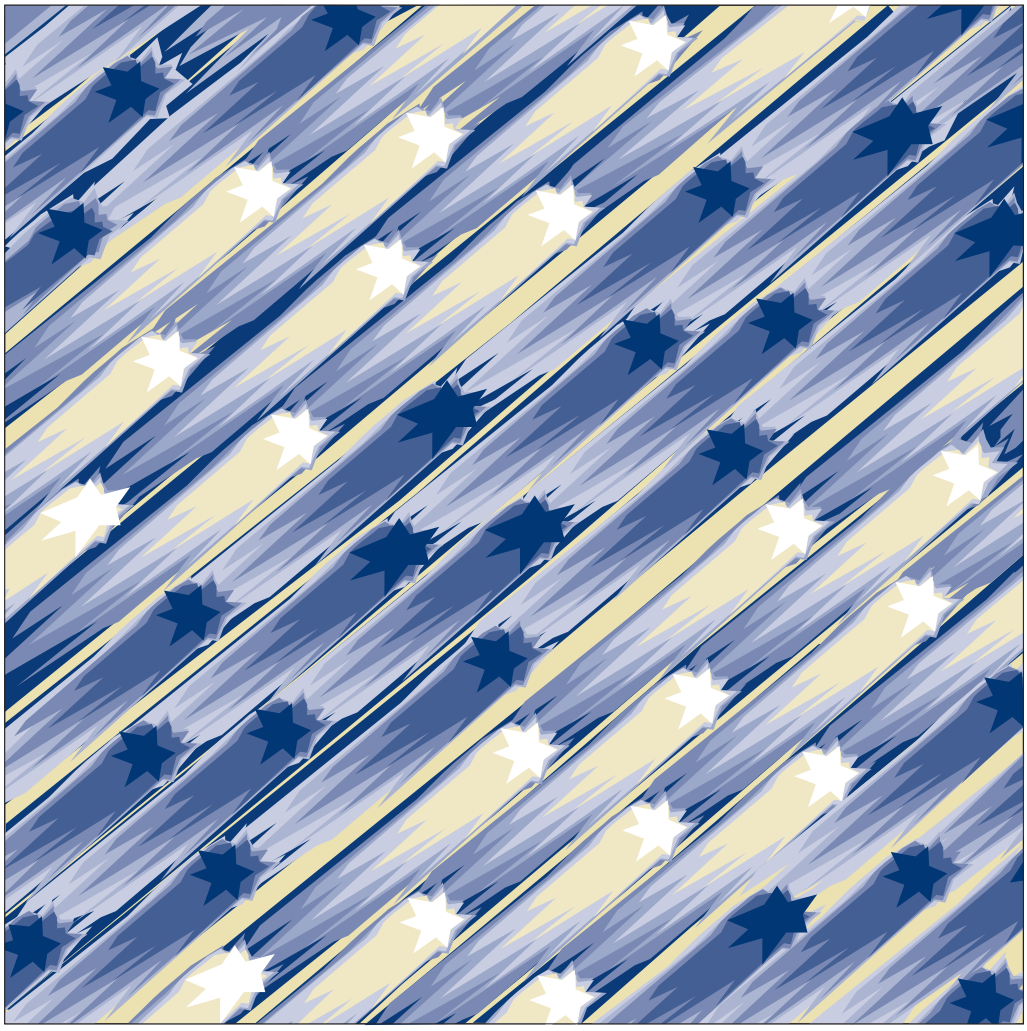
8265 Nways ATM Switch

User's Guide



SA33-0456-02

8265 Nways ATM Switch

User's Guide

SA33-0456-02

Note!

Before using this information and the product it supports, be sure to read the general information under Appendix F, “Notices” on page 179.

Third Edition (September 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

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 book, you should be familiar with:

- 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 191.

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. Overview

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**.

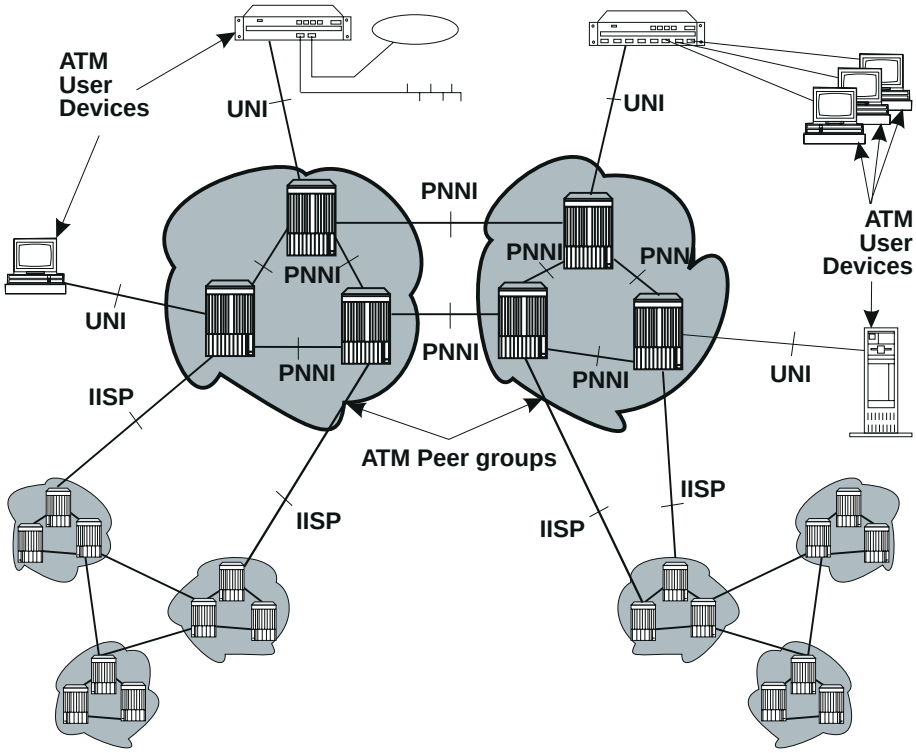


Figure 1. Components of an ATM Campus Network

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 as defined by the ATM Forum UNI Specifications V3.0, V3.1 and V4.0, as well as UNI for Public carriers.

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.

VOID
: Defines an interface between an ATM switch and a Wide Area Network (WAN) that is used to carry a Virtual Path Connection (VPC). ILMI is not supported on VOID ports, however when a VP tunnel is defined, signalling is supported through the VP.

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

Switched Virtual Connections (SVCs)

The IBM 8265 supports Switched Virtual Connections (SVCs), both Virtual Paths (VPs) and Virtual Channels (VCs). SVCs can use either Reserved Bandwidth (CBR and VBR) or Best Effort (ABR and UBR) routing.

Permanent Virtual Connections (PVCs)

The IBM 8265 supports Permanent Virtual Connections (PVCs), both Virtual Paths (VPs) and Virtual Channels (VCs). Point-to-Point PVCs can be configured for Reserved Bandwidth (CBR and VBR) or Best Effort (ABR and UBR) routing. Point-to-Multipoint PVCs can be configured for Reserved Bandwidth (CBR and VBR) or Best Effort (UBR only) routing.

Virtual Path Connections (VPCs)

The IBM 8265 supports Virtual Path Connections (VPCs) as a means of extending ATM connectivity across standard WAN connections. Each VPC can be of UNI, IISP, or PNNI type. The physical connection to the WAN is made across a VOID or Public UNI interface.

PNNI

The IBM 8265 supports a multi-level PNNI hierarchy using a best-match algorithm for Summary Addresses. Peer Group Identifiers may be derived from the NSAP prefix or may be defined explicitly. IBM's PNNI routing supports:

- CBR, rtVBR, and nrtVBR Reserved Bandwidth routing with shortest-path path selection
- ABR Best Effort routing with precomputed or on-demand path selection
- UBR Best Effort routing with widest-path or shortest-path path selection.

Keeping Control Point Code Up-to-Date

New versions of code for upgrading 8265 CPSW and media 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 Microcode Upgrades' home page. From here, you can select the code for the appropriate 8265 module.

Automatic Notification of Updates

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

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

Chapter 2. Configuring the IBM 8265

Before You Start

This chapter describes procedures for configuring your IBM 8265. Before beginning these procedures, be sure you have:

1. Installed the ATM Workgroup Switch and attached a local configuration console, as described in the *IBM 8265 Installation Guide*
2. Installed your ATM media modules, as described in the *IBM 8265 Media Module Reference Guide*.

For information on:

- Using special console keyboard functions
- Viewing command-line help
- Entering ATM commands

see the *IBM 8265 Command Reference Guide*.

Configuration Procedures

Procedures in this chapter correspond to the three main parts of this manual. To configure the 8265, follow the procedures described in each of the following sections:

- “Preparing the Switch for Operation” on page 8
- “Configuring Network Connections” on page 9
- “Managing the Switch Hardware” on page 10.

Screen Samples

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.

Preparing the Switch for Operation

To configure the ATM Workgroup Switch in preparation for connecting it to a network:

__ 1. *Logon* to the 8265 as Administrator, as described in "Logging On to the 8265 ATM Switch."

__ 2. Configure the *basic switch settings* as described in Chapter 3, "Configuring Basic Parameters" on page 13.

Note: It is recommended to perform the initial configuration of the basic switch settings using a local configuration console, before connecting the 8265 to the network.

__ 3. If you will be accessing the 8265 Control Point using Classical IP Over ATM, configure the *IP settings* as described in Chapter 4, "Configuring TCP/IP Settings" on page 27.

Note: Configuring the 8265 over a TELNET connection can only occur after the IP settings have been configured.

__ 4. If you will be accessing the 8265 Control Point using LAN Emulation Over ATM, configure the *LANE settings* as described in Chapter 5, "Configuring LAN Emulation Settings" on page 29.

__ 5. If you will be using an SNMP application to manage the 8265 Control Point, configure the *SNMP* settings as described in Chapter 6, "Configuring SNMP and Web Server Parameters" on page 35.

Logging On to the 8265 ATM Switch

When the configuration console is properly connected to the 8265, the screen below is displayed:

```
ATM Control Point Switch Telnet server at address 9.999.99.999
Press Enter
```

To log on to the switch:

1. Press Enter. The following prompt is displayed:

```
8265 ATM Control Point and Switch Module
(C) Copyright IBM Corp. 1997, 1998. All rights reserved.

Password:
```

2. Enter the Administrator password and press Enter. (The factory default Administrator password is **8265**.)

Note: 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.

3. The console prompt appears, ready for receiving ATM commands:

```
8265ATM>
```

Configuring Network Connections

To configure ATM network connections from the ATM Control Point:

__ 1. Configure the *links* that connect the 8265 to other ATM devices, as described in Chapter 7, “Working with Ports and Media Modules” on page 37.

__ 2. To connect to switches across a WAN, configure *VPCs* (Virtual Path Connections), as described in Chapter 9, “Linking Networks Through a WAN (VPCs)” on page 53.

__ 3. To create PNNI peer groups, see the guidelines for configuring *PNNI settings* (**PNNI Card only**) as described in Chapter 11, “PNNI Networks” on page 61.

__ 4. To define *PVCs* and to manage *SVC* capacity, see the guidelines in Chapter 12, “Managing Virtual Connections (PVCs and SVCs)” on page 63.

__ 5. To manage and optimize *ATM traffic* on the 8265, see the guidelines in Chapter 13, “Managing ATM Traffic” on page 67.

__ 6. To control *access security* on the network, see the guidelines in Chapter 14, “Managing Network Access Security” on page 77.

Managing the Switch Hardware

To configure the ATM Workgroup Switch:

__ 1. For general guidelines on commands used to display switch or module information, and to reset modules or the switch, see Chapter 15, “Management Tools” on page 93.

__ 2. To configure *power budgets* for modules, *fault-tolerant* operation, and *power-down* strategy, see the guidelines in Chapter 17, “Managing the Power Subsystem” on page 103

__ 3. To configure the *Intelligent Cooling Subsystem*, see the guidelines in Chapter 18, “Managing the Intelligent Cooling Subsystem” on page 113.

__ 4. To *upload* switch or security settings, dumps, traces, or error logs, see the procedures in “Uploads to a Server” on page 120.

__ 5. To *download* switch or security settings, see the procedures in “Downloads from a Server” on page 122.

__ 6. To *update microcode* or FPGA picocode on the CPSW module, any ATM media module, or a power controller module, see the guidelines in “Code Upgrades” on page 123.

Part 2. Preparing the 8265 ATM Switch

Chapter 3. Configuring Basic Parameters

This chapter describes how to configure the ATM switch address and basic Control Point/Switch (CPSW) module parameters.

Basic Configuration Steps

To configure the CPSW, follow the steps listed below.

__ 1. Define the *ATM address* of the IBM 8265, as described in “Configuring the ATM Switch Address” on page 14.

__ 2. Set the CPSW user and administrator *passwords*, as described in “Setting CPSW Passwords” on page 15.

__ 3. Set the node *clock*, as described in “Setting the Node Clock” on page 17.

__ 4. Define the switch *name*, as described in “Switch Name” on page 18.

__ 5. Record the service *contact* and *location* information, as described in “Service Contact Information” on page 19.

__ 6. Specify the console *prompt*, as described in “Console Prompt” on page 20.

__ 7. Set the console *timeout* value, as described in “Console Timeout” on page 21.

__ 8. Enable the sending of *alert* messages to an SNMP workstation or the local console, as described in “Alert Settings” on page 22.

__ 9. Select the *memory configuration* you want to apply to the 8265 Control Point (according to the type and volume of traffic the switch will be handling), as described in “Memory Configuration” on page 24.

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

Configuring the ATM Switch Address

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.

The ATM address of the IBM 8265 is configured using the command SET PNNI NODE:0 ATM_ADDRESS.

Notes:

1. The PNNI commands necessary for working with the ATM address are available on both the PNNI and the IISP code versions.
2. The following procedure describes how to set the address for the 8265 switch itself. For information on setting up PNNI peer groups, see Chapter 11, “PNNI Networks” on page 61.

To configure the ATM address:

__ 1. Set the address using the command SET PNNI NODE:0 ATM_ADDRESS, followed by the 20-byte ATM address.

__ 2. Activate the new address using the command COMMIT PNNI. **This resets the ATM system.**

To display the current ATM address, use the commands SHOW PNNI NODE:0, or SHOW FUTURE_PNNI NODE:0. See Chapter 11, “PNNI Networks” on page 61 for further information on these and related PNNI commands.

