ATM Switch Diagnostics and Troubleshooting Manual

MANU0232-05
Revision A
March 5, 1999

FORE SYSTEMS®

Software Version 6.0.x

FORE Systems, Inc.

1000 FORE Drive
Warrendale, PA 15086-7502
Phone: 724-742-4444
FAX: 724-742-7742

http://www.fore.com

Legal Notices

TRADEMARKS

FCC CLASS A NOTICE

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void this user's authority to operate this equipment.

NOTE: The *ASX*™-200WG, *ASX*-200BX, *ASX*-1000, *ASX*-1200, *ASX*-4000, *ESX*™-3000, *ForeRunnerLE*™ 25, *ForeRunnerLE* 155, *TNX*™-210, and *TNX*-1100 have been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of the equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

DOC CLASS A NOTICE

This digital apparatus does not exceed Class A limits for radio noise emission for a digital device as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

CE NOTICE

Marking by the symbol **CE** indicates compliance of this system to the EMC (Electromagnetic Compatibility) directive of the European Community and compliance to the Low Voltage (Safety) Directive. Such marking is indicative that this system meets or exceeds the following technical standards:

- EN 55022 - "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment."
- EN 50082-1 - "Electromagnetic compatibility - Generic immunity standard Part 1: Residential, commercial, and light industry."
- IEC 1000-4-2 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 2: Electrostatic discharge requirements."
- IEC 1000-4-3 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 3: Radiate electromagnetic field requirements."
- IEC 1000-4-4 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 4: Electrical fast transient/burst requirements."

VCCI CLASS A NOTICE

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

AUSTRALIA EMC COMPLIANCE

This product has been tested and found to comply with the Class A electromagnetic compatibility limits specified in AS/NZ 3548.

FCC REQUIREMENTS (Notice to Users of DS1 Service)

The following instructions are provided to ensure compliance with the FCC Rules, Part 68.

(1) This device must only be connected to the DS1 network connected behind an FCC Part 68 registered channel service unit. Direct connection is not allowed.

(2) Before connecting your unit, you must inform the telephone company of the following information::

Port ID	REN/SOC	FIC	USOC
NM-6/DS1C NM-2/DS1C NM-8/DS1D NM-4/DS1D	6.0N	04DU9-BN, 04DU9-DN, 04DU9-1ZN 04DU9-1SN, and 04DU9-1KN	RJ48C

(3) If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.

(4) If the telephone company finds that this equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give you advance notice if possible.

(5) Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.

(6) If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.

CANADIAN IC CS-03 COMPLIANCE STATEMENT

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Industry Canada label does not guarantee the equipment will operate to the user’s satisfaction.

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

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

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

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

E1 AND E3 NOTICE

The E1 (NM-6/E1C and NM-2/E1C) and E3 (NM-4/E3C and NM-2/E3C) network modules that are described in this manual are approved for use in FORE Systems' host systems providing that the instructions below are strictly observed. Failure to follow these instructions invalidates the approval.

Pan European Approval - CE Marking

Pan European approval of the E1 network module was issued by BABT following assessment against CTR12. This means that it can be connected to ONP and unstructured PTO-provided private circuits with 120 Ω interfaces in all European countries, according to Telecommunications Terminal Equipment (TTE) Directive 91/263/EEC. Thus, the following CE mark applies:

CE168X

The E1 and E3 network modules conform to safety standard EN60950 1992 following the provisions of Low Voltage Product Safety Directive 73/23/EEC and CE Marking Directive 93/68/EEC, and can be marked accordingly with the CE symbol.

The E1 and E3 network modules conform to EN55022 1994 and EN50082-1 1992 following the provisions of the EMC Directive 89/336/EEC, and can be marked accordingly with the CE symbol.

National Approvals

UK

Network Module	Connects to	Approval Number
E1	Structured and unstructured PTO-provided private circuits with 75 Ω interfaces	AA60953
E3	PTO-provided private circuits with 75 Ω interfaces	NS/4387/1/T/605954

Germany

Network Module	Connects to	Approval Number
E3	Structured PTO-provided private circuits with 75 Ω interfaces	A127535H for the ASX-1000 A127534H for the ASX-200BX or ASX-200WG

Switzerland

Network Module	Connects to	Approval Number
E1	Structured PTO-provided private circuits with 120 Ω interfaces	96.0872.J.N
E3	Structured PTO-provided private circuits with 75 Ω interfaces	96.0873.J.N

Required User Guide Statements - UK Installation

The use of auxiliary products not authorized by FORE Systems® in FORE Systems ATM Switches may cause the power specification to be exceeded and is a potential safety hazard.

The equipment must be installed such that with the exception of the connections to the host, clearance and creepage distances shown in the table below are maintained between the network module and any other assemblies which use or generate a voltage shown in the table below. The larger distance shown in brackets applies where the local environment within the host is subject to conductive pollution or dry non-conductive pollution which could become conductive due to condensation. Failure to maintain these minimum distances invalidates the approval.

Clearance (mm)	Creepage (mm)	Voltage Used or Generated by Host or by Network Modules
2.0	2.4 (3.8)	Up to 50 V_{rms} or V_{dc}
2.6	3.0 (4.8)	Up to 125 V_{rms} or V_{dc}
4.0	5.0 (8.0)	Up to 250 V_{rms} or V_{dc}
4.6	6.4 (10.0)	Up to 300 V_{rms} or V_{dc}

For a host or other expansion card fitted in the host, using or generating voltages greater than 300V (rms or dc), advice from a competent telecommunications engineer must be obtained before installation of the relevant equipment.	Above 300 V_{rms} or V_{dc}

NOTE: Installing the network modules in the appropriate FORE Systems hosts, according to the installation instructions provided, satisfies the requirements listed above.

The following tables show the available ports and their safety status:

NM-6/E1C and NM-2/E1C

Ports	Safety Status
E1 Ports	TNV operating at SELV
Bus Connector	SELV

NM-4/E3C and NM-2/E3C

Ports	Safety Status
E3 Ports	TNV operating at SELV
Bus Connector	SELV

SAFETY CERTIFICATIONS

ETL certified to meet Information Technology Equipment safety standards UL 1950, CSA 22.2 No. 950, and EN 60950.

Table of Contents

CHAPTER 2 Error Messages

Preface

This manual provides diagnostic and troubleshooting information for the for the *ForeRunner*® family of ATM Switches, *ForeRunnerLE*® Switches, *TNX*™ ATM Switches, *ESX*™-3000 Switch, network modules, and the accompanying *ForeThought*® software. This document was created for users with various levels of experience. If you have any questions or problems, please contact FORE Systems' Technical Assistance Center (TAC).

Chapter Summaries

Chapter 1 - AMI Debug Commands: Describes debug level AMI commands. The information that is displayed or logged by these commands may assist you in troubleshooting.

Chapter 2 - Error Messages: Describes error messages that display on the console and in the syslog output and also provides possible solutions for the errors.

Chapter 3 - SCP Diagnostics: Describes the diagnostic hardware tests that can be run when there is a problem with the switch control processor (SCP). This chapter is not applicable to the *ForeRunner ASX*-4000, *ForeRunnerLE* 25, or *ForeRunnerLE* 155.

Chapter 4 - Loopback Modes: Describes the diagnostic loopback modes available for each type of network module.

Chapter 5 - Debugging PNNI: Describes methods for troubleshooting the most common configuration problems in a network based on ATM Forum PNNI (hereafter referred to as PNNI) routing. This chapter assumes that you are already familiar with the configuration of a PNNI network. If you are not familiar with PNNI, please read Chapter 6, "ATM Forum PNNI" in the *ATM Switch Network Configuration Manual*.

Acronyms - Contains a list of common networking acronyms.

Glossary - Contains definitions for networking terms, both general and ATM-specific.

Related Manuals

References are made in this manual to the following manuals:

AMI Configuration Command Reference Manual, Part 1 - Describes the configuration level AMI commands and menus from **`configuration alarms>`** to **`configuration nsap>`**.

AMI Configuration Command Reference Manual, Part 2 - Describes the configuration level AMI commands and menus from **`configuration port>`** to **`configuration vpt>`**.

ATM Management Interface (AMI) Manual - Describes the root, display, operation, and statistics level AMI commands and menus.

ATM Switch Network Configuration Manual - Discusses topics such as LAN Emulation, Classical IP, ATM Forum PNNI, and *ForeThought*® PNNI.

These manuals can be found on the CD and can be read and printed using Acrobat Reader which is also included on the CD. If Acrobat Reader is installed locally, run Acrobat and open the manual from the `/DOCS` directory of the CD. If Acrobat Reader is not installed locally, run the Acrobat installer to load Acrobat Reader on your machine. Then run the `ACROREAD.EXE` file in the `/DOCS` directory of the CD.

Technical Support

In the U.S.A., you can contact FORE Systems' Technical Assistance Center (TAC) using one of the following methods:

1. Select the "Support" link from FORE's World Wide Web page:

   http://www.fore.com/

2. Send questions, via e-mail, to:

   support@fore.com

3. Telephone questions to "support" at:

   800-671-FORE (3673) or **724-742-6999**

4. FAX questions to "support" at:

   724-742-7900

Technical support for customers outside the United States should be handled through the local distributor or via telephone at the following number:

+1 724-742-6999

No matter which method is used to reach FORE Support, customers should be ready to provide the following:

- A support contract ID number
- The serial number of each product in question
- All relevant information describing the problem or question

Typographical Styles

Throughout this manual, all specific commands meant to be entered by the user appear on a separate line in bold typeface. In addition, use of the `Enter` or `Return` key is represented as `<ENTER>`. The following example demonstrates this convention:

cd /usr <ENTER>

File names that appear within the text of this manual are represented in the following style: "...the `fore_install` program installs this distribution."

Command names that appear within the text of this manual are represented in the following style: "...using the **flush-cache** command clears the bridge cache."

Subsystem names that appear within the text of this manual are represented in the following style: "...to access the **bridge** subsystem..."

Parameter names that appear within the text of this manual are represented in the following style: "...using *<seg-list>* allows you to specify the segments for which you want to display the specified bridge statistics."

Any messages that appear on the screen during software installation and network interface administration are shown in `Courier` font to distinguish them from the rest of the text as follows:

```
.... Are all four conditions true?
```

Important Information Indicators

To call your attention to safety and otherwise important information that must be reviewed to ensure correct and complete installation, as well as to avoid damage to the FORE Systems product or to your system, FORE Systems utilizes the following *WARNING/CAUTION/NOTE* indicators.

WARNING statements contain information that is critical to the safety of the operator and/or the system. Do not proceed beyond a **WARNING** statement until the indicated conditions are fully understood or met. This information could prevent serious injury to the operator, damage to the FORE Systems product, the system, or currently loaded software, and is indicated as follows:

WARNING!

Hazardous voltages are present. To reduce the risk of electrical shock and danger to personal health, follow the instructions carefully.

CAUTION statements contain information that is important for proper installation/operation. Compliance with **CAUTION** statements can prevent possible equipment damage and/or loss of data and are indicated as follows:

CAUTION

You risk damaging your equipment and/or software if you do not follow these instructions.

NOTE statements contain information that has been found important enough to be called to the special attention of the operator and is set off from the text as follows:

NOTE

If you change the value of the LECS control parameters while the LECS process is running, the new values do not take effect until the LECS process is stopped, and then restarted.

Invisible Laser Warning Notice

Every FORE Systems network module having a single mode fiber optic interface contains a Class 1 laser.

Class 1 Laser Product:
This product conforms to applicable requirements of 21 CFR 1040 at the date of manufacture.

Class 1 lasers are defined as products which do not permit human access to laser radiation in excess of the accessible limits of Class 1 for applicable wavelengths and durations. These lasers are safe under reasonably foreseeable conditions of operation.

WARNING!

Do not stare into the beam or view the beam with optical instruments.

CHAPTER 1 AMI Debug Commands

This chapter describes the AMI commands that are available under the **debug** root level. Debug commands should normally be used when a problem has been encountered at the switch or network level. Debug commands should not be used during day to day operation or configuration of the switch.

The main **debug** menu can be found at the root level and contains several commands. Commands that are submenus are immediately followed by a “>” symbol. Typing **?** at the **debug** level displays these commands as follows:

```
myswitch:: debug> ?
abr>                dump>               mode                oam
protectedubr>       spvxcongestion>     trace>
```

NOTE Debug commands are only available to users who have administrative privileges. See Chapter 8 of the *ATM Switch Network Configuration Manual* for information about AMI command privileges.

NOTE Not all debug commands are displayed on every platform. Commands not displayed on certain platforms are noted in each section.

NOTE For information about hardware addressing schemes used to reference ports on an ATM switch, see Appendix A, ”Hardware Addressing Schemes”. This information is helpful when interpreting debug messages.

1.1 AMI Typographical Styles

AMI is described throughout this chapter using the following conventions:

- All AMI output, including user prompts, is shown in `courier` font.
- All user input; e.g., sub-commands, is shown in **`bold courier`** font.
- Each submenu is described in a separate section.
- Commands that are submenus are immediately followed by a “>” symbol. The “>” should not be entered as part of the command.
- Required parameter values are indicated inside angle brackets “< >”. The “< >” should not be entered as part of the command.
- Optional parameter values are indicated inside square brackets “[ ]”. The “[ ]” should not be entered as part of the command.
- Parameter values that require a choice are separated by vertical bars and are enclosed in parentheses “(|)” Neither the vertical bar nor the parentheses should be entered as part of the command.
- Optional parameter names are indicated with dashes “**-**”.
- AMI commands are not case-sensitive.

1.2 Changing the Debug Mode

The **mode** command lets you change the debug mode in which it is running. The debug interface in AMI has two modes: novice and wizard.

```
myswitch::debug> mode [(novice | wizard)]
```

The parameters are defined as follows:

Parameter	Description
novice	This mode allows you to run the debug commands, but it prompts you with a warning before executing the command. It asks you if you really want to execute the command since some of the commands will run for a few minutes and stop other activities temporarily. This gives you a chance to abort the command.
wizard	This mode is only for users who have a great deal of experience in troubleshooting. The wizard mode does not give you a chance to abort commands; it executes them immediately.

The default mode is set to novice. This mode is recommended for most users.

Novice mode:

```
myswitch::debug dump cdb> size
                ***** WARNING *****
Debug commands may have negative effects on the switch software.
Dump commands pause the switch control software for their duration,
may have many pages of output, and cannot be stopped mid-execution.
Various trace commands can overload the switch with syslog messages.
You can turn off this warning with: “debug mode wizard”
Execute the debug command [n]? y
CDB size = 7998 bytes
```

Wizard mode:

```
myswitch::debug dump cdb> size
CDB size = 7998 bytes
```

Current mode:

```
myswitch::debug> mode
debug mode is set to novice
```

AMI Debug Commands

1.3 ABR Commands

The **abr** commands can be used to configure Available Bit Rate (ABR) performance. Although the default settings are sufficient, the parameters can be adjusted to provide optimal ABR performance. Table 1.1 shows the default settings for the user-configurable parameters (RIF, RDF, Scale) and for TBE (Transient Buffer Exposure) and ICR (Initial Cell Rate) as outlined in the UNI4.0 specification. Type **?** at the **abr** level to list these commands.

```
myswitch::debug abr> ?
module>           port>            reset
```

NOTE

Currently, ABR commands are applicable to Series D network modules only.

Table 1.1 - ABR Default Values

ABR Parameter	Default Value
RIF	1/8
RDF	1/8
Scale	100
TBE	256
ICR	Minimum Cell Rate (MCR) of ABR connections

NOTE

For more detailed information on ABR service, see the ATM Forum Traffic Management Specification Version 4.0.

1.3.1 Configuring ABR at the Module Level

The commands listed under the **module** root level, let you configure ABR at the network module level. These commands let you display the current percentage of total buffer space available on a network module and adjust the ABR buffer threshold for calculating the Explicit Rate (ER). Type **?** at the **module** level to list the available subcommands.

```
myswitch::debug abr module> ?
scale              show
```

1.3.1.1 Scaling the ABR Buffer Occupancy for Explicit Rate

The **scale** command lets you adjust the ABR buffer occupancy threshold for the Explicit Rate. The Explicit Rate of the ABR VCs is derived by comparing the ABR queue lengths against certain internal buffer thresholds to check if the ER needs to be decreased or maintained. An increased queue length causes a switch to enter the congestion state indicating that the ER should be decreased. Lowering the percentage of total buffer space results in a more conservative behavior of the ER and decreases the probability of cell loss.

The default scale percentage is set to 100.

```
myswitch::debug abr module> scale <module> <scale in percentage>
```

For example, to set the scale percentage to 90% for network module 1A, enter the following:

```
myswitch::debug abr module> scale 1a 90
```

The parameters are described as follows:

Parameter	Description
module	Enter the network module for which you want to adjust the ABR buffer occupancy threshold.
scale in percentage	Enter the percentage of the total buffer space you want to scale.

AMI Debug Commands

1.3.1.2 Displaying Current Percentage of Total Buffer Space

This command lets you display the configured “scale” value and the number of bad RM cells (forward and backward) received by the ingress side of the network module. All bad RM cells are dropped by the network module.

```
myswitch::debug abr module> show
```

The fields are defined as follows:

Field	Description
Module	The network modules installed in the switch.
Scale	The percentage of the total buffer space to scale for the network module. N/A displays if. N/A displays if the scale has not been configured.
Bad RM Cells	The total number of bad RM cells. N/A displays if ABR has not been configured.

```
myswitch::debug abr module> show
                Bad RM
Module  Scale   Cells
1A      100     0
1B      N/A     N/A
1C      N/A     N/A
```

1.3.2 Configuring ABR at the Port Level

The commands listed under the **port** root level, let you configure port level ABR and display current port level configurations. Type**?** at the **port** level to list these commands.

```
myswitch::debug abr port> ?
porttype          rif                 rdf                 show
```

1.3.2.1 Configuring the Port Environment (LAN or WAN)

This command lets you configure the port type to LAN or WAN, based on the environment to which the port is connected. This command is useful when the network modules are hooked up to both LAN and WAN environments.

You must specify for which port you want to configure. The default is set to LAN.

```
myswitch::debug abr port> porttype <bnp> (lan | wan)
```

The parameters are described as follows:

Parameter	Description
bnp	The port for which you want to configure the port type. If a specific port is not specified, the port type configuration applies to all ports for a switch fabric
lan	Sets the port type to LAN.
wan	Sets the port type to WAN.

1.3.2.2 Configuring the Rate Increase Factor (RIF)

This command lets you specify the rate increase factor for a particular port during signalling setup. The RIF controls the amount by which the cell transmission rate may increase upon receipt of an RM cell. The RIF is expected to be lower or less aggressive in the WAN than in the LAN due to a higher Round Trip Time (RTT) in the WAN.

The RDF/RIF ratio can not be decreased. ABR call setups will fail on encountering a decreased RDF/RIF ratio in the network.

The actual value is computed as 1/(2^x), where x is the specified value. You must specify for which port you want to configure and the specified RIF factor must be between 0 and 15. The default is set to 1/8.

```
myswitch::debug abr port> rif  <bnp> <rate increase factor>
```

The parameters are described as follows:

Parameter	Description
bnp	The port for which you want to configure a rate increase factor.
rate increase factor	Specifies the rate increase factor (RIF) between 0 and 15.

AMI Debug Commands

1.3.2.3 Configuring the Rate Decrease Factor (RDF)

This command lets you specify the rate decrease factor for a particular port during signalling setup. The RDF controls the amount by which the cell transmission rate may decrease upon receipt of an RM cell. The RDF can be increased or decreased depending on the constraint that the RDF/RIF ratio not be decreased. The RDF is expected to be lower or less aggressive in the WAN than in the LAN due to a higher Round Trip Time (RTT) in the WAN.

The actual value is computed as 1/(2^x),where x is the specified value.You must specify for which port you want to configure and the specified RDF factor must be between 0 and 15.

The default is set to 1/8.

```
myswitch::debug abr port> rdf <bnp> <rate decrease factor>
```

The parameters are described as follows:

Parameter	Description
bnp	The port for which you want to configure the rate decrease factor.
rate decrease factor	Specifies the rate decrease factor (RIF) between 0 and 15.

1.3.2.4 Displaying Port Level ABR Configurations

This command lets you display the current port level configurations.

```
myswitch::debug abr port> show
Port    Type    RIF     RDF
1A1     LAN     1/8     1/8
1A2     LAN     1/8     1/8
1A3     LAN     1/8     1/8
1A4     LAN     1/8     1/8
1C1     N/A     N/A     N/A
1C2     N/A     N/A     N/A
1C3     N/A     N/A     N/A
1C4     N/A     N/A     N/A
1C5     N/A     N/A     N/A
1C6     N/A     N/A     N/A
1CTL    N/A     N/A     N/A
```

The fields are described as follows:

Field	Description
Port	The port number.
Type	The port type (LAN or WAN)
RIF	The rate increase factor set for the port.
RDF	The rate decrease factor set for the port.

1.3.3 Resetting Default ABR Configurations

This command lets you reset the switch to the default ABR configurations. You must reboot the switch to reset all ABR related items to the default settings.

```
myswitch::debug abr> reset
To reset all the ABR related items to defaults, you must reboot the switch.
Continue [n]? y
```

1.4 Dump Commands

The **dump** commands are used to display the contents of internal data structures to check for consistency and correctness. Type**?** at the **dump** level to list these commands.

```
myswitch::debug dump> ?
atmroute>         atmstat>          callrecording>      cdb>
cem               connections>      dualscp>            fram>
hardware>         ipfilter          memory>             signalling>
utilities>        utilization>      version
```

NOTE

If nothing is printed to the screen after you issue a dump command, then there is no information available.

NOTE

Not all of the above commands are displayed on every platform. The **cem** command is only displayed on platforms supporting CEM network modules. The **fram** command is only displayed on platforms supporting *FramePlus*™ network modules. The **dualscp** command only displays on platforms supporting dual SCPs.

1.4.1 ATM Route Dump Commands

The commands listed under the **atmroute** root level, let you display ATM routing information. Type**?** at the **atmroute** level to list these commands.

```
myswitch::debug dump atmroute> ?
  defsum            ftpnni>           local             pmp
  pnni>             pol               ptab              spans>
  sctmr             scstats
```

1.4.1.1 Displaying ATM Route Default Summary Information

This command lets you display PNNI ATM route default summary policy information. Enter the following:

```
myswitch::debug dump atmroute> defsum [<domain>][<index>]
atmr_defsum_domain_dump: [domain 1] :: state ENABLED
Nodix = 1
Default Sum Policy 47:0:5:80:ff:e1:0:0:0:f2:0:0/80
End of ATMR Defsum Info for domain 1
```

1.4.1.2 *ForeThought* PNNI Dump Commands

The commands listed under the **ftpnni** level, let you display *ForeThought* PNNI ATM route information. Type **?** at the **ftpnni** level to list these commands.

```
myswitch::debug dump atmroute ftpnni> ?
  dtl                map                ptab
```

1.4.1.2.1 Displaying *ForeThought* PNNI DTLs

This command lets you display the Designated Transit Lists (DTLs). A DTL is a source route for the *ForeThought* PNNI router which specifies the preferred call routing for the SVC portion of a directed SPVC. Enter the following:

```
myswitch::debug dump atmroute ftpnni> dtl
```

1.4.1.2.2 Displaying the *ForeThought* PNNI Map Table

This command lets you display information from the *ForeThought* PNNI topology database. This command can be useful when you cannot route in an FT-PNNI peergroup. Enter the following:

```
myswitch::debug dump atmroute ftpnni> map [src |dst]
```

1.4.1.2.3 Displaying the *ForeThought* PNNI Prefix Table

This command lets you display reachability address prefixes that are imported from the *ForeThought PNNI routing table.* Enter the following:

```
myswitch::debug dump atmroute ftpnni> ptab
```

1.4.1.3 Displaying Local ATM Route Information

This command lets you display local ATM route information, which includes ILMI-registered addresses and static routes. This command is useful to help verify that a particular host's ILMI address registration was successful or to see if a configured static route is valid and being advertised. Enter the following:

```
myswitch::debug dump atmroute> local
Local Routes for Domain 1
Destination Address 47.000580ffe1000000f21a2cf0.0020480697b9.00
   adv_rte (e62480x) pte (0xe36638)
   adv_rte: port (0x100000) nodeix(0) ilmi
   Logport 0x100000 Valid   NON-VPCAP Mtag 0 Nodix 0
Destination Address 47.000580ffe1000000f21a2cf0.0020480697ba.00
   adv_rte (e84940x) pte (0xe36598)
   adv_rte: port (0x110000) nodeix(0) ilmi
   Logport 0x110000 Valid   NON-VPCAP Mtag 0 Nodix 0
Destination Address 47.000580ffe1000000f21a2cf0.0020480d0000.00
adv_rte (d88080x) pte (0xe36818)
   adv_rte: port (0xffffffff) nodeix(-1) ilmi
   Logport 0xffffffff Valid   VPCAP     Mtag 0 Nodix -1
Destination Address 47.000580ffe1000000f21a2cf0.0020481a3f9e.00
   adv_rte (e5a480x) pte (0xe36778)
   adv_rte: port (0x380000) nodeix(0) ilmi
   Logport 0x380000 Valid   NON-VPCAP Mtag 0 Nodix 0
```

NOTE

If a static route was configured on a port with no carrier by mistake, it would show up as an invalid entry in the output.

1.4.1.4 Displaying ATM Route Point-to-Multipoint Information

This command lets you display information about ATM route point-to-multipoint connections. Enter the following:

```
myswitch::debug dump atmroute> pmp [<port><cref>]
```

1.4.1.5 ATM Forum PNNI Dump Commands

The commands listed under the **pnni** level, let you display ATM Forum PNNI ATM route information. Type **?** at the **pnni** level to list these commands.

```
myswitch::debug dump atmroute pnni> ?
     interface          link               node               peer
     peergroup          prefix             svccrcc            ptab
     ptse               tdb                tdball             trans
```

1.4.1.5.1 Displaying PNNI Internal Reachability Address Information

This command lets you display the PNNI internal reachability address information. Enter the following:

```
myswitch::debug dump atmroute pnni> interface
itf(0x10000018) nodeix(0) aggr token(0) VPC capability(FALSE)
     flags(0x0) domain id(1) local routes validity(VALID)
     type(unknown) user/network type(network) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(511) vc depletion status(FALSE)
itf(0x10000019) nodeix(0) aggr token(0) VPC capability(FALSE)
     flags(0x0) domain id(1) local routes validity(VALID)
     type(unknown) user/network type(network) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(511) vc depletion status(FALSE)
itf(0x1000001a) nodeix(0) aggr token(0) VPC capability(FALSE)
     flags(0x0) domain id(1) local routes validity(INVALID)
     type(unknown) user/network type(network) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(511) vc depletion status(FALSE)
itf(0x1000001b) nodeix(0) aggr token(0) VPC capability(FALSE)
     flags(0x0) domain id(1) local routes validity(INVALID)
     type(unknown) user/network type(network) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(511) vc depletion status(FALSE)
itf(0x10000020) nodeix(1) aggr token(0) VPC capability(FALSE)
     flags(0x800) domain id(1) local routes validity(VALID)
     type(afpnni) user/network type(user) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(7167) vc depletion status(FALSE)
itf(0x10000021) nodeix(1) aggr token(0) VPC capability(FALSE)
     flags(0x800) domain id(1) local routes validity(VALID)
     type(afpnni) user/network type(user) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(7167) vc depletion status(FALSE)
itf(0x10000022) nodeix(1) aggr token(0) VPC capability(FALSE)
     flags(0x800) domain id(1) local routes validity(VALID)
     type(afpnni) user/network type(network) sig scope(vp)
     ftpnni link costs orig(100) term(0)
     vci range min(32) max(7167) vc depletion status(FALSE)
```

1.4.1.5.2 Displaying PNNI Link Information

This command lets you display information about all of the links attached to each node. Enter the following:

```
myswitch::debug dump atmroute pnni> link [index]
LINKS ATTACHED TO NODE INDEX 0
LINKS ATTACHED TO NODE INDEX 1
  (LinkID, VPI)=(8, 0) Rmt portID=0x1000001b State=2WAYIN
    Rmt nodeID=80:160:47.000580ffe1000000f21a0097.ff1a39e60001.00
    Hello intv=15000 (msec), rcvd=863, xmit=864
```

1.4.1.5.3 Displaying PNNI Node Information

This command lets you display information about each PNNI node. You must specify for which node index you want to display information. Enter the following:

```
myswitch::debug dump atmroute pnni> node [index]
NODE index: 1, domain: 1
  nodeid: 80:160:47.000580ffe100facefeed0000.ff1a2eae0001.00
  patma:  47.000580ffe100facefeed0000.ff1a2eae0001.00
  pgid:   80:47000580ffe1000000f2000000, level: 80, lowest: yes
  admin: UP       oper: UP       no. peers in exch/load: 0 Gband failures: 0
```

1.4.1.5.4 Displaying PNNI Peer Information

This command lets you display information about all of the peers (neighbors) that this node knows about. Enter the following:

```
myswitch::debug dump atmroute pnni> peer [index]
PEERS OF NODE INDEX 0
PEERS OF NODE INDEX 1
  Peer nodeID: 80:160:47.000580ffe1000000f21a0097.ff1a39e60001.00
    State: FULL  , #ports: 1, #reqs: 0, #acks: 0, #rexmts: 0
```

1.4.1.5.5 Displaying PNNI Peer Group Information

This command lets you display information about the members of a peer group. Given the nodeix of a node within the peer group, the command displays the PGID and the current peer group leader (PGL), as well as the leadership priority and preferred PGL of every member of that peer group. Enter the following:

```
myswitch::debug dump atmr pnni> peergroup <nodeix>
myswitch::debug dump atmr pnni> peergroup 2

------------------------------------------------------
PeerGroup ID     : 80:470005000000ae1e1e1e000000
Members of this peergroup
...NodeID: 80:88:47.0005000000ae1e1e1e1e0000.ff1a58640002.00
......Leadership Priority: 0
...NodeID: 80:88:47.0005000000ae1e1e1e2e0000.ff1c5e020002.00
......Leadership Priority: 0
...NodeID: 80:88:47.0005000000ae1e1e1e3e0000.ff1a57aa0002.00
......Leadership Priority: 0
...NodeID: 80:88:47.0005000000ae1e1e1e4e0000.ff1a57410002.00
......Leadership Priority: 0
------------------------------------------------------

myswitch::debug dump atmr pnni> peergroup 2

------------------------------------------------------
PeerGroup ID     : 88:470005000000ae1e1e1e2e0000
PeerGroup Leader : 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
Members of this peergroup
...NodeID: 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
......Leadership Priority: 105
......Preferred PGL 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
...NodeID: 88:160:47.0005000000ae1e1e1e2e0546.ff1c5ce40001.00
......Leadership Priority: 4
......Preferred PGL 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
...NodeID: 88:160:47.0005000000ae1e1e1e2e0545.ff1c5d9a0001.00
......Leadership Priority: 3
......Preferred PGL 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
...NodeID: 88:160:47.0005000000ae1e1e1e2e0544.ff1c5de40001.00
......Leadership Priority: 2
......Preferred PGL 88:160:47.0005000000ae1e1e1e2e0543.ff1c5e020001.00
------------------------------------------------------
```

