied, follow these steps:

1. From the Control Point and Switch module console, enter `show module 18.1 verbose` and verify that the level of the controller module code is at least 1.01. If it is not, the slots in which media modules are installed may not receive power.
2. Make sure that the CPSW and media modules are properly inserted in their slots and are plugged into the connectors on the backplane of the 8265.
3. Verify that all CPSW media module LEDs are operative by pressing the LED Test button on the controller module. If one or more LEDs on the module do not come on, replace the module.

Diagnosing Problems Concerning the Power Supply

If after switching on the 8265 you suspect that power is not reaching all modules, see if the problem is caused by one of the conditions described below. If you cannot solve the problem and the CPSW Active LED does not come on, contact an IBM service representative before configuring the ATM subsystem.

There is a power supply failure due to poor power prioritization (configured with the SET POWER command).

Steps to Take:

1. Refer to Chapter 9, “Managing the Power Subsystem” on page 103.

An ATM module is not in service.

Steps to Take:

1. Use the SHOW PORT command to verify that the module's status is `hardware KO` and `failure`.
2. Replace the module.

The power load capacity has been set to a higher value than the power supply capability.

Steps to Take:

1. Refer to Chapter 9, “Managing the Power Subsystem” on page 103.

Diagnosing Problems Concerning the CPSW Console

The following section describes the problems that may arise after attaching the local console to the CPSW module through the RS-232 Console port.

No prompt appears on your console screen when you press ENTER.

Steps to Take:

1. Check that the RS-232 cable meets the specifications described in *IBM 8265 Planning and Site Preparation Guide*, GA33-0460.
2. Check that the RS-232 cable is securely plugged into the CPSW module and the console in the correct ports.
3. The terminal parameters do not match the 8265 communications parameters. Use Telnet to modify the terminal parameters, using the SET TERMINAL command.
   - Try using the default settings on the terminal (the default parameters are: 9600 bauds, 8 data bits, 1 stop bit, no parity). If this does not work, try different settings until you find the right configuration.

Characters appear on the screen but they are not legible.

Steps to Take:

1. Make sure that the attached console is an ASCII terminal.
2. Check the terminal parameters, especially the baud-rate, parity, and data bits. The default parameters are: 9600 bauds, 8 data bits, 1 stop bit, no parity. If these values do not work, try different settings until you find the right configuration.
3. Replace the ASCII terminal.

You cannot enter commands reserved for the ATM network administrator, or the SET commands do not work.

Steps to Take:

1. Make sure that you are logged on as the administrator.

After you enter the first part of a command and press the space bar, the rest of the command is not automatically filled in.

Steps to Take:

1. Enter more letters in the command in order to distinguish it from other commands that are written similarly. Then press the space bar again.

Random characters are lost.

Steps to Take:

1. Set the flow control on the console to XON/XOFF.

Some characters are lost when you are connected to the CPSW module through a modem.

Steps to Take:

1. Make sure that the STOP_BITS parameter on the console is set to 1.

The passwords do not work or you forgot a password.

Steps to Take:

1. Enter `force` at the password prompt. Then press the ATM Reset button on the front panel of the CPSW module within 3 seconds. This will reboot the CPSW with the factory default password settings.

When you turn on the 8265, your last configuration settings are not loaded. A different configuration is activated.

Steps to Take:

1. Re-enter the configuration settings and save them using the SAVE command.

The >> prompt appears on the screen and you have not entered the MAINTAIN command.

Steps to Take:

1. The CPSW module is running in maintenance mode. To return to normal operation mode, enter the BOOT command. This resets the ATM subsystem.

The >>*abcd*>> prompt appears, where *a,b,c,d* are 4 hexadecimal digits.

Steps to Take:

1. The CPSW entered maintenance mode because of an error, which is indicated by the error-code prompt. Refer to "Maintenance Codes" on page 157 for the meaning of the code, and take the corrective steps required.

Control Point and Switch Module Problems

Standby Control Point and Switch Module Does Not Mirror Active Control Point and Switch Module

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

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

Steps to Take: There are two cases to consider:

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

   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 Control Point and Switch module.