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: 39.99.99.99.99.99.99.00.00.99.99.01.01.99.
99.99.99.99.99.01
```

Using an ATM Host Name

To use define a *host name* that can be used in place of the 8265's ATM address, see “Using Host Names in Place of Addresses” on page 25.

Setting CPSW Passwords

You can restrict access to switch configuration commands by defining two CPSW passwords:

- The *Administrator* password, which provides access to *all* CPSW commands with read-write (configuration) access. The factory default is **8265**.
- The *User* password, which provides access to a *subset* of CPSW commands including most SHOW commands, PING and TELNET. The factory default is a **null string**. If you assign the same password for both Administrator and User, the User will have full access to all ATM commands.

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

Administrator Password

To define the Administrator Password:

__ 1. Enter the command SET DEVICE PASSWORD ADMINISTRATOR and 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.

```
8265ATM> set device password administrator

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

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

```
Password changed.
```

__ 3. To save the new password settings, use the command SAVE DEVICE or SAVE ALL.

The new administrator password will take effect the next time you log on to the CPSW.

User Password

__ 1. Log on to the CPSW using the Administrator password.

__ 2. Enter the command SET DEVICE PASSWORD USER and 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:

```
8265ATM> set device password user

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

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

```
Password changed.
```

__ 4. To save the new password settings, use the command SAVE DEVICE or SAVE ALL.

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 use the SET CLOCK command followed by the time and date parameters.

For example, the following command sets the node clock to 4:44 p.m. on September 20, 1998:

```
8265ATM> set clock 16:44 1998/09/20
```

The CPSW node clock uses its own battery and functions even when the CPSW is not operating.

Switch Name

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, use the command SET DEVICE NAME followed by the name you choose:

```
8265ATM> set device name helsinki
```

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:

__ 1. SET DEVICE LOCATION to specify where the 8265 is installed

__ 2. SET DEVICE CONTACT to specify the name of the service personnel to contact.

```
8265ATM> set device location
Enter text:
Building M4, ground floor, patch panel 1, hub number 4
8265ATM> set device contact
Enter text:
Network Manager, IBM Engineering Support, tel: 692-4444
8265ATM>
```

Console Prompt

It is recommended that you customize the prompt for each CPSW. This will help you recognize the CPSW to which you are connected when you are logged on from a remote console.

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.

To customize the CPSW prompt, use the command SET TERMINAL PROMPT:

```
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 configuration 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
```

Alert Settings

You can configure the CPSW to issue alert messages when certain system events are detected. These alerts can be trapped to an SNMP workstation, displayed on the configuration console, or both. There are three types of alerts:

- Hello
- Authentication
- Change.

Alerts are configured via the SET ALERT command. You can specify whether or not each type of alert is to be trapped and sent to the trap receiver (using the TRAP parameter), and/or displayed at the local configuration console (using the DISPLAY parameter).

By default, all alerts are set to NOTRAP and NODISPLAY. To display the current alert settings, use the SHOW ALERT command.

Hello Alerts

A *Hello* alert is sent when:

- The ATM subsytem is reset in one of the following ways:
  - 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)
  - The ATM address of the ARP server (using the SET DEVICE ARP_SERVER command)
  - The IP address of the default gateway (using the SET DEVICE DEFAULT_GATEWAY command)
  - The memory configuration (using the SET DEVICE CONFIG_FUNCTIONS command).

A Hello alert is sent once a minute until an SNMP request is received. After 4 hours and 15 minutes, if no request is received, 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.

The following example directs Hello alerst to the trap receiver and the local configuration console:

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

Authentication Alerts

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.

The following example sends Authentication alerts to the local configuration console only:

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

Change Alerts

A *Change* alert is sent when any of the following changes 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.

The following example sends Change alerts to the trap receiver only:

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

Memory Configuration

Depending on the type of CPSW module, the amount of memory installed, and the type and volume of traffic the switch will be handling, select from among the predefined memory configurations available.

__ 1. Check to see which memory configurations are available using the SET DEVICE CONFIG_FUNCTIONS command:

```
8265ATM> set device config_functions help
Here are possible values :
 number  !    Name   ! Comments
-------------------------------------------------------------------------------
Config 1 ! 32_P_P    ! P2P
Config 2 ! 32_P_M    ! Mixed

Current Memory Profile is 32_P_M.
8265ATM>
```

__ 2. To see the details for a selected memory type enter help after selecting one of the available configurations:

```
8265ATM> set device config_functions config_1 help
Configuration 1 is: 32_P_P
   P2P
  Number of VPCs                : 512
  Number of trees               : 10
  Number of branches            : 32000
  Number of parties             : 100
  Number of PVCs                : 512
  Number of reachable addresses : 64
  Number of dynamic addresses   : 512
  Number of E164 addresses      : 60
  LES                           : Disabled
8265ATM>
```

__ 3. Select the memory configuration you want.

```
8265ATM> set device config_functions config_1
Configuration 1 is: 32_P_P
   P2P
  Number of VPCs                : 512
  Number of trees               : 10
  Number of branches            : 32000
  Number of parties             : 100
  Number of PVCs                : 512
  Number of reachable addresses : 64
  Number of dynamic addresses   : 512
  Number of E164 addresses      : 60
  LES                           : Disabled
Accepting this configuration will reset the ATM subsystem.
Are you sure ? (Y/N)
```

Note: Activating a LAN Emulation Server (LES) affects the memory configuration currently in use.

Using Host Names in Place of Addresses

You can define a host name to be used in place of any ATM or IP address using the SET HOST command. This allows you to assign a meaningful, easy to remember name to devices on the network.

Note: Host names are not case-sensitive – for example, *LabC* and *labc* refer to the same switch.

For example, an 8265 located in Laboratory C with an ATM address of 39.99.99.99.99.99.99.00.00.99.99.01.01.99.99.99.99.55.86.01 could be called LabC. This can be set using the SET HOST command as shown in the following example:

```
8265ATM>set host LabC atm 39.99.99.99.99.99.99.00.00.99.99.01.01.99.99.99.99.55.
86.01
```

An 8265 located in the Development Department with an IP address of 9.100.109.203 could be called DevelA. This can be set using the SET HOST command as shown in the following example:

```
8265ATM>set host DevelA ip 9.100.109.203
```

To display currently defined ATM and IP host names, use the SHOW HOST command.

Chapter 4. Configuring TCP/IP Settings

This chapter describes how to define the necessary TCP/IP settings to access the 8265 through a Classical IP subnetwork.

TCP/IP Configuration Steps

To configure the TCP/IP settings, follow the steps listed below

__ 1. Define the *IP address* and *subnetwork mask*, as described in “IP Address and Subnetwork Mask” on page 28.

__ 2. Specify the IP address of the *default gateway*, as described in “Default Gateway” on page 28.

__ 3. Specify the ATM address of the *ARP server*, as described in “ARP Server” on page 28.

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

IP Address and Subnetwork Mask

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

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
```

You can also assign a separate IP address to the CPSW when accessed via the Ethernet port on the front panel of the CPSW by using the SET DEVICE IP_ADDRESS ETH command.

Using an IP Host Name

To use define a *host name* that can be used in place of the 8265's ATM address, see “Using Host Names in Place of Addresses” on page 25.

Default Gateway

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.

To specify the IP address of the default gateway, use the SET DEVICE DEFAULT_GATEWAY command:

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

ARP Server

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.

To specify the ATM address of the ARP server, use the SET DEVICE ARP_SERVER command:

```
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
```

Chapter 5. Configuring LAN Emulation Settings

This chapter describes how to define the necessary LAN emulation (LANE) settings to access the 8265 through a LANE subnetwork.

Note: Activating a LAN Emulation Server (LES) affects the memory configuration currently in use (See “Memory Configuration” on page 24.).

LANE Configuration Steps

To configure LANE settings, follow the steps listed below.

__ 1. Configure the *Lan Emulation Client (LEC)*, as described in “LEC Settings” on page 30.

__ 2. Specify the access method for connecting to the *LAN Emulation Configuration Server (LECS)*, as described in “LECS ATM Address” on page 31.

__ 3. To start a *Lan Emulation Server (LES/BUS)*, follow the instructions in “Setting Up LAN Emulation Servers (LES/BUS)” on page 33.

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

LEC Settings

In order for SNMP to run properly, every device in the network must have a unique IP address. 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 command with the following parameters:

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

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 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.
3. If two LECs are configured, they must have different IP addresses, even if they are connected to different LESs.
4. The MAC address must be in a 802.3 format. Local and universal administrated MAC addresses are supported.
5. 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.
6. The maximum frame size and emulated LAN name are provided by the associated LES.
7. The SET DEVICE LAN_EMULATION_CLIENT command automatically starts the LEC.
8. No command to stop the LEC is available.
9. 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.

Example

For example, to configure an Ethernet LEC:

```
8265ATM> set device lan_emulation_client eth eth_type DIX ip_address 9.100.20.55
ip_address:9.100.102.98 mac_address:185093928473 subnet_mask:00.44.82.56 no_lecs
_with_les:les024a
Client starting.
8265ATM>
```

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

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.A0.3E.00.00.01.00
and
C5.00.79.00.00.00.00.00.00.00.00.00.00.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 this_hub_port:2.3 5 channel_point_to_point 0.17 0.33 best
_effort

PVC set and started.
8265ATM>
```

Checking the LEC Configuration

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

```
8265ATM> show lan_emul configuration_server
Index            ATM address
--------------------------------------------------------------------------------
  1            39.99.99.99.99.99.99.00.00.00.00.01.94.00.82.65.82.65.00.00
  2            39.99.99.99.99.99.99.00.00.00.00.01.94.00.82.65.82.62.02.02
8265ATM>
```

Setting Up LAN Emulation Servers (LES/BUS)

You can define either one or two separate LAN Emulation Servers (LESs). Either one, or both, may be Token Ring or Ethernet. If you start two LESs, the maximum number of LECs (128) applies to both LESs *combined*.

When you start a LES, its associated BUS is automatically started.

Starting a LES

To start a LES, use the SET LAN_EMUL SERVER command.

For example, to start an Ethernet LES:

__ 1. Define the LES parameters using SET LAN_EMUL SERVER and press Enter. You are prompted for the name of the LES:

```
8265ATM> set lan_emul server 1 start eth 4 2 4544
Emulated LAN Name:
```

__ 2. Type the name you want to assign to the LES and press Enter:

```
8265ATM> set lan_emul server 1 start eth 4 2 4544
Emulated LAN Name: LAN1eth

Starting server.
8265ATM>
```

Displaying LES Parameters

Use the SHOW LAN_EMUL SERVERS command to display the current status and parameters defined for both LESs:

```
8265ATM> show lan_emul servers
-------------------------------------------------------------------------------
--------------------------- LAN Emulation Server 1 ----------------------------
Status                : Running.
LAN type              : Ethernet.
Actual ELAN name      : "IBM_ETHERNET_LAN1".
Desired ELAN name     : "".
Actual max frame size : 1516.
Desired max frame size: 1516.
ATM address : 39.99.99.99.99.99.99.00.00.99.99.01.50.50.50.50.50.50.50.02
LEC Id Range          : 1 to 3.
Current number of operational clients   : 10.
-------------------------------------------------------------------------------
--------------------------- LAN Emulation Server 2 ----------------------------
Status                : Running.
LAN type              : Token Ring.
Actual ELAN name      : "IBM_TOKEN_RING_LAN2".
Desired ELAN name     : "".
Actual max frame size : 4544.
Desired max frame size: 4544.
ATM address : 39.99.99.99.99.99.99.00.00.99.99.01.50.50.50.50.50.50.50.03
LEC Id Range          : 4 to 6.
Current number of operational clients   : 4.

8265ATM>
```

Stopping a LES

Use the STOP parameter on the SET LAN_EMUL SERVER command to stop a LES.

For example to stop emulated LAN number 2:

```
8265ATM> set lan_emul server 2 stop
```

Stopping a LES also stops its associated BUS.

Depending on the number of LECs that are connected to the LES, there may be a delay from the time the command is issued to the time the LES is completely stopped. For this reason, you should verify that the LES has stopped using the SHOW LAN_EMUL SERVERS command before trying to start the LES again.

LEC Access Control

The LECs connected to an LES must have their Emulated LAN Name set equal to that of the LES, if it is specified. LECs with a non-empty name that is different from that of the LES will be rejected.

Chapter 6. Configuring SNMP and Web Server Parameters

Carry out the procedures in this section only if you want to manage your ATM subsystem from an SNMP workstation or from a web browser attached to the network.

SNMP Access Requirements

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)

__ 1. Define the *IP address* and *subnetwork mask*, as described in “IP Address and Subnetwork Mask” on page 28.

__ 2. Specify the IP address of the *default gateway*, as described in “Default Gateway” on page 28.

__ 3. Specify the ATM address of the *ARP server*, as described in “ARP Server” on page 28.

__ 4. Enable the sending of *alert messages*, as described in “Alert Settings” on page 22.

__ 5. Define the *community table* as described in “Community Table” on page 36.

LAN Emulation over ATM subnetwork (LE)

__ 1. Configure the *Lan Emulation Client (LEC)*, as described in “LEC Settings” on page 30.

__ 2. Specify the IP address of the *default gateway*, as described in “Default Gateway” on page 28.

__ 3. Enable the sending of *alert messages*, as described in “Alert Settings” on page 22.

__ 4. Define the *community table* as described in “Community Table” on page 36.

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.

Web Access Requirements

To access the 8265 Control Point integrated web server from a web browser attached to the network:

__ 1. Define the *IP address* and *subnetwork mask*, as described in “IP Address and Subnetwork Mask” on page 28.

__ 2. Add an entry to the *community table* for each IP address from which you will access the integrated web server. See “Community Table” on page 36.

Community Table

SNMP Access

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, 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.

Web Access

The Community table also defines which IP addresses can access the integrated web server on the 8265 Control Point.

To create a web-access entry in the Community table, use the SET COMMUNITY command. For example, the following command specifies that a community name called `webmgr` with an IP address of `195.44.22.544` can access the integrated web server:

```
8265ATM> set community webmgr 195.44.22.544 http_enable
```

Remember that the community name parameter is *case-sensitive*.

Chapter 7. Working with Ports and Media Modules

This chapter describes:

- How to connect and disconnect a module from the network
- How to enable ports and interfaces.
- How to display module and port information.

Connecting Modules to the Network

Before the ports on a module can be enabled for operation, the module must be connected to the network. To connect the module in slot 5 to the network:

```
8265ATM> set module 5 connected
```

When you connect a module to the network, you may also enable or disable **all** the ports on the module together, at the same time:

```
8265ATM> set module 5 connected enable
```

Enabling ATM Ports

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)
- Interim Inter-Switch Signalling (IISP)
- Private Network-to-Network (PNNI)
- VOID
- AUTO.

8260 Modules on the 8265

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 bandwidth).
- If you have a 3-port 155 Mbps module, you can only enable one of the ports. (155 Mbps bandwidth).

Displaying Module and Port Settings

Module Settings

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.

Example – SHOW MODULE: In the following example, the SHOW MODULE command displays 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>
```

Example – SHOW MODULE VERBOSE: In the following example, SHOW MODULE VERBOSE displays 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>
```

Example – SHOW MODULE ALL: In this example, SHOW MODULE ALL displays 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>
```

Port Settings

Enter the SHOW PORT command to display information for one or more ports on the 8265.