1.4.1.5.6 Displaying PNNI Prefix Information

This command lets you display information about the prefixes of both ATM Forum PNNI exterior and internal reachability addresses that are currently being advertised by each one of the PNNI nodes. Exterior reachability addresses can be PNNI static routes (route address entries), addresses imported from a different node in the same domain, or inter-domain static routes. Internal reachability addresses can be ILMI-registered addresses or locally configured FT-PNNI static routes. Enter the following:

```
myswitch::debug dump atmr pnni> prefix
Pnni prfx table for nodix 1 (0x0x1d625b8)
Prfx info 0xef7bc, intp 0xef8a8, extp 0xef900, ignodes 0xef988
intpg 0xef958, extpg 0xef970, inth 0xef7f0, exth 0xef84c, timer 0x0
SG_Q
.Internal prefix ptsegs:
.PtseG 0xfbec4: Type IntP, PTSEId 0x50000000, ptseh 0x0x1d58798, len
2048, flags
0x0
..Deleted IG
..ScopeG 0xfb524: IG 0xfb504, scope 0, flags 0x0, sg_flags 0x10
...opaq_s 0, opaq_e 0, ptseg 0xfbec4, len 288, prfxh 0x1a6bc78, sysch 0x0
...RAIGH 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
...OPAQH
..ScopeG 0xfbe70: IG 0xfbe50, scope 0, flags 0x8000, sg_flags 0x10
...opaq_s 0, opaq_e 0, ptseg 0xfbec4, len 248, prfxh 0x1d58728, sysch 0x0
...RAIGH 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
...OPAQH
.Exterior prefix ptsegs:
.PtseG 0xf0c4c: Type ExtP, PTSEId 0x60000000, ptseh 0x0x1a6bc08, len
1024, flags
0x0
..Deleted IG
..ScopeG 0x1a738f4: IG 0x1a738d4, scope 0, flags 0x8000, sg_flags 0x10
...opaq_s 0, opaq_e 0, ptseg 0xf0c4c, len 268, prfxh 0x1a6bb98, sysch 0x0
...RAIGH 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
...OPAQH
.IG nodes:
.IGNode 0x1a727ec: type IntP, #opaq 0, #dups 0, Max_opaq 0
..opaqigs 0x0, minfo 0x0, foreinfo 0xf2388
..FOREInfo: area 0, scope 0, pnni_flags 0x0, pnni_scope 0
..OPAQ: (flags, scope, tlvh)
..IG_Q 0xfb504,
..IG: 0xfb504, aic 3, max_sg_len 288
...scopegs 0xfb524,
```

```
...Prefixes:
...1: c5.000500000000ae1e1e3e0550.000000000000.00/104
...2: c5.000500000000ae1e1e4e0550.000000000000.00/104
...3: c5.000500000000ae1e1e5e0550.000000000000.00/104
.IGNode 0xf2838: type IntP, #opaq 0, #dups 0, Max_opaq 0
..opaqigs 0x0, minfo 0x0, foreinfo 0xfbe3c
..FOREInfo: area 0, scope 0, pnni_flags 0x8000, pnni_scope 0
..OPAQ: (flags, scope, tlvh)
..IG_Q 0xfbe50,
..IG: 0xfbe50, aic 1, max_sg_len 248
...scopegs 0xfbe70,
...Prefixes:
...1: 47.000500000000ae1e1e3e0550.000000000000.00/104
.IGNode 0x1a74d30: type ExtP, #opaq 0, #dups 0, Max_opaq 0
..opaqigs 0x0, minfo 0x0, foreinfo 0xfdbd4
..FOREInfo: area 0, scope 0, pnni_flags 0x8000, pnni_scope 0
..OPAQ: (flags, scope, tlvh)
..IG_Q 0x1a738d4,
..IG: 0x1a738d4, aic 2, max_sg_len 268
...scopegs 0x1a738f4,
...Prefixes:
...1: d5.000500000000ae1e1e3e0550.000000000000.00/104
...2: e5.000500000000ae1e1e3e0550.000000000000.00/104
```

1.4.1.5.7 Displaying SVCC RCC Information

This command lets you display information about the PNNI SVCC RCC. It provides information such as whether or not the node is the initiator of the SVCC RCC, the state of the SVCC RCC, and the service category that is being used for the SVCC RCC. Enter the following:

```
myswitch::debug dump atmr pnni> svccrcc

LINKS ATTACHED TO NODE INDEX 0
LINKS ATTACHED TO NODE INDEX 1
LINKS ATTACHED TO NODE INDEX 2
(LinkID, VPI)=(65535, 4095)
Link Ptr : 0xfa3dc
Rmt portID=0xffffffff State=2WAYIN  Type=SVCCRCC link=0x0xfa3dc
Rmt nodeID=80:88:47.00050000000000ae1e2e0000.ff1a576f0002.00
Hello intv=15000 (msec), rcvd=359, xmit=361
Svcc_Rcc State = ACTIVE
Is_Initiator = FALSE
Curr_SVC_CAT = nrtVBR
```

1.4.1.5.8 Displaying PNNI Prefix Table Information

This command lets you display the PNNI prefix table. The prefix table contains information about all the reachability address prefixes that are currently being advertised by all of the nodes in the network as well as locally registered addresses such as ILMI registered addresses and static routes. This command is useful when the switch is unable to route to a given address. You can see if that address is being advertised by any node in the network. Enter the following:

```
myswitch::debug dump atmroute pnni> ptab
PREFIX TABLE: domain id=1
  flags: 0x1, pn_cnt: -1, cl_bits: 0x1
  sc_cnt: 50, sc_period: 5000, sc_bits: 0x0
  range: 00.000000000000000000000000.000000000000.00/0
  last:  00.000000000000000000000000.000000000000.00/-1
  Prefix: 47.000580ffe1000000f21a0091.000000000000.00/104
  Tstamp: 889542861 Path flags: 0x0 Level: 5 Proto: pnni     CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    pnni                5    5     0       0 int  1   907424
  Prefix: 47.000580ffe1000000f21a0095.000000000000.00/104
  Tstamp: 889542854 Path flags: 0x0 Level: 0 Proto: bogus    CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    pnni          L     5    5     0       0 int  1   885728
  Prefix: 47.000580ffe1000000f21a0095.0020481a2eb0.00/152
  Tstamp: 889542853 Path flags: 0x0 Level: 255 Proto: ilmi     CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    ilmi              255    0     0       0 int  0   882156
  Prefix: 47.000580ffe1000000f21a0097.000000000000.00/104
  Tstamp: 889542858 Path flags: 0x0 Level: 5 Proto: pnni     CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    pnni                5    5     0       0 int  1   899016
```

AMI Debug Commands

1.4.1.5.9 Displaying PTSE Information

This command parses the external form of a stored PTSE and displays formatted output. Enter the following:

```
myswitch::debug dump atmroute pnni> ptse <nodeix> <originating nodeid> <ptseid>
```

The parameters are defined as follows:

Parameter	Description
nodeix	The local node whose topology database you want to display. Only PTSEs from originating nodes that are at the same hierarchical level or higher as this nodeix are shown.
originating nodeid	Shows only PTSEs that are originated by the indicated nodeid.
ptseid	Shows only the PTSE that matches the indicated ptseid.

NOTE

All parameters are optional, but they must be supplied in the order shown (e.g., you cannot enter a ptseid without both a nodeix and an originating nodeid). If no arguments are given, this command dumps all PTSEs from all nodes in all topology databases. This generates a great deal of data, so you may want to follow the example shown here.

The following is a practical example for using this command:

1. First dump the topology database (TDB) as follows:

```
myswitch::> debug dump atmr pnni tdb
TDB of Nodix = 1
ORIGINATOR 72:80:47.000500000000ae1e1e000000.ff1a58640003.00
LGTH TYPE PTSE_ID    SEQN   XSUM   TTL  AGE   PR ER HNDL
ORIGINATOR 72:80:47.000500000000ae1e1e000000.ff1c5e020003.00
LGTH TYPE PTSE_ID    SEQN   XSUM   TTL  AGE   PR ER HNDL
68   97   0x        1 3      0x3452 3600 1046   0  1   0x3d3fb00
196  96   0x        7 4      0x15ce 3600 1038   0  1   0x3d3fa30
220  288  0x30000000 3      0xdf5b 3600 106    0  1   0x3d30700
56   224  0x50000000 3      0x453c 3600 1045   0  1   0x3d32068
152  256  0x60000000 7      0x85d3 3600 595    0  1   0x3d31f98
ORIGINATOR 72:88:47.000500000000ae1e1e3e0000.ff1a57aa0002.00
LGTH TYPE PTSE_ID    SEQN   XSUM   TTL  AGE   PR ER HNDL
```

```
68   97   0x        1 223    0x957a 3599 1119  0  1   0x3d3f9c8
196  96   0x        7 222    0x31f2 3599 1042  0  1   0x3d30a40
220  288  0x30000000 224    0x32ce 3599 592   0  1   0x3d30768
56   224  0x50000000 219    0x5924 3599 1118  0  1   0x3d30028
ORIGINATOR 80:88:47.000500000000ae1e1e1e0000.ff1a58640002.00
LGTH TYPE PTSE_ID    SEQN   XSUM   TTL  AGE   PR ER HNDL
68   97   0x        1 5      0x1bd1 3599 1144  0  1   0x3d2ff58
196  96   0x        7 5      0x6aca 3599 542   0  1   0x3d2fef0
420  289  0x20000001 2      0x9566 3599 1039  0  1   0x3d2c010
220  288  0x30000000 5      0x87dd 3599 670   0  1   0x3d330c4
56   224  0x50000000 3      0x921b 3599 1143  0  1   0x3d2f7b0
(output truncated to save space)
```

2. Decode the individual PTSEs as follows:

```
myswitch::> debug dump atmr pnni ptse 1
72:80:47.000500000000ae1e1e000000.ff1c5e020003.00 0x60000000

[PTSE IG (64) tags = 0000]
PTSE Type  : External Reachable ATM Address
PTSE Id    : 0x60000000       SeqNumber  : 7
Checksum   : 34259            RemLifeTm  : 3600
->[External Reachable ATM Address (256) tags = 0000]
Flags      : VPCa [0x8000]
PortId     : 0xfffffffe       Scope      : 64
Ail        : 20
01. 104:c5000500.000000ae.1e1e2e0a.bc000000.00000000
02. 104:c5000500.000000ae.1e1e2e0b.cd000000.00000000
03. 104:c5000500.000000ae.1e1e2e0c.de000000.00000000
04. 104:c5000500.000000ae.1e1e2e0d.ef000000.00000000
->[External Reachable ATM Address (256) tags = 0000]
Flags      : [0x0]
PortId     : 0xfffffffe       Scope      : 64
Ail        : 20
01. 104:c5000500.000000ae.1e1e2e0e.ee000000.00000000
-----------------------------------------------------------------

myswitch::> debug dump atmr pnni ptse 1
72:80:47.000500000000ae1e1e000000.ff1c5e020003.00 0x30000000

[PTSE IG (64) tags = 0000]
PTSE Type  : Horizontal Links IG
PTSE Id    : 0x30000000       SeqNumber  : 3
```

```
Checksum   : 57179           RemLifeTm  : 3600
->[Horizontal Links IG (288) tags = 0000]
Flags      : VPCa [0x8000]
RmtId : 72:88:47.000500000000ae1e1e3e0000.ff1a57aa0002.00
RemotePort : 0x30000000      LocalPort  : 0x30000000
AggToken   : 0
--->[Outgoing Resource Availability (128) tags = 0000]
Flags      : CBR [0x8000]
AdmnWeight : 5040
MCR        : 1412830         ACR        : 1411990
CTD        : 100021          CDV        : 182
CLP (0)    : 8               CLP (0+1)  : 8
(output truncated to save space)
```

1.4.1.5.10 Displaying PNNI Topology Database Information

This command lets you show PNNI topology database (TDB) information. Enter the following:

```
myswitch::debug dump atmroute pnni> tdb [index][advanced]
 TDB of Nodix = 1
ORIGINATOR 80:160:47.000580ffe1000000f21a0091.ff1a33ff0001.00
LGTH TYPE PTSE_ID    SEQN   XSUM  TTL  AGE   PR ER HNDL
68   97   0x       1 8      0xe282 3598 1550  0  0  0x   dd508
220  288  0x10000008 8      0x87a2 3598 1535  0  0  0x   dc540
56   224  0x50000000 9      0xe816 3598 1100  0  0  0x   dd6a8
ORIGINATOR 80:160:47.000580ffe1000000f21a0095.ff1a2eb00001.00
LGTH TYPE PTSE_ID    SEQN   XSUM  TTL  AGE   PR ER HNDL
68   97   0x       1 9      0x788c 3600 198   0  0  0x   d5be8
220  288  0x10000008 8      0x60ef 3600 1993  0  0  0x   dad48
56   224  0x50000000 9      0x3318 3600 648   0  0  0x   c09c0
ORIGINATOR 80:160:47.000580ffe1000000f21a0097.ff1a39e60001.00
LGTH TYPE PTSE_ID    SEQN   XSUM  TTL  AGE   PR ER HNDL
68   97   0x       1 7      0x878  3599 1099  0  0  0x   dab40
220  288  0x10000000 8      0x87aa 3599 190   0  0  0x   dcd0c
220  288  0x1000001b 8      0x60dc 3599 1092  0  0  0x   dbaa0
56   224  0x50000000 9      0xfb0a 3599 1099  0  0  0x   db5b8
```

1.4.1.5.11 Displaying All PNNI Topology Database Information

This command lets you display all topology database (TDB) information after individual PTSEs and the containing IGs have been parsed and digested into the internal data structures. Enter the following:

```
myswitch::debug dump atmroute pnni> tdball [index][advanced]
```

1.4.1.5.12 Displaying the Prefix Table Entries Added by PNNI

This command lets you display the prefix table entries that were added by PNNI. Enter the following:

```
myswitch::debug dump atmroute pnni> trans
Extp Transactions in Domain 1
Trans ID 0xea1908, Scope 0, Src Area 0
Prefix 47.000580ffe100facefeed0000.000000000000.00/104, Flags 0x2
```

1.4.1.6 Displaying ATM Route Policy Information

This command lets you display PNNI policy information. A policy allows you to impose rules on how a node propagates to its peer group information that was learned from another node in the same domain. This command is useful to see if a configured policy is active. Enter the following:

```
myswitch::debug dump atmroute> pol [<domain>[<index>]
Policy table for node index: 1
  Prot id: 1, Flags: 0, Pol_cnt: 2, Rechk_cnt: 0
  Area: 8, Level: 8, cl_id: 1, Max_cback: 50, Chk_int: 1000
  Policy node, 00.000000000000000000000000.000000000000.00/0
   flags: INT|EXT|ADV, scope: 0, src_area: 0x0, met_tag: 0, t_stamp: 0 nodix 1
  Policy node, 47.000580ffe100facefeed0000.000000000000.00/104
   flags: ACT|INT|AGG, scope: 0, src_area: 0x0, met_tag: 0, t_stamp: 0 nodix 1
Policy table for FTPNNI node:
  Prot id: 65535, Flags: 1073741824, Pol_cnt: 2, Rechk_cnt: 0
  Area: 4, Level: 4, cl_id: 0, Max_cback: 50, Chk_int: 1000
  Policy node, 00.000000000000000000000000.000000000000.00/0
   flags: INT|EXT|ADV, scope: 0, src_area: 0x0, met_tag: 0, t_stamp: 0 nodix 65535
  Policy node, 47.000580ffe1000000f2000000.000000000000.00/80
flags: INT|EXT|DFL|AGG, scope: 0, src_area: 0x0, met_tag: 0, t_stamp: 0 nodix 65535
```

1.4.1.7 Displaying ATM Route Prefix Table Information

This command lets you display the ATM route prefix table, which consists of prefix nodes. There are prefix table entries (PTEs) associated with each prefix node. Enter the following:

```
myswitch::debug dump atmroute> ptab [<domain>[<index>]
PREFIX TABLE: domain id=1
  flags: 0x1, pn_cnt: -1, cl_bits: 0x1
  sc_cnt: 50, sc_period: 5000, sc_bits: 0x0
  range: 00.000000000000000000000000.000000000000.00/0
  last:  00.000000000000000000000000.000000000000.00/-1
  Prefix: 47.000580ffe100facefeed0000.000000000000.00/104
  Tstamp: 870104544 Path flags: 0x0 Level: 0 Proto: bogus    CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    pnni          L     8    8     0       0 int  1   15286360
  Prefix: 47.000580ffe100facefeed0000.0020481a2eae.00/152
  Tstamp: 870104536 Path flags: 0x0 Level: 255 Proto: ilmi     CL bits: 0x0
    PROTO    PFLAGS LEVEL AREA SCOPE SR-AREA TYPE PID PHNDL
    ilmi              255    0     0       0 int  0   15348392
```

1.4.1.8 SPANS ATM Route Dump Command

The command under the **spans** level, lets you display the SPANS topology of the ATM network of which this switch is a part. Type **?** at the **spans** level to list the command.

```
myswitch::debug dump atmroute spans> ?
  map
```

1.4.1.8.1 Displaying SPANS ATM Routing Information

This command displays the SPANS routing information of the ATM network of which this switch is a part. Each entry in this table is a link in the network between a given source and a given destination. Some of the entries (the first four in this example) are used to advertise group membership. This command is useful to check and see if all links in the network show up in this output and to see if a particular remote switch in the network is reachable. Enter the following:

```
myswitch::debug dump atmroute spans> map
1: f21a39e6.00.0->f21a33ff.08.0  598682 kbps 4 freshness ZPD -1: SPD -1: OPD -1: VD 0: LOCAL
2: f21a2eb0.08.0->f21a39e6.27.0  40346 kbps  2 freshness ZPD -1: SPD -1: OPD -1: VD 0: LOCAL
3: f21a33ff.08.0->f21a39e6.00.0  598682 kbps 2 freshness ZPD -1: SPD -1: OPD -1: VD 0: LOCAL
4: f21a39e6.27.0->f21a2eb0.08.0  40346 kbps  0 freshness ZPD -1: SPD -1: OPD -1: VD 0: LOCAL
```

1.4.2 Displaying Scheduler Timer List

This command lets you display the scheduler timer list. Enter the following:

```
myswitch::debug dump atmroute> sctmr
  pnni_sch_hello                  6552  0xeebe8    1   892729286.816340
  pnni_sch_background             500   0xe6efc    0   892729277.316500
  pnni_sch_hello                  1439  0xedb34    1   892729289.316440
  pnni_sch_hello                  2066  0xea374    1   892729289.1809140
  pnni_sch_ptse_refresh           37752 0xeecdc    0   892729455.817120
  pnni_sch_hello_inact            26691 0xed98c    0   892729357.368680
  pnni_sch_hello_inact            2030  0xed9c0    0   892729355.338680
  pnni_sch_hello_inact            4385  0xed9f4    0   892729350.953640
  pnni_sch_ptse_refresh           417799 0xeed8c    0   892729907.316460
  pnni_sch_ptse_refresh           364626 0xed33c    0   892730255.316020
  pnni_sch_ptse_refresh           531149 0xebd24    0   892730737.316080
  pnni_sch_ptse_refresh           376529 0xe9774    0   892731046.819260
Printing FT-PNNI High Priority Timer Queue
   Queue empty
Printing FT-PNNI Low Priority Timer Queue
   Queue empty
```

1.4.3 Displaying Scheduler Statistics

This command lets you display the scheduler statistics. Enter the following:

```
myswitch::debug dump atmroute> scstats
   ImmPri   HighPri               LowPri
Ri Received Received Dropped QLen Received Dropped QLen
0  2789     830      0       0    7        0       0
Process Stats
Process Name          Events
```

1.4.4 AAL Statistics Dump Commands

The commands under the **atmstat** root level, let you display AAL statistics. Type **?** at the **atmstat** level to list these commands.

```
myswitch::debug dump atmstat> ?
  aal4                aal5                all
```

1.4.4.1 Displaying AAL4 Statistics

This command lets you display AAL4 statistics. Enter the following:

```
myswitch::debug dump atmstat> aal4
AAL4 statistics:
         Output                Input                      Errors
     Cells   CS-PDUs      Cells   CS-PDUs    CSProto Pay-CRC SARProto   Drops
  21865515   5960054   19308593   4703302          0       0        0       0
```

1.4.4.2 Displaying AAL5 Statistics

This command lets you display AAL5 statistics. Enter the following:

```
myswitch::debug dump atmstat> aal5
AAL5 statistics:
         Output                Input                      Errors
     Cells   CS-PDUs      Cells   CS-PDUs    CSProto Pay-CRC Congestn   Drops
       321       208        368       166          0       0        0       0
```

1.4.4.3 Displaying All AAL Statistics

This command lets you display all AAL statistics. Enter the following:

```
myswitch::debug dump atmstat> all
PHY/ATM/AAL statistics:
         Output                Input                            Errors
       ATM      AAL*        ATM      AAL*     4B5B     4B5B      ATM     AAL*     AAL*
     Cells   CS-PDUs      Cells   CS-PDUs Framing Hdr-CRC VPI/VCI Pay-CRC    Proto
      3544      1261       2840       973        0       0       0       0        0
```

1.4.5 Call Recording Dump Commands

The commands under the **callrecording** root level, let you display call recording information. Type **?** at the **callrecording** level to list these commands.

```
myswitch::debug dump callrecording> ?
  calls              check              info
```

1.4.5.1 Displaying Call Recording Call Information

This command lets you display call recording call information. Enter the following:

```
myswitch::debug dump callrecording> calls
CRM context is absent - CallRecording may be OFF
```

1.4.5.2 Displaying the State of Call Recording Calls

This command lets you display the state of call recording calls. Enter the following:

```
myswitch::debug dump callrecording> check
CRM context is absent - CallRecording may be OFF
```

1.4.5.3 Displaying Call Recording Module Information

This command lets you display call recording module information. Enter the following:

```
myswitch::debug dump callrecording> info
CRM context is absent - CallRecording may be OFF
```

1.4.6 CDB Dump Commands

The commands under the **cdb** root level, let you display configuration database (CDB) information. Type **?** at the **cdb** level to list these commands.

```
myswitch::debug dump cdb> ?
  show               size
```

1.4.6.1 Displaying CDB Information

This command lets you display all of the CDB's entries. The CDB contains all of the switch configuration information that is persists across reboots. There are three kinds of configurations: hardware, software, and system configurations.

Hardware configuration pertains to the configuration of physical devices on the switch, which includes the environmental sensors/monitors and port configurations for interfacing to WAN services. Software configuration pertains to the switch software configuration, which includes paths, channels, and signalling configuration. System configuration controls the setup of the switch itself; e.g., the IP address, etc.

This command displays all the entries by listing each directory and the path to the entry. The value type (Integer, String, etc.) is indicated. This command is useful for quickly determining the exact configuration of a switch. Enter the following:

```
myswitch::debug dump cdb> show
CDB: Root: (Directory)
CDB: Root:hardware: (Directory)
CDB: Root:hardware:asx_switch: (Directory)
CDB: Root:hardware:asx_switch:board0: (Directory)
CDB: Root:hardware:asx_switch:board0:clockScalingFactor: 1, 00000001 (Integer)
.
.
```

NOTE Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.6.2 Displaying the CDB Size

This command lets you display the CDB size. Enter the following:

```
myswitch::debug dump cdb> size
CDB size = 7998 bytes
```

1.4.7 Displaying Circuit Emulation Services Information

This command lets you display information about the current state of the potentially 128 connections on the Circuit Emulation Services (CES) network modules that are installed in the switch fabric. The **cem** command is only displayed on the platforms that can support Circuit Emulation (CEM) network modules. Enter the following:

```
myswitch::debug dump> cem
tTelnetAmi[X]:debug:Connection 01   ConnId1   IfIndex 24  Biscuit 2   pNm0xe80248
tTelnetAmi[X]:debug:Connection 02   ConnId2   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 03   ConnId3   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 04   ConnId4   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 05   ConnId5   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 06   ConnId6   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 07   ConnId7   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 08   ConnId8   IfIndex 0   Biscuit 0   pNm0xe80248
tTelnetAmi[X]:debug:Connection 09   ConnId9   IfIndex 0   Biscuit 0   pNm0xe80248
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

The fields in this display are defined as follows:

Field	Description
Connection	These are identified by the number 1 through 27. In the example above, 0 indicates the network module slot.
ConnID	Indicates the connection ID.
IfIndex	Indicates the external interface ID of the connection.
Biscuit	Indicates the internal identifier
pNm	Indicates the network module the connection is currently running on.

1.4.8 Connections Dump Commands

The commands under the **connections** root level, let you display information about the connections on the switch. Type **?** at the **connections** level to list these commands.

```
myswitch::debug dump connections> ?
  vcl                 vcltm               vpl                 vpltm
  vpm
```

1.4.8.1 Displaying Virtual Channel Link Information

This command lets you display virtual channel link information. Enter the following:

```
myswitch::debug dump connections> vcl
vcl: IN     0|000|3      ->    0|000|3      vcindex: 00401   cells: 0
vcl: IN     0|000|4      ->    0|000|4      vcindex: 00402   cells: 0
vcl: IN     0|000|14     ->   56|000|36     vcindex: 0040c   cells: 0
vcl: IN     0|000|15     ->   56|000|35     vcindex: 0040d   cells: 0
vcl used/reserved = 4/479
.
.
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.8.2 Displaying Virtual Channel Traffic Management Information

This command lets you display virtual channel traffic management information. Enter the following:

```
myswitch::debug dump connections> vcltm
vcl: IN    8|000|3    ->   8|000|3      GCRApol    (PCR=1   SCR=-1  MBS=-1 CDVT=250)
vcl: IN    8|000|4    ->   8|000|4      GCRApol    (PCR=1   SCR=-1  MBS=-1 CDVT=250)
vcl: IN    8|000|5    ->  56|000|37                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    8|000|14   ->  56|000|36                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    8|000|15   ->  56|000|35                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    8|000|16   ->  56|000|38                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl used/reserved = 6/479

vcl: IN    9|000|3    ->   9|000|3      GCRApol    (PCR=1   SCR=-1  MBS=-1 CDVT=250)
vcl: IN    9|000|4    ->   9|000|4      GCRApol    (PCR=1   SCR=-1  MBS=-1 CDVT=250)
vcl: IN    9|000|5    ->  56|000|41                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    9|000|14   ->  56|000|40                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    9|000|15   ->  56|000|39                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl: IN    9|000|16   ->  56|000|42                (PCR=-1  SCR=-1  MBS=-1 CDVT=250)
vcl used/reserved = 6/479
        .
        .
        .
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.8.3 Displaying Virtual Path Link Information

This command lets you display virtual path link information. Enter the following:

```
myswitch::debug dump connections> vpl
vpl:  IN     0|0      vpindex: 00000000   vcindex: 000003fe   cells: 5481198
vpl:  IN     1|0      vpindex: 00000400   vcindex: 000005fd   cells: 0
vpl:  IN     2|0      vpindex: 00000800   vcindex: 000007fc   cells: 0
vpl:  IN     3|0      vpindex: 00000c00   vcindex: 000009fb   cells: 0
vpl:  IN    33|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl:  IN    34|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl:  IN    35|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl:  IN    56|0      vpindex: 00007000   vcindex: ffffffff   cells: 176230120
vpl:  IN    56|1      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl: OUT     0|0      vpindex: 00000000   vcindex: 00000201   cells: 0
vpl: OUT     1|0      vpindex: 00000400   vcindex: 00000400   cells: 0
vpl: OUT     2|0      vpindex: 00000800   vcindex: 000005ff   cells: 0
vpl: OUT     3|0      vpindex: 00000c00   vcindex: 000007fe   cells: 0
vpl: OUT    33|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl: OUT    34|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl: OUT    35|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
vpl: OUT    56|0      vpindex: ffffffff   vcindex: ffffffff   cells: 0
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.8.4 Displaying Virtual Path Traffic Management Information

This command lets you display virtual path traffic management information. Enter the following:

```
myswitch::debug dump connections> vpltm
     AAL5 TAG GCRApol PPpol UBRtag  (PCR=-1    SCR=-1    MBS=-1    CDVT=-1   )
               PktDisc SCD AltCLP rr+rc (-1 cps, group 127)
```

1.4.8.5 Displaying Virtual Path Multiplexer Information

This command lets you display virtual path multiplexer information. Enter the following:

```
myswitch::debug dump connections> vpm
vpm:  IN    0|0     [  1 ->  511]   cells: 5482480
vpm:  IN    1|0     [  1 ->  511]   cells: 0
vpm:  IN    2|0     [  1 ->  511]   cells: 0
vpm:  IN    3|0     [  1 ->  511]   cells: 0
vpm:  IN   33|0     [  0 -> 7167]   cells: 0
vpm:  IN   34|0     [  0 -> 7167]   cells: 0
vpm:  IN   35|0     [  0 -> 7167]   cells: 0
vpm:  IN   56|0     [  1 -> 1023]   cells: 176279944
vpm: OUT    0|0     [  1 ->  511]   cells: 0
vpm: OUT    1|0     [  1 ->  511]   cells: 0
vpm: OUT    2|0     [  1 ->  511]   cells: 0
vpm: OUT    3|0     [  1 ->  511]   cells: 0
vpm: OUT   33|0     [  0 -> 7167]   cells: 0
vpm: OUT   34|0     [  0 -> 7167]   cells: 0
vpm: OUT   35|0     [  0 -> 7167]   cells: 0
vpm: OUT   56|0     [  1 -> 1023]   cells: 0
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.9 Dual SCP Dump Commands

The commands listed under the **dualscp** root level, let you display information about dual SCPs. These commands are applicable only if you have dual SCPs configured. The **dualscp** command is only displayed on the platforms that can support dual SCP functionality. Type **?** at the **dualscp** level to list these commands.

```
myswitch::debug dump dualscp> ?
  synclist           mailbox
```

1.4.9.1 Displaying Dual SCP Synchronization Information

This command lets you display file synchronization information between dual SCPs. It displays which files, if any, you have configured using **conf system dualscp sync** to be synchronized between the the two SCPS. Enter the following:

```
myswitch::debug dump dualscp> synclist
Sync list is empty.
```

1.4.9.2 Displaying Dual SCP Mailbox Information

This command lets you display dual SCP mailbox information. Enter the following:

```
myswitch::debug dump dualscp> mailbox
```

1.4.10 FRAM Dump Commands

The commands listed under the **fram** root level, let you display configuration information for the Frame/FUNI network module. These commands are applicable only if you have a *FramePlus* network module installed in your switch. The **fram** command is only displayed on the platforms that can support *FramePlus* network module. Type **?** at the **fram** level to list these commands.

```
myswitch::debug dump fram> ?
  nmconf              cdb>                aal5dump            funi>
```

1.4.10.1 Displaying Frame Relay Network Module Configuration Information

This command lets you display configuration attributes for all *FramePlus* network modules present within the fabric. Enter the following:

```
myswitch::debug dump fram> nmconf
-FRAM netmod:-----board 3, netmod 0 --------
EpdPpdBufferProportion:     1
Epdclp1HighPrio:            37
Epdclp0HighPrio:            62
Ppdclp1HighPrio:            50
Epdclp1LowPrio:             37
Epdclp0LowPrio:             62
Ppdclp1LowPrio:             50
OamF5Supervision:           1
OamF5AISRxPeriod:           3
OamF5AISTxPeriod:           1
OamF5RDIRxPeriod:           3
OamF5RDITxPeriod:           1
ApplSwRelease: 0.0.8
BootSwRelease: 0.1.5
SerialNumber: 00000007
Application:             FR/ATM
OosLED:                     1
MaxSigPathsPerPort:         0
StatsEnabledTimestamp:      890150612
StatsMonitor:               disabled
```

1.4.10.2 Frame Relay CDB Dump Commands

The commands listed under the **cdb** level, let you display *FramePlus* network module related information currently stored within the CDB. Type **?** at the **cdb** level to list these commands. For more information about each command, type **inmcdbhelp** to display the help screen.

```
myswitch::debug dump fram cdb> ?
  inmcdbverbose      inmcdbget          inmcdbgetnext      inmcdbhelp
```

1.4.10.2.1 Expanding or Condensing Output Information

This command lets you expand or condense the output format of other *FramePlus* related commands. The expanded output format (verbose mode) reflects data structure objects. Enter the following:

```
localhost::debug dump fram cdb> inmcdverbose (on | off)
```

AMI Debug Commands

1.4.10.2.2 Displaying Frame Relay Information Stored in the CDB

This command lets you view selected information that is currently stored within the CDB. Enter the following:

```
myswitch::debug dump fram cdb> inmcdbget <type> <id> <datamask>
```

1.4.10.2.3 Displaying the Next CDB Entry

This command lets you view the next CDB entry currently stored within the CDB. Note that the information displayed is the CDB entry immediately after the selected object. Enter the following:

```
myswitch::debug dump fram cdb> inmcdbgetnext <type> <id> <datamask>
```

1.4.10.2.4 Displaying Help

This command displays the help menu and provides information on how to execute and invoke the identified commands. Enter the following:

```
myswitch::debug dump fram cdb> inmcdbhelp
inmcdbverbose on|off
inmcdbget     <type> <id> <datamask>
inmcdbgetnext <type> <id> <datamask>
inmcdbhelp    print out this help message

<type> is one of FRF8|FUNI|Gen|RE|EPPD|Service|Netmod|Port|Conn
<id> - is of the form B:N:P:S:C -us only the ones appropriate
       for the selected type
<datamask> - n octetstring representing the data to be  retrieved
, the value -1 will get all the data
```

1.4.10.3 Displaying Frame Relay AAL5 Statistics

This command lets you display selected service related aal5 statistics. Enter the following:

```
       myswitch::debug dump fram> aal5dump <board>
[<netmod>][<service_fabric_ifindex>][<interval>]
```

1.4.10.4 FUNI Service and Connection Dump Commands

The commands listed under the **funi** level, let you display FUNI service and FUNI connection related information. Type **?** at the **funi** level to list these commands.

```
myswitch::debug dump fram funi> ?
  service            conn
```

1.4.10.4.1 Displaying FUNI Service Configuration Information

This command lets you display FUNI service configuration information for all FUNI services supported by the associated fabric. Enter the following:

```
myswitch::debug dump fram funi> service
IfIndex: 29
fabIfindex: 24
sid: 0
timeslotBitMap: 1
adminStatus: 1
operStatus: 2
serviceIfType: 106
inBwAllocated: 0
outBwAllocated: 0
profileServiceIndex: 0
statsMonitor: 2
statsEnabledTimestamp:890755227
serviceTrapSupport: 1
serviceName:
IfEstablishedPvccs: 0
IfEstablishedSvccs: 0
profileFuniIndex: 0
funiIfExtSigStatus: 2
NeighborIpAddress: 0.0.0.0
bundled_vp_splay keys:0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
```

AMI Debug Commands

1.4.10.4.2 Displaying FUNI Connection Configuration Information

This command lets you display FUNI connection configuration information for all FUNI connections supported by the associated fabric. Enter the following:

```
myswitch::debug dump fram funi> conn
funi_conn_index: {29, 0, 59}
cid: 0
connFabricServiceIfIndex: 24
connFabricVpi: 0
connFabricVci: 59
connRowStatus: 1
connAdminStatus: 1
connOperStatus: 2
connName:
profileEpdPpdIndex: 0_
```

1.4.11 Hardware Dump Commands

The commands listed under the **hardware** root level, let you display hardware information. Type **?** at the **hardware** level to list these commands.