2. The active CPSW module microcode is at a newer level than the standby Control Point and Switch module.

   Perform the following steps:

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

   b. On the standby Control Point and Switch module, 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 Control Point and Switch module to the standby Control Point and Switch module.
      - Remove the active Control Point and Switch module from the 8265.
      - Enter the right TFTP parameters on the remaining Control Point and Switch console, in order to download the new microcode.
      - Download the new microcode.
      - Swap the microcode.
      - Remove the Control Point and Switch module from the 8265 (non are installed now).
      - Reinsert the original CPSW module.
      - Reinstall the second CPSW module, which will copy all the configuration parameters of the active one.

Diagnosing Problems from the CPSW System Status LCD

The System Status LCD on the CPSW module can be used to troubleshoot a problem that occurs during initialization of the module.

Each time the CPSW module is initialized (at power on or after a reset), the following sequence should be displayed on the LCD:

1. `INIT` - the initialization process is started.
2. `SET1`, `RFW1`, `RBW1`, `BRST` - testing of the first bank of DRAM memory is in progess. These are only displayed if diagnostics are enabled.
3. `CLR1` - the first bank of DRAM is being cleared.
4. `SET2`, `RFW2`, `RBW2`, `BRST` - testing of the second bank of DRAM memory is in progess. These are only displayed if diagnostics are enabled.
5. `CLR2` - the second bank of DRAM is being cleared. This is only displayed if two banks of DRAM are installed.
6. `LOAD` - the operational code is being copied from the PCMCIA card into the DRAM.
7. `ACTV` or `STBY` - the CPSW module has become active (ACTV) or gone into standy (STBY) mode.

If the LCD does not show either ACTV or STBY after the initialization routine above, then an error has occured:

- If the error was critical and halted the intialization process, `--->` is displayed on the LCD. Press the Display Control button below the ---> to view an explanation of the error.
- If the error was not critical, the CPSW is placed into Maintenance mode. An error code and explanation of the error will be displayed on the LCD automatically.

Diagnosing Problems in the Hardware Configuration

If you suspect that a problem is due to an error in your hardware configuration (for example, when using a LAN Emulation server, 8282 host, 25 Mbps client, and so on), check the following:

- If the attached device is an 8282 host, enter the SHOW PORT command to see if the port's status is `UP`. If the status is not `UP`, follow the troubleshooting steps in the *IBM 8265 Media Module Reference Guide*, SA33-0459.
- If a trap or error message is displayed on the client when you start the 8265, enter the SHOW PORT command to make sure that the media port's status is `UP`. If the status is not `UP`, restart the client.

  If the port's status does not change to `UP`, run a trace by entering the SET TRACE and UPLOAD INBAND commands. Then contact your IBM service representative.
- Use the MIB browser or the Campus Manager - ATM Version 2 for AIX to make sure that the client addresses are configured in the 8265's ATM address table.

  If the media port's status does not change to `UP`, contact your IBM service representative.
- If the attached device is a LAN Emulation server (LES), make sure that it is installed and running properly, and that:
  - The status of the port that connects the LES to the 8265 is `UP`.
  - The LES is configured with the ATM network prefix used by the 8265.

8265 Cannot PING an ARP Client

Steps to Take: Check if the 8265 can ping the ARP server. If not, then see “8265 Cannot PING the ARP Servers and Vice-versa” on page 138. If it can ping the server:

1. The status of the port of the ARP client is not `UP`.

   Check that the port of that ARP client is enabled. If it is enabled, then the problem comes from the ARP client or from the cable attached to it.

2. The ARP client is not registered in the ARP server.

   Check that the ARP client has TCP/IP running, and that the address configured for its ARP server is correct.

3. If the 8265 and the ARP client are not in the same IP subnet, there may be a gateway definition problem.

   Check the Default Gateway addresses in both machines. In general, they correspond to one common gateway.

4. The SVC between the 8265 and the ARP client cannot be established.

   Check the ATM Call Logging panel in the Campus Manager - ATM to see the cause of the failure.