Example – SHOW PORT ALL

```
8265ATM> show port all


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

8265ATM>
```

The following information is displayed about each port:

Port Number of the port on the CPSW.

Type Type of ATM interface used (UNI, IISP, PNNI).

Mode Whether the port has been `enabled` or `disabled` using the SET PORT command.

Status Operational status of the port.

The following statuses are displayed during normal port operation:

- DOWN: Establishing *
- DOWN: Configuring *
- DOWN: Retrieving *
- UP: Registering *
- UP

If any other port status is displayed, or if any of the transient statuses (marked with * in the list) are displayed continuously, see the “Problem Determination” section in the *IBM 8265 Media Module Reference Guide*.

Example – SHOW PORT VERBOSE

```
8265ATM> show port 8.1 verbose

      Type Mode     Status
-------------------------------------------------------------------------------
 8.01: UNI disabled

UNI Type             : Private
Signalling Version   : Auto
ILMI status          : DOWN:Not in service
ILMI vci             : 0.16
RB Bandwidth         : unlimited
Police admin.        : on
Signalling vci       : 0.5
RB Admin weight      : 5040
NRB Admin weight     : 5040
VPI range admin.     : 0-15 (4 bits)
VCI range admin.     : 0-1023 (10 bits)
VPI range oper.      : 0-15 (4 bits)
VCI range oper.      : 0-1023 (10 bits)
Connector            : SC DUPLEX
Media                : multimode fiber
Port speed           : 155000 kbps
Connection shaping   : Off.
Remote device is active

Frame format    : SONET STS-3c
Scrambling mode : frame and cell
Clock mode      : internal

Signal Detect         : active
RDOOL Status          : inactive
Loss Of Signal        : inactive
Loss Of Frame         : inactive
Line FERF             : inactive
Line AIS              : inactive
Path FERF             : inactive
Path AIS              : inactive
Loss Of Pointer       : inactive
Loss Cell Delineation : inactive
Out Of Frame          : inactive

B1 Errors Counter  : 0
HCS Errors Counter : 0

8265ATM>
```

The Information displayed depends on the settings available for the port type.

Part 3. Configuring ATM Network Connections

Chapter 8. Linking to ATM Devices

This chapter discusses the basic procedures for linking ATM ports on the 8265 ATM Switch directly to:

- ATM User Devices
- Non-PNNI ATM Switches
- PNNI ATM Switches

To link the 8265 to another ATM switch across a WAN, see the procedures in Chapter 9, “Linking Networks Through a WAN (VPCs)” on page 53.

Linking to ATM User Devices (UNI)

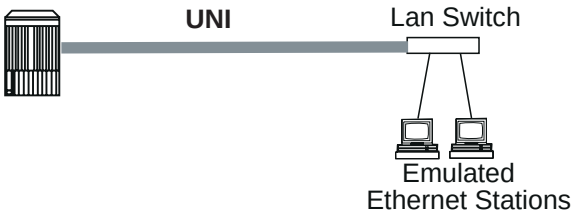


Figure 2. UNI Link to a User Device

To link one port on the 8265 directly to an ATM User Device (such as a Server or LAN ATM Bridge):

__ 1. Connect the port's module to the network using the SET MODULE command.

__ 2. Enable the port as UNI using the SET PORT command, defining any traffic management settings that are needed.

```
8265ATM> set module 7 connected
Slot 7:Module set.
8265ATM> set port 7.1 enable uni bandwidth_rb:100
 7.01:Port set
8265ATM>
```

__ 3. If the device does not support ILMI address registration, use SET REACHABLE ADDRESS to define the reachable address prefix necessary to reach the device. (See “Defining Reachable Addresses” on page 51 for further information.)

```
8265ATM> set reachable address 5.2 96 39.99.99.99.99.99.99.00.00.99.99.08
Entry set.
8265ATM>
```

If several reachable addresses on a PNNI switch share the same network prefix, they should be entered as a PNNI summary address to reduce routing overhead. See Chapter 11, “PNNI Networks” on page 61 for details on configuring summary addresses.

For guidelines on configuring traffic management settings, see Chapter 13, “Managing ATM Traffic” on page 67.

Linking PNNI Switches in the Same Peer Group (PNNI)

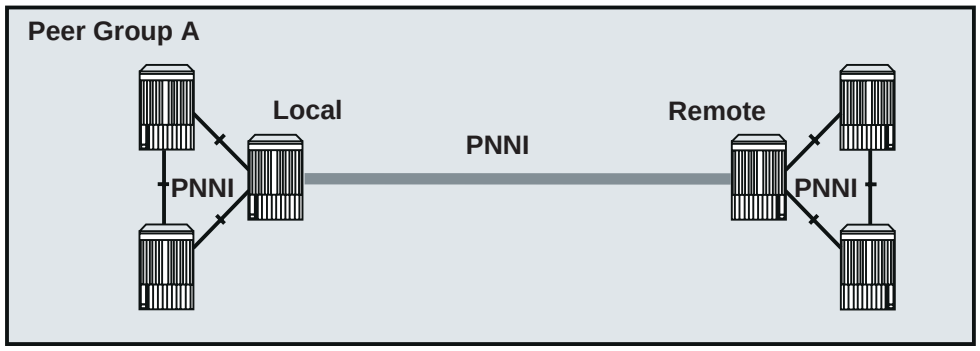


Figure 3. PNNI Link to a PNNI Switch

(Requires the PNNI Code Card.)

To link one port on the 8265 directly to an ATM switch that supports PNNI routing:

__ 1. On the local switch, connect the port's module to the network using the SET MODULE command.

__ 2. On the local switch, enable the port as PNNI using the SET PORT command, defining any traffic management settings that are needed.

```
LOCAL> set module 4 connected
Slot 4:Module set.
LOCAL> set port 4.2 enable PNNI
 4.02:Port set
LOCAL>
```

__ 3. On the remote switch, connect the port's module to the network using the SET MODULE command.

__ 4. On the remote switch, enable the port as PNNI using the SET PORT command, defining any traffic management settings that are needed.

```
REMOTE> set module 8 connected
Slot 8:Module set.
REMOTE> set port 8.4 enable PNNI
 8.04:Port set
REMOTE>
```

For guidelines on configuring traffic management settings, see Chapter 13, “Managing ATM Traffic” on page 67.

Linking Non-PNNI ATM Switches (IISP)

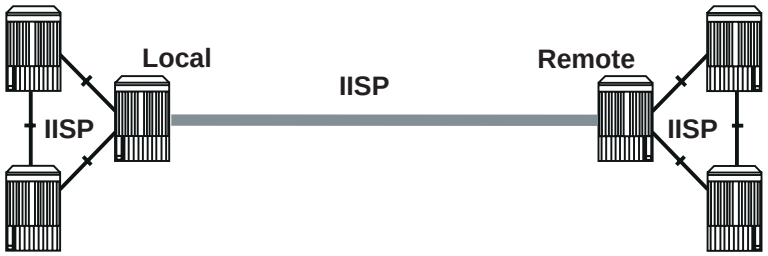


Figure 4. IISP Link to Non-PNNI Switch

When linking to another ATM switch using IISP, one switch must be defined as "NETWORK" and the other switch defined as "USER".

To link one port on the 8265 directly to an ATM switch that does not support PNNI routing:

__ 1. On the local switch, connect the port's module to the network using the SET MODULE command.

__ 2. On the local switch, enable the port as IISP using the SET PORT command, defining any traffic management settings that are needed.

```
LOCAL> set module 5 connected
Slot 5:Module set.
LOCAL> set port 5.2 enable IISP network bandwidth_rb:125
 5.02:Port set
LOCAL>
```

__ 3. On the local switch, use SET REACHABLE ADDRESS to define the reachable address prefix of the remote switch, and of any devices attached to the remote switch that do not support ILMI registration. (See “Defining Reachable Addresses” on page 51 for further information.)

```
LOCAL> set reachable address 5.2 96 39.99.99.99.99.99.99.00.00.99.99.10
Entry set.
LOCAL>
```

Note: Do not specify a VPI when defining a reachable address on an IISP link.

__ 4. On the remote switch, connect the port's module to the network using the SET MODULE command.

__ 5. On the remote switch, enable the port as IISP using the SET PORT command, defining any traffic management settings that are needed.

```
REMOTE> set module 3 connected
Slot 3:Module set.
REMOTE> set port 3.1 enable IISP user bandwidth_rb:125
 3.01:Port set
REMOTE>
```

__ 6. On the remote switch, use SET REACHABLE ADDRESS to define the reachable address prefix of the local switch, and of any devices attached to the local switch that do not support ILMI registration.

```
REMOTE> set reachable address 5.2 96 39.99.99.99.99.99.99.00.00.99.99.08
Entry set.
REMOTE>
```

For guidelines on configuring traffic management settings, see Chapter 13, “Managing ATM Traffic” on page 67.

Linking PNNI Switches in Different Peer Groups (IISP)

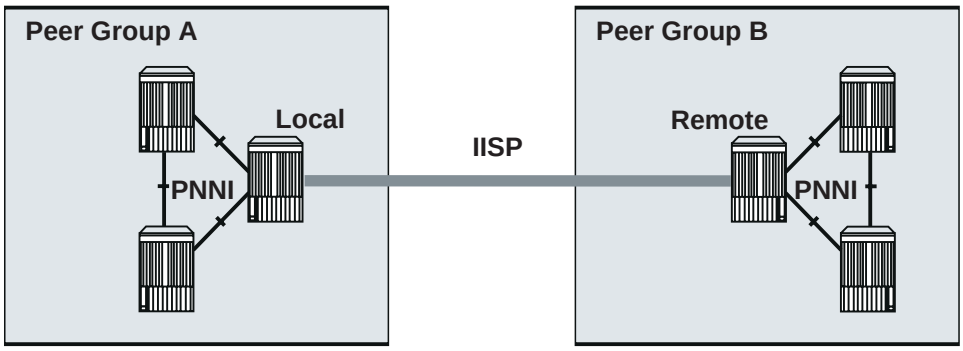


Figure 5. IISP Link to PNNI Switch in Different Peer Group

(Requires the PNNI Code Card.)

When linking to a PNNI switch in another peer group, you use IISP, and one switch must be defined as "NETWORK" and the other switch defined as "USER".

To link one port on the 8265 to an ATM switch in another peer group:

__ 1. On the local switch, connect the port's module to the network using the SET MODULE command.

__ 2. On the local switch, enable the port as IISP using the SET PORT command, defining any traffic management settings that are needed.

```
LOCAL> set module 5 connected
Slot 5:Module set.
LOCAL> set port 5.2 enable IISP network bandwidth_rb:125
 5.02:Port set
LOCAL>
```

__ 3. On the local switch, use SET REACHABLE ADDRESS to define the reachable address prefix of the remote switch, and of any devices attached to the remote switch that do not support ILMI registration. (See “Defining Reachable Addresses” on page 51 for further information.)

```
LOCAL> set reachable address 5.2 96 39.99.99.99.99.99.99.00.00.99.99.10
Entry set.
LOCAL>
```

Note: Do not specify a VPI when defining a reachable address on an IISP link.

__ 4. On the remote switch, connect the port's module to the network using the SET MODULE command.

__ 5. On the remote switch, enable the port as IISP using the SET PORT command, defining any traffic management settings that are needed.

```
REMOTE> set module 3 connected
Slot 3:Module set.
REMOTE> set port 3.1 enable IISP user bandwidth_rb:125
 3.01:Port set
REMOTE>
```

__ 6. On the remote switch, use SET REACHABLE ADDRESS to define the reachable address prefix of the local switch, and of any devices attached to the local switch that do not support ILMI registration.

```
REMOTE> set reachable address 5.2 96 39.99.99.99.99.99.99.00.00.99.99.08
Entry set.
REMOTE>
```

For guidelines on configuring traffic management settings, see Chapter 13, “Managing ATM Traffic” on page 67.

Defining Reachable Addresses

The PNNI protocol automatically determines routing information for all devices in a PNNI hierarchical peer group. In those circumstances where PNNI cannot automatically determine this information, you must provide it manually, by defining entries in the table of Reachable Addresses.

For User Devices

When a user device that does not support ILMI address registration is linked to an ATM network (over a UNI link), you must define a reachable address entry at the UNI link that encompasses the ATM address of the user device.

For IISP Switches

When linking two ATM switches that do not support PNNI (for example, an 8265 running on the IISP code card), you must define reachable address entries that encompass all ATM addresses to be reached through the IISP link.

For PNNI Switches Reachable Over IISP Links

When linking to another PNNI peer group over an IISP link, you must define reachable address entries at the IISP link that encompass all ATM addresses to be reached in the other peer group.

For Non-Hierarchical PNNI Switches

Linking a hierarchical PNNI peer group to a non-hierarchical peer group requires special consideration when defining reachable address entries.

Scope of the Reachable Address

To limit the distribution of the reachable address to a a specified PNNI level (or organizational/administrative scope), use the SCOPE parameter on the SET REACHABLE ADDRESS command.

Organizational levels correspond to PNNI routing levels as follows:

Scope	Level	Scope	Level
1-3	96	11-12	48
4-5	80	13-14	32
6-7	72	15	0
8-10	64		

Chapter 9. Linking Networks Through a WAN (VPCs)

Guidelines for VPCs

Virtual Path Connections (VPCs), also known as VP tunneling, allow ATM switches to connect to each other across Wide Area Network (WAN) links. When an 8265 is physically attached to a WAN, and a VPC is established across the WAN link, the device attached at the other side of the WAN appears to the local switch as if it were an adjacent device. A VPC extends the connectivity of the 8265 and can provide multiple VP tunnels across the same physical WAN link.