```
myswitch::debug dump hardware> ?
  fabric>            netmod>            pams               timing
```

1.4.11.1 Fabric Dump Commands

The commands listed under the **fabric** level, let you display information about the switch fabric. Type **?** at the **fabric** level to list these commands.

```
myswitch::debug dump hardware fabric> ?
  lookup             multicast          oam                qca
```

1.4.11.1.1 Displaying the Lookup ASIC State

This command lets you display information about the state of the lookup ASIC, which is only present on an *ASX*-1000, *ASX*-1200, or *TNX*-1100 switch. This ASIC translates from internal connection IDs (used across the backplane) to external VPI/VCIs (used on the network modules). The first field is the connection ID that is being translated. The first part is the board that allocated the connection ID (always the ingress board). The next field is the pseudo-VCI. Together, these two parts identify a connection on the switch board.

The next field is the output route mask, which shows the ports where the connection is going. The other fields give the port/VPI of the connection, indicate if it is a terminating (term) or through path, show the type of traffic on the connection (UBR/ABR/VBR/CBR), and indicate if it is a unicast (ucast) or multicast (mcast) connection. Enter the following:

```
myswitch::debug dump hardware fabric> lookup
lookup1000: lkup @ 40004000
lookup1000:  ctrl/stat: 0000000d
lookup1000:    invalid: 0000002a
lookup1000: invalid rw: 00000000
  lkup 000e:   0,000e  ->  56|4095|0     c1fff  q0  w1    mcast  term
  lkup 000e:   0,000e  ->   3|1023|0     c1fff  q0  w1    mcast  term
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.11.1.2 Displaying Multicast and Backplane Information

This command lets you display multicast and backplane information. Enter the following:

```
myswitch::debug dump hardware fabric> multi
rt_dump: route: rt=cdbbc, head_order=e4e28, head_free=e4eb8
rtes_dump: route order: rtes=e4e28, low=0, high=1022, prev_order=0, next_order=cdac4,
prev_free=0, next_free=0, isFree=n
rtes_dump: route order: rtes=cdac4, low=1023, high=1533, prev_order=e4e28,
next_order=e4e4c, prev_free=0, next_free=0, isFree=n
rtes_dump: route order: rtes=e4e4c, low=1534, high=2044, prev_order=cdac4,
next_order=e4e70, prev_free=0, next_free=0, isFree=n
rtes_dump: route order: rtes=e4e70, low=2045, high=2555, prev_order=e4e4c,
next_order=e4e94, prev_free=0, next_free=0, isFree=n
rtes_dump: route free: rtes=e4eb8, low=3067, high=32767, prev_order=e4e94, next_order=0,
prev_free=0, next_free=0, isFree=y
alloc_shmem_mcast:     3    4
alloc_vcl_cid_mcast:    14
alloc_vcl_cid_local:    32   33   34   35   36   37   38   39   40   41   42   43   44
45   46   47   48   49   50   51   52   53   54
 55   56   57   58   59   60   61   62   63
alloc_vcl_cid_local:    64   65   66   67   68   69   70   71   72   73   76
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.11.1.3 Displaying OAM Information

This command lets you display OAM cell generation information. Enter the following:

```
myswitch::debug dump hardware fabric> oam
F4 OAM VPI = 1
F5 OAM VPI = 0
       VCI = 55
0 unidentified OAM cells received
        0 F4 (VP) AIS cells transmitted
        0 F4 (VP) RDI cells transmitted
        0 F4 (VP) LOOPBACK cells transmitted
        0 F5 (VC) AIS cells transmitted
        0 F5 (VC) RDI cells transmitted
        0 F5 (VC) LOOPBACK cells transmitted
Last fault management cycle began at THU JAN 01 00:00:00 1970
and required 0.000 seconds
```

1.4.11.1.4 Displaying Queue Control ASIC Information

This command lets you display queue control ASIC information about all five queue control ASICS. Enter the following:

```
myswitch::debug dump hardware fabric> qca
Queue Control ASIC 0
fs1000c: @ addr 40020000
fs1000c: ctrl reg:  00000000
fs1000c: 0: CIBOT:      0003
fs1000c: 0: CIBXT:      0f00
fs1000c: 0: REJ_CLP_T:  0003
fs1000c: 0: MIN_Q_SZ:   0000
fs1000c: 0: current count:  0000
fs1000c: 0: lost count:     0fff
fs1000c: 0: max count:      0fff
fs1000c: 1: CIBOT:      0000
fs1000c: 1: CIBXT:      0f00
fs1000c: 1: REJ_CLP_T:  0000
fs1000c: 1: MIN_Q_SZ:   0000
fs1000c: 1: current count:  0000
fs1000c: 1: lost count:     0000
fs1000c: 1: max count:      0000
fs1000c: 2: CIBOT:      0003
fs1000c: 2: CIBXT:      0f00
fs1000c: 2: REJ_CLP_T:  0003
fs1000c: 2: MIN_Q_SZ:   0000
fs1000c: 2: current count:  0000
fs1000c: 2: lost count:     0fff
fs1000c: 2: max count:      0fff
fs1000c: 3: CIBOT:      0000
fs1000c: 3: CIBXT:      0f00
fs1000c: 3: REJ_CLP_T:  0000
fs1000c: 3: MIN_Q_SZ:   0000
fs1000c: 3: current count:  0000
fs1000c: 3: lost count:     0000
fs1000c: 3: max count:      0000
.
.
.
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.11.2 Network Module Dump Commands

The commands listed under the **netmod** level, let you display network module information. Type **?** at the **netmod** level to list these commands.

```
myswitch::debug dump hardware netmod> ?
  shmem              shtable
```

1.4.11.2.1 Displaying Shared Memory Information

This command lets you display the hardware contents of the connection tables on the network module for the connections. You must specify for which network module you want to display information. Enter the following:

```
myswitch::debug dump hardware netmod> shmem (a | b | c | d)
myswitch::debug dump hardware netmod> shmem b
SM_MCR:          00000000
SM_MSR:          00000030
SM_MEM_AMT:      000022e0
SM_AAL5_RJT:     00001f64
SM_VPI_TBL:      0000003f
SM_VCI_TBL:      0000003c
SM_VI_LISTS:     00000070
SM_CELLHEAD_MEM:  00000030
SM_UCAST_CONN_TBL: 00000038
SM_MCAST_CONN_TBL: 00000036
SM_NUM_MCAST:     00000010
SM_INV_LOOKUP_LSW: 000000f0
SM_INV_LOOKUP_MSW: 00008000
SM_MEM_CELLCOUNT:  00000009
SM_MEM_FREE_LIST:  00000003
SM_INV_LOOKUP_CNT: 00000000
port 0:  SM_PORT_CR: 00000003
port 0:  prio 0:
port 0:  prio 0:  SM_CIBOT:        00000040
port 0:  prio 0:  SM_CIBXT:        00000001
port 0:  prio 0:  SM_REJ_CLP_T:    00000100
port 0:  prio 0:  SM_MIN_QUE_SZ:   00000100
.
```

On an *ASX*-4000, the following parameter is displayed:

```
myswitch::debug dump hardware netmod> shmem <linknumber>
```

On an *ASX*-4000, a link number must be specified since a port card contains a variable number of connection tables. The link number is the software port number assigned to a specific port. This link number is what the enterprise Management Information Base (MIB) refers to for ports on port cards. On an *ASX*-4000, link numbers range from 0 to 1024 where link 0 refers to 1A1 (port card 1, interface group A, port 1) and link number 1024 refers to the control port (5CTL). There are 64 links reserved for each interface group on a port card. For example, link 64 refers to 1B1, link 128 refers to 1C1, link 192 refers to 1D1 and so on. See Section A.4 in Appendix A for a listing of hardware port addressing numbers used by the MIBs to reference ports on an *ASX*-4000.

For example, to display the hardware contents of the connection tables for 1A6 (port card 1, interface group A, port 6), you would enter the following:

```
myswitch::debug dump hardware netmod> shmem 5
```

1.4.11.2.2 Displaying the Shared Memory VCI Table

This command lets you print the routing table that is maintained in the software for the connections that exit through a particular network module. You must specify for which network module you want to display the table. Enter the following:

```
myswitch::debug dump hardware netmod> shtable (a | b | c | d)
myswitch::debug dump hardware netmod> shtable b
shmem_dump_tables:
rt_dump: vctable: rt = eb9950
rt_dump:  free: rtes = eb9964, low = 2558, high = 12287
rt_dump: alloc: rtes = ebafb0, low = 2047, high = 2557
rt_dump: alloc: rtes = ebae28, low = 1536, high = 2046
rt_dump: alloc: rtes = ebaca0, low = 1025, high = 1535
rt_dump: alloc: rtes = ebab18, low = 514, high = 1024
rt_dump: alloc: rtes = eb9978, low = 0, high = 513
uni low:    32   64   96  128  160  192  224  256
uni high:   288  320  352  384
multi low:    96
VPIVCI bits:     0    1    2    3
```

On an ASX-4000, the following parameter is displayed:

```
myswitch::debug dump hardware netmod> shtable <linknumber>
```


AMI Debug Commands

On an *ASX*-4000, the link number must be specified since a port card contains a variable number of routing tables. The link number is the software port number assigned to a specific port. This link number is what the enterprise Management Information Base (MIB) refers to for ports on port cards. On an *ASX*-4000, link numbers range from 0 to 1024 where link 0 refers to 1A1 (port card 1, interface group A, port 1) and link number 1024 refers to the control port (5CTL). There are 64 links reserved for each interface group on a port card. For example, link 64 refers to 1B1, link 128 refers to 1C1, link 192 refers to 1D1 and so on. See Section A.4 in Appendix A for a listing of hardware port addressing numbers used by the MIBs to reference ports on an *ASX*-4000.

For example, to display the routing table for 2D3 (port card 2, interface group D, port 3), you would enter the following link number:

```
myswitch::debug dump hardware netmod> shtable 450
```

1.4.11.3 Displaying Power and Management Subsystem Information

This command lets you display power and management subsystem information. This command is only valid on an *ASX*-1000, *ASX*-1200, or *TNX*-1100. Enter the following:

```
myswitch::debug dump hardware> pams
PAMS & Common Equipment Card state dump
Platform: FORE Systems ASX-1000    Switch board: A
PAMS Local Variables state dump...
status=0x00 -> status OK
protocolVersion=6    slot=0    boardType=192    boardRevision(EEPROM)=3
alarmAndLedStatus=0xc1 -> active alarms: MAJOR  MINOR
info1=0x08 -> executing from flash (sector 0),  fabric power active,  bus-slave
PAMS Common Equipment Card Variables state dump...
protocolVersion=3   boardType=64   boardVersion=6   serialNumber=1007   macAdd
r=0xef31d48200
(obs. should be OK) tempSensors=0x07 -> switch: OK,  ps-a: OK,  ps-b: OK
fans=0x0f -> fan1: OK (3301 RPM),  fan2: OK (3348 RPM),  fan3: OK (3348 RPM),  fan
4: OK (3348 RPM),
signals=0xf0: switch boards -> switch a: PRESENT,  switch b: PRESENT,  switch c: P
RESENT,  switch d: PRESENT,
signals=0xf0: early power supplies only -> ps-b secondary: FAILED,  ps-b primary:
FAILED,  ps-a secondary: FAILED,  ps-a primary: FAILED,
Power Supply A (ps-a) Variables state dump...
ps-a is not responding.
Power Supply B (ps-b) Variables state dump...
ps-b: boardType=132    boardVersion=1    serialNumber=128
ps-b: rawStatus=0x00 -> DC: OK, input power: OK, temperature: NORMAL
ps-b: load: 0x48 -> 36.0%
ps-b: rawStatus (LSB to MSB) ->
00.48.00.48.00.48.00.48.00.47.00.47.00.47.5c2e6e6f.720a226e
```

If the switch is not an *ASX*-1000, *ASX*-1200, or *TNX*-1100, then the following is displayed:

```
PAMS & Common Equipment Card state dump
PAMS is not supported on this switch
```

1.4.11.4 Displaying Hardware Timing Information

This command lets you display hardware information about the distributed timing network modules in this switch fabric. Enter the following:

```
myswitch::debug dump hardware> timing
Netmod #0
Netmod Clock Source Control Register(0x40001810): 0x0
Import Clock Disabled, Source: Mgmt Station
Netmod #1
Netmod Clock Source Control Register(0x40001814): 0x0
Import Clock Disabled, Source: Mgmt Station
Netmod #2
Netmod Clock Source Control Register(0x40001818): 0xe
Import Clock Enabled, Source: Netmod 2
(nmod5) : oc3_c_timing_dump: NM-C-OC3c/STM1c-MM-ST-TIMING-128K-4PT netmod 1C: Cl
ock Control Register (0x40060014): 0xffffa01f
Netmod #3
Netmod Clock Source Control Register(0x4000181c): 0xe
Import Clock Enabled, Source: Netmod 2
(nmod5) : oc12_lc_timing_dump: NM-LC-OC12c/STM4c-MM-SC-TIMING-1PT netmod 1D:
Clock Control Register (0x40070014): 0xfffff018
```

1.4.12 Displaying IP Filter Information

This command lets you display IP filtering information for this switch fabric. Enter the following:

```
myswitch::debug dump> ipfilter
IpFilter flags:
        Initialized = 1
        ipfilter_g  = 0
        Inband      = 0
        NoSSR       = 0
        NoLSR       = 0
IpFilter table: (0 entries):
```

1.4.13 Fabric Memory Dump Commands

The commands listed under the **memory** root level, let you display information about the switch fabric's memory configuration. Type **?** at the **memory** level to list these commands.

```
myswitch::debug dump memory> ?
  afmemtest          allheaps          amiheap           check
  mbuf               mainheap          mgmtheap          pool
```

1.4.13.1 Displaying Address Filter Memory Test Information

This command lets you display address filter memory test information. Enter the following:

```
myswitch::debug dump memory> afmemtest
```

1.4.13.2 Displaying Memory Statistics

This command lets you display memory statistics for all heaps. Enter the following:

```
myswitch::debug dump memory> allheaps
Memory, Bytes Free     6211024
Memory, Bytes Used     3756816
Memory, Blocks Free         43
Memory, Blocks Used       1249
Memory, Largest Block  5332784
Memory, Total Mallocs    49537
Memory, Total Frees      48288
```

1.4.13.3 Displaying AMI Heap Statistics

This command lets you display memory statistics for the AMI heap. Enter the following:

```
myswitch::debug dump memory> amiheap
Ami Heap, Bytes Free      356272
Ami Heap, Bytes Used      692272
Ami Heap, Blocks Free         29
Ami Heap, Blocks Used        153
Ami Heap, Largest Block   298240
Ami Heap, Total Mallocs    12256
Ami Heap, Total Frees      12103
```

1.4.13.4 Displaying Memory Check Information

This command lets you display memory check information. The **check** command is not available on an *ASX*-4000, *ESX*-3000, LE 155, or LE 25. Enter the following:

```
myswitch::debug dump memory> check
MEMCHK == start 866472554 ==
MEMCHK == end ==
```

1.4.13.5 Displaying Memory Buffer Statistics

This command lets you display memory buffer statistics. Enter the following:

```
myswitch::debug dump memory> mbuf
Type    Number
----    ------
DATA    2
HEADER  1
PCB     12
RTABLE  8
IFADDR  7
Total number of mbufs : 256
Number of mbufs in use : 30
Total Mapped pages : 96
Mapped pages in use : 0
Kbs allocated to network : 128
Kbs in use by network : 3
Requests for memory denied : 0
Requests for memory delayed : 0
Calls to protocol drain routines : 0
```

1.4.13.6 Displaying Main Heap Statistics

This command lets you display main heap memory statistics. Enter the following:

```
myswitch::debug dump memory> main
Main Heap, Bytes Free     5343904
Main Heap, Bytes Used     3313280
Main Heap, Blocks Free         11
Main Heap, Blocks Used        963
Main Heap, Largest Block  5332784
Main Heap, Total Mallocs    32865
Main Heap, Total Frees      31902
```

1.4.13.7 Displaying Management Heap Statistics

This command lets you display management heap memory statistics. Enter the following:

```
myswitch::debug dump memory> mgmtheap
Mgmt Heap, Bytes Free      250896
Mgmt Heap, Bytes Used       11216
Mgmt Heap, Blocks Free          8
Mgmt Heap, Blocks Used        115
Mgmt Heap, Largest Block   246848
Mgmt Heap, Total Mallocs   171617
Mgmt Heap, Total Frees     171502
```

1.4.13.8 Displaying Pre-allocated Memory Pool Information

This command lets you display information about the pre-allocated memory pools. Enter the following:

```
myswitch::debug dump memory> pool
             NAME     ITEMS        CHUNKS          BYTES            TOTALS
                   CURR   MAX   CURR   MAX     CURR      MAX      ALLOC    FREE     FAIL
        list_cust  0x10   0x1f   0x10   0x10   0x2280    0x2280    0x18da   0x18ca   0x0
             list  0x1c   0x2b   0x4    0x4    0x310c    0x310c    0x7878   0x785c   0x0
          asx_vpm  0xa    0x12   0x2    0x3    0x4ce     0x6ed     0x12     0x8      0x0
          asx_vcf  0x0    0x2    0x9    0x9    0x6da7    0x6da7    0x3178   0x3178   0x0
   crankback_info  0x0    0x1    0x40   0x40   0xa850    0xa850    0x18bc   0x18bc   0x0
   pmp_called_uni  0x0    0x0    0x8    0x8    0x2988    0x2988    0x0      0x0      0x0
         q93b_pcb  0x0    0x0    0x20   0x20   0x9470    0x9470    0x0      0x0      0x0
          pmp_vcc  0x0    0x0    0x1    0x1    0x10af    0x10af    0x0      0x0      0x0
              vcc  0x0    0x1    0x8    0x8    0x10188   0x10188   0x18bc   0x18bc   0x0
         q93b_ccb  0x0    0x1    0x13   0x13   0x17edd   0x17edd   0x18c6   0x18c6   0x0
    dtl_node_elem  0x0    0x0    0x41   0x41   0x12cef   0x12cef   0x0      0x0      0x0
              dtl  0x1    0x4    0x21   0x21   0x468f    0x468f    0x318a   0x3189   0x0
         q93b_sdu  0x1    0x4    0x102  0x102  0x1447ce  0x1447ce  0x318a   0x3189   0x0
    sscop_message  0x0    0x7    0x14   0x14   0x7afc    0x7afc    0x34226  0x34226  0x0
sscop_signal_args  0x0    0x3    0x4    0x4    0x110c    0x110c    0x4d05   0x4d05   0x0
          asx_vcl  0x0    0x0    0x90   0x90   0x32a00   0x32a00   0x0      0x0      0x0
          timeout  0x1e   0x24   0x4    0x4    0x510c    0x510c    0x9ef85  0x9ef67  0x0
Total Memory Currently allocated to pools--> 1998781 Bytes
```

AMI Debug Commands

1.4.14 Signalling Dump Commands

The commands listed under the **signalling** root level, let you display information about the signalling connections on the switch. Type **?** at the **signalling** level to list these commands.

```
myswitch::debug dump signalling> ?
  link               q93b>              spans>              sscop>
```

1.4.14.1 Displaying Link Information

This command lets you display information on the state of the ports in the switch (also referred to as the links). Each port is treated as two unidirectional links, one coming into the switch and one going out. This command is useful in finding out if there is a problem with a particular port. The administrative state should be UP and carrier should be ON on both the in and out links. The links should also show cell traffic in either directions if a peer is attached on that port. Enter the following:

```
myswitch::debug dump signalling> link
link:  IN    0     ADMIN: UP       CARRIER  cells: 5517245
link:  IN    1     ADMIN: UP    NO-CARRIER  cells: 0
link:  IN    2     ADMIN: UP    NO-CARRIER  cells: 0
link:  IN    3     ADMIN: UP    NO-CARRIER  cells: 0
link:  IN   33     ADMIN: UP       CARRIER  cells: -1
link:  IN   34     ADMIN: UP       CARRIER  cells: -1
link:  IN   35     ADMIN: UP       CARRIER  cells: -1
link:  IN   56     ADMIN: UP       CARRIER  cells: 177659977
link: OUT    0   ADMIN: DOWN    NO-CARRIER  cells: 5442997
link: OUT    1   ADMIN: DOWN    NO-CARRIER  cells: 797556
link: OUT    2   ADMIN: DOWN    NO-CARRIER  cells: 797556
link: OUT    3   ADMIN: DOWN    NO-CARRIER  cells: 797556
link: OUT   33     ADMIN: UP       CARRIER  cells: -1
link: OUT   34     ADMIN: UP       CARRIER  cells: -1
link: OUT   35     ADMIN: UP       CARRIER  cells: -1
link: OUT   56     ADMIN: UP       CARRIER  cells: 25559993
```

1.4.14.2 Q93b Signalling Connections Dump Commands

The commands listed under the **q93b** level, let you display Q93b information about the signalling connections on the switch. Type **?** at the **q93b** level to list these commands.

```
myswitch::debug dump signalling q93b> ?
  ccapi              pmp                pp                 pmp_svc
  pmp_svp            pp_svc             pp_svp             uni
  vxc                vcc                vpc                timers
  vmt
```

1.4.14.2.1 Displaying Call Control Applications Information

This command lets you display call control applications information. This command is only useful for debugging the internals of the call control software module. Enter the following:

```
myswitch::debug dump signalling q93b> ccapi
CC-API APPLICATION INFORMATION:
CC-API EVENT INFORMATION:
```

1.4.14.2.2 Displaying Q93b Point-to-Multipoint Calls

This command lets you display the Q93b point-to-multipoint calls for SVCs and SVPs that have been setup using the ATM Forum UNI/PNNI signalling procedures. It gives the port/VPI/VCI values on both sides of the connection, indicates the status of the VCC (i.e., whether or not it is active), gives the call reference value used during call setup, and gives the end point reference in the multicast connection. If information is not available, either a 0 or 0xffffffff is displayed. Enter the following:

```
myswitch::debug dump signalling q93b> pmp
CALL_FWD: Point To Multipoint VxC's
CALL_FWD: ACTIVE 24| 0|195 (cref 0x80011f) ->
                 -> ACTIVE 56| 0|67  (cref 0x5 endp_ref 0x7)
                 -> ACTIVE 27| 0|32  (cref 0xe endp_ref 0x8)
                 -> ACTIVE 11| 0|32  (cref 0x17 endp_ref 0x9)
CALL_FWD: ACTIVE 24| 0|196 (cref 0x800120) ->
                 -> ACTIVE 56| 0|68  (cref 0x6 endp_ref 0x7)
                 -> ACTIVE 27| 0|33  (cref 0xf endp_ref 0x8)
                 -> ACTIVE 11| 0|33  (cref 0x18 endp_ref 0x9)
CALL_FWD: ACTIVE 24| 0|197 (cref 0x800123) ->
                 -> ACTIVE 56| 0|69  (cref 0x9 endp_ref 0x7)
                 -> ACTIVE 27| 0|34  (cref 0x12 endp_ref 0x8)
                 -> ACTIVE 11| 0|34  (cref 0x1b endp_ref 0x9)
```

1.4.14.2.3 Displaying Q93b Point-to-Point Calls

This command lets you display the Q93b point-to-point SVC and SVP calls that have been established using the ATM Forum UNI/PNNI signalling procedures. It shows the port/VPI/VCI values on both sides of the connection, indicates the status of the VCC (i.e., whether or not it is active), and gives the call reference value used during call setup. If information is not available, either a 0 or 0xffffffff is displayed. Enter the following:

```
myswitch::debug dump signalling q93b> pp
CALL_FWD: Point To Point VxC's
CALL_FWD: ACTIVE 10| 0|62  (cref 0x800055) -> ACTIVE 24| 0|194 (cref 0x2)
CALL_FWD: ACTIVE 10| 0|63  (cref 0x800056) -> ACTIVE 24| 0|199 (cref 0x1d)
CALL_FWD: ACTIVE 10| 0|65  (cref 0x800057) -> ACTIVE 24| 0|200 (cref 0x1f)
CALL_FWD: ACTIVE 10| 0|67  (cref 0x800059) -> ACTIVE 24| 0|201 (cref 0x21)
CALL_FWD: ACTIVE 10| 0|69  (cref 0x80005b) -> ACTIVE 24| 0|202 (cref 0x23)
CALL_FWD: ACTIVE 10| 0|71  (cref 0x80005e) -> ACTIVE 24| 0|203 (cref 0x25)
CALL_FWD: ACTIVE 10| 0|72  (cref 0x80005f) -> ACTIVE 24| 0|204 (cref 0x26)
CALL_FWD: ACTIVE 10| 0|73  (cref 0x800060) -> ACTIVE 24| 0|205 (cref 0x27)
CALL_FWD: ACTIVE 10| 0|74  (cref 0x800061) -> ACTIVE 27| 0|63  (cref 0x28)
CALL_FWD: ACTIVE 10| 0|75  (cref 0x800062) -> ACTIVE 24| 0|206 (cref 0x29)
```

1.4.14.2.4 Displaying Q93b Point-to-Multipoint SVC information

This command lets you display information about the point-to-multipoint SVC calls. Enter the following:

```
myswitch::debug dump signalling q93b> pmp_svc
CALL_FWD: Point To MultiPoint VCC's
CALL_FWD: ACTIVE 24| 0|195 (cref 0x80011f) ->
                 -> ACTIVE 56| 0|67  (cref 0x5 endp_ref 0x7)
                 -> ACTIVE 27| 0|32  (cref 0xe endp_ref 0x8)
                 -> ACTIVE 11| 0|32  (cref 0x17 endp_ref 0x9)
CALL_FWD: ACTIVE 24| 0|196 (cref 0x800120) ->
                 -> ACTIVE 56| 0|68  (cref 0x6 endp_ref 0x7)
                 -> ACTIVE 27| 0|33  (cref 0xf endp_ref 0x8)
                 -> ACTIVE 11| 0|33  (cref 0x18 endp_ref 0x9)
CALL_FWD: ACTIVE 24| 0|197 (cref 0x800123) ->
                 -> ACTIVE 56| 0|69  (cref 0x9 endp_ref 0x7)
                 -> ACTIVE 27| 0|34  (cref 0x12 endp_ref 0x8)
                 -> ACTIVE 11| 0|34  (cref 0x1b endp_ref 0x9)
```

1.4.14.2.5 Displaying Q93b Point-to-Multipoint SVP Information

This command lets you display information about the point-to-multipoint SVP calls. Enter the following:

```
myswitch::debug dump signalling q93b> pmp_svp
CALL_FWD: Point To MultiPoint VPC's
```

1.4.14.2.6 Displaying Q93b Point-to-Point SVC Information

This command lets you display information about all point-to-point SVC calls. Enter the following:

```
myswitch::debug dump signalling q93b> pp_svc
CALL_FWD: Point To Point VCC's
CALL_FWD: ACTIVE 24| 0|39  (cref 0x800cbd) -> ACTIVE 32| 0|56  (cref 0x1a)
CALL_FWD: ACTIVE 24| 0|40  (cref 0x800cbe) -> ACTIVE 32| 0|57  (cref 0x1b)
CALL_FWD: ACTIVE 25| 0|40  (cref 0x800770) -> ACTIVE 32| 0|54  (cref 0x18)
CALL_FWD: ACTIVE 25| 0|41  (cref 0x800771) -> ACTIVE 32| 0|55  (cref 0x19)
CALL_FWD: ACTIVE 56| 0|80  (cref 0x80000e) -> ACTIVE 32| 0|58  (cref 0x1c)
CALL_FWD: ACTIVE 56| 0|81  (cref 0x80000f) -> ACTIVE 32| 0|59  (cref 0x1d)
```

1.4.14.2.7 Displaying Q93b Point-to Point SVP Information

This command lets you display information about the point-to-point SVP calls. Enter the following:

```
myswitch::debug dump signalling q93b> pp_svp
CALL_FWD: Point To Point VPC's
CALL_FWD: ACTIVE 24| 0|39  (cref 0x800cbd) -> ACTIVE 32| 0|56  (cref 0x1a)
CALL_FWD: ACTIVE 24| 0|40  (cref 0x800cbe) -> ACTIVE 32| 0|57  (cref 0x1b)
CALL_FWD: ACTIVE 25| 0|40  (cref 0x800770) -> ACTIVE 32| 0|54  (cref 0x18)
CALL_FWD: ACTIVE 25| 0|41  (cref 0x800771) -> ACTIVE 32| 0|55  (cref 0x19)
```

1.4.14.2.8 Displaying Q93b UNI Data Structures

This command lets you display the Q93b UNI data structure. Information includes the call control debugging status (`ccdbg_T`=enabled, `ccdbg_F`=disabled) and signalling debugging status for each of the signalling interfaces (`sigdbg_T`=enabled, `sigdbg_F`=disabled). Enter the following:

```
myswitch::debug dump signalling q93b> uni
UNI[ 0| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0x e805c ILMI_DOWN net  aal5 VPCAP=False ccdbg_F
sigdbg_T
UNI[ 1| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xe4d7c ILMI_DOWN net  aal5 VPCAP=False ccdbg_F
sigdbg_T
UNI[ 2| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf0d98 ILMI_DOWN net  aal5 VPCAP=False ccdbg_F
sigdbg_F
UNI[ 3| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf2234 ILMI_DOWN net  aal5 VPCAP=False ccdbg_T
sigdbg_F
UNI[24| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf5b6c ILMI_DOWN net  aal5 VPCAP=False ccdbg_F
sigdbg_F
UNI[25| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf71b8 ILMI_UPnet  aal5 VPCAP=False ccdbg_F
sigdbg_F
UNI[26| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf8804 ILMI_DOWN net  aal5 VPCAP=False ccdbg_T
sigdbg_T
UNI[27| 0] VP NonA PRIV_UNI SigVCI 5 Dmn  1 If0xf9e50 ILMI_DOWN net  aal5 VPCAP=False ccdbg_T
sigdbg_F
```

1.4.14.2.9 Displaying All Q93b SVCs and SVPs

This command lets you display all SVC and SVP calls that have been established using the ATM Forum UNI/PNNI signalling procedures.

```
myswitch::debug dump signalling q93b> vxc
CALL_FWD: Point To Point VxC's
CALL_FWD: ACTIVE 24| 0|39  (cref 0x800cbd) -> ACTIVE 32| 0|56  (cref 0x1a)
CALL_FWD: ACTIVE 24| 0|40  (cref 0x800cbe) -> ACTIVE 32| 0|57  (cref 0x1b)
CALL_FWD: ACTIVE 25| 0|40  (cref 0x800770) -> ACTIVE 32| 0|54  (cref 0x18)
CALL_FWD: ACTIVE 25| 0|41  (cref 0x800771) -> ACTIVE 32| 0|55  (cref 0x19)
CALL_FWD: ACTIVE 56| 0|80  (cref 0x80000e) -> ACTIVE 32| 0|58  (cref 0x1c)
CALL_FWD: ACTIVE 56| 0|81  (cref 0x80000f) -> ACTIVE 32| 0|59  (cref 0x1d)
CALL_FWD: Point To MultiPoint VxC's
```

1.4.14.2.10 Displaying All Q93b VCC Information

This command lets you display information for all SVC calls that have been established using the ATM Forum signalling procedures. If information is not available, either a 0 or 0xffffffff is displayed. Enter the following:

```
myswitch::debug dump signalling q93b> vcc
CALL_FWD: Point To Point VCC's
CALL_FWD: ACTIVE 56| 0|63  (cref 0x800003) -> ACTIVE  0| 0|35  (cref 0x4)
CALL_FWD: ACTIVE 56| 0|64  (cref 0x800004) -> ACTIVE  0| 0|36  (cref 0x5)
CALL_FWD: Point To Multipoint VCC's
```

1.4.14.2.11 Displaying All Q93b VPC Information

This command lets you display information for all SVP calls that have been established using the ATM Forum signalling procedures. Enter the following:

```
myswitch::debug dump signalling q93b> vpc
CALL_FWD: Point To Point VPC's
CALL_FWD: [SVP]: ACTIVE 0| 1|-1  (cref 0x800003) -> ACTIVE  16| 1|-1  (cref 0x4)
CALL_FWD: [SVP}: ACTIVE 0| 2|-1  (cref 0x800004) -> ACTIVE  16| 2|-1  (cref 0x5)
CALL_FWD: Point To MultiPoint VPC's
```