Two Devices Using IP Over a PVC Cannot Ping Each Other

Steps to Take:

1. If the PVC is not active, make sure that the PVC is 'in-service' (from the PVC List panel in Campus Manager - ATM) or 'active' (from the SHOW PVC command). If not, then try to re-enable that PVC.
2. The hardware connections may be failing, in which case replug the cables attached to the devices.
3. If the source and destination IP addresses are not in the same IP subnet, check both IP addresses. Change them so that they belong to the same IP subnet.

PVC failure, Cause Code 3, on NNI or ISSP ports

After having defined a PVC ending at NNI or IISP ports, the PVC is not active.

Steps to Take:

1. The PVC was defined using an '*' as a value for VPI. re-enable that PVC.
2. Redefine the PVC using an implicit value for the VPI.

Problems with the ATM Network

The problems in this phase occur after ATM traffic is started in the network between ATM devices attached to media module 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 media module is exceeded. The maximum number of virtual connections supported (in a burst) is as follows:

- **6144** per switch
- **4064** per media module (with up to 4064 VCs per 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
- 512 PVCs per switch
- 512 ESIs per switch.

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 50 for valid settings.

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

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 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`. 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.

8265 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 8265.

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 8265 (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 8265 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.

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 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 the *IBM 8265 Media Module Reference Guide*, SA33-0459.
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 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 the *IBM 8265 Media Module Reference Guide*, SA33-0459.
2. Use the SHOW REACHABLE_ADDRESS command to:
   - Make sure that the ATM address of each switch is configured with a reachable address of the other one.
3. Use the SHOW PORT command to make sure that the VPI of the media ports on each boundary switch 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 8265s located in different peer groups.

Explanation:

- This is normal. The 8265 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 A4-MF155 module, 100 Mbps for an A4-SC100 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 A4-MF155 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 8265 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 8265 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 8265 and 25 Mbps Adapters

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

The flow control on all 25 Mbps adapters attached to the 8265 must be disabled. This flow control (of OAM F4 cells) is not supported on the 8265, whereas it is supported on the ATM concentrator 8282.

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

Diagnosing LAN Emulation Problems

8265 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 8265.

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 8265 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.

8265 LEC Cannot PING another Client and Vice-versa

Steps to Take:

1. Check that the port of the LEC is enabled. If it is enabled, and its stauts is not `UP`, then the problem comes from the LEC or from the cable attached to it.
2. The LEC does not support the same LAN type as the 8265 LEC.

   Check that the LEC is emulating IEEE 802.3 or DIX Ethernet frames, or Token-Ring 802.5.
3. If the 8265 LEC and the other LEC are not in the same IP subnet, there may be a Gateway definition problem.

   Check the Default Gateway addresses in both machines. In general, they correspond to one common gateway.

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

Default parameters of DOS TCP/IP and 8265 Ethernet LEC do not match; a DOS TCP/IP station cannot ping an 8265.

The 8265 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 8265

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 8265 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.

LAN Emulation JOIN failed. ATM Forum LE status xx

When this message occurs, the LEC is stopped. To restart the LEC, enter the SET DEVICE LAN_EMULATION_CLIENT ETH command (for Ethernet) or SET DEVICE LAN_EMULATION_CLIENT TR command (for Token-Ring). The additional parameters will automatically retain their previous values. For more information, see the *IBM 8265 Command Reference Guide*.

Cause Cod: 1

Explanation: The LE version for the LEC is not compatible with the LES/BUS version.

Cause Code: 2

Explanation: The 8265 LEC parameters are incompatible with the LES/BUS. For example, the emulated LAN type of the 8265 LEC may be Ethernet IEEE 802.3 while that of the LES may be Ethernet DIX or Token-Ring.

Steps to Take:

1. Change the LES ATM address to reach a LES with the same LAN type.

Cause Code: 4

Explanation: The same MAC address is already registered to the LES.

Steps to Take:

1. Change the 8265 MAC address (with the SET DEVICE LAN_EMULATION_CLIENT command), or deregister the LEC with the same MAC address from the LES.