VPCs are created using the SET VPC_LINK command, and may only be created on VOID ports. Each VPC can be of UNI, IISP, PNNI, or AUTO type, and is functionally equivalent to the corresponding physical link. This means that ILMI, signalling, and routing may be defined separately on each VPC.

Figure 6 shows various possible VPC configurations.

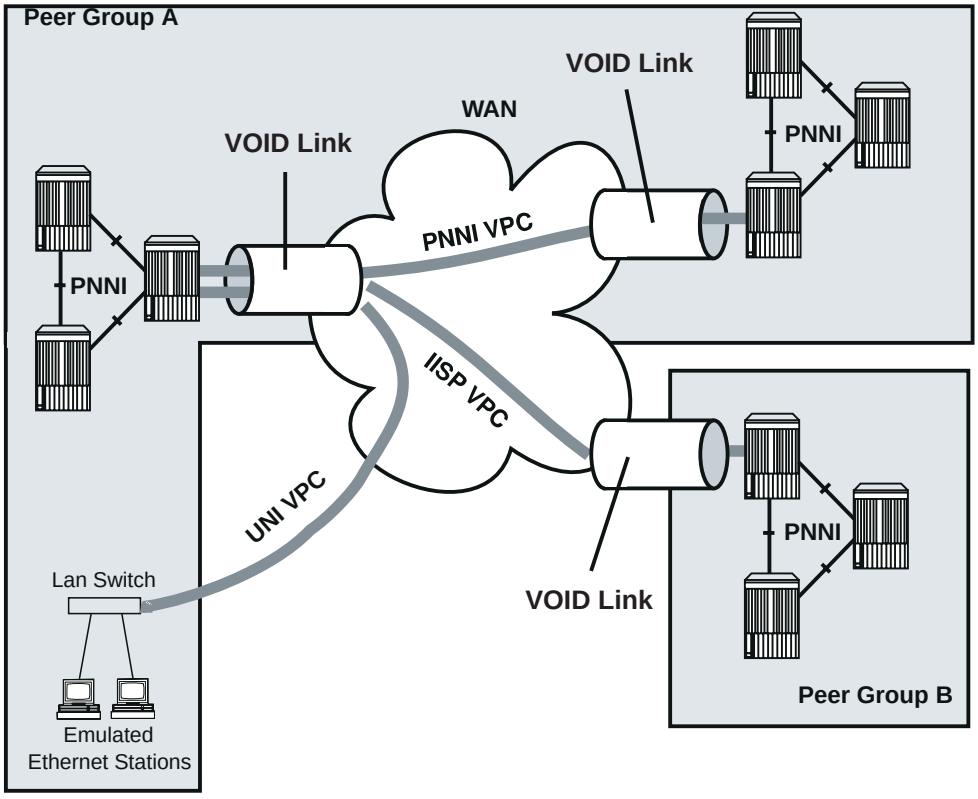


Figure 6. UNI, IISP, and PNNI VPC Links

Note: The maximum permissible number of VPCs depends on the memory configuration currently in use (See “Memory Configuration” on page 24.)

Example: Linking PNNI Switches Across a WAN (PNNI VPC)

(Requires the PNNI Code Card.)

To link the 8265 across a WAN to a another switch that supports PNNI routing:

__ 1. On the local switch, connect the port's module to the network using the SET MODULE command.

__ 2. On the local switch, enable the port as VOID using the SET PORT command, defining any traffic management settings that are needed.

```
LOCAL> set module 4 connected
Slot 4:Module set.
LOCAL> set port 4.2 enable VOID
 4.02:Port set
LOCAL>
```

__ 3. On the local switch, define a VPC on the VOID port.

```
LOCAL> set vpc_link 4.2 15 enable PNNI bandwidth: 130
Accepted
LOCAL>
```

__ 4. On the remote switch, connect the port's module to the network using the SET MODULE command.

__ 5. On the remote switch, enable the port as VOID using the SET PORT command, defining any traffic management settings that are needed.

```
REMOTE> set module 8 connected
Slot 8:Module set.
REMOTE> set port 8.4 enable PNNI
 8.04:Port set
REMOTE>
```

__ 6. On the remote switch, define the same VPC on the VOID port.

```
REMOTE> set vpc_link 8.4 15 enable PNNI bandwidth: 130
Accepted
REMOTE>
```

For guidelines on configuring traffic management settings, see Chapter 13, “Managing ATM Traffic” on page 67.

VPC Traffic Shaping

VPC Traffic Shaping regulates traffic out to a lower rate than the line speed. Control at the VPC level means that the switch can have different shaping values for different VPCs that are active on the same port.

Note: VPC Traffic shaping not available on 8260 modules.

To define traffic shaping on a VPC, use the SET VPC_LINK command:

__ 1. Define the total bandwidth of the VPC using the BANDWIDTH: parameter (mandatory).

__ 2. Set the SHAPING: parameter to ON to enable traffic shaping.

__ 3. Specify the traffic type on the VPC using the TUNNELED_SERVICE_CATEGORY: parameter:

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

```
8265ATM> set vpc_link 5.1 3 enable uni bandwidth:500 shaping:on tunneled_servi
ce_category:cbr_vbr_only
Accepted
8265ATM>
```

Reachable Addresses and VPC Links

When a VPC link connects to devices that do not support ILMI address registration, you must also define reachable address prefixes for those devices using the SET REACHABLE_ADDRESS command.

If you define a VPC link of type IISP, check that the VPI of the VPC link is also defined in your reachable address.

If several reachable addresses share the same network prefix in a PNNI network, they should be entered as a PNNI summary address to reduce routing overhead. See Chapter 11, “PNNI Networks” on page 61 for details on configuring summary addresses.

See “Defining Reachable Addresses” on page 51 for more information on defining reachable addresses.

Shifting the Range of VPI Values

To create a new range of VPI values on a VOID port, you can specify a number to be added to the default VPI values, using the VPI_OFFSET: parameter of the SET PORT command.

For example, with VPI_VCI set to 6.8, the default range of values is 0-63. To shift the range to 192-255, use VPI_OFFSET:192.

Notes:

1. All VPCs must be defined with VPI values that are within the new range.
2. SVCs will be allocated using the smallest value in the VPI range (for example, vpi.vci 192.32, 192.33, and so on).
3. The maximum VPI value (original value plus offset) is 255.

Chapter 10. Linking to E.164-Based Networks

The 8265 ATM Switch supports two methods of connecting private ATM networks through UNI links to an E.164 public network:

E.164 Address Mapping Table
When the private networks being connected use DCC or ICD NSAP address formats, you must create entries in an E.164 address table that will map reachable 20-byte ATM addresses to the 15-digit E.164 address used by the public network.

Imbedded E.164 Addresses
When the private ATM network uses the E.164 NSAP address format, the imbedded E.164 address can be automatically extracted for use by the public network.

Each method is described below. For further information on DCC, ICD, and E.164 ATM addresses, see Appendix A, “ATM Address Formats” on page 129.

E.164 Address Mapping Table

On the edge switches on each side of the private network you must create a table that maps NSAP addresses on the remote network to the corresponding E.164 address on the public network.

Each entry in the table maps one private NSAP address, or address prefix, to the E.164 address of the public link used to reach the NSAP address. You must create mapping entries for both **originating** addresses and **destination** addresses on the remote network.

When the call is made to the public network, the destination NSAP address is demoted to a sub-field for transit across the public network. After leaving the public network, the destination NSAP address is promoted again and the E.164 address is discarded. The same process occurs in the reverse direction.

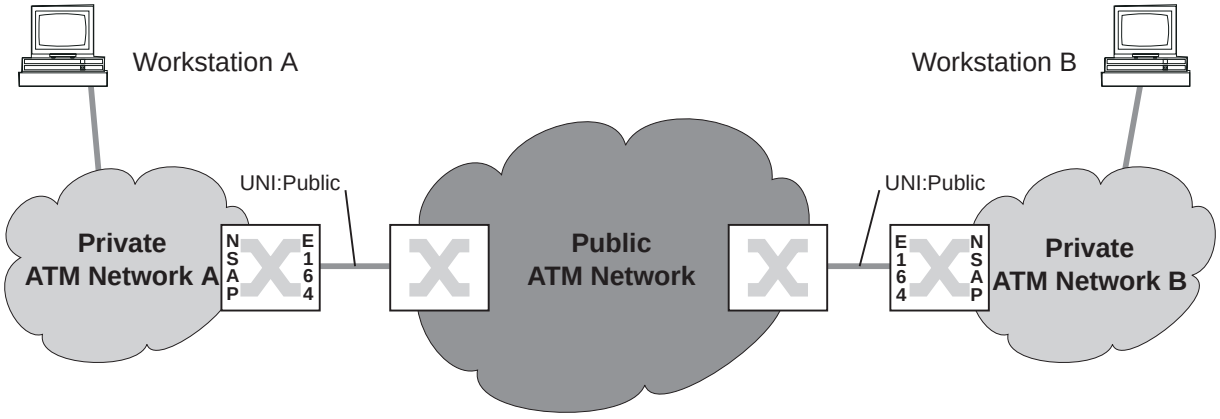


Figure 7. DCC - E.164 - DCC Address Translation (Mapping Table)

For example, in order to set up a connection between workstation A and workstation B in Figure 7 on page 57 you define the link from A to B on the local edge switch:

__ 1. Define the port on the edge switch that connects to the public network using the UNI_TYPE:PUBLIC parameter of the SET PORT command.

__ 2. Create the entry in the address mapping table that links the NSAP address of workstation B to the E.164 address of the public network.

```
8265ATM> set port 5.2 enable uni uni_type:public user address_translation_method
:table 5.02:Port set
8265ATM> set e164 24 39.99.78 003057302026730
Entry set.
8265ATM>
```

Then, you define the link from B to A on the remote edge switch:

__ 3. Define the port on the edge switch that connects to the public network using the UNI_TYPE:PUBLIC parameter of the SET PORT command.

__ 4. Create the entry in the address mapping table that links the NSAP address of workstation A to the E.164 address of the public network.

```
8265ATM> set port 3.1 enable uni uni_type:public user address_translation_method
:table 3.01:Port set
8265ATM> set e164 24 39.99.76 003057302026728
Entry set.
8265ATM>
```

Note: The maximum permissible number of PVCs depends on the memory configuration currently in use (See “Memory Configuration” on page 24.)

Imbedded E.164 Addresses

When the NSAP addresses in the private ATM network are in E.164 ATM format, address translation is simplified. Address translation takes place automatically when the UNI port is defined as to use IMBEDDED address translation.

To set up a connection between workstation A and workstation B in Figure 7 on page 57 you define the link from A to B on the local edge switch:

__ 1. Define the port on the edge switch that connects to the public network using the UNI_TYPE:PUBLIC parameter of the SET PORT command.

```
8265ATM> set port 5.2 enable uni uni_type:public user address_translation_method
:imbedded_e164 5.02:Port set
8265ATM>
```

Then, you define the link from B to A on the remote edge switch:

__ 2. Define the port on the edge switch that connects to the public network using the UNI_TYPE:PUBLIC parameter of the SET PORT command.

```
8265ATM> set port 3.1 enable uni uni_type:public user address_translation_method
:imbedded_e164 3.01:Port set
8265ATM>
```

Chapter 11. PNNI Networks

Guidelines for configuring PNNI Peer Groups and managing PNNI traffic are described in the separate document: ***PNNI: What It Is, What It Does, and How to Configure It.***

Chapter 12. Managing Virtual Connections (PVCs and SVCs)

The IBM 8265 ATM Switch supports Switched Virtual Connections (SVCs) and Permanent Virtual Connections (PVCs) in both point-to-point and point-to-multipoint configurations.

- SVCs are established dynamically on the request of a user device.
- PVCs are permanent connections established by a network administrator.

Note: The maximum permissible number of PVC connections depends on the memory configuration currently in use (See “Memory Configuration” on page 24.)

Setting Up PVCs

The 8265 ATM Switch supports two types of PVC: **point-to-point** and **point-to-multipoint**. Both Virtual Path Connections (VPCs) and Virtual Channel Connections (VCCs) are supported for each type. Each PVC can be defined with either Best-Effort or Reserved Bandwidth, and with or without Frame-Discard enabled.

PVCs are defined by their **origin** and **destination** endpoint ports. The endpoints of a PVC may reside on the same 8265 switch or may cross multiple links. Routing of a PVC across multiple links may be:

- Dynamic, by defining a single PVC to the destination end-point and letting PNNI determine the route. This type of routing can only occur across PNNI links.

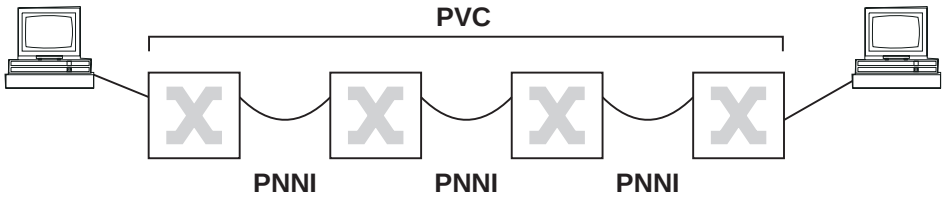


Figure 8. PVCs Across PNNI Links

- Fixed, by defining end-to-end PVCs across multiple IISP links until the destination end-point is reached. This type of routing is required when creating a PVC across IISP links.

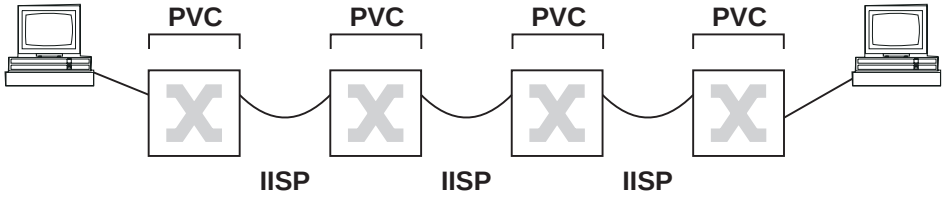


Figure 9. PVCs Across IISP PNNI Links

Notes:

1. VPI.VCI settings must fall within the VPI.VCI range defined for the end-point ports. The VPI.VCI range on the local and remote end-point ports of a PVC must be identical.
2. PVC settings are automatically saved to NVRAM after the PVC is successfully started.
3. If a network failure occurs after a PVC has been established, the ATM system will make up to 20 attempts, after 15-second intervals, to re-establish the PVC. An already established PVC can be re-activated manually using the ACTIVATE parameter in the SET PVC command.