1.4.14.2.12 Displaying Q93b Values for Signalling Timers

This command lets you display information about the Q93b timers. Enter the following:

```
myswitch::debug dump signalling q93b> timers
Signalling Instance 3:
Signalling Timer Values:
  T301 = 180000ms  T303 = 4000ms  T308 = 30000ms  T309 = 10000ms
  T310 = 10000ms  T313 = 4000ms  T316 = 120000ms  T317 = 60000ms
  T322 = 4000ms  T397 = 180000ms  T398 = 4000ms  T399 = 14000ms
Signalling Timer Retries:
  T301 = 0  T303 = 1  T308 = 1  T309 = 1
  T310 = 1  T313 = 1  T316 = 2  T317 = 1
  T322 = 3  T397 = 0  T398 = 1  T399 = 1
```

1.4.14.2.13 Displaying the VPCI Groups and VPCI Map Indices

This command lets you display all the VPCI groups that use a particular VPCI map index or all the signalling interfaces (active interfaces as well as the interfaces in the CDB) that use a particular VPCI group index. Enter the following:

```
myswitch::debug dump signalling q93b> vmt (maps|groups) [<index>]
```

You must specify whether you want the VPCI map index or group index. For instance, to display the VPCI group that contains a particular VPCI map index, enter something similar to the following:

```
myswitch::debug dump signalling q93b> vmt maps 10

map index=10, status=active, ref count=1
        in use by group 10
```

To display the VPCI map index for a particular VPCI group, enter something similar to the following:

```
myswitch::debug dump signalling q93b> vmt groups 10

group index=10, status=active, ref count=1
        count(maplist)=1, count(vpci)=1
        in use by interface 1C1(16)|25
```

1.4.14.3 SPANS Signalling Dump Commands

The commands listed under the **spans** level, let you display information about the SPANS signalling connections on the switch. Type **?** at the **spans** level to list these commands.

```
myswitch::debug dump signalling spans> ?
  group              sigpath            spvc               stats
  vcc
```

1.4.14.3.1 Displaying Multicast Group ID Information

This command lets you display SPANS multicast group ID information. Enter the following:

```
myswitch::debug dump signalling spans> group
Group  e0000001:   SUBSCRIBERS:
      f21c1e07.e0000001
      f21a3f9e.e0000001
      f21c1fe0.e0000001
      f21c20ec.e0000001
      f21c1f4e.24.00
      f21c1f4e.25.00
```

1.4.14.3.2 Displaying SPANS Signalling Path Information

This command lets you display SPANS signalling path information. Enter the following:

```
myswitch::debug dump signalling spans> sigpath
UP   (FT-PNNI):  f21c078b <----> f20f01fa    0|0     2 bt   0 VCC    0 o   0 f   0
rj    20682 CI       3 CO   949504 SI  947081 SO, nbr INTRA_UP
DOWN (uni)    :  f21c078b <----> HOST       1|0     0 bt   0 VCC    0 o   0 f   0
rj        0 CI       3 CO        0 SI  449926 SO
DOWN (uni)    :  f21c078b <----> HOST       2|0     0 bt   0 VCC    0 o   0 f   0
rj        0 CI       3 CO        0 SI  449926 SO
DOWN (uni)    :  f21c078b <----> HOST       3|0     0 bt   0 VCC    0 o   0 f   0
rj        0 CI       3 CO        0 SI  449926 SO
UP   (FT-PNNI):  f21c078b <----> f21c07be   33|0     2 bt   0 VCC    0 o   0 f   0
rj    20695 CI       3 CO   948089 SI  947031 SO, nbr INTRA_UP
UP   (FT-PNNI):  f21c078b <----> f21c0a9a   34|0     2 bt   0 VCC    0 o   0 f   0
rj    20114 CI       3 CO   934185 SI  938075 SO, nbr INTRA_UP
UP   (FT-PNNI):  f21c078b <----> f21c06f7   35|0     6 bt   0 VCC    0 o   0 f   0
rj    19619 CI       3 CO   941461 SI  946716 SO, nbr INTRA_UP
UP   (uni)    :  f21c078b <----> HOST      56|0     2 bt   0 VCC    0 o   0 f   0
rj        4 CI       5 CO   438954 SI  449927 SO
```

1.4.14.3.3 Displaying SPVC Information

This command lets you display SPANS SPVC information. Enter the following:

```
myswitch::debug dump signalling spans> spvc
```

1.4.14.3.4 Displaying SPANS Signalling Path Statistics

This command lets you display SPANS signalling path statistics. Enter the following:

```
myswitch::debug dump signalling spans> stats
spans stats:  14 boots     0 VCCs     0 opens    0 fails    0 rejects  4212961 IN
  5579628 OUT
```

1.4.14.3.5 Displaying SPANS Connection Information

This command lets you display SPANS VCC information. Enter the following:

```
myswitch::debug dump signalling spans> vcc
```

1.4.14.4 SSCOP Dump Commands

The commands listed under the **sscop** level, let you display information about the Service Specific Connection Oriented Protocol (SSCOP). Type **?** at the **sscop** level to list these commands.

```
myswitch::debug dump signalling sscop> ?
  queue              unprocessed
```

1.4.14.4.1 Displaying SSCF Queue Information

This command lets you display SSCF queue information. Enter the following:

```
myswitch::debug dump signalling sscop> queue
 SSCOP[ 0] transmit buffer contents:
 SSCOP[ 0] retransmit buffer contents:
 SSCOP[ 0] receive buffer contents:
 SSCOP[ 0] unprocessed message queue contents:
 SSCOP[ 1] transmit buffer contents:
 SSCOP[ 1] retransmit buffer contents:
 SSCOP[ 1] receive buffer contents:
 SSCOP[ 1] unprocessed message queue contents:
 SSCOP[ 2] transmit buffer contents:
 SSCOP[ 2] retransmit buffer contents:
 SSCOP[ 2] receive buffer contents:
 SSCOP[ 2] unprocessed message queue contents:
 SSCOP[ 3] transmit buffer contents:
 SSCOP[ 3] retransmit buffer contents:
 SSCOP[ 3] receive buffer contents:
 SSCOP[ 3] unprocessed message queue contents:
 SSCOP[33] transmit buffer contents:
```

1.4.14.4.2 Displaying SSCF Unprocessed Message Queue Information

This command lets you show SSCF unprocessed message queue information. Enter the following:

```
myswitch::debug dump signalling sscop> unprocessed
SSCOP[0]:Unprocessed Mesg Q len: 0, Max len: 2
SSCOP[33]:Unprocessed Mesg Q len: 0, Max len: 1
SSCOP[34]:Unprocessed Mesg Q len: 0, Max len: 13
SSCOP[35]:Unprocessed Mesg Q len: 0, Max len: 8
```

1.4.15 Utilities Dump Commands

The commands listed under the **utilities** root level, let you display information about switch utilities. Type **?** at the **utilities** level to list these commands.

```
myswitch::debug dump utilities> ?
  lastbad            time               rproc
```

1.4.15.1 Displaying the Stack Trace from the Last Log Error

This command lets you show the stack trace from the last LOG_ERROR. Enter the following:

```
myswitch::debug dump utilities> lastbad
 UNI[ 8] t316_timeout expiry:
  00. 00529244
  01. 0052936c
  02. 00530ae0
  03. 00539234
  04. 00532244
  05. 003ca684
  06. 001a0f30
  07. 003c9914
  08. 0012ba94
 UNI[ 8]   did not receive restart_ack from remote host
  00. 00529244
  01. 0052936c
  02. 00530b00
  03. 00539234
  04. 00532244
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

1.4.15.2 Displaying Timeout Information

This command lets you display information about the timeout function on the switch. Enter the following:

```
myswitch::debug dump utilities> time
timeout: 003b5f90(00000000)  in    19 ms    500 ms period
timeout: 00537340(00cc3894)  in    19 ms
timeout: 004276e0(00cc9a08)  in    39 ms    500 ms period
timeout: 0054a200(00cb5288)  in    82 ms
timeout: 003bbf10(00cc9a08)  in   141 ms   1000 ms period
timeout: 00355f70(00000000)  in   227 ms
timeout: 004623d0(00000000)  in   235 ms   1000 ms period
timeout: 005372b0(00cc3894)  in   358 ms    500 ms period
timeout: 0051e600(00000000)  in   364 ms    500 ms period
timeout: 003828c0(00cc4c14)  in   399 ms    500 ms period
timeout: 00462360(00000001)  in   617 ms
timeout: 0057b7a0(00000000)  in   655 ms   1000 ms period
timeout: 0037ae50(00cc49d0)  in   742 ms
timeout: 0053b280(00cc3894)  in   851 ms   1000 ms period
timeout: 00386ce0(00000000)  in   846 ms   1000 ms period
timeout: 0053c9e0(00000000)  in   902 ms   2000 ms period
timeout: 002e3cd0(00000000)  in  1124 ms   10000 ms period
timeout: 002c9e50(00000000)  in  1122 ms   5000 ms period
timeout: 00355960(00efb9dc)  in  1203 ms   5000 ms period
timeout: 0052d2c0(00cc3894)  in  2533 ms
timeout: 002fa380(00000000)  in  2892 ms   10000 ms period
timeout: 0053cc60(00000000)  in  2890 ms   10000 ms period
timeout: 0037caa0(00cbec38)  in  3545 ms
timeout: 00538970(00cc3894)  in  4820 ms   5000 ms period
timeout: 003f8af0(00cbe2b8)  in  7900 ms
timeout: 0054a320(00cb5288)  in  9040 ms
timeout: 00530fa0(00cc38f8)  in  9811 ms   10000 ms period
timeout: 0052d260(00cc3894)  in  9814 ms   10000 ms period
timeout: 00520a20(00cc3894)  in  9811 ms   10000 ms period
timeout: 002c8440(00000000)  in  9816 ms   10000 ms period
timeout: 003f4570(00cbe2b8)  in  9830 ms   10000 ms period
timeout: 00551eb0(00091478)  in  10881 ms
timeout: 00551eb0(00091a18)  in  11058 ms
timeout: 00551eb0(00091838)  in  11533 ms
timeout: 00551eb0(00091298)  in  12509 ms
```

1.4.15.3 Displaying RPROC Information

This command lets you display reassembly process connection (RPROC) information. Enter the following:

CAUTION

Executing this AMI command from the console when there are many VCCs to the control port, will cause switch signalling to go down. Recovery time will take more than one minute. However, executing this command from a telnet AMI session will allow a faster dump of the information and will not cause the signalling to go down.

```
myswitch::debug dump utilities> rproc
vci:32 aal:4 state:open    mbufs:0 clusters:0 ipkts:19874 drops:0
vci:33 aal:4 state:open    mbufs:0 clusters:0 ipkts:2 drops:0
vci:34 aal:5 state:open    mbufs:0 clusters:0 ipkts:20123 drops:0
vci:35 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:36 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:37 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:38 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:39 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:40 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:41 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:42 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:43 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:45 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:46 aal:4 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:47 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:49 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:50 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:51 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
vci:52 aal:5 state:open    mbufs:0 clusters:0 ipkts:0 drops:0
Total: mbufs:0 clusters:0
```

1.4.16 Utilization Dump Commands

The commands listed under the **utilization** root level, let you display utilization information. Type **?** at the **utilization** level to list these commands.

```
myswitch::debug dump> utilization ?
  cpuload            processor          malloc            mbufs
```

1.4.16.1 Displaying the CPU Utilization

This command lets you display CPU load information. Enter the following:

```
myswitch::debug dump utilization> cpuload
Processor load = 15 %
Processor load last updated at TUE MAR 10 19:50:29 1998
Update interval = 15 secs
MAX Processor load = 31 %
Maximum processor load last updated at TUE MAR 10 15:14:28 1998
```

1.4.16.2 Displaying the Processor Utilization

This command lets you display current, minimum, and maximum processor utilization information. Enter the following:

```
myswitch::debug dump utilization> processor
Processor Utilization Updated every            : 15 secs
Current Processor Utilization                  : 12 %
Time Current Processor Utilization Calculated  : TUE APR 21 14:37:17 1998
Minimum Processor Utilization                  : 9 %
Time Minimum Processor Utilization Calculated  : TUE APR 21 14:23:21 1998
Maximum Processor Utilization                  : 91 %
Time Maximum Processor Utilization Calculated  : TUE APR 21 13:53:17 1998
System Malloc Partition ID                     : 7284192
Number of malloc partitions                    : 1
System Malloc Partition ID                     : 7284192
Number of malloc partitions                     : 1
```

1.4.16.3 Displaying Memory Allocation Utilization

This command lets you display memory allocation (malloc) utilization information. Enter the following:

```
myswitch::debug dump utilization> malloc
Malloc Partition ID        :  6592608
Number of Bytes Free       :  5248576
Number of Blocks Free      :  8
Max block size that is free:  5247504
Number of Bytes Allocated  :  3623712
Number of Blocks Allocated :  1046
```

1.4.16.4 Displaying Memory Buffer Utilization

This command lets you display memory buffer utilization information. Enter the following:

```
myswitch::debug dump utilization> mbufs
mbufs obtained from page pool                           : 256
clusters obtained from page pool                        : 96
interface pages obtained from page pool                 : 0
Free Clusters                                           : 96
Times failed to find space                              : 0
Times waited for space                                  : 0
Times drained protocols for space                       : 0
# of mbufs allocated to free list                       : 232
# of mbufs allocated to dynamic (data) allocation       : 1
# of mbufs allocated to packet headers                  : 1
# of mbufs allocated to socket structures               : 0
# of mbufs allocated to protocol control blocks         : 11
# of mbufs allocated to routing tables                  : 6
# of mbufs allocated to IMP Host Tables                 : 0
# of mbufs allocated to Address Resolution Tables       : 0
# of mbufs allocated to Socket Name                     : 0
# of mbufs allocated to Zombie Processes                : 0
# of mbufs allocated to Socket Options                  : 0
# of mbufs allocated to Fragment Re-assembly Headers    : 0
# of mbufs allocated to Access Rights                   : 0
# of mbufs allocated to Interface Addresses             : 5
```

1.4.17 Displaying the Software Version

This command lets you display information about which version of switch software is currently running on the switch. Enter the following:

```
myswitch::debug dump> version
ForeThought Switch Control Software (swswbld)
@(#) $Id: FORE Systems Release: S_ForeThought_6.0.0 FCS (1.22260) $
```

1.5 OAM Commands

The **oam** commands can be used to debug ATM/OAM information Type **?** at the **oam** level to list these commands.

```
myswitch::debug oam> ?
monitor>            transmit>
```

1.5.1 Setting Up OAM Cell Receive Monitor

The commands listed under the **monitor** root level, let you set up the OAM cell receive monitor. Type **?** at the **monitor** level to list these commands:

```
localhost::debug oam monitor> ?
  disable             enable              filter              show
```

1.5.1.1 Disabling the Monitoring of Received OAM Cells

This command lets you disable the monitoring of received OAM cells. Enter the following:

```
localhost::debug oam monitor> disable
```

1.5.1.2 Enabling the Monitoring of Received OAM Cells

This command lets you enable the monitoring of received OAM cells. Enter the following:

```
localhost::debug oam monitor> enable
```

1.5.1.3 Setting/Showing the Monitor Filter

This command lets you set or show the monitor filter. Enter the following:

```
        localhost::debug oam monitor> filter [-port (<bnp> | any)] [-vpi (<vpi> | any)]
[-vci (<vci> | any)]
[-layer (f4 | f5 | any)] [-flow (end2end | segment | any)] \
        ([-fmType (ais | rdi | cc | loop)]
                | [-oamType (0-f | any)] [-funcType (0-f | any)])
```

1.5.1.4 Displaying the Current Monitor Operation

This command lets you display the current monitor operation. Enter the following:

```
localhost::debug oam monitor> show
```

1.5.2 Transmitting an OAM Cell

The commands listed under the **transmit** root level, let you set up information for transmitting an OAM cell. Type **?** at the **transmit** level to list these commands:

```
myswitch::debug oam transmit> ?
  ais                 cc                  loopback            raw
  repeat              rdi                 show
```

1.5.2.1 Transmitting AIS OAM Cells

This command lets you transmit AIS OAM cells. Enter the following:

```
myswitch::debug oam transmit> ais <bnp> <vpi> [<vci>] (end2end | segment) [-
defectType <xx>] \[-defectLoc <ssssssssssssssssssssssssssssssss>]
```

1.5.2.2 Transmitting Continuity Check Cells

This command lets you transmit continuity check cells. Enter the following:

```
myswitch::debug oam transmit> cc <bnp> <vpi> [<vci>] (end2end | segment)
```

1.5.2.3 Transmitting Loopback OAM Cells

This command lets you transmit loopback OAM cells. Enter the following:

```
myswitch::debug oam transmit> loopback <bnp> <vpi> [<vci>] (end2end | segment) \
 [-loopInd <xx>] [-ctag <xxxxxxxx>] \
 [-loopLoc <ssssssssssssssssssssssssssssssss>] \
 [-srcLoc <ssssssssssssssssssssssssssssssss>]
```

1.5.2.4 Transmitting Raw OAM cells

This command lets you transmit raw OAM cells. Enter the following:

```
myswitch::debug oam transmit> raw <bnp> <vpi> [<vci>] (end2end | segment) \
 [-oamType <x>] [-funcType <x>] \
 [-funcSpec <max 45 hex octets>]
```

1.5.2.5 Transmitting RDI OAM Cells

This command lets you transmit RDI OAM cells. Enter the following:

```
myswitch::debug oam transmit> rdi <bnp> <vpi> [<vci>] (end2end | segment) [-
defectType <xx>] \[-defectLoc <ssssssssssssssssssssssssssssssss>]
```

1.6 Protected UBR Commands

Protected UBR is similar to UBR traffic in that it offers a best-effort service. However, protected UBR and UBR differ when traffic overloads a single output port for a sustained period of time such that the queue memory fills up and cells must be dropped. Protected UBR protects UBR VCs that are within their offer load from UBR VCs that are causing the output overload by utilizing the CLP bit for a cell. The CLP bit will be tagged for any cell that exceeds that connection's proportion of the bandwidth. When congestion occurs, all cells with a tagged CLP bit will be dropped first, and then based fairly on the cell arrival rate. Each VC on a protected UBR output port is allocated a fraction of the output bandwidth of the output port.

The **protectedubr** commands can be used to configure protected UBR traffic on a port-by-port basis. The **protectedubr** commands are only available for the *ASX*-4000. Type **?** at the **protectedubr** level to list these commands.

NOTE

Currently, protected UBR is only supported in the *ASX*-4000 and is applicable to PVCs and PVPs that have a UPC contract with an estimated bandwidth value and to SPVCs under FT-PNNI with load-balanced UBR enabled.

```
myswitch::debug protectedubr> ?
port            clp1            use-rr            use-wrr            show
```

1.6.1 Enabling/Disabling Protected UBR

This command lets you enable or disable the protected UBR feature on all ports or for a specific port. Since ports can be configured individually, the switch can support both UBR and protected UBR links simultaneously. Protected UBR is off by default. Enter the following:

```
myswitch::> debug protectedubr> port (ALL|<bnp>) (ON|OFF)
```

The parameters are described as follows:

Parameter	Description
ALL	Enable or disable protected UBR on all VCs transmitted on a protectedUBR link.
bnp	Enable or disable protected UBR for all VCs transmitted on a particular protected UBR port (in BNP notation).
ON	Enable protected UBR.
OFF	Disable protected UBR.

1.6.2 Setting the UBR CLP1 Threshold for a Fabric

This command lets you set the CLP1 threshold on a fabric. The fabric will admit all cells (CLP=1 and CLP=0) until it approaches the threshold. Any cell that arrives beyond the desired percentage of buffers on the fabric will be discarded if CLP=1 or if admitted with CLP=0. Enter the following:

```
myswitch::> debug protectedubr> clp1 <board> <threshold>
The threshold is to be given in the form of a percentage.
```

The parameters are described as follows:

Parameter	Description
board	The fabric for which you want to set the CLP1 threshold.
threshold	The UBR CLP1 threshold for a specific fabric (as a percentage of the total buffering available).

1.6.3 Scheduling Round-Robin UBR

This command lets you select regular round robin UBR scheduling for protected UBR output ports. Round-Robin scheduling handles de-queuing cycles equally. The scheduling selected applies to all ports on the switch (all ports use regular round-robin or all ports use weighted round-robin). Enter the following:

```
myswitch::> debug protectedubr> use-rr
```

1.6.4 Scheduling Weighted Round-Robin UBR

This command lets you use weighted round-robin scheduling for all protected UBR output ports. The egress scheduler can be configured to transmit protected UBR VCs in a weighted round-robin fashion, based on weight (based on the same weight used for load-balanced UBR). Weighted round-robin scheduling will be used on all output ports regardless of whether the protected UBR feature is enabled or disabled. The scheduling selected applies to all ports on the switch (all ports use regular round-robin or all ports use weighted round-robin). Enter the following:

```
myswitch::> debug protectedubr> use-wrr
```

1.6.5 Displaying Protected UBR Settings

This command lets you display all protected UBR settings or for a particular fabric. Enter the following:

```
myswitch::> debug protectedubr> show [<board>]
```

To show all protected UBR settings, just enter **show** as follows:

```
myswitch::> debug protectedubr> show
UBR Round Robin Scheduling: normal

               CLP1
Board          Threshold
1              100%
2              100%

               Protected
Port           UBR Status
1A1            OFF
1A2            OFF
1A3            OFF
1A4            OFF
1B1            OFF
1B2            OFF
1B3            OFF
1B4            OFF
```

The fields are described as follows:

Field	Description
UBR Round Robin Scheduling	The type of round-robin scheduling configured for the protected UBR link. `Normal` means that all service for the protected UBR links use regular round-robin scheduling. `Weighted` means weighted round-robin scheduling is used.
Board	The switch fabric number.
CLP1 Threshold	The CLP1 threshold set for the fabric (as a percentage).
Port	The port number in BNP notation.
Protected UBR Status	The protected UBR status for a particular port on a fabric. `OFF` means protected UBR is not enabled for the port. `ON` means protected UBR is enabled for the port.

1.7 SPVX Congestion Commands

The **spvxcongestion** commands allow you to modify the default settings of SPVPC and SPVCC congestion related parameters. When tracing is enabled for all PNNI SPVPCs and SPVCCs using the **debug trace signalling q93b pnnispvxall** command, congestion related debugging is also enabled. Type **?** at the **spvxcongestion** root level to list these commands.

```
myswitch::debug spvxcongestion> ?
  show              spvcc_nmax        spvcc_nskip       spvcc_tcongest
  spvcc_cthresh     spvpc_nmax        spvpc_nskip       spvpc_tcongest
  spvpc_cthresh
```

1.7.1 Displaying SPVX Congestion Parameters

This command lets you display all SPVPC and SPVCC congestion parameters. Enter the following:

```
myswitch::debug spvxcongestion> show
Congestion Parameter Values are:
spvcc_nmax     - Max tries before congestion for spvccs = 16.
spvcc_nskip    - Skip tries after congestion for spvccs 8.
spvcc_tcongest - Congestion monitoring time interval for spvccs = 10 seconds.
spvcc_cthresh  - Congestion Improvement Threshold for spvccs = 10
spvpc_nmax     - Max tries before congestion for spvpcs = 16.
spvpc_nskip    - Skip tries after congestion for spvpcs = 8.
spvpc_tcongest - Congestion monitoring time interval for spvpcs = 10 seconds.
spvpc_cthresh  - Congestion Improvement Threshold for spvpcs = 10
```

1.7.2 Configuring Maximum SPVCC Setup Attempts

This command lets you configure the maximum number of tries an SPVCC will be attempted before it is considered to be in a congested state. The default is 16. Enter the following parameter:

```
myswitch::debug spvxcongestion> spvcc_nmax <value>
```

1.7.3 Configuring Number of SPVCC Selections to Skip

Once a SPVCC is in a congested state, this command lets you configure the number of SPVCC selections that will be skipped to attempt to try the SPVCC again. The default is 8. Enter the following:

```
myswitch::debug spvxcongestion> spvcc_nskip <value>
```

1.7.4 Configuring SPVCC Congestion Monitoring Time Interval

This command lets you configure the regular intervals that the congested SPVCCs are monitored. Congestion improvement is determined at every interval. The default is 10 seconds. Enter the following:

```
myswitch::debug spvxcongestion> spvcc_tcongest <value>
```

1.7.5 Configuring SPVCC Congestion Improvement Threshold

This command lets you configure the improvement threshold of the congestion state. If the congestion threshold is reached, the SPVCC setup rate is increased. The default is 10%. Enter the following:

```
myswitch::debug spvxcongestion> spvcc_cthresh <value>
```

1.7.6 Configuring Maximum SPVPC Setup Attempts

This command lets you configure the maximum number of tries an SPVPC will be attempted before it is considered to be in a congested state. The default is 16. Enter the following parameter:

```
myswitch::debug spvxcongestion> spvpc_nmax <value>
```

1.7.7 Configuring Number of SPVPC Selections to Skip

Once a SPVPC is in a congested state, this command lets you configure the number of SPVPC selections that will be skipped to attempt to try the SPVPC again. The default is 8. Enter the following:

```
myswitch::debug spvxcongestion> spvpc_nskip <value>
```

1.7.8 Configuring SPVPC Congestion Monitoring Time Interval

This command lets you configure the regular intervals that the congested SPVPCs are monitored. Congestion improvement is determined at every interval. The default is 10 seconds. Enter the following:

```
myswitch::debug spvxcongestion> spvpc_tcongest <value>
```

1.7.9 Configuring SPVPC Congestion Improvement Threshold

This command lets you configure the improvement threshold of the congestion state. If the congestion threshold is reached, the SPVPC setup rate is increased. The default is 10%. Enter the following:

```
myswitch::debug spvxcongestion> spvpc_cthresh <value>
```

1.8 Trace Commands

The **trace** commands enable and disable the logging of additional debugging information to the console (if enabled) and to the remote syslog host (if enabled). Type **?** at the **trace** root level to list these commands.

```
myswitch::debug> trace ?
  all               atmroute>         atmstat>          calldebugging
  callrecording>    cdb               cem>              connections>
  dualscp>          filtering>        fram>             hardware>
  lane>             performance       securid           signalling>
  show              snmp>             sscop>            traceback>
  utility>
```

NOTE

All debug trace commands that are enabled (except **debug trace sscop** and **debug trace calldebugging>**) are saved across reboots via the configuration database (CDB). To see which trace commands are enabled, use the **debug trace show** command.

NOTE

Not all of the above commands are displayed on every platform. The **cem** command is only displayed on platforms supporting CEM network modules. The **fram** command is only displayed on platforms supporting *FramePlus* network modules. The **dualscp** command only displays on platforms supporting dual SCPs.

1.8.1 Debugging All Modules

This command lets you enable or disable the logging of debugging information for all network modules. Enter the following:

```
myswitch::debug trace> all (on | off)
```

CAUTION

Enabling all of the debugging traces results in logging of excessive volume of debugging information. This command should be used with caution.

1.8.2 ATM Route Trace Commands

The commands listed under the **atmroute** level, let you enable or disable the logging of debugging information for ATM routes. Type **?** at the **atmroute** level to list these commands.

```
myswitch::debug trace atmroute> ?
  atmroute          ftpnni            pnni>             rtmsgq
  rtloop            sctmr             scproc            ddtl
```

1.8.2.1 Debugging ATM Routing

This command lets you enable or disable the logging of debugging information for ATM routes. Enter the following:

```
myswitch::debug trace atmroute> atmroute (on | off)
```

1.8.2.2 Debugging *ForeThought* PNNI

This command lets you enable or disable the logging of debugging information for *ForeThought* PNNI. Enter the following:

```
myswitch::debug trace atmroute> ftpnni (on | off)
```

1.8.2.3 ATM Forum PNNI Trace Commands

The commands listed under the **pnni** level, let you enable or disable the logging of debugging information for ATM Forum PNNI. Type **?** at the **pnni** level to list these commands.

```
myswitch::debug trace atmroute pnni> ?
  basic             buffers           enhanced
```

1.8.2.3.1 Debugging Basic ATM Forum PNNI

This command lets you enable or disable the logging of basic debugging information for ATM Forum PNNI. Enter the following:

```
myswitch::debug trace atmroute pnni> basic (on | off)
```

1.8.2.3.2 Debugging ATM Forum PNNI Buffers

This command lets you enable or disable the logging of debugging information for ATM Forum PNNI buffers. This command parses the contained IGs for the Hello and PTSP packets, and displays formatted output. Enter the following:

```
myswitch::debug trace atmroute pnni> buffers (on | off) [-form (hex|parse)]
[-msg <hello|ptsp|dbsummary|ptsereq|ptseack>] [<portid>]
```

These parameters are defined as follows:

Parameter	Description
on | off	Entering **on** enables the logging of debugging information for the selected message type and / or port. Entering **off** disables the logging of debugging information for the selected message type and / or port.
-form (hex | parse)	Entering **hex** means the output is a hex dump. Entering **parse** means the output is a parsed, formatted output.
-msg (hello | ptsp | dbsummary | ptsereq | ptseack)	Indicates which type of packet to trace. If no type is entered, then all packets are affected.
portid	A 32-bit binary number that uniquely identifies the logical port on the node at each hop. Together, the *<nodeid>* and *<portid>* identify a PNNI link. Look in the `PortId` field under **display atmr pnni link** to find this number.

The following are examples of LGN hellos, outside hellos, inside hellos and PTSPs.