Problems in an IBM Proprietary LAN Emulation Environment

This section details the problems that may occur during the setup of the IBM LAN emulation environment. Such an environment may include concentrators (8282) and bridges (8281), the external IBM LAN Emulation Server (LES), workstations (WS), ATM Workgroup Switches (8285), Nways Ethernet LAN Switch (8271), Nways Token-Ring LAN Switch (8272), Nways Ethernet RouteSwitch (8273), Nways LAN RouteSwitch (8274), Nways Multiprotocol Switch Services Server (8210), and the 8265s.

A workstation/bridge cannot connect to another workstation/bridge.

Steps to Take:

1. Using the LES monitor, check in the list of registered end stations that both workstation/bridge addresses are present. If you do not know the ATM addresses of your workstation bridge, use the Campus Manager - ATM Interface Configuration panel for the ports attached to your workstation/bridge. If both addresses are registered in the LES, then proceed to step 2).

   If one workstation/bridge address is missing, then use the Call Status History provided by the LES monitor to get the Q2931 cause of the failing call. The missing station/bridge has probably a wrong LES ATM address defined in its configuration. Check the missing station's configuration.

2. Both workstation/bridges are registered to the LES, but one cannot call the other one, because the LES is not available any more (port disabled, or not-in-service). The LES does not tell you that it has lost its address, because it only tells that once the connection to the 8265 is returned.

   Check that the LES cable is well plugged, then check that the LES port is enabled. If it stays enabled and not-in-service, then the LES is faulty. Contact your IBM representative for investigation, or re-boot the LES.

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

Steps to Take:

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.

Note: You can check whether the station is registered in the 8265 by using the command SHOW REACHABLE_ADDRESS.

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

Clear Table: a lot of SVCs were cleared with Cause 31.

Explanation:

- A high-bandwidth (100 Mbps or 155 Mbps) workstation or bridge has tried to call a low-bandwidth workstation (25 Mbps). The call was rejected by the low-bandwidth workstation because the bandwidth specified in the Q2931 parameters (even for a UBR call) was too large. This is normal.
- The source or bridge retried to call the destination station with a lower bandwidth/bit-rate successfully. No action required.

Some ATM stations cannot talk to LAN stations behind PARALLEL bridges.

Explanation:

- The 8281 bridge has a limitation of 256 ATM connections. One would think that multiplying the number of 8281 bridges (in parallel) would multiply the number of available connections. Doing so will lead to the problem that only 256 stations can immediately establish connections with the bridges.
- In a configuration with parallel 8281 bridges (bridges registered to the same LAN Emulation Server, and connected to the same LAN), there may be collisions in terms of connections. Indeed, when an ATM station calls a LAN station behind the 8281 bridges, each 8281 bridge will respond by establishing a connection to the originating ATM station. In a network where the number of ATM stations exceeds 256, which is the maximum number of SVCs per 8281, some stations will not be able to connect until the bridges clear their SVCs that are unused (aging out process).

Steps to Take:

1. Wait up to 4 minutes (aging time on the 8281 bridge), or avoid parallel bridging.

LES Monitor: after 3 minutes, the workstation is de-registered from the LES (valid only for IBM proprietary LAN emulation).

Explanation: The workstation did not send the re-registration message within 3 minutes.

Steps to Take:

1. Ensure that the port for the workstation is connected properly.
2. Ensure that the cable between the 8265 and the workstation is connected properly.
3. Shutdown, then power off the workstation and restart.

If the problem persists, contact your workstation/adapter supplier.

In a multi Token-ring bridges configuration, a Token-ring bridge cannot register to the LES. (valid only for IBM proprietary LAN emulation).

Explanation: Different ring numbers are assigned to the ATM ports of two bridges connected to the same LES.

Steps to Take:

1. Check the ring numbers of the ATM ports of all the bridges attached to the same LES; these numbers should be equal. Change them if necessary.

LES Monitor: Bridge is on General Multicast Tree, but not on Bridge Multicast Tree. (valid only for IBM proprietary LAN emulation).

Explanation: The bridge did not send its route descriptors to the LES.

Steps to Take:

1. The bridge is faulty. Contact your IBM representative.

At workstation reboot: the ATM adapter initialization failed.

Explanation: The switch or concentrator port attached to the workstation is not enabled, or is not a UNI port.