Point-to-Point PVCs

A point-to-point PVC is defined between one origin port and a single destination port.

The following example defines a point-to-point PVC (VCC):

- Originating at local port 14.1
- With a *pvc_id* of 3
- Ending at port 3.2 on a switch with the ATM host name "athena"
- With both local and remote *vpi.vci* selected automatically by ATM system
- With Best-Effort bandwidth allocation.

```
8265ATM> set pvc 14.1 3 athena 42.00.00.00.03.02 channel_point_to_point * * bes
t_effort
PVC set and started.
8265ATM>
```

Frame Discard

To enable "smart" frame-discard (discard of ATM cells pertaining to the same discarded message) on a selected PVC, use the FRAME_DISCARD parameter in the SET PVC command:

```
8265ATM> set pvc 14.3 4 helsinki 42.00.00.00.06.01  path_point_to_point 3 2 bes
t_effort frame_discard
PVC set and started.
8265ATM>
```

Point-to-Multipoint PVCs

A point-to-multipoint PVC consists of:

- One **Base PVC** between an origin port and one destination port, plus
- One or more **Party PVCs** between the origin port and each of the destination ports. Each Party PVC inherits the bandwidth and frame-discard settings of the Base PVC it depends on.

To define a point-to-multipoint PVC (VPC) with 120 Kbps reserved bandwidth from local port 12.1 to 4 ports residing on a different module on the same local 8265:

__ 1. Define the Base PVC:

```
8265ATM> set pvc 12.1 6 this_hub_port:5.1 path_point_to_multipoint * * reserved
_bandwidth:120
PVC set and started.
8265ATM>
```

__ 2. Then define each of the 3 Party PVCs with IDs of 12, 13, and 14:

```
8265ATM> set party_pvc 12.1 6 12 this_hub_port:5.2 *
PVC set and started.
8265ATM> set party_pvc 12.1 6 13 this_hub_port:5.3 *
PVC set and started.
8265ATM> set party_pvc 12.1 6 14 this_hub_port:5.4 *
PVC set and started.
8265ATM>
```

Chapter 13. Managing ATM Traffic

This chapter discusses the following ATM traffic controls supported by the 8265 ATM Switch for ATM ports and VPC links:

- Bandwidth: Reserved and Best Effort
- Policing
- ILMI Related Settings
- Control Connections
- Port Traffic Shaping
- Call Pacing
- Accounting
- PNNI Path Selection
- PNNI Crankback

Bandwidth

The 8265 ATM Switch supports both Reserved-Bandwidth and Best-Effort connections.

Best Effort

Unspecified Bit Rate (UBR) and Available Bit Rate (ABR) are supported over Best-Effort connections. If Reserved Bandwidth is not allocated on a port or VPC, Best Effort is used.

Reserved Bandwidth

The 8265 ATM Switch supports Continuous Bit Rate (CBR), both real-time and non-real-time Variable Bit Rate (VBR-rt and VBR-nrt; supported as CBR) on Reserved Bandwidth connections.

To allocate Reserved Bandwidth on a port or VPC, use the BANDWIDTH_RB: parameter of the SET PORT or SET VPC_LINK command. You may specify either an amount in Kbps or "UNLIMITED", which allocates the maximum bandwidth allowable (85% of total port bandwidth).

```
8265ATM> set port 8.4 enable uni bandwidth_rb:225
 8.04:Port set
8265ATM>
```

Notes:

1. Setting *rb_bandwidth* equal to the port or VPC bandwidth means that no Unspecified Bit Rate (UBR) or Available Bit Rate (ABR) connections can be established on the selected port.
2. Setting *rb_bandwidth* equal to zero means that no RB connections (CBR, rtVBR, nrtVBR, ABR MCR≠0) can be established on the selected port.

Policing

Policing on the 8265 ensures that contracts are respected at the Virtual Connection (VC) level by dropping cells over contract. Policing is only available for CBR and VBR traffic only. To enable policing, use the POLICING parameter of the SET PORT or SET VPC_LINK command:

```
8265ATM> set port 8.4 enable iisp policing:on
 8.04:Port set
8265ATM>
```

Port policing is not available on 8260 modules.

ILMI Related Settings

UNI Signalling Versions

Ports and VPCs may be defined to use UNI 3.0, 3.1, or 4.0. By using the AUTO parameter, a port or VPC will automatically adjust to the detected signal (this is the default).

```
8265ATM> set port 2.1 enable uni signalling_version:sign_3_1
8265ATM>
```

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 allow duplicate addresses, enter the following command:

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

ILMI, Signalling, and Routing VPI.VCI Settings

The default *vpi.vci* settings for ILMI, Signalling, and Routing (PNNI) control connections are:

- ILMI: 0.16
- Signalling: 0.5
- Routing: 0.18

To change these to another *vpi.vci* setting, use the corresponding parameter (ILMI_VPI_VCI, SIGNALLING_VPI_VCI, ROUTING_VPI_VCI) on the SET PORT parameter. To disable the setting on the selected port, specify NONE.

For example, to change the ILMI *vpi.vci* setting to 3.12:

```
8265ATM> set port 3.1 enable uni ilmi_vpi_vci:3.12
 3.01:Port set
8265ATM>
```

To disable ILMI on port 5.1, use the ILMI_VPI_VCI:NONE parameter:

```
8265ATM> set port 5.1 enable uni ilmi_vpi_vci:none
 5.01:Port set
8265ATM>
```

Port Traffic Shaping

Traffic shaping on 8265 ATM ports is VC (Virtual Connection) shaping, which is applied in two ways, depending on the traffic type:

- For CBR and VBR connections, shaping is applied *per connection*, at the output's peak cell rate.
- For ABR and UBR connections, shaping is applied to a *bundle* of connections, with bandwidth specified for each type of connection.

Traffic shaping can be applied to any type of port using the CONNECTION_SHAPING parameter of the SET PORT command.

To enable VC shaping on a selected port:

__ 1. Set the CONNECTION_SHAPING parameter in the SET PORT command to ON

__ 2. Select the UBR bandwidth to be applied to the port using the ALL_UBR: parameter. To disable shaping for UBR connections use the NONE_UBR parameter.

__ 3. Select the ABR bandwidth to be applied to the port using the ALL_ABR: parameter. To disable shaping for ABR connections use the NONE_ABR parameter.

```
8265ATM> set port 4.3 enable uni connection_shaping:on none_ubr all_abr:150
 4.03:Port set
8265ATM>
```

Notes:

1. The sum of the shaping bandwidths on a port cannot exceed the port's physical bandwidth.
2. When a port is configured with reserved bandwidth (using the BANDWIDTH_RB parameter):
   - If reserved bandwidth is specified on the selected port, then the sum of UBR and ABR shaped bandwidths must not exceed the remaining bandwidth (that is, total physical bandwidth less the reserved bandwidth).
   - If reserved bandwidth is set to UNLIMITED, then the sum of the UBR and ABR shaped bandwidths on a port must not exceed the port's physical bandwidth. In this case, only the remaining bandwidth (that is, total physical bandwidth less the UBR and ABR shaped bandwidth) is allocated to reserved bandwidth.
3. VC shaping does not apply to control connections, such as ILMI.
4. In the case of a VPC link across a VOID port, shaping can be applied either:
   - As VP shaping on the connections of the VPC link (see “VPC Traffic Shaping” on page 55), if the SHAPING parameter on the SET VPC_LINK command is set to ON.
   - As VC shaping on the port connections, which is described here.

Call Pacing

Call pacing in the 8265 allows the pacing of new set-up requests to the Control Point following an interruption in service. You can specify the length of the window, or pacing cycle, (up to 255 increments of 100 msec) and the maximum number of parallel calls (up to 255) to be admitted during each cycle. You can optionally limit call pacing to set-up requests from a specific ATM address (the default is all addresses.)

To enable call pacing, use the SET SIGNALLING CALL_PACING command:

```
8265ATM> set signalling call_pacing on 150 30
This call will reset the ATM subsystem.
Are you sure ? (Y/N)
```

Accounting

To enable per-connection accounting for all connections in the 8265 ATM Switch, use the SET DEVICE ACCOUNTING command:

```
8265ATM> set device accounting:enable
This call will reset the ATM subsystem.
Are you sure ? (Y/N)
```

Notes:

1. Even when accounting on all connections is disabled using the SET DEVICE ACCOUNTING command, counters on individual connections may still be enabled by network management software.
2. Enabling accounting on all connections reduces the maximum number of connections available.

PNNI Path Selection

IBM's PNNI supports three methods of path selection, corresponding to 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 and Variable Bit Rate (CBR, rtVBR, and nrtVBR)

Routing is **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 administrative weights. If more than one path is found with the same sum of administrative weights, the path with the highest available bandwidth is chosen. See “Administrative Weight” on page 74 for more information.

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

Available Bit Rate (ABR)

IBM's PNNI Path Selection supports Available Bit Rate (ABR) calls in two ways:

Precomputed
The specific route is obtained via table look-ups, resulting in fast connection setup. The path is computed according to the "widest path" criterion.

On-Demand
The path is computed according to the "shortest path" criterion, based on administrative weights, as described under “Constant and Variable Bit Rate (CBR, rtVBR, and nrtVBR).” This results in slower connection setups, but allows more optimization for the individual routes.

The default configured setting is "precomputed", which can be changed to "on-demand" by entering the following command: This results in slower connection setups, but allows more optimization for the individual routes.

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

Unspecified Bit Rate (UBR)

IBM's PNNI Path Selection supports Unspecified Bit Rate (UBR) using **Precomputed** paths calculated in two ways:

Shortest 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.

Widest 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 default configured setting is "widest_path", which can be changed to shortest path by entering the following command:

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

Administrative Weight

Connections on ports and VPCs may be assigned relative ranking through the use of the Administrative Weight parameter. Administrative Weights are used in calculating *on-demand* path selections. Separate Administrative Weights may be assigned for Reserved and Non-Reserved Bandwidth connections.

```
8265ATM> set vpc_link 5.2 3 enable uni bandwidth_rb:unlimited rb_admin_weight:2006
8265ATM>
```

Displaying Path Selection Settings

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

```
8265ATM> show pnni path_selection
Unspecified bit rate : widest path.
  Available bit rate : precomputed path.
8265ATM>
```

PNNI Crankback

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. Two methods for rerouting alternate paths are supported:

Try Alternate Link (TAL)
This method retries establishing the connection on parallel links, without recomputing the route.

Try Alternate Route (TAR)
This method retries on alternate routes, which requires recomputing the route.

To enable or disable the crankback function, use the SET PNNI CRANKBACK command.

The follow example shows how to enable the crankback function with TAR set to OFF and TAL set to 5 retries.

```
8265ATM> set pnni crankback on tar_off tal_tries:5
To activate issue COMMIT after your last 'set pnni...' entry.
To cancel all changes since previous COMMIT, issue UNCOMMIT.
 8265ATM>
```

You can view the current status of the crankback function with the SHOW PNNI CRANKBACK command.

Chapter 14. Managing Network Access Security

This chapter describes

- How Network Access Security operates
- How to configure and manage the Network Access Security system.

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) against the Access Control Address Table 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 “Defining Reachable Addresses” on page 51.)

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 uses an ATM Control Point configuration console, 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
- Violation trapping
- Violation logging
- Default values for new ports

Suggested Strategy

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

__ 1. SET SECURITY MODE NO_SECURITY (to stop the security system - only required if the system is active). This command is described in “Enabling Security” on page 79.

__ 2. SET SECURITY DEFAULT MODE NO_SECURITY (to disable security on all ports newly detected after security is activated). This command is described in “Default Values for New Ports” on page 88.

__ 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). This command is described in “Enabling Security” on page 79.

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

__ 1. SET SECURITY MODE NO_SECURITY (to stop the security system - only required if the system is active). This command is described in “Enabling Security” on page 79.

__ 2. SET SECURITY DEFAULT MODE ACCESS_CONTROL (to enable security on all ports newly detected when security is activated). This command is described in “Default Values for New Ports” on page 88.

__ 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). This command is described in “Enabling Security” on page 79.

After the basic security controls have been established, you can proceed with more specific security settings:

__ 5. Configure the ATM *access control address table* to enable access by specific ATM addresses or groups of addresses, as described in “Creating Address Table Entries” on page 81.

__ 6. Specify address *autolearn* controls, as described in “Enabling Autolearn” on page 84.

__ 7. Configure *violation traps*, as described in “Enabling Violation Traps” on page 85.

__ 8. Configure *violation logging*, as described in “Enabling the Violation Log” on page 86.

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

Global and Per-Port 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 88.)