```
tAsx[X]:   debug: (2-fffffff): Received Hello packet
tAsx[X]:   debug: ********Start of Hello
Packet*******************************
tAsx[X]:   debug: NodeId   :
0:88:47.0005000000ae1e1e1e2e0000.ff1c5ce40002.00
tAsx[X]:   debug: PGId     : 0:00000000000000000000000000
tAsx[X]:   debug: AtmAddr  : 47000500.0000ae1e.1e1e2e05.46ff1c5c.e4000200
tAsx[X]:   debug: RmtNodeId:
0:88:47.0005000000ae1e1e1e3e0000.ff1c5e020002.00
tAsx[X]:   debug: PortIds  : Local (fffffff), Remote (fffffff)
tAsx[X]:   debug: Details  : Flags (0) Hello Interval (15)
tAsx[X]:   debug:
tAsx[X]:   debug: Horizontal link extension elems
```

AMI Debug Commands

```
tAsx[X]:   debug: aggr_token 0 local_lgn_port 0x30000001 rmt_lgn_port
0x30000000
tAsx[X]:   debug:
tAsx[X]:   debug: ********End of Hello
Packet*********************************
tAsx[X]:   debug: (2-ffffffff): Transmiting Hello packet
tAsx[X]:   debug: ********Start of Hello
Packet*******************************
tAsx[X]:   debug: NodeId   :
0:88:47.0005000000ae1e1e1e3e0000.ff1c5e020002.00
tAsx[X]:   debug: PGId     : 0:00000000000000000000000000
tAsx[X]:   debug: AtmAddr  : 47000500.0000ae1e.1e1e3e05.43ff1c5e.02000200
tAsx[X]:   debug: RmtNodeId:
0:88:47.0005000000ae1e1e1e2e0000.ff1c5ce40002.00
tAsx[X]:   debug: PortIds  : Local (ffffffff), Remote (ffffffff)
tAsx[X]:   debug: Details  : Flags (0) Hello Interval (15)
tAsx[X]:   debug:
tAsx[X]:   debug: Horizontal link extension elems
tAsx[X]:   debug: aggr_token 0 local_lgn_port 0x30000000 rmt_lgn_port
0x30000001
tAsx[X]:   debug:
tAsx[X]:   debug: ********End of Hello
Packet*********************************
tAsx[X]:   debug: (1-10000023): Transmiting Hello packet
tAsx[X]:   debug: ********Start of Hello
Packet*******************************
tAsx[X]:   debug: NodeId   :
88:160:47.0005000000ae1e1e1e3e0543.ff1c5e020001.00
tAsx[X]:   debug: PGId     : 88:470005000000ae1e1e1e3e0000
tAsx[X]:   debug: AtmAddr  : 47000500.0000ae1e.1e1e3e05.43ff1c5e.02000100
tAsx[X]:   debug: RmtNodeId:
88:160:47.0005000000ae1e1e1e2e0546.ff1c5ce40001.00
tAsx[X]:   debug: PortIds  : Local (10000023), Remote (10000020)
tAsx[X]:   debug: Details  : Flags (0) Hello Interval (15)
tAsx[X]:   debug: Ag. token: 0x0
tAsx[X]:   debug: [Nodal Hierarchy List (33) tags = 0000]
tAsx[X]:   debug:  SeqNumber  : 862960605        LevelCount : 1
tAsx[X]:   debug:  01. NdId :
0:88:47.0005000000ae1e1e1e3e0000.ff1c5e020002.00
tAsx[X]:   debug:      ATMA :
47000500.0000ae1e.1e1e3e05.43ff1c5e.02000200
tAsx[X]:   debug:      PgId : 0:00000000000000000000000000
tAsx[X]:   debug: [ULIA (34) tags = 0000]
```

```
tAsx[X]:   debug:  SeqNumber  : 862960613
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : CBR [0x8000]
tAsx[X]:   debug:    AdmnWeight : 5040
tAsx[X]:   debug:    MCR        : 5660377          ACR        : 5660377
tAsx[X]:   debug:    CTD        : 0                CDV        : 0
tAsx[X]:   debug:    CLP (0)    : 8                CLP (0+1)  : 8
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : rt-VBR [0x4000]
tAsx[X]:   debug:    AdmnWeight : 5040
tAsx[X]:   debug:    MCR        : 5660377          ACR        : 5660377
tAsx[X]:   debug:    CTD        : 0                CDV        : 0
tAsx[X]:   debug:    CLP (0)    : 8                CLP (0+1)  : 8
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : nrt-VBR [0x2000]
tAsx[X]:   debug:    AdmnWeight : 5040
tAsx[X]:   debug:    MCR        : 5660377          ACR        : 5660377
tAsx[X]:   debug:    CTD        : 0                CDV        : 0
tAsx[X]:   debug:    CLP (0)    : 8                CLP (0+1)  : 8
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : ABR [0x1000]
tAsx[X]:   debug:    AdmnWeight : 5040
tAsx[X]:   debug:    MCR        : 5660377          ACR        : 5660377
tAsx[X]:   debug:    CTD        : 0                CDV        : 0
tAsx[X]:   debug:    CLP (0)    : 8                CLP (0+1)  : 8
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : UBR [0x800]
tAsx[X]:   debug:    AdmnWeight : 5040
tAsx[X]:   debug:    MCR        : 5660377          ACR        : 5660377
tAsx[X]:   debug:    CTD        : 0                CDV        : 0
tAsx[X]:   debug:    CLP (0)    : 8                CLP (0+1)  : 8
tAsx[X]:   debug: ********End of Hello
Packet*********************************
tAsx[X]:   debug: (1-10000021): Received Hello packet
tAsx[X]:   debug: ********Start of Hello
Packet*******************************
tAsx[X]:   debug: NodeId   :
88:160:47.0005000000ae1e1e1e3e0544.ff1c5de40001.00
tAsx[X]:   debug: PGId     : 88:470005000000ae1e1e1e3e0000
tAsx[X]:   debug: AtmAddr  : 47000500.0000ae1e.1e1e3e05.44ff1c5d.e4000100
tAsx[X]:   debug: RmtNodeId:
88:160:47.0005000000ae1e1e1e3e0543.ff1c5e020001.00
tAsx[X]:   debug: PortIds  : Local (10000020), Remote (10000021)
```

```
tAsx[X]:   debug: Details  : Flags (0) Hello Interval (15)
tAsx[X]:   debug: ********End of Hello
Packet*********************************
tAsx[X]:   debug: (1-10000000): Transmiting PTSP packet
tAsx[X]:   debug: ********Start of PTSP
Packet********************************
tAsx[X]:   debug: Length (176)
tAsx[X]:   debug: NodeId :
88:160:47.00050000000000ae1e1e5864.ff1a58640001.00
tAsx[X]:   debug: PGId : 88:47000500000000000ae1e1e0000
tAsx[X]:   debug: Length : 140
tAsx[X]:   debug: PtseId (60000000) Sequence Number (11) Checksum (497c)
tAsx[X]:   debug: Remaining Lifetime (3599) Type (256) Flags (0)
tAsx[X]:   debug: [External Reachable ATM Address (256) tags = 0000]
tAsx[X]:   debug:  Flags      : VPCa [0x8000]
tAsx[X]:   debug:  PortId     : 0xfffffffe       Scope      : 0
tAsx[X]:   debug:  Ail        : 20
tAsx[X]:   debug:  01. 104:c5000500.00000000.ae1e1e05.56000000.00000000
tAsx[X]:   debug:  02. 104:d5000500.00000000.ae1e1e05.56000000.00000000
tAsx[X]:   debug: ->[Incoming Resource Availability (129) tags = 0000]
tAsx[X]:   debug:    Flags      : ABR [0x1000]
tAsx[X]:   debug:    AdmnWeight : 10
tAsx[X]:   debug:    MCR        : 3000             ACR        : 3000
tAsx[X]:   debug:    CTD        : -1               CDV        : -1
tAsx[X]:   debug:    CLP (0)    : 65535            CLP (0+1)  : 65535
tAsx[X]:   debug: ->[Outgoing Resource Availability (128) tags = 0000]
tAsx[X]:   debug:    Flags      : CBR rt-VBR [0xc000]
tAsx[X]:   debug:    AdmnWeight : 10
tAsx[X]:   debug:    MCR        : 1000             ACR        : -1
tAsx[X]:   debug:    CTD        : -1               CDV        : -1
tAsx[X]:   debug:    CLP (0)    : 65535            CLP (0+1)  : 65535
tAsx[X]:   debug: ********End of PTSP
Packet**********************************
tAsx[X]:   debug: (1-10000000): Received PTSE Ack packet
tAsx[X]:   debug: ********Start of PTSE Acknoledgement
Packet*****************
tAsx[X]:   debug: Length (40)
tAsx[X]:   debug: NodeId :
88:160:47.00050000000000ae1e1e5864.ff1a58640001.00
tAsx[X]:   debug: PtseId (60000000) Sequence Number (11) Checksum (497c)
tAsx[X]:   debug: Remaining Lifetime (3599) Type (0) Flags (0)
tAsx[X]:   debug: ********End of PTSE Acknoledgement
Packet*******************
```

1.8.2.3.3 Enhanced ATM Forum PNNI Debugging

This command lets you enable or disable the logging of enhanced debugging information for ATM Forum PNNI. This command is useful to debug obvious PNNI problems such as when a link does not reach two way inside. Enter the following:

```
myswitch::debug trace atmroute pnni> enhanced (on | off)
```

1.8.2.4 Debugging Routing Task Message Queues

This command lets you enable or disable the logging of routing task message queues. Enter the following:

```
myswitch::debug trace atmroute> rtmsgq (on | off)
```

1.8.2.5 Debugging Routing Task Loop

This command lets you enable or disable the logging of routing task loops. Enter the following:

```
myswitch::debug trace atmroute> rtloop (on | off)
```

1.8.2.6 Debugging Scheduler Timers

This command lets you enable or disable the logging of debug information of scheduler timers. Enter the following:

```
myswitch::debug trace atmroute> sctmr (on | off)
```

1.8.2.7 Debugging Scheduler Processes

This command lets you enable or disable the logging of scheduler processes. Enter the following:

```
myswitch::debug trace atmroute> scproc (on | off)
```

1.8.2.8 Debugging Directed DTLs

This command lets you enable or disable the logging of debugging information for directed Designated Transit Lists (DTLs). Enter the following:

```
myswitch::debug trace atmroute> ddtl (on | off)
```

1.8.3 ATM Trace Commands

The commands listed under the **atmstat** level, let you enable or disable the logging of debugging information for ATM statistics. Type **?** at the **atmstat** level to list these commands.

```
myswitch::debug trace atmstat> ?
  aal4                aal5                all
```

1.8.3.1 Debugging the AAL4 Layer

This command lets you enable or disable the logging of debugging information for the AAL4 layer. When enabled, this command displays statistics for the AAL 4 layer. It keeps dumping and logging the values periodically (every 1000 ms) until you disable it. Enter the following:

```
myswitch::debug trace atmstat> aal4 (on | off)
```

1.8.3.2 Debugging the AAL5 Layer

This command lets you enable or disable the logging of debugging information for the AAL5 layer. When enabled, this command displays statistics for the AAL 5 layer. It keeps dumping and logging the values periodically (every 1000 ms) until you disable it. Enter the following:

```
myswitch::debug trace atmstat> aal5 (on | off)
```

1.8.3.3 Debugging All AAL Layers

This command lets you enable or disable the logging of debugging information for all AAL layers. When enabled, this command displays statistics for the physical, ATM, and AAL layers. It keeps dumping and logging the values periodically (every 1000 ms) until you disable it. Enter the following:

```
myswitch::debug trace atmstat> all (on | off)
```

1.8.4 Per Call Debugging Commands

These commands let you enable call debugging for an SVC. Type **?** at the **calldebugging** level to list these commands.

```
myswitch::debug trace calldebugging> ?
  delete             new                show               templates
  transflag
```

To use this feature, first use **conf security template new** to create a template. Then specify that template when you create a Per Call Debugging (PCD) filter for an SVC based on its source and destination address. The PCD filter is compared to all incoming SVC SETUP and ADD-PARTY messages. If a match occurs, PCD debugging is enabled for the sending switch on which the match first occurs (matching switch) and for every subsequent switch (transient switch) in the path of the SVC.

For example, in Figure 1.1, since the matching switch is the actual origin of the SVC and the destination NSAP is another switch, then all four switches in this SVC will have PCD debugging enabled.

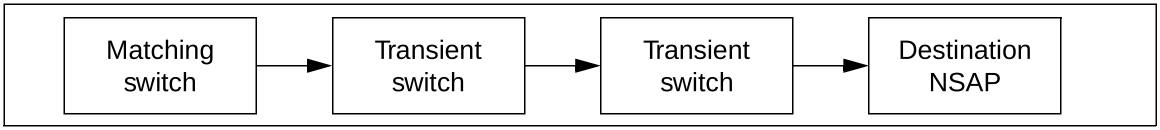

Figure 1.1 - SVC from an Matching Switch to a Destination NSAP

However, in the example in Figure 1.2, the matching switch is not the actual origin of the SVC. Switch A is the origin of the SVC. Also, in this example, the destination NSAP is not a switch. Therefore, only the matching switch (where the match first occurred) and the two transient switches in this SVC will have PCD debugging enabled.

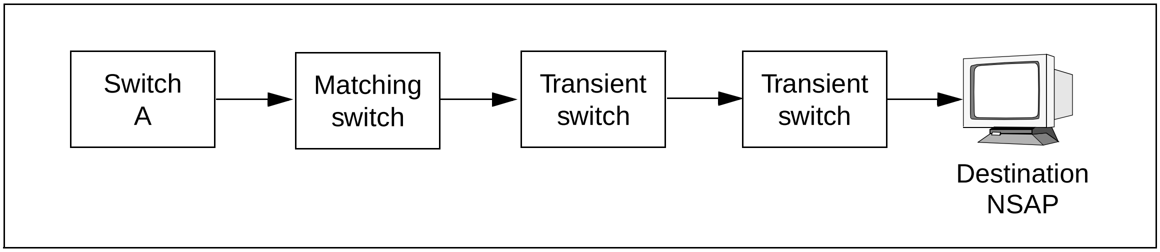

Figure 1.2 - SVC from Source to Destination

NOTE

PCD cannot be enabled on any originating switches for SPVX, NSAP-ping, or SVC RCCs calls. You must create a PCD filter on a transient switch for these types of calls.

1.8.4.1 PCD Templates and Filters

When creating a PCD filter, a template is used to minimize the amount of typing for filters that duplicate some information. The template menu, which was previously only used for address filtering, is located under **conf security template**. The parameter **-action** (**accept** | **reject**) is ignored by the PCD filter.

First, you create a template under **conf security template new** specifying the following:

- Ingress Port - Port on which the SVC is entering the switch.
- Ingress VPI -Virtual Path on which the SVC is entering the switch.
- Egress Port - Port on which the SVC is exiting the switch.
- Egress VPI -Virtual Path on which the SVC is exiting the switch.
- Source NSAP - NSAP address of the device where the SVC request originated.
- Destination NSAP - NSAP address of the destination device for the SVC.

A mask must be used when specifying the source and destination NSAPs. Any parameters that are not specified are wild carded.

Then you create a PCD filter using **conf security filter new** that specifies that template. If you want, you can re-use the template to create more filters. Filters can be viewed and modified through AMI. No more than 20 filters can be created on a switch. A current count of the number of SVCs matched for each filter is maintained.

(For more information about the **conf security template new** and **filter new** commands, please see Part 2 of the *AMI Configuration Commands Reference Manual*.)

NOTE

If a very generic filter were to be created, the switch could waste valuable memory processing large amounts of SVCs. Therefore, filters are automatically deleted after they have enabled PCD debugging on 20 SVCs.

Once a filter is created, all point-to-point, multipoint-to-point, and point-to-multipoint call setups are compared to the filter. Setup messages with no calling address have the source NSAP wild carded. If a match is found, PCD is enabled on the matching switch for that SVC. A Generic Application Transportation (GAT) Information Element is forwarded with the call setup to let the transient switches know that PCD is enabled for the SVC.

When the PCD GAT IE is received, that switch remains as a transient switch no matter what PCD filters are enabled on it. You can stop the logging of the PCD debugging on a switch by setting the **`-transflag`** to **`disabled`**. This disables logging at the switch level. When this parameter is disabled and the switch receives a PCD GAT IE, the switch does not log the PCD debugging, but it still forwards the PCD GAT IE, and the switch will not become a PCD matching switch.

NOTE

If a third-party switch receives the GAT IE, the GAT IE and/or the call set-up request may or may not be forwarded.

FORE switches that are running pre-*ForeThought* 5.0 versions, discard the GAT IE as an unrecognized element and reply with a STATUS message. However, the STATE within the STATUS message will be incorrect, so the call will probably get torn down.

FORE switches that are running a *ForeThought* 5.x or greater that receive the GAT IE on a PNNI interface simply forward the IE.

FORE switches that are running a *ForeThought* 5.x or greater that receive the GAT IE on a non-PNNI interface simply discard the IE as an unrecognized element.

Because the GAT IE is not standard for all of the various signalling versions and interface types, the following table shows which versions and types are supported.

Table 1.2 - Signalling Versions and Interface Types that Support the GAT IE

Interface	UNI 3.x	UNI 4.0	PNNI 1.0
Private UNI	Not Forwarded	Forwarded	N/A
Private NNI	N/A	N/A	Forwarded
FT-PNNI	Forwarded	Forwarded	N/A
Public UNI	Not Forwarded	Forwarded	N/A
IISP	Not Forwarded	Forwarded	N/A

If PCD debugging is enabled for an SVC that is exiting the switch on an unsupported interface, the debugging remains enabled on that switch and a warning message is logged.

1.8.4.2 Debug Message Format

The PCD debug messages are similar in format to the q93b messages, but they contain a unique prefix. This prefix consists of PCD plus a unique identifier which associates the message with a specific SVC. The identifier follows the SVC across each switch hop and consists of the following elements:

- Name - When you create a PCD filter, you can optionally assign a 16-character name. This name is printed with each debug message that is generated for SVCs that are enabled by the associated filter. If no name is assigned, it defaults to the <NSAP prefix> - <filter-id>.
- Counter - A counter is kept for each filter on which PCD is enabled. The counter increments for each SVC setup message that matches the filter.
- Hop Count - A counter is kept and incremented at each switch that the PCD GAT crosses and is processed.
- Call Ref - This is a representation of the Call Reference value associated with the call when the filter was first enabled.

1.8.4.3 Deleting a PCD Filter

This command lets you delete a PCD filter. Enter the following:

```
myswitch::debug trace calldebugging> delete [<Filter-id>]
```

This parameter is defined as follows:

Parameter	Description
<Filter-id>	The filter that you want to delete. This can be found by looking at the `Filter Id` field under **debug trace calldebugging show**.

For example, you would enter something similar to the following:

```
myswitch::debug trace calldebugging> delete 5
```

1.8.4.4 Creating a PCD Filter

This command lets you create a PCD filter. Enter the following:

```
myswitch::debug trace calldebugging> new <filter-id> <template-id> [<name>]
```

These parameters are defined as follows:

Parameter	Description
<filter-id>	The unique, user-assigned identifier for this filter. A filter-id is a positive, decimal integer (index). Zero is not a valid index.
<template-id>	The identifier for the existing template that you want to use. This can be found by looking at the `Index` field under **`conf security template show`**.
<name>	An optional, alphanumeric name which uniquely identifies the template. The name may be up to 16 characters. If no name is specified, a default name, which consists of the last six digits of the matching switch's default NSAP prefix, is assigned.

For example, you would enter something similar to the following:

```
myswitch::debug trace calldebugging> new 3 les1
```

1.8.4.5 Displaying the PCD Filters

This command lets you display all of the PCD filters or just a specific filter as follows:

```
myswitch::debug trace calldebugging> show [<Filter-id>]
Per Call Debugging Filter Table
-------------------------------------------
Filter    Template              Matches
 Id          Id         Name         Found
  1           1         les1         2
  2           3         1a3449       4
  3           2         shark        0
  4           5         badSvc       2
-------------------------------------------
```

The fields in this display are defined as follows:

Field	Description
Filter Id	The unique index number that identifies this filter.
Template IDs	The index number of the template specified in this filter. Only one template may be specified in a PCD filter.
Name	An optional, user-assigned name that identifies this filter.
Matches Found	The number of SVCs that matched the criteria in the filter.

1.8.4.6 Viewing a PCD Template

This command lets you view a PCD template. Enter the following:

```
myswitch::debug trace calldebugging> templates [<template-id or template-name>]
```

These parameters are defined as follows:

Parameter	Description
<template-id>	The identifier for the existing template that you want to view. This can be found by looking at the `Index` field under **`conf security templates show`**.
<template-name>	The name for the existing template that you want to view. This can be found by looking at the `Name` field under **`conf security templates show`**.

1.8.4.7 Enabling/Disabling PCD on a Transient Switch

This command lets you enable or disable PCD debugging on a transient switch or view the current state. To enable or disable PCD debugging, enter the following:

```
myswitch::debug trace calldebugging> transflag [<enabled | disabled>]
```

These parameters are defined as follows:

Parameter	Description
enabled | disabled	**enabled** means this transient switch will generate and print call debugging messages when it receives a PCD GAT IE. **disabled** means this transient switch will not generate and print call debugging messages when it receives a PCD GAT IE. The default is **enabled**.

To display whether PCD debugging is currently enabled or disabled, enter the following:

```
myswitch::debug trace calldebugging> transflag
The transflag is currently set to enabled.
```

1.8.5 Call Recording Trace Commands

The commands listed under the **callrecording** level, let you enable or disable the logging of call recording information. Type **?** at the **callrecording** level to list these commands.

```
myswitch::debug trace callrecording> ?
  crm                buffers
```

1.8.5.1 Debugging Call Recording Module

This command lets you enable or disable the logging of debugging information for the call recording module. Enter the following:

```
myswitch::debug trace callrecording> crm (on | off)
```

1.8.5.2 Debugging Call Recording Module Buffers

This command lets you enable or disable the logging of debugging information for the call recording module buffers. Enter the following:

```
myswitch::debug trace callrecording> buffers (on | off)
```

1.8.6 Debugging the Configuration Database

This command lets you enable or disable the logging of debugging information for the configuration database (CDB). Enter the following:

```
myswitch::debug trace> cdb (on | off)
```

1.8.7 CEM Trace Commands

The command listed under the **cem** level, let you enable or disable debugging information about the Circuit Emulation Services (CES) network modules that are installed in the switch fabric. The **cem** command is only displayed on platforms that can support Circuit Emulation (CEM) network modules. Type **?** at the **cem** level to list these commands.

```
myswitch::debug trace cem> ?
  cem                 cemsh               fdl                 memcheck
  rfc1406
```

1.8.7.1 Debugging Circuit Emulation

This command lets you enable or disable the logging of debugging information for the Circuit Emulation Services (CES) network modules. Enabling this command displays information that indicates that the scan routine is processing messages from the network module. Enter the following:

```
myswitch::debug trace cem> cem (on | off)
```

1.8.7.2 Debugging the Shared Memory

This command lets you enable or disable the logging of debugging information for the shared memory of the Circuit Emulation Services (CES) network modules. Enabling this command displays information that indicates the current state of the shared memory interface. If any messages are pending or the interface is experiencing problems, the queue is not likely to be empty. Enter the following:

```
myswitch::debug trace cem> cemsh (on | off)
```

1.8.7.3 Debugging CEM FDL

This command lets you enable or disable the logging of debugging information for the Circuit Emulation Services (CES) FDL. Currently, entering this command does not have any effect. Enter the following:

```
myswitch::debug trace cem> fdl (on | off)
```

1.8.7.4 Debugging Memory Check

This command lets you enable or disable the logging of memory check debugging information for the Circuit Emulation Services (CES) network modules. Entering this command does not have any effect.

```
myswitch::debug trace cem> memcheck (on | off)
```

1.8.7.5 Debugging the RFC 1406 Module

This command lets you enable or disable the logging of debugging information for the RFC1406 module. Enabling this command displays information that indicates that rfc1406 statistics are being correctly stored on the SCP for the indicated links. Only links in the administrative UP state will have statistics stored for them. Enter the following:

```
myswitch::debug trace cem> rfc1406 (on | off)
```

1.8.8 Connections Trace Commands

The commands listed under the **connections** level, let you enable or disable debugging information about connections. Type **?** at the **connections** level to list these commands.

```
myswitch::debug trace connections> ?
  driver             pvc                tm                 vc
```

1.8.8.1 Debugging the Virtual Channel Driver

This command lets you enable or disable the logging of debugging information for the VC driver. Enter the following:

```
myswitch::debug trace connections> driver (on | off)
```

1.8.8.2 Debugging PVC Module

This command lets you enable or disable the logging of debugging information for PVCs. Enter the following:

```
myswitch::debug trace connections> pvc (on | off)
```

1.8.8.3 Debugging Traffic Management Module

This command lets you enable or disable the logging of debugging information for traffic management. Enter the following:

```
myswitch::debug trace connections> tm (on | off)
```

1.8.8.4 Debugging Virtual Channel Module

This command lets you enable or disable the logging of debugging information for VCs. Enter the following:

```
myswitch::debug trace connections> vc (on | off)
```

1.8.9 Dual SCP Trace Commands

The commands listed under the **dualscp** level, let you enable or disable debugging information about dual SCPs. These command are applicable only if dual SCP configuration is utilized. The **dualscp** command is only displayed on platforms that can support dual SCP configuration. Type **?** at the **dualscp** level to list these commands.

```
myswitch::debug trace dualscp> ?
  selection          synchronization    mailbox            standby
```

1.8.9.1 Debugging Dual SCP Selection

This command lets you enable or disable the logging of debugging information for dual SCP selection. Enter the following:

```
myswitch::debug trace dualscp> selection (on | off)
```

1.8.9.2 Debugging Dual SCP File Synchronization

This command lets you enable or disable the logging of debugging information for the synchronization of files between dual SCPs. Enter the following:

```
myswitch::debug trace dualscp> synchronization (on | off)
```

1.8.9.3 Debugging the Dual SCP Mailbox Messages

This command lets you enable or disable the logging of debugging information for the dual SCP mailbox messages. Enter the following:

```
myswitch::debug trace dualscp> mailbox (on | off)
```

1.8.9.4 Debugging the Standby File System

This command lets you enable or disable the logging of debugging information for the standby file system for dual SCPs. Enter the following:

```
myswitch::debug trace dualscp> standby (on | off)
```

1.8.10 Filtering Trace Commands

The commands listed under the **filtering** level let you enable or disable debugging information about filtering. Type **?** at the **filtering** level to list these commands.

```
myswitch::debug trace filtering> ?
  address            failures           iefilter           ipfilter
```

1.8.10.1 Debugging Address Filtering

This command lets you enable or disable the logging of debugging information for address filtering. Enter the following:

```
myswitch::debug trace filtering> address (on | off)
```

1.8.10.2 Debugging Address Filtering Rejected Calls

This command lets you enable or disable the logging of debugging information for calls rejected by address filtering. Enter the following:

```
myswitch::debug trace filtering> failures (on | off)
```

1.8.10.3 Debugging Element (IE) Filtering Information

This command lets you enable or disable the logging of debugging information for IE filtering. Enter the following:

```
myswitch::debug trace filtering> iefilter (on | off)
```

1.8.10.4 Debugging IP Filtering

This command lets you enable or disable the logging of debugging information for IP filtering. Enter the following:

```
myswitch::debug trace filtering> ipfilter (on | off)
```

1.8.11 FRAM Trace Commands

The commands listed under the **fram** level, let you enable or disable debugging Frame/FUNI related information. These commands are applicable only if a *FramePlus* network module is installed in your switch. The **fram** command is only displayed on platforms that can support the *FramePlus* network module. Type **?** at the **fram** level to list these commands.

```
myswitch::debug trace fram> ?
  inmsdpm          ifcallback         iwf                funiconnsnmp
  frf8connsnmp     profiles
```

1.8.11.1 Debugging the Shared Dual Port Memory API

This command lets you enable or disable shared dual port memory debugging information for the *FramePlus* network module. Enter the following:

```
myswitch::debug trace fram> inmsdpm (on | off)
```

1.8.11.2 Debugging the Ifcallback Function

This command lets you enable or disable debugging information for the ifcallback function. Enter the following:

```
myswitch::debug trace fram> ifcallback (on | off)
```

1.8.11.3 Debugging the Interworking Functions

This command lets you enable or disable debugging information for the interworking functionality (IWF) of the *FramePlus* network module. Enter the following:

```
myswitch::debug trace fram> iwf (on | off)
```

1.8.11.4 Debugging FUNI Connection SNMP Agent

This command lets you enable or disable SNMP debugging information for the FUNI connection SNMP agent. Enter the following:

```
myswitch::debug trace fram> funiconnsnmp (on | off)
```

1.8.11.5 Debugging FRF8 Connection SNMP Agent

This command lets you enable or disable SNMP debugging information for the FRF8 connection SNMP agent. Enter the following:

```
myswitch::debug trace fram> frf8connsnmp (on | off)
```

1.8.11.6 Debugging the Frame Relay Network Module Tools

This command lets you enable or disable debugging information for the profiles. Enter the following:

```
myswitch::debug trace fram> profiles (on | off)
```

1.8.12 Hardware Trace Commands

The commands listed under the **hardware** level, let you enable or disable debugging information about the switch hardware. Type **?** at the **hardware** level to list these commands.

```
myswitch::debug trace hardware> ?
esic                fabric>             netmod>             timing
```

1.8.12.1 Debugging ESIC Control Module

This command lets you enable or disable debugging information for the ESIC control module. Enter the following:

```
myswitch::debug trace hardware> esic (on | off)
```

1.8.12.2 Fabric Trace Commands

The command listed under the **fabric** level, let you enable or disable debugging information about the switch fabric. Type **?** at the **fabric** level to list these commands.

```
myswitch::debug trace hardware fabric> ?
  aal                 fabric              oam                 shmem
```

1.8.12.2.1 Debugging the AAL Layer

This command lets you enable or disable the logging of debugging information for the AAL layer. Enter the following:

```
myswitch::debug trace hardware fabric> aal (on | off)
```

1.8.12.2.2 Debugging the Fabric Layer

This command lets you enable or disable the logging of debugging information for the fabric layer. Enter the following:

```
myswitch::debug trace hardware fabric> fabric (on | off)
```

1.8.12.2.3 Debugging the OAM Processing Cells

This command lets you enable or disable the logging of debugging information for OAM cells. Enter the following:

```
myswitch::debug trace hardware fabric> oam (on | off)
```

1.8.12.2.4 Debugging the Shared Memory Module

This command lets you enable or disable the logging of debugging information for the shared memory module. Enter the following:

```
myswitch::debug trace hardware fabric> shmem (on | off)
```

1.8.12.3 Network Module Trace Commands

The commands listed under the **netmod** level, let you enable or disable debugging information about the network modules. Type **?** at the **netmod** level to list these commands.

```
myswitch::debug trace hardware netmod> ?
  netmod              scan
```

1.8.12.3.1 Debugging the Network Modules

This command lets you enable or disable the printing of debug messages during the initialization of the network module, and the generation of alarms due to physical layer defects. Enter the following:

```
myswitch::debug trace hardware netmod> netmod (on | off)
```

1.8.12.3.2 Debugging the Network Module Scan Routines

This command lets you enable or disable the logging of debugging information for network module scan routines that aggregates the physical layer defects, generates alarms/traps and generates physical layer statistics. Enter the following:

```
myswitch::debug trace hardware netmod> scan (on | off)
```

1.8.12.4 Debugging Timing

This command lets you enable or disable debugging information about timing. Enter the following:

```
myswitch::debug trace hardware> timing (on | off)
```

1.8.13 LANE Trace Commands

The commands listed under the **lane** level, let you enable or disable debugging information about LAN Emulation (LANE). Type **?** at the **lane** level to list these commands.

```
myswitch::debug trace lane> ?
  lanem              leframe
```

1.8.13.1 Debugging LAN Emulation

This command lets you enable or disable LANE debugging information. Usually, the messages that display are those that happen when LANE control messages get exchanged or there is transition in the state of a LANE entity. Enter the following:

```
myswitch::debug trace lane> lanem (on | off)
```

1.8.13.2 Debugging LAN Emulation Control Framing

This command lets you enable or disable debugging information about LAN Emulation control framing received and transmitted by a LANE server (LES/BUS/LECS) to the debug port. To help aid in debugging, the frames are printed in readable text format rather than printing a hex dump of the frame. Enter the following:

```
myswitch::debug trace lane> leframe (on | off)
```

1.8.14 Debugging Performance/Utilization Statistics

This command lets you enable or disable periodic dumps of system performance/utilization statistics such as timeouts and dispatches per second. Enter the following:

```
myswitch::debug trace> performance (on | off)
```

1.8.15 Debugging SecurID Information

This command lets you enable or disable SecurID debugging information. Enter the following:

```
myswitch::debug trace> securid (on | off)
```

1.8.16 Signalling Trace Commands

The commands listed under the **signalling** level, let you enable or disable the debugging of signalling information. Type **?** at the **signalling** level to list these commands.

```
myswitch::debug trace> signalling> ?
  clip               cls                q93b>              spans>
```

1.8.16.1 Debugging Classical IP

This command lets you enable or disable debugging information about Classical IP. Enter the following:

```
myswitch::debug trace signalling> clip (on | off)
```

1.8.16.2 Debugging Connectionless Service

This command lets you enable or disable debugging information about connectionless service. Enter the following:

```
myswitch::debug trace signalling> cls (on | off)
```

1.8.16.3 Q93b Trace Commands

The commands listed under the **q93b** level, let you enable or disable debugging Q93b information. Type **?** at the **q93b** level to list these commands.