Steps to Take:

1. From the console, or from the SNMP Manager (Campus Manager - ATM), enable the corresponding port as a UNI port.

A station cannot register to an LES located behind a WAN (VP-tunnel).

Explanation:

- Some of the connections through the VP tunnel work, but not all, especially the ADD_PARTY to put the stations on the LES Multicast Tree. The 8265 error-log is full of messages like 'Invalid Message Length'.
- The WAN (public network providing the VP-tunnel) uses the VCI=5 for its own purposes, and there is a conflict with the 8265 which also uses VCI=5 (ATM-Forum Signalling VCI).

Steps to Take:

1. Ask your public network provider if they use the VCI=5. If necessary, change the setting of the port.

No Traffic in a Client Environment.

Steps to Take:

1. Make sure that each LES client does not have more than 128 virtual
2. Make sure that the unit providing the LES function has enough vitrual channels. connections.

Problems between two LAN-emulated stations, or between a LAN-emulated station and a LAN station located behind a bridge (valid only for IBM proprietary LAN emulation).

Steps to Take:

1. For performance problems, first consider the frame sizes defined at the workstation level and at the bridge level.
2. For connection problems, first consider the
   - if you know neither the emulated MAC addresses of the stations nor the ATM addresses of these stations, use the Campus Manager - ATM Interface Configuration panel to get their ATM addresses.
   - Once you know either the ATM addresses or emulated MAC addresses of the stations, look at the Registered End-systems window of the LES monitor and check that your stations are registered.
   - Once you know which station is NOT registered, record its ATM address and look at the Call Status History window of the LES monitor. You should find a recorded call from that ATM address that failed for a certain 'cause X, reason Y'. The cause X shows you the Q2931 cause of the failure. Refer to “Q.2931 Error Codes for Clear Causes” on page 155.
   - If you not find any call from that ATM address, that station has not been able to reach the LES. Use the Campus Manager - ATM Statistics application to open the Clear Table of the 8265/8285 directly attached to the failing station. That table should have entries with a source ATM address being the one of the failing station. You will get a Q2931 cause of the failure. Refer to “Q.2931 Error Codes for Clear Causes” on page 155.

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 (by issuing the SHOW SECURITY ATM_ADDRESS command).

2. Ports are enabled.

   The problem is due to an empty address table. 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 table contents by issuing the SHOW SECURITY ATM_ADDRESS command.
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 loaded).

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

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 83 for information on how to remove addresses.

Administrative Problems (Netview/SNMP/Telnet)

This section details problems occurring during the administration of your 8265

PING: Your 8265 cannot ping your management station.

Steps to Take:

1. Since all the management services are running over IP, you have to ensure that your 8265 can ping the destination station where you will run either Telnet, the TFTP daemon (TFTP server), or the SNMP manager (Campus Manager - ATM). If the ping fails, see previous sections on ping failures in Classical IP or LAN emulation networks.

Telnet: You cannot Telnet to your 8265 from your management station.

Steps to Take:

1. If the ping does not work, see previous sections on ping failures.
2. Someone is already logged on the 8265 by another Telnet session. It is not possible to have more than one Telnet session per 8265

   To know from which station the other Telnet session is active, use the Campus Manager - ATM SVC Tracking tool to determine at least which SVCs are connected to the internal port of the 8265 (interface 1). You will then know the ATM addresses of the remote ends, as well as the 8265 ports to which they are connected to.

   Note: It is recommended to set the Terminal Timeout parameter to a non-zero value, to force Telnet sessions to close themselves after some inactivity.

TFTP: Upload fails from your 8265

Explanation: The upload can be done either from the terminal dialog (console or Telnet) or from the SNMP Manager (Campus Manager - ATM or MIB Browser).

Before performing any upload, make sure that the machine hosting the TFTP server can ping the 8265

When an upload fails, an error code is returned. That error code can be different between the terminal dialog and the Campus Manager - ATM/MIB browser, which is why both return codes are documented.

Note: When the upload fails from the terminal dialog (console or Telnet), check the return code by using the SHOW TFTP command.