Enabling Security

To enable security globally, use:

```
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, for example, on port 5.3, enter:

```
8265ATM> set security port 5.3 mode access_control
```

Disabling Security

To disable security globally, enter:

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

To disable security on port 5.2, use:

```
8265ATM> set security port 5.2 no_security
```

Displaying Security Settings

To see the current security settings for one or more specific ports use the SHOW SECURITY PORT command. To see the current global security settings, use SHOW SECURITY CONTROL:

```
8265ATM> show security control
               mode           autolearn      trap             log
-------------------------------------------------------------------------------
Control Flags  NO_SECURITY    ENABLED        ACCESS_VIOLATION ACCESS_VIOLATION
8265ATM>
```

To see the current security settings on a specific port, use the SHOW SECURITY PORT command:

```
8265ATM> show security port all
slotport       mode           autolearn      trap             log
-------------------------------------------------------------------------------
01.01          ACCESS_CONTROL 00             DISABLED         ENABLED
01.02          ACCESS_CONTROL 01             DISABLED         ACCESS_VIOLATION
01.03          NO_SECURITY    00             DISABLED         ENABLED
01.04          NO_SECURITY    00             ACCESS_VIOLATION ENABLED
8265ATM>
```

The Access Control Address Table

Creating Address Table Entries

ATM address can be validated by comparing either the full ATM address (19 bytes) or just the ESI portion (bytes 14 through 19) of the address to entries in the access control address table. Table entries can be applied either to an individual port, or to all ports on the switch.

For example, to accept calls from a specific address on port 5.3, use:

```
8265ATM> set security atm_address 39.99.99.99.99.99.99.00.00.00.00.45.60.22.22.4
3.89.38.73 5.3
```

Alternatively, to validate calls to all ports based on an ESI only, enter:

```
8265ATM> set security esi_address 22.22.43.89.38.73 any
```

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 a Table Entry

To remove an entry from the access control address table:

__ 1. Locate the entry you want to remove using the SHOW SECURITY ATM_ADDRESS command

__ 2. Clear the entry using CLEAR SECURITY ATM_ADDRESS.

Displaying Table Entries

To display the ATM addresses that have been granted access, for example on all ports.enter:

```
8265ATM> show security atm_address all
index port    ATM_ADDRESS
------------------------------------------------------------------------------
 1   05.02  00.00.00.00.00.00.00.00.00.00.00.00.08.00.5A.EE.EE.EE
 2   00.00  00.00.00.00.00.00.00.00.00.00.00.00.08.00.5A.EE.EE.EF
 3   05.01  39.99.99.99.99.99.99.00.00.01.57.08.00.5A.AA.AA.AA.AA.AA
 4   00.00  39.99.99.99.99.99.99.00.00.01.57.08.00.5A.AA.AA.AA.AA.AB
 5   05.03  39.99.99.99.99.99.99.00.00.99.99.58.58.00.80.05.A9.92.8D
8265ATM>
```

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

Working with the Address Table

The access control address table may be uploaded, via TFTP, to a server for backup, or for manually entering, updating, or removing ATM addresses. You can download the saved (or modified) table back onto the 8265. If security is enabled, the new access control address table will automatically come into effect.

Uploading the Address Table to a Server: To upload the access control address table to a server, follow the procedures in “Access Control Address Table” on page 120.

Manually Updating the Table: If you intend to enter ATM addresses entries directly into the access control address table while it is 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 “Uploads to a Server” on page 120.

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 00000000000000000000000000ffffffffff 01 01
00000000000000000000000000010203040502 00000000000000000000000000ffffffffff 01 02
00000000000000000000000000010203040503 00000000000000000000000000ffffffffff 02 04
39020304050607080910111213141516171819 ffffffffffffffffffffffffffffffffffff 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.

Downloading the Address Table from a Server: To download the access control address table from a server, follow the procedures in “Saved Access Control Address Table” on page 122.

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).

Autolearn Values

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 learned. If 0 is specified, autolearning is disabled. When autolearn is enabled:

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

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.

Enabling Autolearn

The autolearn function can be enabled or disabled either for all ports or for specific ports. To enable the autolearn function for all ports, enter the following command:

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

To set an autolearn value of 10 for port 14.2, enter the following command:

```
8265ATM> set security port 14.2 autolearn 10
```

To disable the autolearn function (no addresses may be learned) on a specific port, enter a value of 0.

Note: 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.

Displaying Autolearn Settings

To display global or per-port Autolearn settings, use the SHOW SECURITY CONTROL and SHOW SECURITY PORT commands as described in “Displaying Security Settings” on page 80.

Violation Traps

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.

Enabling Violation Traps

You can enable or disable traps on either all ports or selected ports. To enable or disable traps on all ports, enter:

```
8265ATM> set security trap access_violation
```

To disable traps on, for example port 3.5, enter:

```
8265ATM> set security port 3.5 trap disable
```

Displaying Violation Trap Settings

To display global or per-port Violation Trap settings, use the SHOW SECURITY CONTROL and SHOW SECURITY PORT commands as described in “Displaying Security Settings” on page 80.

The Violation Log

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.

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.

Enabling the Violation Log

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

```
8265ATM> set security log access_violation
```

To disable logging, for example, on port 4.2, enter:

```
8265ATM> set security port 4.2 log disable
```

Displaying Violation Log Settings

To display global or per-port Violation Log settings, use the SHOW SECURITY CONTROL and SHOW SECURITY PORT commands as described in “Displaying Security Settings” on page 80.

Displaying the Log

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

```
8265ATM> show security violation_log
         VIOLATION LOG
   Type       Intf Date Time       Data
-------------------------------------------------------------------------------
01 ACCESS_CTRL  0101 7-31 14:50:25 add:399999999999990000999923030800 5A9902BE
02 ACCESS_CTRL  0101 7-31 14:50:31 add:399999999999990000999923030800 5A9902BE
03 ACCESS_CTRL  0101 7-31 14:50:31 add:399999999999990000999923030800 5A9902BE
04 ACCESS_CTRL  0101 7-31 14:50:38 add:399999999999990000999923030800 5A9902BE
05 ACCESS_CTRL  0101 7-31 14:50:38 add:399999999999990000999923030800 5A9902BE
06 ACCESS_CTRL  0101 7-31 14:50:38 add:399999999999990000999923030800 5A9902BE
07 ACCESS_CTRL  0101 7-31 14:51:05 add:399999999999990000999923030800 5A9902BE
08 ACCESS_CTRL  0101 7-31 14:51:05 add:399999999999990000999923030800 5A9902BE
09 ACCESS_CTRL  0101 7-31 14:51:17 add:399999999999990000999923030800 5A9902BE
10 ACCESS_CTRL  0101 7-31 14:51:17 add:399999999999990000999923030800 5A9902BE
  ⋮
63 ACCESS_CTRL  0101 7-31 16:47:40 add:399999999999990000999923030800 5A9902BE
64 ACCESS_CTRL  0101 7-31 16:47:40 add:399999999999990000999923030800 5A9902BE
8265ATM>
```

Note: Violation logging must be enabled. See “Enabling the Violation Log” on page 86. only.

Displaying the Last Violation

To display information regarding the last security violation, enter:

```
8265ATM> show security last_violation all
slotport    last_atm_violation                                  datetime
-------------------------------------------------------------------------------
0501 __.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__
0502 __.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__
0503 39.99.99.99.99.99.99.00.00.99.99.58.58.00.80.05.A9.92.8D 21 Dec 97 17:29:37
0504 __.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__.__

8265ATM>
```

Clearing the Log

You can clear the contents of the violation log by entering:

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

Uploading the Violation Log to a Server

To upload the security violation log to a server, follow the procedures in “Security Violation Log” on page 120.

Default Values for New Ports

Because ATM ports may be dynamically added to a switch (when new modules are inserted), you can set the default settings to be applied to newly detected ports. You can define default settings for:

- The security setting for the new port
- The autolearn setting for the port
- Violation trapping
- Violation logging.

Unless the default values are changed, Security, Autolearn, Violation Trapping, and Violation Logging are all *disabled* on newly detected ports.

Security Mode Default

To automatically enable security on newly detected ports:

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

Autolearn Default

To disable the autolearn function on newly detected ports:

```
8265ATM> set security default autolearn 0
```

Suggestions: 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 Trapping Default

To enable violation trapping on newly detected ports:

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

Violation Logging Default

To disable the logging of security violations on newly detected ports:

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

Displaying Default Security Settings

To see the current default security settings, use the SHOW SECURITY DEFAULT command:

```
8265ATM> show security default
               mode           autolearn      trap             log
-------------------------------------------------------------------------------
Default Flags  NO_SECURITY    00             DISABLED         DISABLED
8265ATM>
```

Saving and Reverting 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 to NVRAM. If not, the changes will be lost at the next reset.

If you want to discard security settings *before* they have been saved, enter

```
8265ATM> revert security
```

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

To save the current security settings, enter:

```
8265ATM> save security
```

This will save the parameter settings to NVRAM.

Part 4. Managing the 8265 ATM Switch Hardware

Chapter 15. Management Tools

This chapter describes the commands used to display information about the 8265 and its 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 17, “Managing the Power Subsystem” on page 103.
- 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, its model number, and whether the CPSW integrated power controller or a controller module is controlling the power supply
- Fan - indicates the status of each 8265 fan
- Temperature - indicates 8265 temperature at three locations.

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              OKAY                8265PS-HO

Temperature Information:

    A/D Converter Status      : OKAY
    Overall Temperature Status: OKAY

    Probe           Location            Temperature
    -----           --------            -----------
     1              FAN_1               28 Degrees Celsius
     2              FAN_2               30 Degrees Celsius
     3              FAN_3               31 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 SHOW POWER ALL command:

```
8265ATM> show power all

                Power Management Information
                (Power Control by CPSW 11, power switch = CPSW)
                ---------------------------

Hub Power Modes:

        Fault_Tolerant Mode:       FAULT_TOLERANT
        Fault_Tolerant Status:     FAULT_TOLERANT
        Overheat Power Down Mode:  ENABLE

Slot Power Information:

Slot     Class         Admin Status         Operating State
----     -----         ------------         ---------------
2        6             ENABLE               ENABLED
3        6             ENABLE               ENABLED
4        6             ENABLE               ENABLED
6        3             ENABLE               ENABLED
7        6             ENABLE               ENABLED
8        6             ENABLE               ENABLED
9        8             ENABLE               ALWAYS_ENABLED
11       8             ENABLE               ALWAYS_ENABLED
13       6             ENABLE               ENABLED
14       6             ENABLE               ENABLED
15       6             ENABLE               ENABLED
17       3             ENABLE               ENABLED

Hub Power Budget (A/D Converter is OKAY):

Voltage Type  Voltage Level  Watts Capacity  Watts Available  Watts Required
------------  -------------  --------------  ---------------  --------------
     +5V          5.20         1084.00          343.00          741.00
     -5V          OKAY           51.00           38.25           12.75
    +12V          OKAY          244.00          145.00           99.00
    -12V          OKAY           61.00           45.75           15.25
     +2V          OKAY           28.40           17.30           11.10

8265ATM>
```

Displaying 8265 Module Information

Show the Inventory of Modules

Use the SHOW INVENTORY command to display information about installed modules. When you enter SHOW INVENTORY, 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:

To display basic inventory information for the 8265, use the SHOW INVENTORY command:

```
8265ATM> show inventory

HUB/                    Hardware
Slot  Module            Version  Serial #         Vendor           Date
----- ---------------   -------- ---------------- ---------------- ------
HUB   8265-S17          A        L9915            IBM              980708

01.01 53-58G9611FC5004 C38844   VIM R034         IBM              970531

03.01 53-51H4297FC5003 E28143                    IBM              970425
03.02 53-58G9578FC8800 D55936                    IBM              970628
03.03 53-58G9578FC8800 D55936   3528             IBM              970105
03.04 53-58G9578FC8800 D55936   3427             IBM              970105

09.01 93076H8108FC6501 E95775   16               IBM              970620
09.02 93002L2428FC6501 E95775   24               IBM              970620

8265ATM>
```

SHOW INVENTORY VERBOSE:

To display more detailed inventory information for the 8265, use the SHOW INVENTORY VERBOSE command:

```
8265ATM> show inventory verbose

HUB/                    Hardware
Slot  Module            Version  Serial #         Vendor           Date
----- ---------------   -------- ---------------- ---------------- --------
HUB   8265-S17          A        0                IBM              19971017

      Type:     8265-S17          Number of slots:    17
      Note Pad:

   ATM Backplane EC Level:F12594
   Burned In MAC Addresses (BIA):
    . Ethernet Port           : 0056291F83D6
    . LAN Emulation Ethernet  : 0056291F03D6
    . LAN Emulation Token-Ring: 0056297703D6

02.01 93002L40776561   f12446   19119            IBM              19980407

      Note Pad: 02L3561 CARRIER 25 WAN
      Hardware features: 0x00000001
      Operational Version: n/a         Boot Version: n/a

02.02 53-10J2219FC8501 E28263   1607             IBM              19971009

      Note Pad: WAN E3 G832 34Mbps Daughter Coax
      Hardware features: 0x20202020
      Operational Version: v0.05.2     Boot Version: v0.05.2

02.03 53-10J2161FC8507 E95633   1207             IBM              19970310

      Note Pad: WAN T1E1 1_5Mbps 2Mbps Daughter Copper and Coax
      Hardware features: 0x20202020
      Operational Version: v0.02.6     Boot Version: v0.02.6


03.01 93076H8330       E46642   1116             IBM              19971002

      Note Pad: _        CARRIER 2
      Hardware features: 0x00000001
      Operational Version: n/a         Boot Version: n/a

03.02 9300213436fc6512 f12516                    ibm              19971017

      Note Pad: 0212413 622 smf pic
      Hardware features: 0x00000000
      Operational Version: n/a         Boot Version: n/a


04.01 93002L3242FC6543 F12447   10873            IBM              19971223

      Note Pad: 13J8738 155 FLEX
      Hardware features: 0x00000001
      Operational Version: n/a         Boot Version: n/a

04.02 53-76H8241FC6580 E46632   251              IBM              19970808

      Note Pad: High Speed 155 Mbps Daughter Multimode
      Hardware features: 0x20202020
      Operational Version: n/a         Boot Version: n/a
```

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 resets the module in the specified slot to its last-saved configuration.

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.

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) ?
```

Chapter 16. Diagnostic Tools

Startup Diagnostics

Each time the 8265 is started or reset, a self-check diagnostic routine is performed, to ensure that the 8265 switch is operational. While it is not recommended, it is possible to disable, and subsequently enable, startup diagnostics using the SET DEVICE DIAGNOSTICS command.

Startup diagnostics are enabled by default.

ATM PING

The ATM ping allows you to differentiate a pure ATM problem from a Classical IP or LANE problem.

An ATM ping consists of:

- A connection set between the source switch and the target switch (only other 8265 switches respond to ATM pings)
- Data sent from the source switch to the target switch
- Data returned from the target switch to the source switch
- The results displayed on the configuration console.

For example, to determine whether the ATM switch with host name CAIRO is reachable over a UBR connection, enter:

```
8265ATM> atm_ping cairo service_category:ubr
Starting ATM ping (hit CTRL-C to stop) ...
--- ATM ping statistics ---
SVC established. Packets sent
ATM address: 47.41.82.65.13.13.00.00.00.00.00.13.13.65.00.00.00.94.13.00
ATM Ping (hostname: ATMG13): 1 packets sent, 1 received
ATM Ping (hostname: ATMG13): 2 packets sent, 2 received
ATM Ping (hostname: ATMG13): 3 packets sent, 3 received

8265ATM>
```

Traces and Error Logs

Setting Traces

Traces are available for numerous ATM Switch transactions, and may be restricted to specific modules, ports, or VPCs.