```
myswitch::debug trace signalling q93b> ?
  autoconf           callfwd            dbuf               driver
  fail-locate        ilmi               ilmidump           pnnispvxall
  pnnispvxcongest    pnnispvxdst        pnnispvxgen        pnnispvxsrc
  pnnispvxstat       q93b               q93b_translate_uni3x_atc
```

1.8.16.3.1 Debugging the Autoconfiguration Module

This command lets you enable or disable the autoconfiguration of the signalling entity. Events from ILMI, signalling, and routing are received. You can specify a specific port and vpi. Enter the following:

```
myswitch::debug trace signalling q93b> autoconf  (on | off) [<port> <vpi>]
```

1.8.16.3.2 Debugging the Call Forwarding and CAC Modules

This command lets you enable or disable the logging of debugging information for the call control layer. You can either enable/disable debugging information on all interfaces or on a per-interface basis. If the port and vpi are specified, then the call control debugging is enabled/disabled for the signalling events received on that particular signalling interface only. Both port and vpi must be specified to enable per-port call control debugging information.

The call control debugging state is stored in the CDB so that the per-interface call control debugging state is retained across reboots. The debugging state for the control port is not retained across reboots. The debugging state for the control port is automatically turned off.

Enter the following:

```
myswitch::debug trace signalling q93b> callfwd (on | off) [port][vpi]
```

To see if call control debugging is enabled/disabled for a particular interface, you can enter the **`debug trace show`** command or **`debug dump signalling q93b uni`** command.

NOTE

SPVPC/SPVCC module also uses the call control module for some common functions. To display debugging information during this interaction, call control debugging has to be enabled globally. Enabling per-interface debugging on all interfaces does not cause this debugging information to be printed on the console.

1.8.16.3.3 Debugging the Q93b Packets

This command lets you enable or disable the logging of debugging information for Q93b packets. Enabling this feature allows you to display packets in raw hexadecimals. Enter the following:

```
myswitch::debug trace signalling q93b> dbuf (on | off)
```

1.8.16.3.4 Debugging the Q93b Driver

This command lets you enable or disable the logging of debugging information for the Q93b driver. Enter the following:

```
myswitch::debug trace signalling q93b> driver (on | off)
```

1.8.16.3.5 Determining Call Failure Location

This command lets you enable/disable the call failure location feature. When a call fails to be established, enabling this command will help determine at which point in the network the call had failed. The generation of call failure location information is disabled by default. The **`fail-locate`** setting is saved across reboots. Enter the following:

```
myswitch::debug trace signalling q93b> fail-locate (on | off)
```

To view the failure location of an SPVC or SPVP, enter **`configuration spvx spvcc pnni pp show advanced, configuration spvx spvcc pnni pmp show advanced`**. or **`configuration spvx spvpc show advanced`**. Once the failing location is pinpointed, enable debugging of selected ports to display more detail to help identify the individual call that is failing.

AMI Debug Commands

The failed location of an SVC can be displayed via the syslog or a telnet session to the debug port (6532). To view the failure location, turn on Q93b tracing using the **debug trace signalling q93b q93b on** command, turn on the raw hexadecimal display of packets using the **debug trace signalling q93b dbuf on** command, and then examine the output using the ATM Signalling Trace (SigTrace) utility. SigTrace is a utility written to parse debug output produced by FORE ATM switches and adapters. SigTrace produces a meaningful decode of hexadecimal dumps of ATM Forum UNI and PNNI signalling messages received or transmitted from the device. The following is the output of a sample sigTrace:

```
Call Reference Value:        0x002b2d
Message Type:                Release Complete
  Message Length:            36 bytes
Information Element Name:    Cause
  Element Length:            3 bytes
  Location:                  Private network serving the local user
  Cause:                     No route to destination
  Diagnostics:               Present (listed below)
  Location of Error:         Network service - Provider
  Type of Error:             Normal
  Condition:                 Unknown
Information Element Name:    Cause
  Element Length:            25 bytes
  Location:                  Private network serving the local user
  Cause:                     Call rejected
  Diagnostics:               Present (listed below)
  Rejection Reason:          User Specific
  Condition:                 Unknown
  FORE Specific:             00-20-48
  Call Failure Location:     Local
  Port Name:                 D2
  VPI Value:                 0
  Switch Prefix Type:        Default
  NSAP Prefix:               0x47.0005.80ffe1000000f21a39ab
```

Enabling the fail-locate command inserts the NSAP prefix of where the call failed.

1.8.16.3.6 Debugging ILMI Request Processing

This command lets you enable or disable the logging of debugging information for ILMI request processing. Enter the following:

```
myswitch::debug trace signalling q93b> ilmi (on | off)
```

1.8.16.3.7 Displaying ILMI Packets

This command lets you enable or disable the logging of debugging information for ILMI packets or display ILMI packets. Enter the following:

```
myswitch::debug trace signalling q93b> ilmidump (on | off | show) [link]
```

1.8.16.3.8 Debugging All SPVPCs and SPVCCs

This command lets you enable or disable the logging of all originating SPVPCs and SPVCCs, all terminating SPVPCs and SPVCCs, and all general debugging information. Enabling this command also enables congestion related debugging of SPVPCs and SPVCCs. See Section 1.8.16.3.9 for more information on the **debug spvxcongestion** commands. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxall (on | off)
```

1.8.16.3.9 Debugging PNNI Congestion SPVPCs and SPVCCs

This command lets you enable or disable the logging of congested SPVPCs and SPVCCs. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxcongest (on | off)
```

1.8.16.3.10 Debugging Terminating PNNI SPVPCs and SPVCCs

This command lets you enable or disable the logging of all terminating SPVPCs and SPVCCs. This command does not allow you to enable or disable on a per SPVPC/SPVCC basis since the destination SPVPC/SPVCC index is picked automatically, and therefore cannot be obtained before the terminating SPVPC/SPVCC is setup successfully. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxdst (on | off)
```

1.8.16.3.11 Debugging General PNNI SPVPCs and SPVCCs

This command lets you enable or disable the logging of debugging information that does not pertain to any particular originating or terminating SPVPCs or SPVCCs. The debugging messages include the messages printed out by the common utility functions, pacing module, reroute module, etc. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxgen (on | off)
```

1.8.16.3.12 Debugging Originating PNNI SPVPCs and SPVCCs

This command lets you enable or disable the logging of originating SPVPCs and SPVCCs. Specifying **on** or **off** enables/disables debugging for all originating SPVPCs and SPVCCs. Any newly created SPVPC or SPVCC will automatically be turned on or off depending on what was specified. Specifying the VCC, VPC, and SPVXID allows you to enable/disable debugging information for a particular SPVPC or SPVCC. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxsrc (on | off) [vcc|vpc] [spvxid]
```

1.8.16.3.13 Displaying the Debugging Status for PNNI SPVPCs and SPVCCs

This command lets you display whether debugging is enabled or disabled for each originating SPVPC/SPVCC, each terminating SPVPC/SPVCC, and each general SPVPC/SPVCC. Enter the following:

```
myswitch::debug trace signalling q93b> pnnispvxstat
Destination PNNI SPVPC/SPVCC Debug Status : Enabled
General PNNI SPVPC/SPVCC Debug Status :Disabled
Source PNNI SPVCC Debug Status :
SPVCC 1 : debug state = disabled
SPVCC 16567 : debug state = enabled
Source PNNI SPVPC Debug Status :
SPVPC 1 : debug state = disabled
SPVPC 2 : debug state = enabled
```

1.8.16.3.14 Debugging Q93b Signalling

This command lets you enable or disable the logging of debugging information for Q93b signalling. Enter the following:

```
myswitch::debug trace signalling q93b> q93b (on | off) [<port> <vpi>]
[pass_along | iwx | testing]
```

1.8.16.3.15 Specifying ATC Translation

This command lets you enable or disable the ATM transfer capability translation option. You can also show the current state of the translation option (off or on). This option allows UNI3.x ATC values to be translated to UNI4.0/PNNI compliant values when routed through UNI4.0/PNNI interfaces. The translation option is off by default. Enter the following:

```
myswitch::debug trace signalling q93b> q93b_translate_uni3x_atc (on | off | show | help )
```

1.8.16.4 SPANS Trace Commands

The commands listed under the **spans** level, let you enable or disable the debugging of SPANS information. Type **?** at the **spans** level to list these commands.

```
myswitch::debug trace signalling spans> ?
  driver            group             nni               spans
  spansspvc
```

1.8.16.4.1 Debugging the SPANS Driver

This command lets you enable or disable the logging of debugging information for the SPANS driver. Enter the following:

```
myswitch::debug trace signalling spans> driver (on | off)
```

1.8.16.4.2 Debugging SPANS Group Messages

This command lets you enable or disable the logging of debugging information for SPANS group messages. Enter the following:

```
myswitch::debug trace signalling spans> group (on | off)
```

1.8.16.4.3 Debugging SPANS Router Information

This command lets you enable or disable the logging of debugging information for the SPANS router. Enter the following:

```
myswitch::debug trace signalling spans> nni (on | off)
```

1.8.16.4.4 Debugging SPANS

This command lets you enable or disable the logging of debugging information for SPANS signalling. Enter the following:

```
myswitch::debug trace signalling spans> spans (on | off)
```

1.8.16.4.5 Debugging SPANS SPVC Connections

This command lets you enable or disable the logging of debugging information for SPANS SPVCCs. Enter the following:

```
myswitch::debug trace signalling spans> spansspvc (on | off)
```

1.8.17 Displaying Debugging Enabled Features

This command lets you display which features have debugging information enabled. In addition, call control debugging status for each of the signalling interfaces are displayed. Enter the following:

```
myswitch::debug trace> show
Q93B

 UNI[ 0, 0]:      Enabled
                  Pass Along - Disabled
                  SSCOP - Disabled: Mask : 0x0
                  Call Ctrl - Disabled

 UNI[ 1, 0]:      Enabled
                  Pass Along - Disabled
                  SSCOP - Disabled: Mask : 0x0
                  Call Ctrl - Disabled

 UNI[ 2, 0]:      Disabled
                  Pass Along - Disabled
                  SSCOP - Disabled: Mask : 0x0
                  Call Ctrl - Disabled

 UNI[26, 0]:      Enabled
                  Pass Along - Disabled
                  SSCOP - Disabled: Mask : 0x0
                  Call Ctrl - Enabled
```

1.8.18 SNMP Trace Commands

The commands listed under the **snmp** level, let you enable or disable debugging SNMP information. Type **?** at the **snmp** level to list these commands.

```
myswitch::debug trace snmp> ?
  errors             packets
```

1.8.18.1 Debugging SNMP Errors

This command lets you enable or disable the printing of debugging information for SNMP errors. Enter the following:

```
myswitch::debug trace snmp> errors (on | off)
```

1.8.18.2 Debugging SNMP Packets

This command lets you enable or disable the printing of every SNMP PDU (including ILMI packets) sent and received by the switch. It dumps the BER encoded PDU which is useful in debugging. Enter the following:

```
myswitch::debug trace snmp> packets (on | off)
```

You should see something similar to the following when this command has been enabled:

```
tAsx[X]:  NOTICE: Sending 55 bytes to ILMI 1/34:
tAsx[X]:  NOTICE: 30 82 00 33  02 01 00 04  04 49 4C 4D   0..3.....ILM
tAsx[X]:  NOTICE: 49 A2 82 00  26 02 04 59  46 E6 7E 02   I...&..YF.~.
tAsx[X]:  NOTICE: 01 00 02 01  00 30 82 00  16 30 82 00   .....0...0..
tAsx[X]:  NOTICE: 12 06 0D 2B  06 01 04 01  82 61 02 02   ...+.....a..
tAsx[X]:  NOTICE: 01 01 09 00  02 01 03                    .......
tAsx[X]:  NOTICE: sending 60 bytes to ILMI 1/32:
tAsx[X]:  NOTICE: 30 82 00 38  02 01 00 04  04 49 4C 4D   0..8.....ILM
tAsx[X]:  NOTICE: 49 A4 2D 06  08 2B 06 01  04 01 03 01   I.-..+......
```

NOTE

Because the output of this command is several pages long, only the beginning of the output is shown here.

AMI Debug Commands

1.8.19 SSCOP Trace Commands

The commands listed under the **sscop** level, let you enable or disable debugging Service Specific Connection Oriented Protocol (SSCOP) information. Type **?** at the **sscop** level to list these commands.

```
myswitch::debug trace sscop> ?
  driver              sscop
```

1.8.19.1 Debugging the SSCOP Driver

This command lets you enable or disable the logging of debugging information for the SSCOP driver. Enter the following:

```
myswitch::debug trace sscop> driver (on | off)
```

1.8.19.2 Debugging SSCOP

This command lets you enable or disable the logging of debugging information for SSCOP. Enter the following:

```
myswitch::debug trace sscop> sscop (on | off) [<mask>] [<port> <vpi> ...]
SSCOP_DEBUG_PDUIO   0x00000001
SSCOP_DEBUG_SIGNAL  0x00000002
SSCOP_DEBUG_TIMEOUT 0x00000004
SSCOP_DEBUG_EVENT   0x00000008
SSCOP_DEBUG_STATS   0x00000020
SSCOP_DEBUG_MEM     0x00000040
SSCOP_DEBUG_ERROR   0x00000080
SSCOP_DEBUG_QUEUE   0x00000100
SSCOP_DEBUG_ALWAYS  0x11111111
```

1.8.20 Traceback Trace Commands

The commands listed under the **traceback** level, let you enable or disable debugging trace-back information for various levels of log messages. Type **?** at the **traceback** level to list these commands.

```
myswitch::debug trace traceback> ?
  error             info              notice            warning
```

1.8.20.1 Debugging Log_Error

This command lets you enable or disable the logging of debugging information for LOG_ERROR. Enter the following:

```
myswitch::debug trace traceback> error (on | off)
```

1.8.20.2 Debugging Log_Info

This command lets you enable or disable the logging of debugging information for LOG_INFO. Enter the following:

```
myswitch::debug trace traceback> info (on | off)
```

1.8.20.3 Debugging Log_Notice

This command lets you enable or disable the logging of debugging information for LOG_NOTICE. Enter the following:

```
myswitch::debug trace traceback> notice (on | off)
```

1.8.20.4 Debugging Log_Warning

This command lets you enable or disable the logging of debugging information for LOG_WARNING. Enter the following:

```
myswitch::debug trace traceback> warning (on | off)
```

1.8.21 Utility Trace Commands

The commands listed under the **utility** level, let you enable or disable debugging utility information. Type **?** at the **utility** level to list these commands.

```
myswitch::debug trace utility> ?
  dispatch          event             listhash          lowlevel
  time              support
```

1.8.21.1 Debugging the Dispatch Module

This command lets you enable or disable the logging of debugging information for the dispatch module. Enter the following:

```
myswitch::debug trace utility> dispatch (on | off)
```

1.8.21.2 Debugging the Event Module

This command lets you enable or disable the logging of debugging information for the event module. Enter the following:

```
myswitch::debug trace utility> event (on | off)
```

1.8.21.3 Debugging the List and Hashing Functions

This command lets you enable or disable the logging of debugging information for the list and hashing functions. Enter the following:

```
myswitch::debug trace utility> listhash (on | off)
```

1.8.21.4 Debugging the Low Level Utility Routines

This command lets you enable or disable the logging of debugging information for the low level utility routines. Enter the following:

```
myswitch::debug trace utility> lowlevel (on | off)
```

1.8.21.5 Debugging the Timeout Module

This command lets you enable or disable the logging of debugging information for the timeout module. Enter the following:

```
myswitch::debug trace utility> time (on | off)
```

1.8.21.6 Debugging the Dispatch and Timeout Modules

This command lets you enable or disable the logging of debugging information for the dispatch and timeout modules. Enter the following:

```
myswitch::debug trace utility> support (on | off)
```

CHAPTER 2 Error Messages

This chapter lists and describes system error messages that may display on the console and syslog output during operation.

The error messages are organized alphabetically according to the system element that produces the messages. Each error message is assigned an entry number between the range 0 through 255. A short error message (prefix) description, a detailed error description, and a possible solution for correcting the error is provided. Not all messages indicate problems with your system. Some are purely informational while others may help diagnose specific hardware or software problems.

2.1 ALRM Error Messages

ALRM0: Defect detected

This indicates that a defect has been detected on the incoming link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects at the physical layer.

Possible Solution **-** Informational message.

ALRM1: Defect cleared

This indicates that a defect has been cleared on the incoming link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects at the physical layer.

Possible Solution **-** Informational message.

ALRM2: Failure declared

This indicates that a failure has been declared on the incoming link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects at the physical layer. When a defect is detected, a failure is declared, usually after the defect is found to persist for a specified period of time. For example, a SONET network module monitors the incoming link for the Loss of Signal (LOS) defect and declares a failure if the defect persists for 2.5 (± 0.5) seconds.

Possible Solution **-** Informational message.

ALRM3: Failure cleared

This indicates that a failure has been cleared on the incoming link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects at the physical layer. When a defect is cleared, the failure that was declared when the defect was detected, is cleared, usually after the defect is found to be absent for a specified period of time. For example, a SONET network module monitors the incoming link for the Loss of Signal (LOS) defect, and clears the LOS failure if the defect is clear for 10 (± 0.5) seconds.

***Possible Solution* -** Informational message.

ALRM4: Signal generated

This indicates that a signal has been generated on an outgoing link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects and/or failures at the physical layer. When a defect is detected or a failure is declared, a signal is generated on the outgoing link to alert upstream terminals of a downstream defect or failure. For example, a SONET network module generates a Remote Defect Indication (RDI) signal upon detecting a defect in the incoming link.

***Possible Solution* -** Informational message.

ALRM5: Signal deactivated

This indicates that a signal has been deactivated on an outgoing link. All incoming signals, optical or electrical, are monitored for the presence or absence of defects and/or failures at the physical layer. When a defect is cleared or a failure is cleared, the signal that was generated on the outgoing link when the defect was detected, is deactivated to inform the upstream terminals. For example, a SONET network module deactivates a Remote Defect Indication (RDI) signal if the defect is clear for 10 (±- 0.5) seconds.

***Possible Solution* -** Informational message.

2.2 ASX Error Messages

ASX0: Information

The user has requested an ID (internal like connid or external like VPI) that does not fall within the available range.

Possible Solution - Verify the actual range. If requesting a VP, verify the link's VP range. If requesting a VC, verify the terminating path's VC range.

ASX1: Error

This software operation is not legal.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

ASX2: Notice

Non extended mode by definition requires the output ID to be equivalent for all outputs.

Possible Solution - Make sure the output requested is the same as all other point-to-multipoint outputs.

ASX3: Notice

This ID has been used previously.

Possible Solution - Verify where the ID has already been allocated.

2.3 ATIF Error Messages

ATIF0: Failure to allocate splay tree for asxatmif table

This message indicates a failure to allocate memory due to some unknown reason. The failure may possibly be due to a lack of free memory on the system, or a corrupt CDB.

Possible Solution - Informational message.

ATIF1: Failure to initialize atmif table

This message indicates a failure to initialize the atmif table.

Possible Solution - Informational message.

2.4 ATMR Error Messages

ATMR0: Failure on restriction

This is a very generic and widely used message type. It is usually printed as a Warning. It mostly reports all restrictions and the complete message gives more information.

Possible Solution - Check the PNNI node, FTPNNI node, and Domain information through AMI for more information. It indicates any of the following restrictions:

1. The maximum number of logical nodes supported in the switch are 2 including the FT-PNNI node. Therefore, (2 PNNI logical nodes) or (1 PNNI node and 1 FT-PNNI node) can exist. Sometimes, one of the nodes has to be deleted to bring the switch up with PNNI or FT-PNNI.
2. The Fore Area of the PNNI node and that of the FT-PNNI node should not be the same.
3. The Fore Level of the PNNI node and that of the FT-PNNI node should not be the same.
4. Two PNNI nodes in the same Fore area should not have different Fore levels.
5. Two PNNI nodes in the same Fore area should not have the same node IDs.
6. Two PNNI nodes in different Fore areas should not have the same Fore levels.
7. Two PNNI nodes in different Fore areas should not have the same peer group IDs.

ATMR1: Sanity check failed

This warning message indicates an internal error situation indicating a sanity check failure for an input link node or for an output link node. The message usually prints the function name. Sanity check basically compares two node IDs or NSAP addresses. In the case of a node ID comparison, if they are equal, a value of TRUE is returned; otherwise, a value of FALSE is returned. In the case of an NSAP comparison, if the first address is greater than the second, a value of 1 is returned and if they are equal, a value of 0 is returned; otherwise, a value of -1 is returned. This check is needed because the DTLs node and the node that receives this DTL should be same.

Possible Solution - Informational message.

ATMR2: DTL transit pointer less than 2

This warning message indicates an internal error situation and prints the function name. Transit pointer:trans_ptr is an element in the DTL structure. It is unsigned integer that should not be less than 2. This check is done generally at the beginning of the function. This is needed only in FT-PNNI (not in PNNI). A DTL is not used when the source and destinations are directly connected. When it is used, at least one hop is required.

Possible Solution - Informational message.

ATMR3: Error in computing

This warning message indicates an internal error situation. The message prints an error in computing bandwidth and shows in which direction the error occurred, and the function name. Bandwidth is computed based only on the traffic descriptors contained in the SDU. The bandwidth is computed in the forward and reverse directions and service type and traffic characteristics are obtained.

Possible Solution - Informational message.

ATMR4: Unknown

This is a generic warning message, used most often when a logical path through the software logic is, for some reason, not taken.

Possible Solution - Informational message.

ATMR5: DTL exhausted prematurely

This warning message indicates an internal error situation and prints the function name. The DTL structure has transit pointer, reference counter, and node elements listed as elements. There are functions like atmr_dtl_atmf_get_cur_transit and atmr_dtl_ft_get_cur_node_elem to get these elements. If they are NULL, then the DTL is said to exhaust prematurely. Sometimes the same error is specified if that DTL has no current transit pointer.

Possible Solution - Informational message.

ATMR6: Failed to flip dtl

This warning message indicates an internal error situation and prints the function name. The path computation is done from destination to source. Then the DTL is flipped so that it is from source to destination, and it is given to signalling software. This function could return an error when there is no node, no horizontal link, or no back link.

Possible Solution - Informational message.

ATMR7: sdu has no

This warning message indicates an internal error scenario in which one of the SDU's elements is NULL or empty. An ATM connection has an SDU of type q93b_sdu. This data structure holds the individual elements which make up the the various messages used in the Q.93B signalling. The presence or absence of an individual element is indicated by the appropriate bit being set in the elems structure. This information structure is used for both the transmitting and receiving of messages.

***Possible Solution* -** Informational message.

ATMR8: local route does not have enough bandwidth for

When path computation reaches the last leg, local routes (ILMI registered routes, static routes and PNNI reachable address) are examined to find the best route to the destination. If any of those routes does not have enough bandwidth to meet the QoS requirements, this message is printed along with the function name.

***Possible Solution* -** Informational message.

ATMR9: Failed to find local route with required qos in

When local route computation is being done for a PNNI exterior reachable address and if none of the addresses satisfy the QoS requirements, this error occurs and this message is printed along with the function name and other information.

***Possible Solution* -** Informational message.

2.5 AUTO Error Messages

AUTO0: Info

This does not indicate any failure.

Possible Solution - Informational message.

AUTO1: Warning

This indicates a warning situation. The condition may not be as serious as an error but warrants attention nonetheless.

Possible Solution - Informational message.

AUTO2: Error

This indicates a serious error situation.

Possible Solution - The message should be recorded and should be reported to the technical support as soon as possible.

AUTO3: Debug

Debugging messages.

Possible Solution - Informational message.

2.6 CACS Error Messages

CACS0: Information

This is used to print the values of certain important variables that give additional information to any preceding warning or error messages.

Possible Solution - Informational message.

CACS1: Notification

If any important events happen in the call control layer that the network administrator should know about, these notification messages are used.

Possible Solution - Informational message.

CACS2: Warning

This indicates a potential source of a problem, that the switch may recover from. These warning messages will be helpful in diagnosing such problems.

Possible Solution - Informational message.

CACS3: Debug

This contains debugging related information which may be useful to trace any error condition.

Possible Solution - Informational message.

CACS4: Parameter Validation Error

To assist debugging, it is a usual practice to validate the parameters passed to a function at first. If the passed parameters or the parameters derived from them are null or invalid pointers, then this error message is printed with the parameter in question that is incorrect.

Possible Solution - These are used for debugging and should not occur normally.

CACS5: Internal Error

If there is some inconsistency in some internal data structures of call control layer, then this internal error is reported. Such errors may be fatal and can potentially lead to memory and/or resource leakage.

Possible Solution - Informational message.

CACS6: Fabric Error/Warning

When a connection establishment message is handled, the fabric resources required for the connection are allocated. If the call establishment message has some combination of QoS parameters that the fabric cannot support, then the connection will be rejected. For a link scope interface, a new dynamic path will be created if needed. If there is a failure in allocation of bandwidth or VPI/VCI, it could be because the resources are depleted for this interface. If you use the command **conf vpt show** from the AMI interface, the bandwidth and the number of VCs used for this interface can be monitored. Similarly if there is a depletion of VCs (VPI/VCI) then the command **conf vcc show** from the AMI interface will show that the VCs are in use. When a connection is being released the fabric resources that was setup for the connection is torn down, so that the fabric resources can be used for another connection. Errors in releasing the fabric resources may result in leakage of resources.

Possible Solution - Informational message.

CACS7: Bandwidth Error/Warning

Bandwidth required for a call is allocated at the call control layer in the switch. Allocation of bandwidth can fail due to unavailability of cell rate and because of depletion of VPI/VCI in the interface. If you use the AMI command **conf vpt show** the bandwidth and the number of VCs used for this interface can be monitored. The AMI command **conf vcc show** will show the VCs that are in use on this interface. If the NNI-interface is the user (secondary) side, bandwidth is reserved when a SETUP is progressed out on that interface. The call control module rejects calls that have incomplete traffic combinations and traffic combinations that are not supported by the fabric. When a connection is being torn down or released, bandwidth allocated to that connection is released, so that it can be used by other calls being setup. Errors encountered while releasing the bandwidth may lead to resource leakage.

Possible Solution - Informational message.

CACS8: VPI unavailable Error

In a link scope interface, the network (primary) side of a NNI interface can allocate VCIs in those paths (VPIs) that do not contain any signalling channel. For example a link scope UNI on VPI=0 can allocate a value of VPI=100, VCI=35 for a data connection. Here the signalling channel is in VPI 0, but VPI 100 is allocated for the call. Now in the user (secondary) side (on the other end) of the NNI-interface, the path VPI=100 may not be valid or free to be used. The call control module tries to allocate the path specified by the network (primary) side and if it finds that the path is not valid for allocation, this error occurs and the call is failed. This could be because the path already exists and is administratively provisioned for some other use.

Possible Solution - To see why this path is invalid you can use the AMI command **conf vpt show** to see if this path is allocated for some other purpose.

CACS9: Resource Allocation Error

In the call control module there are various internal data structures that are dynamically allocated, when a call is setup. The memory allocation can fail due to high memory usage or due to internal memory fragmentation. The description in the error message will indicate which data structure could not be allocated.

Possible Solution - This is not a fatal error and there is a chance that the call will succeed later, if retried when memory becomes available in the switch.

CACS10: Handle ADD PARTY Error

At the call control layer when the ADD PARTY is forwarded to a new interface, the ADD PARTY should be converted to a SETUP and sent out on the new interface. If the switch decides that it has to be the VPI/VCI allocating side based on certain criteria (like being the network or the primary side of a PNNI interface), then bandwidth and VPI/VCI have to allocated at the called interface before forwarding the ADD PARTY as a SETUP. If the switch decides that it is non-allocating side (e.g., user side or secondary side of a PNNI interface) for the call, then it will reserve the bandwidth for the call before forwarding the ADD PARTY as SETUP. If the allocation or reservation of bandwidth fails then the interface has run out of fabric resources. The AMI command **`conf vpt show`** is useful to monitor the bandwidth usage and the VC usage on an interface. The AMI command **`conf vcc show`** lists all the VCs used on this interface. After a successful reservation or allocation of fabric resource, the call control module will try to send out the ADD PARTY as a SETUP. This could fail at signalling layer due to several reasons. Similarly an ADD PARTY can be forwarded as an ADD PARTY on an existing interface. These errors can occur when the signalling layer fails to forward the ADD PARTY. When an ADD PARTY is progressed as an ADD PARTY on an existing interface, no fabric resources need to be allocated.

Possible Solution - Informational message.

CACS11: Call Reject Retry Error

When a call is rejected across a PNNI interface with a crankback information, the call control module under certain conditions will try to re-route the call and re-establish the call. In that process, it has to free up the resources previously allocated or reserved on the interface where the call failed. Any errors encountered during the freeing up of the resources may lead to resource leakage. If an alternate route is found then the resources are allocated on the new interface and the SETUP is retried. If the retry of SETUP on another interface also fails at the signalling layer, then the call is released.

Possible Solution - Informational message.

CACS12: Handle SETUP Error

When a SETUP is received on an ingress (calling) port, it is routed and forwarded to an egress (called) port at the call control layer. A number of internal data structures are dynamically allocated for this call. After these allocations, a check is done to see if the traffic contract is a complete contract and can be supported by the fabric. If the traffic contract is incomplete or cannot be supported by the fabric, the call is failed with error message saying that the class, service or contract is unsupported. If all these checks succeed, bandwidth allocation or reservation is done and the SETUP is progressed out on the called interface. If fabric resource allocation fails then the call is failed.

Possible Solution - Informational message.

CACS13: Handle CALL PROCEEDING Error

In response to a SETUP progressed through an interface, we can get a CALL PROCEEDING message. If we are the network (primary) side of the call, a check is done to make sure that the connection identifier (VPI/VCI) received in the CALL PROCEEDING message is the same as the one that we had previously allocated. If the connection identifier check fails, the call is cleared. If the VPI/VCI is not the same, then either the switch downstream is misbehaving or there is some misconfiguration in the network (primary) and user (secondary) sides of the NNI interface (especially when the interface is IISP or publicUNI).

Possible Solution - Informational message.

CACS14: Handle CONNECT Error

In response to a SETUP forwarded out on an interface, a CONNECT is received if the call is accepted. If we are the user (secondary) side, then while the SETUP was forwarded then we would have only reserved the bandwidth at the called interface. The fabric resources on the called interface are allocated now on reception of the connect. If the resources were not reserved previously then it indicates inconsistency at call control and the call is cleared. If the allocation of the resources now fail, then the call is cleared. If we are the network (primary) side, then while the SETUP was forwarded, we should have already allocated the resources on the called side. If we are the network (primary side), a check is made to ensure that the connection identifier (VPI/VCI) received in the CONNECT message is the same as the connection identifier that we have allocated. If there is a mismatch then it could mean that the switch down stream is misbehaving or there is some misconfiguration in the user/network sides of the NNI interface (especially in case of IISP and publicUNI interfaces).

Possible Solution - Informational message.

CACS15: Handle Call Reject Error

In response to a SETUP forwarded out an interface we can get a RELEASE COMPLETE message indicating the rejection of the call due to several reasons. There are lots of internal data structures that have to be freed. If there is any failure in these operations, then it indicates some inconsistency in call control module.

Possible Solution **-** Informational message.

CACS16: Reoffer PMP Call Error

When a RELEASE is received for an active point to multipoint call and if there is at least one ADD PARTY that is yet to be acknowledged, then one of the ADD PARTYs is retried as a SETUP with a new call reference. This is the concept of reoffering a point to multipoint call. Some internal data structures are allocated for this reoffering and they can fail due to lack of memory. The fabric resources are allocated if we are the network (primary) side and if the allocation fails, the call is failed. If we are the user (secondary) side, bandwidth reservation is done at the called side and if the reservation fails, the call is failed. If the sending of the SETUP fails in the signalling layer, the call is failed and the allocated or reserved resources are freed. Any error during the freeing up of resources may result in resource leakage.

Possible Solution **-** Informational message.

CACS17: Handle ALERTING Error

In response to a SETUP progressed through an interface, the reception of the ALERTING message indicates that the SETUP has reached the destination. If we are the network (primary) side, a check is done to make sure that the connection identifier (VPI/VCI) received in the ALERTING message is the same as the one that we have allocated. If the connection identifier check fails or forwarding of the ALERTING message to the calling side fails at signalling layer, then the call is released and the associated resources are freed.

Possible Solution **-** Informational message.

CACS18: Handle ADD PARTY REJECT Error

In response to an ADD PARTY forwarded out on an interface we can get an ADD PARTY REJECT due to several reasons. Under certain conditions, the ADD PARTY may be retried. If the retry of sending the ADD PARTY fails, the ADD PARTY REJECT is propagated to the calling side. When an ADD PARTY REJECT is being progressed to the caller, the internal data structures previously allocated to this party are released and any error here may result in resource leakage.

Possible Solution **-** Informational message.

CACS19: Handle ADD PARTY Error

An ADD PARTY received at the calling interface is progressed as an ADD PARTY on an existing called interface or as a SETUP on a new called interface. Some internal data structures are allocated in the call control layer for this call and a failure to allocate them could be because of a low memory situation and can result in the failure of the ADD PARTY.

Possible Solution - Informational message.

CACS20: Handle ADD PARTY ACK Error

In response to an ADD PARTY forwarded out on an interface, we get an ADD PARTY ACK as an acceptance to the ADD PARTY message. The ADD PARTY ACK is forwarded to the calling side and if this fails at the signalling layer, the party is dropped from the call.

Possible Solution - Informational message.

CACS21: Handle DROP PARTY Error

To drop a party from the point to multipoint call, the clearing message used is DROP PARTY. The party can be dropped either by the root or by the leaf. The internal data structures previously allocated for this party are freed. Any error in freeing the data structures indicate some inconsistency in the call control module. If this is the last party on an interface then some additional internal data structures are freed.

Possible Solution - Informational message.

CACS22: Connection ID check Failure

In call control module if the switch allocates the connection identifier (VPI/VCI) before forwarding the SETUP message out, it makes sure that the connection identifier (VPI/VCI) received in CALL PROCEEDING or CONNECT or ALERTING message is the same as the one that was previously allocated.

Possible Solution - If there is any mismatch, then it means that the switch down stream has not accepted the VPI/VCI we have sent. This could be because of a misconfiguration of the user and network sides of the NNI interface especially when the interface is IISP or publicUNI.

CACS23: ABR Parameter negotiation error

If an error is encountered while negotiating the values of ABR Setup/Additional parameters during the processing of an ABR SETUP message at either the ingress or egress interfaces, the call will be rejected. If invalid negotiation of the ABR parameters is detected during processing of an incoming ABR SETUP or CONNECT message, the call will be rejected.

Possible Solution - Informational message.

CACS24: Missing or invalid ABR information

The ABR information elements present in the SETUP or CONNECT messages have invalid or missing information.

Possible Solution **-** Informational message.

CACS25: Handle PROGRESS Error

In response to a SETUP progressed through an interface, the reception of the PROGRESS message indicates that the SETUP has reached the final destination and also it could have gone through an ISDN network. In some cases of interworking with ISDN networks there is a need to setup the data connection when the PROGRESS arrives with progress indicator 1 and 8 [please refer to UNI40 for details]. If there is any resource allocation failure at this stage, this error message gets printed.

Possible Solution **-** Informational message.

2.7 CDB Error Messages

CDBe0:

This is an internal error which indicates that an operation to open the indicated directory in the Configuration Database (CDB) failed.

Possible Solution - Informational message.

CDBe1:

This is an internal error which indicates that an operation to set a Configuration Database (CDB) variable failed.

Possible Solution - Informational message.

CDBe2:

This is an internal error which indicates that an operation to get a Configuration Database (CDB) variable failed.

Possible Solution - Informational message.

CDBe3:

This is an internal error which indicates that an operation to delete a Configuration Database (CDB) entry failed.

Possible Solution - Informational message.

CDBe4:

This is an internal error which indicates that a Configuration Database (CDB) variable of unknown format or type was encountered during some CDB operations.

Possible Solution - Informational message.

CDBe5:

This indicates that the specified CDB variable or directory does not exist.

Possible Solution - Informational message.