Steps to Take:

1. Messages: **Error/generic error..Host Access Violation...Access Rights Violation/access-rights-violation...File already exists/file-already exits.**.
   - The file that you want to upload already exists on the target machine, and is read-only.

     Change the attributes of the file on the target machine or change the name of the file to be uploaded.
   - You are trying to upload to a directory that is not uploadable by TFTP.

     If your target host runs AIX or Unix, use the directory /tmp, or configure the file /etc/tftpaccess.ctl with lines beginning with 'allow:' (check the documentation of the daemon/server TFTPD. If you use another operating system (OS/2 or others), configure the TFTP daemon on that system to accept uploads in the desired directory.
   - You are trying to upload a file that can only be downloaded (operational code, boot code, or FPGA picocode).

     Check the file type of the file to be uploaded.
2. Messages: **Cannot connect to Host/no-response-from-host**.
   - Check that you can ping the host from the 8265 If the ping fails, see the previous sections on ping failures.

3. Message: **Connection lost/connection-lost**.
   - The SVC connection between the 8265 and the host has been cleared during the file transfer. Retry the upload. Look at all the Clear Tables of all intermediate 8265s that are on the path between your 8265 and the host. To do that, use the Campus Manager - ATM Statistics application.
4. Message: **File not found/file-not-found**.
   - You tried to upload without specifying the name of the file to be uploaded. Specify the name of the file.
5. Message: **File too big/file-too-big**.
   - There is no space left on the server. Check that space is made available before retrying the upload.

TFTP: Download Inband fails from your 8265

Explanation: The download inband can be done either from the terminal console (console or Telnet) or from the SNMP Manager (Campus Manager - ATM or MIB Browser).

Before performing any download, make sure that the machine hosting the TFTP server can ping the 8265

When an download fails, an error code is returned. That error code can be different between the terminal dialog and the Campus Manager - ATM/MIB browser, which is why both return codes are documented.

Note: When the download fails from the terminal dialog (console or Telnet), check the return code by using the SHOW TFTP command.

1. Messages: **Error/generic error..Host Access Violation...Access Rights Violation/access-rights-violation...File already exists/file-already exits.**.
   - The file that you want to download does not have read permission for TFTP.

     Change the attributes of the file on the host.
   - You are trying to download to a directory that is not downloadable by TFTP.

     If your source host runs AIX or Unix, use the directory /tmp, or configure the file /etc/tftpaccess.ctl with lines beginning with 'allow:' (check the documentation of the daemon/server TFTPD. If you use another operating system (OS/2 or others), configure the TFTP daemon on that system to accept downloads in the desired directory.
   - You are trying to download a file that can only be uploaded (traces, error-log, dumps).

     Check the file type of the file to be downloaded.
2. Message: **Cannot connect to Host/no-response-from-host**.
   - Check that you can ping the host from the 8265 If the ping fails, see the previous sections on ping failures.
3. Message: **Connection lost/connection-lost**.
   - The SVC connection between the 8265 and the host has been cleared during the file transfer. Retry the download. Look at all the Clear Tables of all intermediate 8265s that are on the path between your 8265 and the host. To do that, use the Campus Manager - ATM Statistics application.
4. Message: **File not found/file-not-found**.
   - You tried to download without specifying the name of the file to be downloaded. Specify the name of the file.
   - You tried to download a file that does not exist on the host. Check that you have not misspelled the name (blank spaces are treated as normal characters).
5. Message: **File too big/file-too-big**.
   - You tried to download an operational code to the boot sector of the 8265. Check the filetype for the download, and check the file name of the file to be downloaded.

6. Messages: **Bad file header/Cannot interpret file/invalid-file-header**.
   - You tried to download a file that is not downloadable. If the source file name is correct, and it was obtained by FTP, it might have been transferred in ASCII mode instead of binary. Check the size of your downloadable file, and compare it with the theoretical size provided by your IBM Service. If the size is correct, contact your IBM representative.
7. Message: **Checksum Error/Packet error/checksum-error**.
   - there has been a problem during the transfer.