For example, to trace ILMI transactions on all VPCs on modules 5 and 6:

__ 1. Enter SET TRACE MAIN_TRACE OFF to disable trace recording.

__ 2. Enter SET TRACE MODULES:5 6 ON to enable traces on the selected modules only.

__ 3. Enter SET TRACE ILMI ON to enable tracing of ILMI transactions.

__ 4. SET TRACE MAIN_TRACE ON to enable trace recording.

```
8265ATM> set trace main_trace on
Main trace is ON.
               base trace will be off when main trace is on.
                bus trace will be off when main trace is on.
signalling messages trace will be off when main trace is on.
               ilmi trace will be on when main trace is on.
                lec trace will be off when main trace is on.
                les trace will be off when main trace is on.
          pnni_base trace will be off when main trace is on.
      pnni_messages trace will be off when main trace is on.
      pnni_neighbor trace will be off when main trace is on.
pnni_path_selection trace will be off when main trace is on.
                pvc trace will be off when main trace is on.
            RFC 1577 trace will be off when main trace is on.
               saal trace will be off when main trace is on.
        connections trace will be off when main trace is on.
               snmp trace will be off when main trace is on.
       box_services trace will be off when main trace is on.
VPC 5.* * appears in traces
VPC 6.* * appears in traces
8265ATM>
```

__ 5. When the desired trace is completed, enter SET TRACE MAIN_TRACE OFF to stop trace recording.

See the *Command Reference Guide* for a listing of trace types available.

To display the current trace settings on the configuration console, use SHOW TRACE.

Uploading the Trace File to a Server

To upload the trace file to a server, follow the procedures in “Traces” on page 121.

Uploading the Error Log to a Server

To upload the error log to a server, follow the procedures in “Traces” on page 121.

Port Mirroring

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.

Before enabling port mirroring to a port, you must first disable all ports on the target module. When port mirroring is enabled, all other ports on the target module are automatically 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.

Notes:

1. Port mirroring can be applied to only one port on a module.
2. Port mirroring is not supported on 8260 modules.

Chapter 17. Managing the Power Subsystem

This chapter describes:

- 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.

Note: To determine whether the Integrated Power Controller or a Controller Module is controlling the power supply, examine the top of the SHOW POWER ALL, BUDGET, or MODE displays. The following example indicates that the Integrated Controller Module is controlling the power supply:

```
8265ATM> show power budget

                    Power Management Information
                    (Power Control by CPSW 11, power switch = CPSW)
                    ---------------------------
```

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 power controller powers up an 8265 module, the power controller adjusts the available power budget to reflect the power consumption of the newly powered-up module. The power controller 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 power controller 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 *IBM 8265 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 SET POWER BUDGET command. 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).

For example:

```
8265ATM> show power budget

                    Power Management Information
                    (Power Control by CPSW 11, power switch = CPSW)
                    ---------------------------
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>
```

Note: 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. 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 power controller 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 SHOW POWER MODE command. When the 8265 is running in power fault-tolerant mode, the following information is displayed:

```
8265ATM> show power mode

                     Power Management Information
                     (Power Control by CPSW 11, power switch = CPSW)
                     ---------------------------
 Hub Power Modes:

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

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.

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>
```

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

The power controller employs the following powerup strategy:

- If a power controller module is installed on the 8265, the current unallocated power budget must be sufficient to power up this module.
- Media modules power up according to the following constraints:
  - In order of power class, in descending order from 10 to 0.
  - If more than one media module is assigned the same power class, they are powered up in slot order, going from 1 to 17.
  - Modules are powered up until the power budget is reached.

Specifying Power Up Order

To specify the order in which 8265 modules power up, you change their power class settings, as described in “Changing a Module's Power Class” on page 110.

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 power controller 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 SHOW POWER SLOT command:

```
8265ATM> show power slot 1

               Power Management Information
               (Power Control by CPSW 11, power switch = CPSW)
               ---------------------------
Slot Power Information:

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

Changing a Module's Power Class

The power controller 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.

Each media module is shipped with a default power class setting of 6. Power class settings can range from 10 (highest) to 1 (lowest). A module set to power class 10 does not power down automatically under any circumstances.

To change a module's power class (for example, to assign a higher power class setting to a media module connected to critical network resources), use the SET POWER slot CLASS command:

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

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

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. **(Not Applicable to Integrated Power Controller)**

Power Class 10 Warnings: A media module assigned a power class setting of 10 cannot be automatically powered down by the power controller.

- 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 power controller 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 power controller must reduce the power consumption of all installed modules. The power controller 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 power controller is unable to respond to a power deficit (for example, due to a power failure), the switch resets. Under these conditions, power up (recovery) occurs when the 8265 reboots.

Powering Up With Insufficient Power

If there is insufficient power to power up, the power controller will automatically place modules in insufficient power 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 power controller 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 power controller 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 power controller 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.

Power Down Due to Overheating

For information concerning 8265 module power-down due to an overheat condition, see “Overheating” on page 116.

Specifying Power Down Order

To specify the order in which 8265 modules power down, you change their power class settings, as described in “Changing a Module's Power Class” on page 110.

Chapter 18. 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 **(Not Applicable to Integrated Power Controller)**.

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

Operating Temperature Indicators

(Not Applicable with Integrated Power Controller)

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 power controller 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 1 describes controller module LEDs associated with switch internal operating temperature.

Table 1. 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

(Not Applicable with Integrated Power Controller)

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

(Integrated Power Controller Only) The Intelligent Cooling Subsystem operates as follows:

1. The power controller 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 power controller 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 **(Not Applicable to Integrated Power Controller)**.

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 power controller 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 power controller 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 power controller 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 power controller 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 power controller 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 power controller uses the saved data to restore lost module power configurations.

The power controller saves the power management configuration data shown in Table 2.

Table 2. 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 power controller 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 power controller 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 19. Server Downloads and Uploads

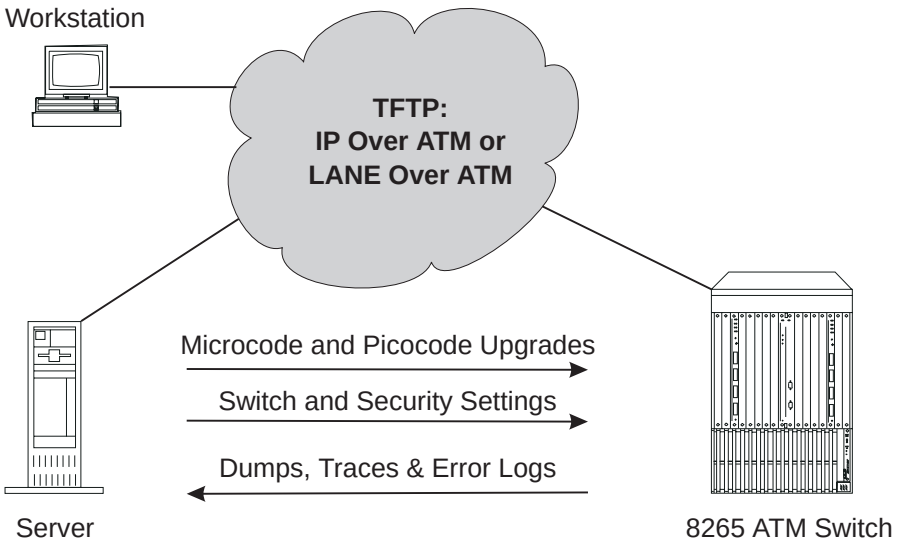


Figure 11. Inband Uploads and Downloads

The 8265 provides facilities for various inband transfers between the switch and an attached server:

Uploads to a Server

The following filetypes can be uploaded from the switch to a file on a server:

- All current switch configuration settings
- The current contents of the access control address table
- The current contents of the security violation log.
- Dumps, Traces, and Error Logs

Downloads from a Server

The following file types can be downloaded from a file on a server to the switch:

- Previously uploaded switch configuration settings
- Previously uploaded access control address table.

Code Upgrades

The following IBM 8265 Switch code upgrades can be downloaded from a file on a server to the switch:

- Boot and operational microcode upgrades for the CPSW module
- FPGA picocode upgrades for ATM modules
- Boot and operational microcode upgrades for Power Controller modules
- Microcode upgrades for WAN2 module daughter cards

For information on where to find microcode and picocode updates on the Internet, see “Automatic Notification of Updates” on page 6.

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

Uploads to a Server

Switch Configuration

To upload the current switch configuration to a file on a server, enter the following CPSW commands:

1. SET TFTP FILE_TYPE CONFIGURATION
2. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
3. SET TFTP FILE_NAME (to define the path name of the file on the server)
4. UPLOAD (to upload the configuration).

Access Control Address Table

To upload the access control address table to a file on a server, enter the following commands:

1. SET TFTP FILE_TYPE SECURITY_CONFIG
2. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
3. SET TFTP FILE_NAME (to define the path name of the file on the server)
4. UPLOAD (to upload the file).

Security Violation Log

To upload the security violation log to a server, enter the following commands:

1. SET TFTP FILE_TYPE SECURITY_LOG
2. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
3. SET TFTP FILE_NAME (to define the path name of the file on the server)
4. UPLOAD (to upload the file).

Dumps

To upload a dump to the host, enter the following CPSW commands:

1. DUMP PNNI DATA_BASE (to take a dump of the topology of the network, for example)
2. SET TFTP FILE_TYPE DUMP
3. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
4. SET TFTP FILE_NAME (to define the path name of the file on the server)
5. UPLOAD (to upload the dump).

Error Log

To upload the error log to the host, enter the following CPSW commands:

1. SET TFTP FILE_TYPE ERROR_LOG
2. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
3. SET TFTP FILE_NAME (to define the path name of the file on the server)
4. UPLOAD (to upload the error log).

Traces

To upload a recorded trace log to the host, enter the following CPSW commands:

1. SET TFTP FILE_TYPE MAIN_TRACE
2. SET TFTP SERVER_IP_ADDRESS (to define the server that will receive the file)
3. SET TFTP FILE_NAME (to define the path name of the file on the server)
4. UPLOAD (to upload the trace).

Note: For information on creating a trace log, see “Setting Traces” on page 100.

Downloads from a Server

Saved Switch Configuration

To download a switch configuration that was previously saved to a file on a server, enter the following CPSW commands:

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

Saved Access Control Address Table

To download an access control address table that was previously saved to a server, enter the following commands:

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

Code Upgrades

CPSW Modules

Boot Microcode

Note: If two CPSW modules are installed in the 8265, make sure that you are logged on to the correct module.

To download new boot microcode to a standard CPSW module, enter the following commands:

1. SET TFTP FILE_TYPE BOOT
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode file is located)
3. SET TFTP FILE_NAME (to define the path name of the microcode file on the server)
4. DOWNLOAD (to transfer the code to the EEPROM).

The new boot microcode is activated the next time the CPSW is reset.

Operational Microcode: New operational microcode is downloaded to the standby area of the CPSW Flash EEPROM. After downloading, you must swap the standby and active areas, which reboots the CPSW using the new code.

Note: If two CPSW modules are installed in the 8265, make sure that you are logged on to the correct module.

To download new operational microcode to a standard CPSW module, enter the following commands:

1. SET TFTP FILE_TYPE OPERATIONAL
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode file is located)
3. SET TFTP FILE_NAME (to define the path name of the microcode file on the server)
4. DOWNLOAD (to transfer the code to the EEPROM).
5. SWAP MICROCODE (to swap the active and standby microcode and reboot the CPSW module with the new code). This can be issued at a later time, when you want the new code to be activated.

To view the current active and standby code versions, use SHOW DEVICE.

FPGA Picocode: New FPGA picocode is downloaded to the standby area of a module's Flash EEPROM. After downloading, you must swap the standby and active areas, which reboots the CPSW using the new code.

To download new FPGA picocode to a standard CPSW module, enter the following commands:

1. SET TFTP FILE_TYPE FPGA
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the picocode file is located)
3. SET TFTP FILE_NAME (to define the path name of the picocode file on the server)
4. SET TFTP TARGET_MODULE (to specify the slot number of the CPSW module)
5. DOWNLOAD to transfer the code to the EEPROM)
6. SWAP FPGA_PICOCODE (to swap the active and standby picocode in the module). If the swap is for an active CPSW module, this causes an automatic reset of the ATM subsystem.

To view the current active and standby FPGA code versions, use SHOW MODULE.

ATM Media Modules

FPGA Picocode: New FPGA picocode is downloaded to the standby area of a module's Flash EEPROM. After downloading, you must swap the standby and active areas.

To download new FPGA picocode to an ATM media module, enter the following commands:

1. SET TFTP FILE_TYPE FPGA
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the picocode file is located)
3. SET TFTP FILE_NAME (to define the path name of the picocode file on the server)
4. SET TFTP TARGET_MODULE (to specify the slot number of the media module)
5. DOWNLOAD (to transfer the code to the EEPROM)
6. SWAP FPGA_PICOCODE (to swap the active and standby picocode in the module).

To view the current active and standby FPGA code versions, use SHOW MODULE.

Microcode for WAN2 Daughter Cards: To download new microcode to WAN2 module daughter cards, enter the following commands:

1. SET PORT DISABLE to disable all ports on the daughter card
2. SET TFTP FILE_TYPE DAUGHTER_CODE
3. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode file is located)
4. SET TFTP FILE_NAME (to define the path name of the microcode file on the server)
5. SET TFTP TARGET_PORT (to specify the number of the first port on the daughter card)
6. DOWNLOAD (to transfer the code to the EEPROM).

Power Controller Modules

(Not Applicable with Integrated Power Controller)

Fault Tolerant Configuration: When a download is performed on the *active* controller module, it passes its "active" status to the standby module and reboots. When a download is performed on the *standby* module, no reboot occurs. Thus, in an 8265 containing with two controller modules installed, it is preferable to download to the *standby* controller module first, and to the *active* module after, to minimize disruption to a single module reboot.

Single Module Configuration: When there is just one controller module installed, keep in mind that 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. To restore the failed module, reinsert the module (with the other module operating as the active module) and reinitiate the download. The failed module will power up as the standby controller module.

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

1. SET TFTP FILE_TYPE CONTROLLER_BOOT (to specify boot microcode)
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode file is located)
3. SET TFTP FILE_NAME (to define the path name of the microcode file on the server)
4. SET TFTP TARGET_MODULE (to specify the slot number of the controller module)
5. DOWNLOAD (to transfer the code to the EEPROM).

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

1. SET TFTP FILE_TYPE CONTROLLER_OPERATIONAL (to specify operational microcode)
2. SET TFTP SERVER_IP_ADDRESS (to define the server where the microcode file is located)
3. SET TFTP FILE_NAME (to define the path name of the microcode file on the server)
4. SET TFTP TARGET_MODULE (to specify the slot number of the controller module)
5. DOWNLOAD (to transfer the code to the EEPROM).

As the download progresses, the TEMP LED on the front panel of the controller module lights and remains lit until the download completes. If the download is ***unsuccessful***, the STBY and ACTIVE LEDs on the controller module light and remain lit until you re-initiate the download.

Note: An unsuccessful download may result in the controller module not appearing in a SHOW MODULE display. However, the module

Part 5. Appendixes

Appendix A. 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).

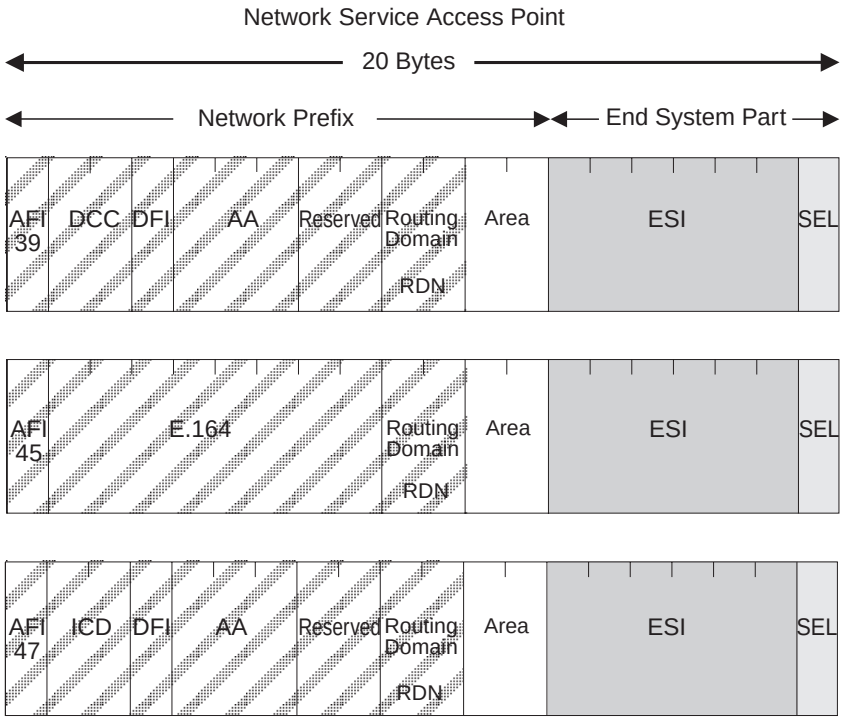


Figure 12. NSAP Address Formats Supported in the 8265 ATM Subsystem

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.

Appendix B. 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:

"Getting Further Assistance" on page 159 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 17, “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 K0` 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 17, “Managing the Power Subsystem” on page 103.

Diagnosing Problems Concerning the Configuration 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 163 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. `COPY` - a new version of BOOT code is being copied to the standby area in the EEPROM.
7. `LOAD` - the operational code is being copied from the PCMCIA card into the DRAM.
8. `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 144. 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 IISP 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 depends on the memory configuration specified. See “Memory Configuration” on page 24 for more information.

You should ensure that the ports and both ends of a connection are using the same VPI/VCI 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 Campus Manager - ATM and LAN emulation server, which can provide you with a lot of information through the LES monitor.
   - 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 161.
   - 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 161.

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 81 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.
- Files containing error log, trace, and dump information, either:
  - Uploaded to a server, as described in “Uploads to a Server” on page 120, or
  - Taken from a browser connected to the Integrated Web Server, as follows:
    1. Click on "Services"
    2. Click on "Dump"
    3. Click on "Everything"
    4. Save the displayed information to a file.
- 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).

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 C. 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 3 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 3 (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 3 (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 4. 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.
>>0025>>	Integrated Power Controller reg. test failed.
>>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.

Q93B Error Codes

Code	Message
1	Unallocated (unassigned) number
2	No route to specified transit network
3	No route to destination
10	VPCI/VCI unacceptable
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (alerted user) - ITU
21	Call rejected
22	Number changed
23	User rejects all calls with CLIR
27	Destination out of order
28	Invalid number format
30	Response to STATUS ENQUIRY
31	Normal unspecified
32	Too many pending add party requests
34	Requested called party soft PVC unavailable
35	Requested VCPI/VCI unavailable
36	VPCI/VCI assignment failure
37	User cell rate not available
38	Network out of order
41	Temporary failure
43	Access information discarded
45	No VPCI/VCI available
47	Resource unavailable
49	Quality of Service unavailable
51	User cell rate not available name
53	Call cleared due to change in PGL
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available
65	Bearer capability not implemented
73	Unsupported comb of traffic parameters
81	Invalid call reference value
82	Identified channel does not exist
88	Incompatible destination
89	Invalid codepoint reference

Code	Message
91	Invalid transit network selection
92	Too many pending add party requests
93	AAL parameters not supported
96	Mandatory information element is missing
97	Message type non-existent or not implemnted
99	Element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
104	Incorrect message length
111	Protocol error
128	Next node unreachable
160	DTL transit not my node identifier

Appendix D. Alternate Configuration Methods

All configuration of the 8265 Control Point can be done using the local (ASCII) configuration console. However, you may use other methods to connect to the Control Point after certain minimum configuration settings have been defined.

Methods for establishing a TELNET session to the Control Point include access from:

- An in-band server or workstation
- A PC connected to the CPSW Ethernet port
- A PC connected to the CPSW Console port over a SLIP connection

Or, for WWW access:

- An in-band Web browser communicating with the Control Point's integrated web server.

This chapter also describes how to reconfigure the default settings on the local (ASCII) configuration console.

In-Band TELNET Connection

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 5, "Configuring LAN Emulation Settings" on page 29.

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 13 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.

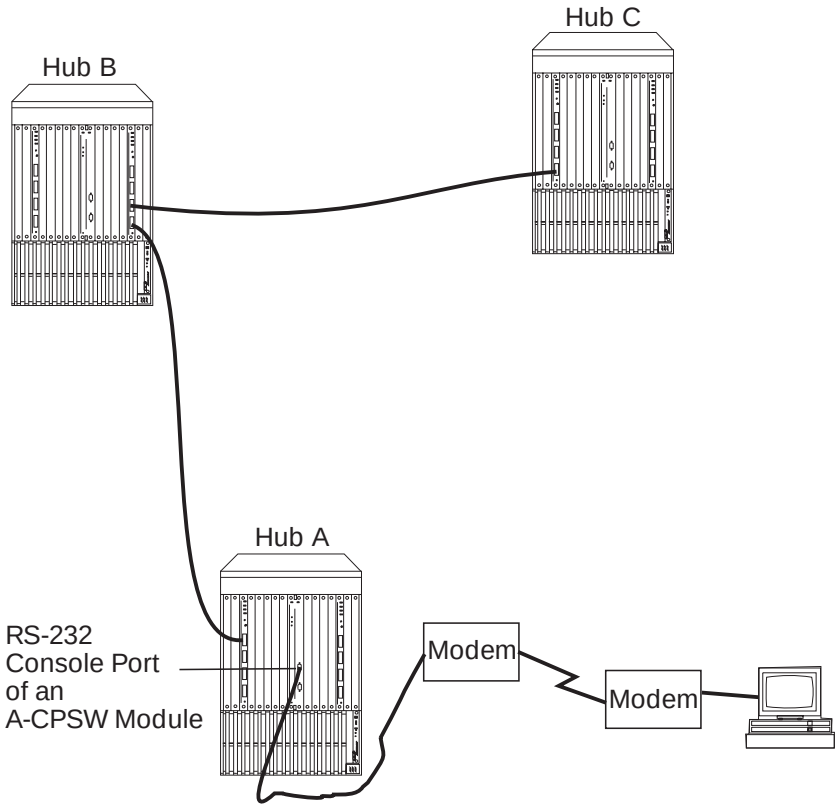


Figure 13. Working in Remote CPSW Sessions

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.

Ethernet Console Connection

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 are configured using the SET DEVICE IP_ADDRESS command, for example:

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

Note: In Maintenance Mode, the IP address and subnet mask are configured using the SET IP_ADDRESS and SET SUBNET_MASK commands.

Setting the Ethernet MAC Address

The MAC address is configured using the SET DEVICE ETHERNET_MAC_ADDRESS command, for example:

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

Note: In Maintenance Mode, the MAC address is configured using the SET MAC_ADDRESS command.

SLIP Console Connection

In SLIP mode, commands are entered over 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 Chapter 19, “Server Downloads and Uploads” 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.

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.
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 13.

Returning to Normal (ASCII) 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

Procedures for establishing these connections are described in the following sections.

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.

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.

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.

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.

Web Browser

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 topology display application to provide an exact image of the topology seen by the PNNI node.
- 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 (traces on-line with Java applet formatter, error log, dump, and connections cleared table).
- Basic SHOW functions.

The web server has been optimized for the following environments:

- 16 to 256 colors
- Display resolution of 800x600 minimum
- A web browser that supports
  - HTTP 1.0
  - Tables
  - Frames
  - JavaScript 1.1
  - Java JDK 1.08
  - Java JAR.

Required Web Browser Configuration

In order to ensure that all updates are displayed immediately, it is required that your web browser be configured as follows:

- Disk cache set to 0 Kb
- Memory cache set to 0 Kb
- 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 168, plus the IP address of the web browser must be registered in the community table as "HTTP_ENABLE".

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"
- The password is the current Administrator password (defined with the "SET DEVICE" command).

Note: To enable IP filtering for the web, you must have at least one other network management community defined with a permission other than "HTTP_ENABLE".

Reconfiguring Local 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
```