CDBe6:

This indicates that not enough memory was available for the CDB operation to succeed.

Possible Solution - Informational message.

CDBe7: Internal Error

This indicates an internal error during CDB operations. The message will give an indication of what the problem is.

Possible Solution - Please contact FORE Systems' Technical Support for assistance, and inform them of the message that was seen.

2.8 COMM Error Messages

COMM0:Info

For printing information on the console. This usually does not indicate a failure.

***Possible Solution* -** Informational Message.

COMM1: Notice

This generally indicates completion of a task or event. It can also indicate a situation that is different than what is normally expected and that the user should be aware of it. It is a very general and widely used message type.

***Possible Solution* -** Informational Message.

COMM2: Warning

This indicates some warning situation, but it may not be a serious error condition. It could also be due to some misconfiguration or other problem situation. It is a very general and widely used message type.

***Possible Solution* -** Look for more information in the printed messages and check the relevant menus in AMI for any misconfigurations.

COMM3: Error

This message usually reports or indicates a major error situation.

***Possible Solution* -** Please record the message and contact FORE Systems' Technical Assistance Center for assistance.

COMM4:

For printing debugging information.

***Possible Solution* -** Informational Message.

COMM5: Unknown sigtype

This message indicates that an attempt was made to set the ablink signalling type to an unknown value.

***Possible Solution* -** Informational Message.

COMM6: Failed to initialize ablink module

This message indicates that the ablink module initialization failed.

Possible Solution - Informational Message.

2.9 CTRR Error Messages

CTRR 0: Counter reset failed

This message can only occur if not enough dynamically allocated memory is available to complete the request (errno 4 is err_noresource).

Possible Solution - Add system memory or free up existing memory.

CTRR1: Counter offset delete failed

This is an internal error that signifies a memory leak.

Possible Solution - Contact FORE Systems' technical support.

CTRR2: Counter routine encountered an invalid index

This is an internal error whereby the index supplied to the counter offset database is inconsistent with the database's actual index.

Possible Solution - Contact FORE Systems' technical support.

2.10 ESIC Error Messages

esic0: ESI facility

This is used to report ESI facility errors. These errors will cause the switch to be unable to communicate with the TCM module.

Possible Solution - - Informational message.

esic1: ESI protocol error

This is used to report ESI protocol errors that have been detected.

Possible Solution - Verify that the versions of the TCM software and the switch control software are compatible.

esic2: Debug

This contains debugging related information which may be useful to trace any error condition.

Possible Solution - - Informational message.

esic3: Status

This contains status information concerning the operation of the TCM interface software.

Possible Solution - - Informational message.

2.11 FRF8 Error Messages

FRF80: error, the object oid is invalid

The specified object oid doesn't exist.

Possible Solution - Informational message.

FRF81: error, the ifindex is invalid

An FRF8 service is uniquely identified by an ifindex with type. This error means that either this ifindex doesn't exist or it is not with type.

Possible Solution - Informational message.

FRF82: error, cannot get configuration info

This error indicates that the calls to get frf8 service or connection configuration information returns an error.

Possible Solution - Informational message.

FRF83: error, ARP addr and addrType bad config

This error indicates that the Address value and Address type are not well configured for a connection supporting ARP protocol translation.

Possible Solution - Informational message.

FRF84: error, the frame relay is out of the supported range

This error indicates that the user tried to create an FR connection with adlci out of the supported range.

Possible Solution - Informational message.

FRF85: error, no netmod cid available

Whenever an frf8 connection is to be created, we need to apply for a network module cid. This error is reported when there is no cid available.

Possible Solution - Informational message.

FRF86: error, failed to store frf8 conn config to CDB

This error indicates that the attempt to save frf8 connection configuration failed.

Possible Solution - Informational message.

FRF87: error, vpi/vci mapping failed

This error indicates that the FR dlci to fabric vpi/vci mapping function has failed.

Possible Solution - Informational message.

FRF88: error, failed to bind cid with fabric layer

This error indicates that the binding of cid with fabric vpi/vci has failed.

Possible Solution - Informational message.

FRF89: error, the frf8 connection already exists

This error message displays when an attempt is made to create an FRF8 connection with an frService and dlci for an FRF8 connection that already exists.

Possible Solution - Informational message.

FRF810: error, the frf8 connection doesn't exist yet

This error message is reported when the user tries to set/get configuration-oriented objects other than the rowstatus while the frf8 connection doesn't exist yet.

Possible Solution - Informational message.

FRF811: error, failed to create a frf8 connection

This is a generic error message indicating that the system failed to create an frf8 connection.

Possible Solution - Informational message.

FRF812: error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfCreateFrf8Conn message to the netmod returns an error.

Possible Solution - Informational message.

FRF813: error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfCtlConnAdmtState message to the netmod returns an error.

Possible Solution - Informational message.

FRF814: error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfDestroyConn message to the netmod returns an error.

Possible Solution - Informational message.

FRF815: error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfStatsOnOff message to the netmod returns an error.

Possible Solution - Informational message.

FRF816: notice, no more funi service

This message indicates that there is no more FR service available.

Possible Solution - Informational message.

FRF817: error, Invalid argument type specified

This message indicates that the type of the value to set rowstatus is incorrect.

Possible Solution - Informational message.

FRF818: error, Invalid argument value specified

This message indicates that the value to set rowstatus is invalid or out of range.

Possible Solution - Informational message.

FRF819: notice, rowstatus unchanged

This message indicates that the new rowstatus value to which is to be set is the same as it is currently.

Possible Solution - Informational message.

FRF820: error, can't change this obj on-the-fly

This message indicates that the user attempted to change the object on-the-fly and was therefore rejected.

Possible Solution - Informational message.

FRF821: error, can't get a IfIndex Biscuit

This message indicates that a failure occurred while attempting to retrieve a biscuit for the IfIndex.

Possible Solution - Informational message.

FRF822: error, can't get FR/ATM statistics

This message indicates that a failure occurred while attempting to retrieve FRF8 statistics.

Possible Solution - Informational message.

FRF823: error, wrong SNMP type

This message indicates that the type of the value to be set in the SNMP object is incorrect.

Possible Solution - Informational message.

FRF824: error, cannot set configuration info

This error indicates that the calls to set frf8 connection configuration information returns an error.

Possible Solution - Informational message.

FRF825: error, there is no profile with such index

This error indicates that the user is making reference to an index of a profile that was not yet created.

Possible Solution - Informational message.

FRF826: error, the type of the Atm Address is wrong

This error indicates that the user is setting an incorrect address type.

Possible Solution - Informational message.

FRF827: error, the type and AtmAddress don't match

This error indicates that the user is making an incorrect combination of AtmAddress, AtmSubAddress or FrAddress with addressing types that are allowed.

Possible Solution - Informational message.

FRF828: error, the value of the object is wrong

This error indicates that the user is managing a value not allowed for the SNMP object.

Possible Solution - Informational message.

FRF829: error, interface with the sdpm failed

This error indicates the call of an SDPM api failed.

Possible Solution - Informational message.

FRF830: error, size not allowed for string

This error indicates that the user is asking the SNMP agent to handle a string size not allowed for the SNMP object.

Possible Solution - Informational message.

FRF831: error, fail to build msg to NM

This error indicates that some error occurred while building a message to be sent to the NM.

Possible Solution - Informational message.

FRF832: error, fail to release NM CID

This error indicates that some error occurred while asking to release the specified NM CID.

Possible Solution - Informational message.

FRF833: error, fail to delete a FRF8 Conn

This error indicates that some error occurred while asking to delete the specified FRF8 connection.

Possible Solution - Informational message.

FRF834: error, fail to update frextDlcmiPvccs

This error indicates that some error occurred while updating the counter of FRF8 connection FRF8 PVCs in the specified FR service.

Possible Solution - Informational message.

FRF835: error, cannot allow any more VCCs in this FRS

This error indicates that there is already the maximum number of VCCs created in this service, and therefore no more connections can be created.

Possible Solution - Informational message.

FRF836: error, the Connection Row is not configured

This error indicates that the connection Row is not completely configured, meaning that the Row cannot change to NotInService or Active states.

***Possible Solution* -** Informational message.

FRF837: error, failed to purge frf8 conn config from CDB

This error indicates that the attempt to delete frf8 connection configuration in CDB failed.

***Possible Solution* -** Informational message.

FRF838: error, failed to allocate bandwidth to a Conn

This error indicates that the bandwidth allocation for the connection has failed.

***Possible Solution* -** Informational message.

FRF839: error, failed to release a bandwidth of a Conn

This error indicates that the bandwidth release for the connection has failed.

***Possible Solution* -** Informational message.

FRF840: error, the AFI and AddrType do not match

This error indicates that the address type and AFI field for the ARP address translation do not match.

***Possible Solution* -** Informational message.

FRF841: error, Recreation of Conn From Cdb Failed

This error indicates that some steps to recreate a connection from Cdb has failed.

***Possible Solution* -** Informational message.

FRF842: error, Bandwidth allocation failed

This error indicates that the allocation of bandwidth cannot be provided for this new connection to be created.

***Possible Solution* -** Informational message.

FRF843: error,Bandwidth deallocation failed

This error indicates that the de-allocation of bandwidth for this connection failed.

***Possible Solution* -** Informational message.

FRF844: warning, FRAM netmod is in down state

This warning indicates that during connection creation, the related network module is in the down state.

Possible Solution - Informational message.

2.12 FSIG Error Messages

FSIG0:

This is used to let the user know of internal actions taken by the signalling module.

Possible Solution - Informational message.

FSIG1:

This is used to print information, usually, following an error message.

Possible Solution - Informational message.

FSIG2: q93b_uni_carrier_loss

This message is printed out whenever signalling on an interface is informed of the loss of carrier on the associated link. The link ID (in decimal) for the signalling interface in question is present as indicated in the message. Such a message would be printed out, for example, if the fiber connection was removed from a port on a network module. For example:

```
UNI[--] q93b_uni_carrrier_loss: link 26
```

This means that the signalling on the interface on link 26 (1D3) has detected the loss of carrier.

Possible Solution - Informational message.

FSIG3: q93b_uni_carrier_detect

This message is printed out whenever signalling on an interface is informed of the presence of carrier (if there was none before) on the associated link. The link ID (in decimal) for the signalling interface in question is present as indicated in the message. Such a message would be printed out, for example, if the fiber connection was removed from a port on a network module and then reconnected. For example:

```
UNI[--] q93b_uni_carrrier_detect: link 26
```

This means that the signalling on the interface on link 26 (1D3) has detected the presence of carrier on port 1D3.

Possible Solution - Informational message.

FSIG4: q93b_unexpected_msg

This message is printed if the protocol state machine on the switch for a given call <call reference> in a state <state> on a link <link ID> receives a message that it does not expect for the call. For example:

```
UNI[3]   q93b_unexpected_msg: CONNECT, state = 0xc, call_ref = 0x41188, linkid=20
```

This message indicates that the call with call reference 0x41188 on the interface on link 3 (1A4) is in state 0xc (Release Indication) and therefore, the CONNECT message received for this call is NOT an expected message. Such messages may be printed under high signalling load. For example, an assumption if made that a CALL PROCEEDING has already been received, therefore the start of T310. The expiration of a T310 timer on an outgoing interface triggers the release of the call (and hence its state will change to Release Indication) and the outgoing RELEASE message for that call crosses the incoming CONNECT message on the wire. Therefore, when the switch receives the CONNECT message, it treats it as an unexpected message. The ATM Forum User-Network Interface(UNI) specifications explains the different call states on a UNI.

Possible Solution - Informational message.

FSIG5: invalid endp_ref

This message is printed if the protocol state machine on the switch receives a message for a Point to Multipoint call with an endpoint reference that is not valid at the time the message is received. The message can appear as a WARNING or an ERROR message, depending on the state of the Point to Multipoint call, the state of the party and the type of the received message. This usually happens under high signalling load conditions, for example, when a party on a Point to Multipoint call is dropped and cleared in the software before the DROP PARTY ACK for the party is received. This would take place under certain conditions that are manifested under high signalling load. For example:

```
UNI[16]   rx_drop_party_ack(): invalid endp_ref = 0x82b6, linkid=16
```

Possible Solution - Informational message.

FSIG6: Memory Resource Error

This message is printed if the signalling module is not able to allocate memory for any of its data structures. This could happen due to a shortage of free space in the switch's memory or if the memory is fragmented to an extent that there is not a single free block of the size that a signalling data structure requires.

Possible Solution - Informational message.

FSIG7: Function returned error

The specified function returned an error. This is a very general error message and denotes a variety of error situations.

Possible Solution - Informational message.

FSIG8: Invalid Parameter

This error indicates that the arguments passed into a function have invalid values. It may be that the argument itself has invalid values such as a NULL pointer, or some other entity that is derived from the argument has an invalid value.

Possible Solution - Informational message.

FSIG9: Internal Warning

This message is to notify of some internal problem in the signalling module.

Possible Solution - Informational message.

FSIG10: Internal Error

This error message is printed out when some error that is internal to the signalling module is encountered. For example, when timer t313 is started on the network side of the interface, this error would be generated. The timer t313 is supposed to be started only on the user side of a User-Network interface.

Possible Solution - Informational message.

FSIG11: UPC index does not exist

This message is printed when the upc index specified (for the input signalling contract option) for creating a signalling entity is not present on the switch. The cell rate values for a specified upc index can be seen from AMI using the **`configuration upc show`** menu.

Possible Solution - Informational message.

FSIG12: VCI range is empty

This message is printed if there is a misconfiguration error when a signalling entity on the switch tries to determine the VCI range that it should use for switched virtual connections(SVCs). The VCI range specified and that of the peer signalling entity do not intersect.

Possible Solution - The VCI ranges of the peer and the local switch should be overlapping for any SVCs to be established. For example, if the signalling entity VCI range is from 50 (min VCI) to 100 (max VCI) and its peer VCI range is from 110 (min VCIi) to 200 (max VCI), there is no intersection of the VCI ranges and the SVC cannot be established.

FSIG13: Unexpected SSCOP msg type

This message indicates that an unexpected message was received from the SSCOP layer.

Possible Solution - Informational message.

FSIG14: CDB Error

This happens when an error relating to the switch configuration database (CDB) occurs. The error could occur in reading a parameter from the CDB, or in writing a parameter to the CDB.

Possible Solution - Informational message.

FSIG15: UNI and Routing Domain Type Mismatch

This message indicates that some type mismatching has happened. For example, the mismatch may be between the UNI type and the routing domain.

Possible Solution - Informational message.

FSIG16: Link Scope Error

This message indicates that an error has occurred while creating a link scope signalling entity.

Possible Solution - Informational message.

FSIG17: Maximum number of Signalling Entities reached

This message indicates that the number of signalling entities on the switch has reached the maximum and a new one cannot be created.

Possible Solution - Informational message.

FSIG18: Path Dynamic

A signalling entity can be created only on a path that is created as a permanent path. This message indicates that the attempt to create a signalling entity on a virtual path that is dynamic will not be successful.

Possible Solution - Informational message.

FSIG19: Address Registration should be Disabled

This message indicates that ILMI address registration is enabled where it is not supposed to be. For example, on a public UNI interface, ILMI address registration should not be enabled. If this message is printed, the signalling entity will not be created.

Possible Solution - Informational message.

FSIG20: Invalid configured type

This message indicates that the configured type for a signalling entity is invalid.

Possible Solution - Informational message.

FSIG21:

This message indicates that the combination of type, mode, and scope used for creating this signalling entity is invalid. Therefore, the signalling entity will not be created.

Possible Solution - Informational message.

FSIG22:

Link scope signalling entity cannot be created on a non-zero VP according to the PNNI signalling specification. If a link scope signalling entity is being created on a non-zero VP, this message will be printed and the signalling entity will not be created.

Possible Solution - Informational message.

FSIG23:

This error message indicates that creation of a vpassoc mode with allocation scope as link scope is attempted. Such a signalling entity will not be created.

Possible Solution - Informational message.

FSIG24:

This message indicates that a non associated mode PNNI signalling entity cannot be created on a non zero VP.

Possible Solution - Informational message.

FSIG25:

This is an error message indicating that a non-associated mode PNNI signalling entity with VP scope is not allowed. The signalling entity with such a combination will not be created.

Possible Solution - Informational message.

FSIG26:

This is an error message indicating that a non-assoc mode PNNI signalling entity cannot be created on a backplane link.

Possible Solution - Informational message.

FSIG27:

Link scope signalling entities cannot be created across a backplane. This is an error message indicating that there is an attempt to create a backplane signalling entity with link scope property.

Possible Solution - Informational message.

FSIG28: Invalid QoS Expansion key

This message indicates that the QoS expansion key with which the signalling entity is created is invalid. This means that this key is not present in the QoS expansion table in the switch. The QoS expansion table entries can be checked from AMI using the command **`conf qos show`**.

Possible Solution - Informational message.

FSIG29: Invalid Signalling Scope

This message indicates that the signalling entity has an invalid signalling connection allocation scope value.

Possible Solution - Informational message.

FSIG30: UNI4.0 Unsupported

This message indicates that the UNI 4.0 signalling stack is not supported by this release.

Possible Solution - Informational message.

FSIG31:

This message indicates that there is already a link scope signalling entity on this link and that another link scope signalling entity cannot be created on this link.

Possible Solution - Informational message.

FSIG32: DTL Processing error

This message is printed out when an error occurs in the processing of the Designated Transit Lists. This is an internal error and the printed message will indicate the internal error. For example, there could have been an error while trying to insert a new designated transit list since there are already the maximum number of DTLs.

Possible Solution - Informational message.

FSIG33: Traffic parameter error

This message indicates that the traffic parameters present in a SETUP message are invalid. This may be due to the fact that the QoS class combinations are invalid or the combination of service category and bearer class are invalid. The valid traffic parameter combinations are listed in Table F-1 (Appendix F) of the UNI 3.1 Signalling Specification for UNI 3.1 signalling and Table A-9 (Annex9) of the UNI 4.0 Signalling Specifications.

***Possible Solution* -** Informational message.

FSIG34: Error while Interworking

Interworking is needed because some information elements have different formats between signalling versions. Interworking module within the signalling layer ensures that signalling messages received on a particular signalling version (e.g. UNI 3.0) are translated to conform to the signalling version on the outgoing link (e.g. UNI 3.1). This error indicates that interworking could not be done successfully.

***Possible Solution* -** Informational message.

FSIG35:

This message indicates that unsuccessful attempts were made to establish SVCs on a signalling interface because it was not fully created.

***Possible Solution* -** Informational message.

FSIG36: Interworking UNSUPPORTED

This message indicates that the particular interworking combination required is not supported by the switch. For example, if a need arises to interwork UNI 3.0 signalling IEs to UNI 4.0 signalling IEs and vice versa, this implementation does not support such an operation.

***Possible Solution* -** Informational message.

FSIG37: Interworking Cause

The SVC portion of a Smart Permanent Virtual Channel (SPVC) terminates on a NNI (Network-Network Interface). This is a warning message that indicates that a cause value associated with SPVCs are passed onto a private User-Network Interface (UNI). The cause value is changed to NORMAL UNSPECIFIED CAUSE and then sent over the private UNI. This is an internal error in the signalling module.

***Possible Solution* -** Informational message.

FSIG38: Cannot Interwork

The QoS class Information Element (IE) is mandatory in the SETUP message in UNI 3.x links. On a PNNI link the QoS class information element is not mandatory in a SETUP message. When such a message is received on a PNNI link, and the SETUP message has to be routed through a UNI 3.x link to reach the called party then Interworking will return this error and the SETUP will not be forwarded to the called party.

Possible Solution - Informational message.

FSIG39: Generic ID Transport IE Error

FORE switches support exactly one type of generic info, which is the call correlation tag. This call correlation tag is geared specifically for billing in Public Networks. Any other type of generic info received by a FORE switch will generate this error message.

Possible Solution - Informational message.

FSIG40: Information Element Error

Signalling messages are composed of variable length Information Elements (IEs). The variable length information element is coded using the Type, Length and Value scheme. This error message is a generic one that indicates an error has occurred with one of the Information Elements received or to be transmitted. Depending on the type of the message (e.g. SETUP or CALL PROCEEDING) and the type of information element for which this error happened (Mandatory or Non_Mandatory IE) the action taken by the signalling module will vary.

Possible Solution - For a detailed description, the user is requested to consult the Error handling section of the ATM Forum UNI 3.1 Specifications or the ATM Forum PNNI Specification.

FSIG41: Information Element Length Error

This indicates that one of the Information Elements Length field has an incorrect value. Depending on whether the Information Element is mandatory or not for that message type, the action taken by the signalling layer will differ.

Possible Solution - Informational message.

FSIG42: Information Element Content Error

This message indicates that the contents of the Information Element has a value not permitted by the signalling specifications (for e.g., UNI 3.1 or PNNI 1.0). Depending on the message type and information element type, the action taken by the signalling entity will vary.

Possible Solution - Informational message.

FSIG43: Information Element Encoding Error

This message indicates that while composing a signalling message, an Information Element could not be encoded properly in the Type, Value, Length scheme.

Possible Solution - Informational message.

FSIG44: Auto Configuration Error

This message indicates that there is some problem in auto configuring the signalling entity types or version. The main purpose of auto configuration is to determine the type and version of the peer signalling entity and accordingly set the type and version of the local signalling entity so that they interoperate.

Possible Solution - Informational message.

FSIG45: Global Call Reference Error

This indicates that the signalling entity has been restarted or in a state where it cannot transmit and receive signalling messages.

Possible Solution - Informational message.

FSIG46: Message Length Greater than MTU

This message indicates that the length of the signalling message is greater than the ATM Maximum Transmission Unit (MTU). The size of the ATM Maximum Transmission Unit supported by FORE switches is 4096 bytes.

Possible Solution - Informational message.

FSIG47: Mandatory Information Element Missing

This message indicates that an Information Element that has to be present in a message is missing. For example, in the SETUP message, the Called Party Number Information Element is a mandatory Information Element. The ATM Forum Specifications document clearly spells out the Information Elements that are mandatory for different types of signalling messages and the action to be taken if a mandatory information element is missing in a particular signalling message. For example, if a mandatory information element is missing in a SETUP message received by the signalling entity, the signalling entity will reject the call by sending a RELEASE COMPLETE.

Possible Solution - Informational message.

FSIG48: Information element must be absent

This warning message indicates that the indicated information element is not supposed to be transmitted in a signalling message on a particular interface. For example, an End to End transit Delay Information Element should not be transmitted in an ADD PARTY message on a User-Network Interface running version 3.0 (UNI 3.0). Internal action is taken not to transmit such Information Elements.

Possible Solution - Informational message.

FSIG49: Signalling Message Length Error

This message indicates that the received signalling message is shorter than the minimum specified length or that the actual length of the message received is not the same as the length indicated by the message length Information Element.

Possible Solution - Informational message.

FSIG50: Bad Protocol Discriminator

This message indicates that the received signalling message has a wrong value for the protocol discriminator field. This message will be ignored (as if it has never been received).

Possible Solution - For the correct values of the Protocol Discriminator field, refer to the ATM Forum Specifications.FSIG51: Call Ref length Error

This indicates that the content of the call reference length field in the received signalling message has an incorrect value. The message (e.g., Setup) for which this error occurs will be ignored.

Possible Solution - Informational message.

FSIG52: Call does not exist

This message indicates that the switch has received a signalling message for a Switched Virtual Connection (SVC) that does not exist on this link of the switch. A particular switched virtual connection is identified by the call reference value in the signalling message. This message is printed out when there is no call existing with the call reference value indicated in the signalling message. This could happen under heavy stress when this switch has already released the SVC with this call reference value but the peer that is connected to it is still sending some signalling message for that call reference.

Possible Solution - Informational message.

FSIG53: Unrecognized Message

This message indicates that a signalling message received on an interface (e.g., User-Network Interface running version 3.0 or UNI 3.1) is not supported on that interface. For example, when an alerting message is received on a UNI 3.0 interface, this message will be printed.

Possible Solution **-** Informational message.

FSIG54: Message Content Error

This indicates that the signalling message received has invalid contents. Depending on the type of error (mandatory Information Element missing or non-mandatory information element content error) the action taken by the signalling entity will vary.

Possible Solution **-** Informational message.

FSIG55: Timeout Error

This message indicates that a timer (e.g., t303) could not be scheduled. One reason for this failure is memory could not be allocated for the timeout. This is an internal error.

Possible Solution **-** Informational message.

FSIG56: Restart Type Error

A restart message could have been sent out by the signalling entity with either requesting to restart a specific virtual channel, or all the virtual channels, or all virtual channels in a specific virtual path. This request type is carried by the restart indicator information element in the RESTART message. If a RESTART ACKNOWLEDGMENT is received with a different type of restart indicator, this message would be printed.

Possible Solution **-** Informational message.

FSIG57: E.164 address not assigned

E.164 format addresses are used for routing in a Public Network. A mapping of an NSAP address to a E.164 address has to be created on the switch for routing from a private network to a public network. The signalling module uses this mapping to convert the calling and the called party NSAP addresses to the E.164 format. If such a mapping does not exist in the switch, this message is printed out.

Possible Solution **-** Informational message.

FSIG58:

This message indicates that a new call reference cannot be allocated. It may be that all the call references are in use for the existing connections.

Possible Solution **-** Informational message.

FSIG59:

According to the UNI 4.0 specification, Section 9.2.2, point to multipoint calls should not have backward QoS parameters. This message indicates that backward QoS parameters were present in a SETUP message that was trying to be sent out. This is a notice message which indicates that the backward QoS parameters will not be sent out in a point-to-multipoint SETUP message.

Possible Solution - Informational message.

FSIG60: Unrecognized Information Element

This indicates that the signalling entity has received a message with an Information Element identifier that it does not support. Depending on the type of the message for which this error occurs, the action taken by the signalling entity will vary. When a signalling message (e.g., SETUP) is received with an unrecognized information element, a STATUS message has to be sent out in return by the signalling entity.

Possible Solution - Informational message.

FSIG61: Unexpected Information Element

This message is generated when an information element that is not expected in a signalling message is present in it. The action taken by the signalling module will be the same as that when a message with unrecognized information element is received.

Possible Solution - Informational message.

FSIG62: Mandatory Information Element Error

This indicates that an Information Element that must be present in a particular signalling message is in error. It might be that the Information Element is absent in the message or has invalid contents.

Possible Solution - Informational message.

FSIG63: Non-Mandatory Information Element Error

This message indicates that a non-mandatory information element has invalid contents. A STATUS message may be sent in response to a message received with this error.

Possible Solution - Informational message.

FSIG64: Extended QoS Error

This message indicates that there is a protocol conformance error in the received signalling message with respect to the Extended QoS information Element. According to UNI 4.0 Specification, Section 9.2.1, the network side will discard any acceptable values for extended QoS parameters and an End-to-End Transit Delay Information Element received in a connect message.

Possible Solution **-** Informational message.

FSIG65: Restart Ack Not Received

When a restart message is sent out on a link the timer t316 is started. Upon the expiry of timer t316, this error message is issued. The restart message will be retransmitted upon the expiry of the t316 timer.

Possible Solution **-** Informational message.

FSIG66: VCI Error

The VCI value for the signalling channel and ILMI channel as specified by the **`-sigvci`** and **`-ilmivci`** options from **`configuration signalling new`** menu should be different.

Possible Solution **-** Informational message.

2.13 FTPN Error Messages

FTPN0: Unable to set value to cdb

This error appears when cdb_set_int does not return cdb_noerror. Various topology variables are set in the CDB file. This setting can fail when the particular directory is not found or when the file is corrupted.

Possible Solution - Informational message.

FTPN1: Unable to identify

This is used with respect to traffic types (CBR, VBR, VBR-RT, UBR, and ABR). UBR and ABR have no bandwidth criteria. In functions like ftpnni_gcac and atmf_simple_gcac, if the traffic argument does not belong to one of these five types, this error is reported.

Possible Solution - Informational message.

FTPN2: Sanity check failed

A sanity check basically compares two node IDs or NSAP addresses. In the case of an NSAP address comparison, if the first address is greater than the second, a value of 1 is returned. If they are equal, a value of 0 is returned; otherwise, a value of -1 is returned. In the case of a node ID comparison, if they are equal, a value of TRUE is returned; otherwise, a value of FALSE is returned. This is reported in function q93b_route_using_dtl. This check is needed because the DTL's node and the node that receives this DTL should be the same.

Possible Solution - Informational message.

FTPN3: Unknown

This is mostly used in switch-case construct as an error message for default. It is generally followed by return bad argument and break statements.

Possible Solution - Informational message.

FTPN4: Dtl transit pointer less than 2

Transit pointer:trans_ptr is an element in the DTL structure. It is an unsigned integer. It should not be less than 2. This check is done generally at the beginning of the function only in FT-PNNI (not in PNNI). A DTL is not used when the source and destination are directly connected. At least one hop is required.

Possible Solution - Informational message.

2.14 FUNI Error Messages

FUNI0: Error, the object OID is invalid

The specified object OID doesn't exist.

Possible Solution - Informational message.

FUNI1: Error, no more memory space for FUNI SNMP agent

This error indicates that there is no more available memory space for FUNI SNMP agent management code.

Possible Solution - Informational message.

FUNI2: Error, cannot set NeighborIpAddress

This error indicates that the user attempts to set NeighborIpAddress for a FUNI service which enables ILMI.

Possible Solution - Informational message.

FUNI3: Error, cannot get configuration info

This error indicates that the calls to get FUNI connection configuration information returns an error.

Possible Solution - Informational message.

FUNI4: Error, the FUNI VPI is out of the supported range

This error indicates that the user tries to create a FUNI connection with a FUNI VPI out of the supported range.

Possible Solution - Informational message.

FUNI5: Error, the FUNI VCI is out of the supported range

This error indicates that the user tries to create a FUNI connection with a FUNI VCI out of the supported range.

Possible Solution - Informational message.

FUNI6: Error, VPI/VCI conflicts with signalling channel

This error indicates that the user tries to create a FUNI connection with a FUNI VPI/VCI which is reserved for the signalling channel.

Possible Solution - Informational message.

FUNI7: Error, VPI/VCI conflicts with ILMI channel

This error indicates that the user tries to create a FUNI connection with a FUNI VPI/VCI-which is reserved for the ILMI channel.

Possible Solution - Informational message.

FUNI8: Error, no netmod CID available

Whenever a FUNI connection is to be created, you need to apply for a CID. This error is reported when there is no CID available.

Possible Solution - Informational message.

FUNI9: Error, can't delete SIG or ILMI PVC or SVC

The user is not allowed to delete FUNI signalling or ILMI PVC or SVC since it is part of the FUNI signalling instance's property.

Possible Solution - Informational message.

FUNI10: Error, failed to store FUNI CONN config to CDB

This error indicates that the attempt to save FUNI connection configuration failed.

Possible Solution - Informational message.

FUNI11: Error, VPI/VCI mapping failed

This error indicates that the FUNI to fabric VPI/VCI mapping function has failed.

Possible Solution - Informational message.

FUNI12: Error, failed to bind CID with fabric layer

This error indicates that the binding of CID with fabric VPI/VCI has failed.

Possible Solution - Informational message.

FUNI13: Error, the FUNI connection already exists

This error indicates that an attempt was made to create a FUNI connection with a <FUNIVPI, FUNIVCI> for a FUNI connection that already exists.

Possible Solution - Informational message.

FUNI14: Error, the FUNI connection doesn't exist yet

This error message is reported when the user tries to set/get configuration-oriented objects other than the rowstatus while the FUNI connection doesn't exist yet.

Possible Solution - Informational message.

FUNI15: Error, failed to create a FUNI connection

This is a generic error message indicating that the system failed to create a FUNI connection.

Possible Solution - Informational message.

FUNI16: Error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfCreateFuniConn message to the network module returns an error.

Possible Solution - Informational message.

FUNI17: Error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfCtlConnAdmtState message to the network module returns an error.

Possible Solution - Informational message.

FUNI18: Error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfDestroyConn message to the network module returns an error.

Possible Solution - Informational message.

FUNI19: Error, NifsSendMessage() failed

This message is reported when the call to NifsSendMessage() to send the sfStatsOnOff message to the network module returns an error.

Possible Solution - Informational message.

FUNI20: Notice, no more FUNI service

There is no more FUNI service available.

Possible Solution - Informational message.

FUNI21: Error, Invalid argument type specified

This message indicates that the type of the value to set rowstatus is incorrect.

Possible Solution - Informational message.

FUNI22: Error, Invalid argument value specified

This message indicates that the value to set rowstatus is invalid or out of range.

Possible Solution - Informational message.

FUNI23: Notice, rowstatus unchanged

This message indicates that the new rowstatus value to which is to be set is the same as it is currently.

Possible Solution - Informational message.

FUNI24: Error, object does not support runtime modification

This message indicates that an attempt was made to change the object that does not support runtime modication and was therefore rejected.

Possible Solution - Informational message.

FUNI25: Error, the ifindex is invalid

A FUNI service is uniquely identified by an ifindex with type atmFUNI. This error means that either this ifindex doesn't exist or it is not with type atmFUNI.

Possible Solution - Informational message.