     Download the file again.
   - A byte is corrupted in the source file.

     either get a new source (re-install the source file from your installation package), or, if it fails again, contact your IBM Service or IBM representative.
8. Message: **Flash memory failure/hardware-error**.
   - Try to download several times. If it always fails, contact your IBM representative.
9. Message: **Target Blade Mismatch**.
   - You tried to download FPGA picocode that is incompatible with the target module number. Check the type of module (A4-SC100, A4-MF155 etc.) and the TFTP FILE_NAME parameter.

8265 cannot restart after a download inband operation is performed and TFTP-supported services are operational.

Steps to Take:

1. Use the DOWNLOAD OUT_OF_BAND command to load the microcode that was previously active. Then restart the 8265.
2. If the 8265 still does not start, replace the CPSW module in the 8265.
3. Contact your IBM service representative.

8265 Terminal/Telnet very slow or Ping to 8265 very slow.

Explanation: The 8265 is congested by Signalling Calls.

Steps to Take:

1. If you cannot be in front of the 8265, perform a remote login using Telnet. First make sure that the trace is not active, then disable the ports one at a time until the Telnet session gives a normal response time. The last port that you disabled should be the one through which the congesting calls were coming.
2. If you can be in front on the 8265, log on to the console, make sure that the trace is not active, then if the ATM switch is an 8265, look at the traffic LEDs and disable the for which the traffic LED is constantly lit. If your ATM switch is an 8285, disable the high-bandwidth port.

When there is congestion, it is often due to the failure of a major ATM component (ARP server, LAN emulation server, switch down, public network down, file server down). You have to determine which of these ATM components failed.

Getting 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 8265.
- Output of the following commands:
  - SHOW DEVICE
  - SHOW HUB
  - 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 8265.
- On/Off condition and color of the all LEDs.
- Any message displayed on the CPSW module System Status LCD.
- 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 8265.
2. For information on how to record trace information, see “TRACE Information” on page 154.
3. For more information on the UPLOAD command, see the *IBM 8265 Command Reference Guide*.

TRACE Information

In order to record trace information, follow these steps:

1. Use a TFTP file server reachable from the 8265.
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: System performance may be degraded while the trace is active.

For more information on the SET TRACE command and types of trace available, see the *IBM 8265 Command Reference Guide*.

Appendix B. Error and Information Codes

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

Q.2931 Error Codes for Clear Causes

Table 5 lists the error codes from the Q.2931 protocol for clear causes generated by 8265s and other ATM devices in an 8265-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.

The Q.2931 error codes are displayed at the CPSW console only (not on the CPSW module System Status LCD).

Table 5 (Page 1 of 2). Q.2931 Error Codes for Clear Causes in 8265-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.

Table 5 (Page 2 of 2). Q.2931 Error Codes for Clear Causes in 8265-based ATM Networks

Error Code ;(decimal)	Error Code ;(hex)	Meaning of Clear Cause
58	0x3A	Bearer capability is not available.
63*	0x3F*	Service or option is not available, unspecified.
65	0x41	Bearer capability is not implemented.
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 8265 are shown with an asterisk (*).

Maintenance Codes

The following table explains the codes during Maintenance mode. The codes are displayed at both the CPSW console and on the CPSW module System Status LCD.

For a more precise explanation of the error, check the System Status LCD on the CPSW module.

Table 6. 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>>	After 3 retries, the switch FPGAs did not initialize properly.
>>0024>>	The PCMCIA is either missing, incorrectly installed, or incompatible with the installation.
>>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.
>>0038>>	The MAC address is invalid.
>>0039>> >>003A>>	Initialization stopped because the code does not know which configuration to load.
>>0040>>	Active to backup CPSW polling does not work, SPI serial link may fail.
>>00BA>>	Maintenance mode is running with the backup daemon.

Appendix C. ATM Address Formats

The 8265 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 12, 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).