Appendix E. Using Maintenance Mode

Maintenance mode is entered:

- Manually, when the MAINTAIN command is issued from a local configuration console session via the RS-232 console port, or
- Automatically, when the CPSW is unable to function under operational code.

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".

When the Maintain 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.

Table 5 provides a summary of the commands available in Maintenance mode. For details of each command, refer to the *IBM 8265 Command Reference Guide*.

Table 5. 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 from the workstation attached as configuration console.
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) whether the attached CPSW module is primary or 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 attached 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.

Upgrading Microcode

While in Maintenance mode, you can download microcode for the CPSW module (but not media modules) out-of-band using a workstation attached to the RS-232 console connector on the CPSW module. The workstation must support emulated VT100 protocol.

CPSW Boot Microcode

To perform an out-of-band download of CPSW Boot Microcode:

1. Attach the workstation to the RS-232 console port on the CPSW module.
2. Locate the directory on the workstation where the microcode updates are stored.
3. Log on to the 8265 as Administrator.
4. Enter the MAINTAIN command (to activate Maintenance mode)
5. DOWNLOAD OUT_OF_BAND BOOT (to specify boot code and to load it in the flash EEPROM of the CPSW module).
6. Start the file transfer in the workstation using the Xmodem protocol. The transfer takes approximately 6 minutes at 9600 bps (the time is halved if the transfer is done at 19200 bps).
7. Once the code is downloaded, Maintenance mode ends and the new Boot Microcode is activated.

CPSW Operational Microcode

To perform an out-of-band download of CPSW Operational Microcode:

1. Attach the workstation to the RS-232 console port on the CPSW module.
2. Locate the directory on the workstation where the microcode updates are stored.
3. Log on to the 8265 as Administrator.
4. Enter the MAINTAIN command (to activate Maintenance mode)
5. DOWNLOAD OUT_OF_BAND OPERATIONAL (to specify operational code and to load it in the flash EEPROM of the CPSW module).
6. Start the file transfer in the workstation using the Xmodem protocol. The transfer takes approximately 6 minutes at 9600 bps (the time is halved if the transfer is done at 19200 bps).
7. Use the SWAP MICROCODE command to make the "Inactive" microcode "Active" when the CPSW reboots.
8. BOOT (to restore normal operation).

Appendix F. 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 is designed according to the specifications of the following industry standards as understood and interpreted by IBM as of October 1992.

International Organization for Standardization (ISO)

- ISO 8802/1
- ISO 8802/3
- ISO 8802/5

IEEE (Institute of Electrical and Electronic Engineers)

- 802.1 Local area network (LAN) management and Internet working
- 802.3 Carrier sense multiple access and collision detection
- 802.5 Token passing ring

ANSI (American National Standard Institute)

The IBM Fiber Distribution Data Interface (FDDI) network is an implementation of the American National Standards Institute (ANSI) X3T9.5 family of standards.

The IBM base standards for the implementation of the FDDI are:

- ANSI X3.166-1990, FDDI physical layer medium-dependent (PMD), ISO 93/4-3
- ANSI X3.148-1988, FDDI token-ring physical layer protocol (PHY), ISO 93/4-1
- ANSI X3.139-1987, FDDI token-ring media access control (MAC)
- ANSI X3.T9, 5/84-49 RFC 1285 FDDI station management (SMI).

ITU-T (International Telecommunications Union - Telecommunication)

The IBM standards for the implementation of ATM are:

- Q.2110 Service Specific Connection-Oriented Protocol (SSCOP)
- Q.2130 Service Specific Coordination Function (SSCF)

ATM Standards

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

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

8265 Documentation

For additional information on the IBM 8265 Nways ATM Switch, please refer to the following documents. The documents are included on the *IBM 8265 Nways ATM Switch Documentation Library* CD, SA33–0454.

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

IBM 8265 Nways ATM Switch User's Guide, SA33-0456.

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, SA33-0459.

IBM 8265 Nways ATM Switch Problem Determination and Service Guide, SY33-2128.

These documents are also available via the Internet:

`http://www.networking.ibm.com/did/8265bks.html`

Related Documentation

The following related publications are included on the *IBM 8265 Nways ATM Switch Documentation Library* CD, SA33–0454.

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

A-MSS 2.5 Server Module / A-MSS Server Module Quick Reference Card, GX27-4018.

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

Nways Multiprotocol Switched Services Configuring Protocols and Features, SC30-3819.

Multiprotocol Switched Services (MSS) Server Service and Maintenance Manual, GY27-0354.

Nways Multiprotocol Switched Services (MSS) Server Module Installation and Initial Configuration Guide, GA27-4141.

Nways MAS/MRS/MSS/MSSC 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.

ATM Forum

For more information on ATM Forum specifications, refer to the following:

- *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. SA33-0456-02

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
- IBM Internal Use: LGERCF at IBMFR
- Internet: lgercf@fr.ibm.com

In advance, thank you.

Your comments:

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SA33-0456-02

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

SA33-0456-02