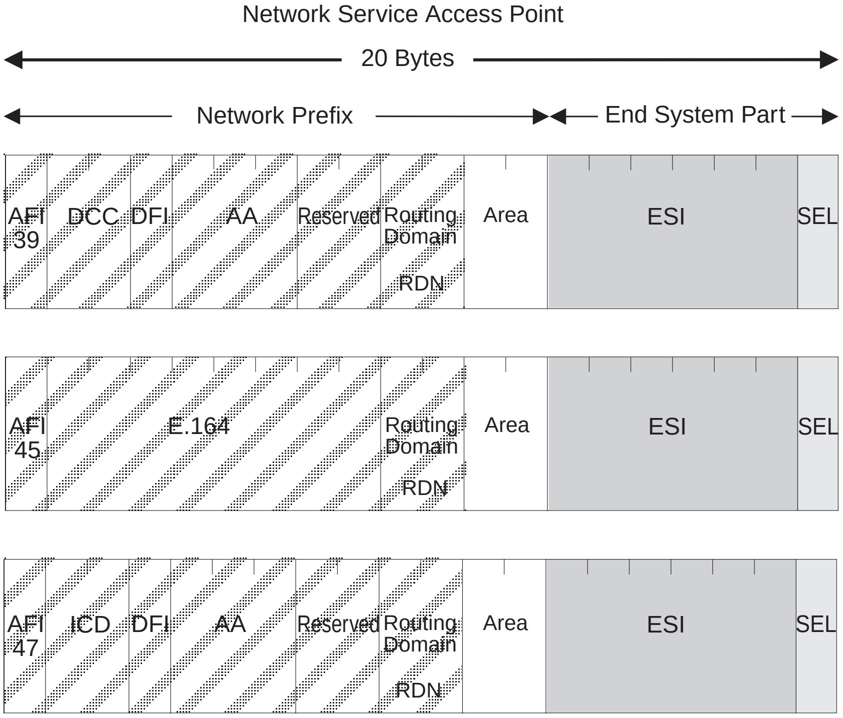


Figure 12. NSAP Address Formats Supported in the 8265 ATM Subsystem

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 8265 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 8265 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 8265 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.

LCD. Liquid Crystal Display.

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 IBM 8265 ATM Switch, please refer to the following documents:

IBM 8265 Nways ATM Switch Product Description, GA33-0449.

IBM 8265 Nways ATM Switch Command Reference Guide, SA33-0458.

IBM 8265 Nways ATM Switch Installation Guide, SA33-0441.

IBM 8265 Nways ATM Switch Planning and Site Preparation Guide, GA33-0460.

IBM 8265 Nways ATM Switch Media Module Reference Guide, SA33-0381.

Multiprotocol Switched Services (MSS) Server Introduction and Planning Guide, GC30-3820.

Nways Multiprotocol Switched Services Server Interface Configuration and Software User's Guide, SC30-3818.

Nways Multiprotocol Switched Services (MSS) Configuring Protocols and Features, SC30-3819.

Multiprotocol Switched Services (MSS) Server Service Manual, GY27-0354.

Multiprotocol Switched Services (MSS) Server Setup and Problem Determination Guide, GA27-4140.

Nways Multiprotocol Switched Services (MSS) Server Module Setup and Problem Determination Guide, GA27-4141.

Nways MAS/MRS/MSS Library, Configuration Program User's Guide for Nways Multiprotocol Access, Routing and Switched Services, GC30-3830.

Nways Event Logging System Messages Guide, SC30-3682.

8271 LAN Switch Module Planning and Installation Guide, GA27-4162.

8272 LAN Switch Module Planning and Installation Guide, GA27-4163.

4-Port 10BASE-T & 3-Port 10BASE-FL UFCs Planning and Installation Guide, GA27-4120.

100BASE-TX and 100BASE-FX Universal Feature Cards Planning and Installation Guide, GA27-4096.

ATM 155 Mbps Multimode Fiber Universal Feature Card Planning and Installation Guide, GA27-4156.

2-Port Fiber and 4-Port UTP/STP Token-Ring Enhanced Universal Feature Card Planning and Installation Guide, GA27-4168.

IBM Video Distribution Module User's Guide, GA27-4173.

The 8260 Nways ATM Kit Development Program, We Carry Your Creativity to ATM, GA33-0371.

The ATM Forum:

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

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

8265 Nways ATM Switch
User's Guide

Publication No. SA33-0456-01

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
SA33-0456-01

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

Cut or Fold
Along Line

SA33-0456-01