FUNI26: Error, can't seat more connection

The maximum number of connections of a FUNI service is defined by its service profile. This error means that no more connections can be created since the current configured connections have reached or exceeded the maximum limit.

Possible Solution - Informational message.

FUNI27: Error, FRAM netmod is in down state

This message indicates that during connection creation, the related network module is in the down state.

Possible Solution - Informational message.

FUNI28: Error, there is no High Priority EpdPpd buffer available

This message indicates that during connection creation, the related network module is not configured to support high priority buffer.

Possible Solution - Informational message.

FUNI29: Error, fail to delete a FUNI Conn

This error indicates that some error occurred while asking to delete the specified FUNI connection.

Possible Solution - Informational message.

2.15 HYDR Error Messages

HYDR0: Unable to read/write portcard CDB

The ESX-3000 switch was unable to read or to write the portcard configuration from non-volatile storage.

Possible Solution - Check the FLASH file system for sufficient free space.

HYDR1: Unable to recognize portcard

The switch was unable to recognize the portcard in the indicated slot.

Possible Solution - 1) Re-seat the portcard. 2) Insert the portcard into a different slot. 3) Verify that the current version of software supports this portcard type. 4) Insert another portcard of the same type into the same slot on this switch. 5) The portcard may be damanged. Return it for repair.

HYDR2: Unable to open portcard

The switch was unable to attach to the portcard in the indicated slot.

Possible Solution - Check the amount of free memory available. Try to free memory, if possible.

HYDR3: Unable to allocate connection on portcard

The switch was unable to allocate a connection entry on the indicated portcard.

Possible Solution - 1) Check the number of connections currently in use on the portcard. Remove some through path connections or reduce the VCI range for some originating/terminating paths. 2) Check the amount of free memory available. Try to free memory, if possible.

HYDR4: Unable to support this option on the portcard

The switch requested an unsupported option or combination of options on theindicated portcard.

Possible Solution - Please file a problem report with FORE Systems' Technical Assistance Center (TAC). Also, please include as many messages that precede and follow this message as possible.

HYDR5: No fabric present for this portcard

The switch detected a portcard in a slot that is supported by a fabric that is not currently present.

Possible Solution - 1) Move the portcard to a slot that is supported by one of the currently present fabric modules. 2) Install the fabric module that supports this slot.

HYDR6: Unable to configure PCI for this portcard

The switch was unable to configure the PCI bridge for the indicated portcard.

Possible Solution - 1) Re-seat the portcard. 2) Insert the portcard into a different slot. 3) Verify that the current version of software supports this portcard type. 4) Insert another portcard of the same type into the same slot on this switch. 5) The portcard may be damaged. Return it for repair.

HYDR7: Unable to connect the hotswap interrupt

The switch was unable to connect the hotswap interrupt handler.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR8: Unknown EPROM device

The switch was unable to read the EPROM from a board.

Possible Solution - The board may be damaged. Return it for repair.

HYDR9: Error reading serial EEPROM

The switch was unable to read the EPROM from a board.

Possible Solution - The board may be damaged. Return it for repair.

HYDR10: Invalid PCI base address

The switch was unable to configure the PCI device.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR11: Invalid PCI device

The switch was unable to configure the PCI device.

Possible Solution - The component may be faulty. Return it for repair.

HYDR12: Unable to configure fabric PCI

The switch was unable to configure the PCI device.

Possible Solution - The component may befaulty. Return it for repair.

HYDR13: Unable to configure fabric

The switch was unable to configure the fabric.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR14: Virtual channel setup failure

The switch was unable to configure a virtual channel in hardware.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR15: Virtual channel preservation failure

The switch was unable to preserve the state of a virtual channel in hardware.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR16: Virtual through path setup failure

The switch was unable to configure a virtual through path in hardware.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR17: Virtual through path preservation failure

The switch was unable to preserve the state of a virtual through path in hardware.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR18: Invalid multicast space index

The specified multicast space is invalid.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR19: Incompatible multicast space

The specified multicast space is incompatible with one or more of the port cards on this fabric.

Possible Solution - Contact FORE Systems Technical Assistance Center (TAC).

HYDR20: ***** Invalid EPROM value

An entry in the EPROM is programmed incorrectly.

Possible Solution - Please contact FORE Systems Technical Assistance Center (TAC).

HYDR21: Unable to set the given value

An error occured during configuration of a request.

Possible Solution - Informational message.

2.16 IFEX Error Messages

IFEX0: IfExtensions SNMP agent: invalid interface type

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX1: IfExtensions SNMP agent: invalid interface index

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX2: IfExtensions SNMP agent: invalid argument

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX3: IfExtensions SNMP agent: system error

This error indicates that there may be some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX4: IfExtensions SNMP agent: invalid object identifier

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX5: IfExtensions SNMP agent: invalid interface service status

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX6: IfExtensions SNMP agent: initialization error

This error indicates that the initialization of ifExtensions objects has failed. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX7: IfExtensions SNMP agent: interface property modification error

This error indicates that the modification of interface property, e.g. ifType, has failed. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

IFEX8: IfExtensions SNMP agent: ifIndex reservation error

This error indicates that the reservation of ifIndex has failed. The requested ifIndex has been reserved by other party.

Possible Solution - Obtain another ifIndex.

IFEX9: IfExtensions SNMP agent: service deletion on connection error

This error indicates that the service deletion has failed. The service can not be deleted if there is any connection on this service. Delete the connection first.

Possible Solution - Delete the connection before attempting to perform a service deletion.

IFEX10: IfExtensions SNMP agent: service id error

This error indicates that the service ID is not valid. A valid service ID should be in the form "BNP:CC" where B can be 1, 2, 3, or 4, N can be A, B, C, or D, P can be 1, 2, 3, up to the maximum number of physical ports per FRAMEPLUS netmod (currently is 4), CC can be 00, 01, 02, ..., up to 23 for DS1 port or up to 30 for E1 port.

Possible Solution - Make sure to specify a valid service ID.

2.17 ILMI Error Messages

ILMI0: Info

This does not indicate any failure.

***Possible Solution* -** Informational message.

ILMI1: Warning

This indicates a warning situation. The condition may not be as serious as an error but warrants attention nonetheless.

***Possible Solution* -** Informational message.

ILMI2: Error

This indicates a serious error situation.

***Possible Solution* -** The message should be recorded and reported to the FORE Systems' Technical Assistance Center (TAC) as soon as possible.

ILMI3: Debug

Debugging messages.

***Possible Solution* -** Informational message.

2.18 ILMI 4.0 Error Messages

IL400: Info

This is used to let the user know of internal actions taken by the common ILMI4.0 module.

***Possible Solution* -** Informational Message.

IL401: Warn

This message is displayed when there could be a possible problem in the ILMI4.0 sub-system.

***Possible Solution* -** Informational Message.

IL402: Timer related failure

This message is displayed when the ILMI4.0 timer sub-system failed. The ILMI4.0 initialization may have been aborted due to the timer initialization failure.

***Possible Solution* -** Reboot the switch.

IL403: ILMI shutdown failure

This message indicates that there were some problems while shutting down the ILMI4.0 sub-system.

Possible reasons:

1. Some IMEs were still active while the shutdown was attempted
2. The timer services couldn't be shut off
3. The SNMP services couldn't be shut off

***Possible Solution* -** Informational Message.

IL404: Resource unavailable

This message indicates that memory couldn't be allocated for some data structure in the ILMI4.0 sub-system. The system is running low on dynamic memory.

***Possible Solution* -** Reboot the switch.

IL405: SNMP failure

This message is displayed when the underlying SNMP sub-system failed. The ILMI initialization may have been aborted due to the SNMP sub-system initialization failure.

***Possible Solution* -** Reboot the switch.

IL406: Link Management failure

This message indicates some failure in the link management sub-system of ILMI4.0.

Possible Solution - Informational Message.

IL407: Prefix Management failure

This message indicates some failure in the prefix management sub-system of ILMI4.0.

Possible Solution - Informational Message.

IL408: Auto-configuration failure

This message indicates some failure in the auto-configuration sub-system of ILMI4.0.

Possible Solution - Informational Message.

IL409: Raw FSM failure

This message indicates some failure in the RAW SNMP access module of the ILMI4.0.

Possible Solution - Informational Message.

IL4010: Address Management failure

This message indicates some failure in the Address Management module of the ILMI4.0.

Possible Solution - Informational Message.

IL4011: Discovery FSM failure

This message indicates some failure in the Service Discovery module of the ILMI4.0.

Possible Solution - Informational Message.

2.19 IPFT Error Messages

IPFT0: initializing to defaults

This message is printed whenever the switch is booted and the CDB contains no information concerning IP filtering. This does not indicate a problem unless the IP filtering settings have been changed for this switch.

Possible Solution - Informational message.

IPFT1: failed to initialize ipfilter

This message indicates a catastrophic failure.

Possible Solution - The only way to manage the switch is via the serial port.

IPFT2: failed to set flag

This message usually indicates that the CDB contains corrupt information.

Possible Solution - Informational message.

IPFT3: IP filter cannot add entry: maximum number of entries reached

The IP filtering feature can only accept 32 entries in its table. An attempt to create more than 32 entries will result in this message being printed.

Possible Solution - Informational message.

IPFT4: IP filter cannot add entry: a duplicate entry already exists

In addition to being printed when an attempt is made to create an exact duplicate of an existing entry, this message can also appear when the masked version of the new entry matches the masked version of an existing entry. If this is the case, then only one of the two entries should really be necessary.

Possible Solution - Informational message.

IPFT5: IP filter failed to add entry

This message indicates a failure due to some unknown reason. It is possibly due to a lack of free memory on the system, or a corrupt CDB.

Possible Solution - Informational message.

IPFT6: IP filter failed to delete entry

This message indicates a failure to delete an entry. If this occurs, the state of IP filtering will be undefined.

Possible Solution - Save the CDB and reboot the switch.

IPFT7: IP filter invalid mask

This message indicates the given mask is not contiguous. For the IP filtering feature, only contiguous masks are acceptable; e.g., mask 255.255.0.128 is not valid, but mask 255.255.128.0 is valid.

Possible Solution - Re-enter the mask using a valid format.

2.20 LANE Error Messages

LANE0: Maximum number of LECs reached

The creation of a new LEC failed because the system already has the maximum number (currently 16) of LECs configured.

Possible Solution - To create a new LEC, you must delete one of the existing LECs.

2.21 MGRD Error Messages

MGRD0:

This error message indicates that the reserve or release operation has encountered an internal error in the memory management module.

Possible Solution - Informational message.

2.22 NMDW Error Messages

NMDW0: no connid available for allocation

This error indicates that no more connection IDs are available for allocation on the designated network module. Connection IDs are a per-network module resource, and they are allocated based on various constraints, including the type of connection (unicast/multicast), the destination port, and the class of service.

Possible Solution - Informational message.

NMDW1: internal error - allocated connid is out of range

This is an internal error indicating that a failure occurred during the connection setup process.

Possible Solution - Informational message.

NMDW2: initialization error

This is an internal error which occurred during the initialization of the designated network module. Possible causes of this error would include faulty hardware or a corrupt configuration database (CDB).

Possible Solution - Informational message.

NMDW3: no rate groups are available

The pool of 64 per-port rate groups has been exhausted on the designated port. This can also occur when an attempt is made to rate limit a port and all 64 rate groups are already consumed.

Possible Solution - This can be avoided by using one of the existing rate groups for the new connection, or by changing the scheduling mode of the connection to round-robin so that it does not require an entry in the rate controller.

NMDW4: requested rate is not supported

The rate controller is not able to support the rate requested. The rate is either too low, or is greater than the maximum rate of the port.

Possible Solution - Change the rate to a value which is within the supported range.

NMDW5: requested scheduling mode not supported

The scheduling mode specified for the connection is not supported by the output port.

Possible Solution - Informational message.

NMDW6: unable to rate limit the specified port

The request to rate limit the port could not be satisfied. The most likely cause for this failure is that the port already has bandwidth committed to existing connections which make it impossible to reduce the rate of the port.

Possible Solution - Check the amount of bandwidth currently allocated to connections on this port, and delete connections as necessary to reduce the amount of committed bandwidth to something less than the desired rate.

NMDW7: output port rate limiting being enabled

This informational message indicates that the rate limiting feature of the Series-D network module is being enabled by the hardware for the indicated port and cell rate.

Possible Solution - See the AMI command **`conf port traffic d ratelimit`** for further information.

NMDW8: the rate controller has no further capacity

The rate controller can support no more than 8,192 connections at one time, and that level has been reached. No more rate controlled connections can be created on this network module.

Possible Solution - Informational message.

NMDW9: there is not enough rate capacity in the rate controller for the requested rate

The most likely cause of this message is a port with a ratelimit that is too small.

Possible Solution - Increase the ratelimit on the port.

NMDW10: There is no appropriate memory map for this network module

There is no memory map which matches the network module's cell ram size, table ram size, and shared memory number of ports.

Possible Solution - Informational message.

2.23 NMOD Error Messages

NMOD0: Unable to allocate enough memory

This is an internal error that occurred due to lack of resources.

Possible Solution - Informational message.

NMOD1: Unexpected argument passed to the routine

This error indicates that an invalid state or configuration has been requested. It is mainly due to improper usage of the configuration routines.

Possible Solution - Informational message.

NMOD2: Hardware failure

This is an internal error that occurred due to a faulty piece of hardware. Possible causes of this error include improper configuration information in the hardware, an inability to read / write from / to certain registers, etc.

Possible Solution - Informational message.

NMOD3: Initialization error

This is an internal error that occurred during the initialization of the network module. Possible causes of this error would include a corrupt configuration database (CDB), faulty hardware, memory allocation problems in certain modules, etc.

Possible Solution - Informational message.

NMOD4: Invalid Configuration for this network module

This is used to indicate that an invalid configuration has been requested. This error could be caused because the entity is not in service or the hardware does not support this configuration. An example of this would be requesting loopback on links that are out of service.

Possible Solution - Informational message.

NMOD5:

This is only used to print certain useful information on the console. This does not indicate a failure.

Possible Solution - Informational message.

NMOD6: Internal Error

This indicates that an internal error occurred during this operation. This could be due to faulty hardware, a corrupt configuration database (CDB), or a lack of resources.

Possible Solution - Informational message.

NMOD7: Framing mode change error

This indicates that the framing mode change request was denied due to lack of resources. When a framing mode is changed on the link, the ATM cell rate that this link can support changes due to the overhead associated with the framing mode. If there is not enough bandwidth left to support this change in ATM cell rate, the framing mode cannot be changed.

Possible Solution - Informational message.

nmod8: Bad FSM state:

This message means that the network module's machine state variable has illegal value.

Possible Solution - Informational message.

nmod9: Sdpm test failed:

This message means that the network module SDPM test from the SCP side has failed.

Possible Solution - Informational message.

nmod10: Bad value returned by SDPM api: line

This message means that call to an SDPM api routine returned a bad value.

Possible Solution - Informational message.

nmod11: Netmod FSM state change:

This message traces network module FSM state transitions during the lifetime of the network module. The message includes previous state, current state, netmod id and line number in the inmfsm.c file.

Possible Solution - Informational message.

nmod12: Application revision callback failed

This message means that during the network module startup procedure the application revision report message callback function failed to allocate memory to post the message to the FSM.

Possible Solution - Informational message.

2.24 OAMS Error Messages

OAMS0: Unable to create OAM VC

When an originating/terminating path pair is created, and the minimum and maximum VCI for the paths contain both VCI 3 and 4, then the OAM functions will attempt to create VCs on VCI 3 and 4 in the path pair. This error message indicates that either a memory allocation error has prevented the creation of the VC, or that a problem was detected when configuring the fabric for the connection.

Possible Solution - More information detailing the specific stage of VC creation that failed can be obtained by enabling the OAM debug feature using the AMI command **`debug trace hardware fabric oam on`**.

2.25 OLCC Error Message

OLCC0:

This is used to let the user know of internal actions taken by the OLCC (One-Legged Call Control) module.

Possible Solution - Informational Message.

OLCC1:

This is used to print information. This usually follows an error message.

Possible Solution - Informational Message.

OLCC2: Memory Resource Error

This message is printed if the OLCC module is not able to allocate memory for any of its data structures. This could happen due to a shortage of free space in the switch's memory or if the memory is fragmented to an extent that there is not a single free block of the size that a signalling data structure requires.

Possible Solution - Informational Message.

OLCC3: Function returned error

The specified function returned an error. This is a very general error message and denotes a variety of error situations.

Possible Solution - Informational Message.

OLCC4: Invalid Parameter

This error indicates that the arguments passed into a function have invalid values. It may be that the argument itself has invalidvalues such as a NULL pointer, or some other entity that is derivedfrom the argument has an invalid value.

Possible Solution - Informational Message.

OLCC5: Internal Error

This error message is printed out when some error that is internal to the OLCC module is encountered.

Possible Solution - Informational Message.

OLCC6: Warning

This is a warning. Attempted operation will proceed, but more errors may occur.

Possible Solution - Informational Message.

2.26 PNNI Error Messages

PNNI0:

This is a critical error message. It indicates that the PNNI node is shutdown. This means its operational status is down. The message usually contains the node index of the node that got shut down and the function name during whose execution this event occurred. A PNNI logical node is shut down when the topology database (TDB) is in unrecoverable error condition due to inconsistencies in the TDB or due to incremental MALLOC failures. When this happens, the operation state of this logical node is set to down and a SNMP trap indicating this situation is generated. Refer to SNMP trap number 1075. A node is said to be shut down when it stops participating in the PNNI protocol operations like sending Hello packets, performing Database Exchange, and flooding PTSES. If any other PNNI nodes are present on this switch, most likely they will also be shut down eventually.

Possible Solution - The switch has to be rebooted to clear the shut down condition and to bring this node up again.

PNNI1:

This is a critical error message indicating that the memory guardband reserve failed. It usually includes the node index and the routine name during whose execution this event occurred. It means that the switch is low on memory. Refer to SNMP trap number 1074. When this event happens, this SNMP trap is generated. The trap includes the node ID information.

Possible Solution - Informational message.

PNNI2: Fail to activate node

This message is printed when there is a failure to activate a PNNI logical node. It is usually a NOTICE message. The message also prints the index of node whose activation failed. The current values can be seen by executing the command **`conf atmr pnni node show`**. The command **`conf atmr pnni node modify`** can be used to change any of these values. This node activation failure could be because of any of the following reasons:

1. The default domain's protocol is FT-PNNI. Therefore, a PNNI node is not activated. The current information can be seen by entering the AMI command: **`conf atmr domain show`**. If the default domain is not PNNI, then to make PNNI as the default domain's protocol, execute the command **`conf atmr domain modify 1 PNNI`** and then reboot the switch.
2. The node ID level is not set correctly, being different from the PG ID level or from level of peer switches.
3. The software is unable to create a PNNI instance for the node. When a PNNI node is not activated or created, it does not participate in PNNI protocol operations.

Possible Solution - Described above.

PNNI3: Open transaction failed in

This warning message indicates that an update of the prefixes failed. The function pnni_db_open_prfx_trans returns a value of 1 if ptse==PNNI_UNDEFHNDL or tdbh==PNNI_UNDEFHNDL. This is an internal error indicating an inconsistency within a key data structure.

***Possible Solution* -** Informational message.

PNNI4: Close transaction failed in

This warning message indicates that an update of the prefixes failed. The function pnni_db_close_prfx_trans returns a value of 1 when tdbh==PNNI_UNDEFHNDL. That is when the failure occurs.

***Possible Solution* -** Informational message.

PNNI5: Failed to post

This warning message indicates that registration for one of the following failed during rcc creation:

1. Post message listen for input port
2. Callback for input port
3. Carrier loss listen
4. Carrier detect listen

When an rcc is created, first the rcc is allocated, rport is created, then callback for the input rport is registered. Depending upon the type of the packet, various functions are called. Then event listeners for carrier loss and carrier detect are registered. The pnni_hello_link_down routine is called for a carrier loss and the pnni_hello_link_up routine is called for carrier detect. When this failure occurs, then rcc is completely destroyed and the routing protocol cannot begin its function.

***Possible Solution* -** Informational message.

PNNI6: Failed to clean rcc from the scheduler

When the function pnni_rcc_destroy is called, the rcc is cleaned and any packets from the queue are removed. If that operation fails, this warning message is printed with the function name.

***Possible Solution* -** Informational message.

PNNI7: Error in advertising link in

This warning message is printed when the advertisement of horizontal links fails. Output typically includes the node index, port ID, and function name. For example, the function pnni_link_advertise_hlink returns this error in a number of possible cases, including:

1. failure to allocate PTSE pars
2. failure to create a PTSE
3. failure to build a horizontal link PTSE
4. failure of the process ablink listen
5. an error in setting sigch params
6. an error in flooding the horizontal link PTSE

Possible Solution - Informational message.

PNNI8: Failed to encode

This warning message is printed when any of the following failures occur, specifying the function name and object name for which encoding failed. Any of the following will result in this warning:

1. failed to encode hello
2. failed to encode dbsum
3. failed to encode ptse
4. failed to encode ptsp
5. failed to encode ptse_ack
6. failed to encode ptse_req
7. failed to encode ptse_acknode
8. failed to encode ptse_reqnode

Basically, the contents of these SDUs are encoded into a general buffer.

Possible Solution - Informational message.

PNNI9: Failed to parse

This warning message and the corresponding function names are printed when the parsing of ptsp, ptse_ack dbsum, and ptse_req fails. This is an internal error.

Possible Solution - Informational message.

2.27 PNSN Error Messages

PNSN0: PNNI Node is SHUTDOWN

This is a critical error message which indicates that PNNI node is in shutdown state. This means the node's operational status is down. The message usually contains the node index of the node which got shut down. It could be that node is already in shutdown state and when admin, modify, delete, or new operations are done on this node, this message is printed. The PNNI logical node is shut down when the topology database (TDB) is in an unrecoverable error condition due to inconsistencies in the TDB or due to incremental MALLOC failures. When this happens, the operational state of this logical node is set to down and an SNMP trap indicating this situation is generated. Refer to SNMP trap number 1075. A node is said to be shut down when it stops participating in the PNNI protocol operations like sending Hello packets, performing Database Exchange, and flooding PTSES. If any other PNNI nodes are present on this switch, most likely they will also be shut down eventually.

Possible Solution - The switch has to be rebooted to clear the shut down condition and bring this node up again. Check **`conf atmr pnni node show`** to get more information.

PNSN1: No hardware map for board

No hardware map for the given board was found.

Possible Solution - Informational message.

PNSN2: Unable to create default pnni node

The switch is unable to create a default node. This is most likely due to a lack of resources. A default PNNI node is created when no other node is explicitly created by the user. When this happens, the switch will be unable to exchange routing information with other switches and will not be able to route connections.

Possible Solution - Rebooting may solve the problem.

PNSN3: Failed to start precomputation for profile

This means that the paths won't be precomputed for the specified profile.

Possible Solution - Informational message. If this message is displayed, the switch will be able to route, but performance may suffer until the condition clears. No user interaction is recommended.

PNSN4: Invalid node index value

This means an invalid node index value was specified.

Possible Solution - The value of the node index should be greater than 0 but less than 65535 (since 65535 is reserved for the *ForeThought* PNNI node).

PNSN5: Can not modify this parameter while the node admin status is up

The specified parameter cannot be modified while the node admin status is up.

Possible Solution - Admin the node status down before attempting to modify the parameter.

PNSN6: can not modify the lowest flag

The flag cannot be modified with this version of software. This requires the support for hierarchy which is not supported in this version.

Possible Solution - Informational message.

PNSN7: Unable to register route

Although the route has been added to the CDB and SNMP tables, the internal registration process was not successful.

Possible Solution - Informational message.

PNSN8: Unable to modify port id

The port ID of a route address entry cannot be modified when the address is of type exterior and it is configured through the local management system. It is assigned by the node.

Possible Solution - Informational message.

PNSN9: Unable to modify node id

The node ID of a route address entry cannot be modified when the address is of type exterior and it is configured through the local management system. It is assigned by the node.

Possible Solution - Informational message.

PNSN10: Unable to modify domain id

The domain ID can only be modified when node admin status is in down state. If there is any interface still pointing to this node, the modification of node domain ID will fail.

Possible Solution - This dependency can be removed by deleting this node and creating a new node with new domain ID. In some cases, you can modify the nodeix field of those PNNI interfaces to other nodes or delete corresponding signalling paths and recreate them with a new domain ID. After the dependency is removed, you can modify the node domain ID without deleting the node.

2.28 POOL Error Messages

POOL0:

This is a fatal error while creating the memory pools during switch software initialization. This error should never occur under normal circumstances.

Possible Solution - Rebooting should fix the problem.

POOL1: Pool initialization failed

This indicates that pool initialization for the indicated parameter failed. This may be due to lack of memory or fragmentation. Switch operation is not affected because of this.

Possible Solution - Informational message.

POOL2:

This indicates that an unknown parameter is provided to the indicated function.

Possible Solution - Informational message.

POOL3:

This indicates, that while trying to grow the pools for the specified parameter, a defensive check against excessive allocation has failed. The attempted operation fails as a result.

Possible Solution - Informational message.

POOL4:

This indicates, that while trying to grow the pools for the specified parameter, the corresponding pools have failed to grow, due to unavailability of memory or due to fragmentation.

Possible Solution - Informational message.

POOL5:

This indicates, that while trying to reduce the pool size for the specified parameter, one of the corresponding pools has failed to shrink due to an internal error.

Possible Solution - Informational message.

2.29 PROF Error Messages

PROF0: Profile SNMP agent: non-zero reference count

This error indicates that there was an attempt to delete a profile which is referenced by existing service or connection. A profile cannot be deleted if it is referenced by another object.

Possible Solution - Informational message.

PROF1: Profile SNMP agent: configuration database access error

This error indicates that there was an unsuccessful read or write access to the configuration database. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

PROF2: Profile SNMP agent: invalid profile type

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

PROF3: Profile SNMP agent: invalid profile index

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

PROF4: Profile SNMP agent: invalid argument

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

PROF5: Profile SNMP agent: system error

This error indicates that there may be some fundamental system error.

Possible Solution - Contact the system administrator.

PROF6: Profile SNMP agent: no resource for creation

This error indicates that there is not enough memory resource in the system to perform the requested operation.

Possible Solution - Contact the system administrator.

PROF7: Profile SNMP agent: invalid object identifier

This error indicates that an invalid value was passed into the function. This may indicate some fundamental system error.

Possible Solution - Contact the system administrator.

PROF8: Profile SNMP agent: can't delete a default profile

This error indicates that there was an attempt to delete a default profile which exists forever.

Possible Solution - Informational message.

2.30 ROUT Error Messages

ROUT0: Info

This usually does not indicate a failure. It is a very general and widely used message type that is used for printing more information on the console. It is generally used for printing the contents of variables such as portid, nodeid, nodix, domain_id, nsap_addr, mask, pgid, peer, etc.

Possible Solution - Informational message.

ROUT1: Notice

This generally indicates the completion of a task or event. Also, if an event occurs differently than normal, this message can be used to bring that situation to the user's attention. It is a very general and widely used message type.

Possible Solution - Informational message.

ROUT2: Warning

This indicates some warning situation, but it may not be a serious error condition. It could also indicate some misconfiguration. Look for more information in the printed messages and check the relevant menus in AMI for any misconfigurations. It could also indicate other problem situations. It is a very general and widely used message type. A warning condition is usually followed by return, continue, or break statements.

Possible Solution - Informational message.

ROUT3: Error

This message usually reports or indicates a major error situation.

Possible Solution - Please record the message and contact FORE Systems Technical Support for assistance.

ROUT4:

This message is used for debugging. It prints the contents of various packets like Hello Sdu, Dbxsum Sdu, Flooding Sdu, PSTE/PTSP/PTSP ACK Packets, etc. These are generally useful for the code developers and for fixing bugs. Currently not reported through commsgs.

Possible Solution - Informational message.

ROUT5: Error in Function

This is very general and widely used to report various kinds of error situations. It indicates the specified function returned an error. The error could be due to an assert failure, failure of alloc, malloc, etc. It usually prints the function name that returned the error. The function name gives some idea about where the problem is coming from (i.e., PNNI, FT-PNNI, or ATM routing).

***Possible Solution* -** Informational message.

ROUT6: Invalid Argument in function

This indicates that a bad argument is passed to a function. The message usually prints the name of the argument and function name.

***Possible Solution* -** Informational message.

ROUT7: Duplicate

This indicates that the specified object is duplicated; i.e., it is present or already exists. It could be that a particular object is being inserted into list/splay tree/patricia tree more than once. It could also be that a loopback exists between two routing interfaces associated with same node index.

***Possible Solution* -** Please check **`conf atmr pnni interface show`** and modify the index of one of the interfaces to have a different PNNI node index.

ROUT8: Failed to alloc

This indicates that allocation of memory failed for the specified object in the message. This rarely happens, but could happen if the Switch is very low on memory. The common reason is that there one or more processes occurring which require a lot of memory; e.g., there are a lot of SNMP Requests and the system is heavily loaded, or there are a lot of call setups with SVCs and PVCs. Another reason for the failure is that there is memory available, but the requested chunk of memory is not available due to memory fragmentation.

***Possible Solution* -** Informational message.

ROUT9: Assert failed on

This indicates that an assert failed. This happens if the object is NULL, empty, or does not exist. It is a common C macro used for program verification during development to verify that certain conditions are TRUE at run time. Usage: void assert (int expression). If expression is zero when assert (expression) is executed, the macro will print on stderr a message, such as Assertion failed:expression, filename, line number. It then calls abort to terminate the execution. The source filename and line number come from the preprocessor macros __FILE__ and __LINE__. When a program is operational, assertions can be disabled by NDEBUG, after which run-time overhead can be minimized. This is an internal error.

***Possible Solution* -** Informational message.

ROUT10: Failed to create

This indicates that a creation failed. It could be that allocation failed before this. Generally, peer, ptse, etc. are created. For example, the function pnni_db_create_ptse fails when the node handle is not defined. The function pnni_create_peer fails when it is not able to alloc peer, if there is a duplicate peer, or if it fails to insert the peer into node's list of peers. This is an internal error.

Possible Solution - Informational message.

ROUT11: Failed to insert

This indicates that an insertion failed. One of the reasons could be that allocation failed before this. For splay tree:usage:int splay_insert (splay_t *st, ptr_t key, caddr_t data), returns -1 on error, 0 on success, and 1 if the key is already present in tree -- duplicates are not allowed. It returns -1 when either the tree itself is not present, or when it is not able to allocate for a new tree node. Similar conditions exist for splay_cust tree list, patricia tree, etc. This is an internal error.

Possible Solution - Informational message.

ROUT12: Failed to find

This indicates a failure to find the specified object. It could be that it does not exist. It also could be that allocation or insertion failed before this or the the object searched could be invalid or a bad argument. For splay tree :usage: caddr_t splay_find (splay_t *st, ptr_t key), return 0 if the item is not found or if the tree itself is not present, else it returns the item. Similar conditions for splay_cust tree. Please look for error conditions for list, patricia tree, etc. Sometimes when situations like x = f(a,b,c..) and if(!x) happen, it is reported that it failed to find x. This is an internal error.

Possible Solution - Informational message.

ROUT13: Failed to Delete

This indicates that a deletion failed. It could be that the particular object does not exist or it could be a bad or invalid argument. For splay tree:usage:int splay_delete(splay_t *st, ptr_t key) returns -1 if item/key is not present in tree or when the tree itself is not present, and 0 when successfully deleted. Similar conditions exist for splay_cust tree, list, and patricia tree. This is an internal error.

Possible Solution - Informational message.

ROUT14: Failed to clear

Clearing generally involves cancelling timers like ack timer, retransmission timers, etc., and clearing and freeing some variable and objects. It also involves clearing various lists like request list, ack list, retransmission list, etc. Freeing also generally involves clearing lists. This is an internal error.

Possible Solution **-** Informational message.

ROUT15: Failed to destroy

This indicates a failure to destroy. It could be that the specified object does not exist. Generally, all the objects that have routines for creation will have functions for destroying. Destroying is nothing but clearing and freeing. If this function returns an error, it means there is an error either in clearing or in freeing. This is an internal error.

Possible Solution **-** Informational message.

ROUT16: Failed to init

This indicates an initialization failure. One of the reasons could be that allocation failed before this; e.g., failed to init rport, pc, hierarchy, etc. This is an internal error.

Possible Solution **-** Informational message.

ROUT17: Failed to build

This indicates a failure to build the specified packet. It could be that allocation failed before this; e.g., the function pnni_fl_build_ptsp fails when pkt ptse alloc fails or when it fails to insert ptse(s) into ptsp sdu. This is an internal error.

Possible Solution **-** Informational message.

ROUT18: Failed to get

This indicates a failure to get or find some variable (like tx.rcc from pnni_peer_get_tx_rcc function). Given a particular peer, it returns the port ID of one of the links if they exist, usually the first one in the PNNI links. This function returns 0 only when it fails to find any links in the PNNI links structure. This is an internal error.

Possible Solution **-** Informational message.

ROUT19: Failed to process

This indicates a failure in the processing of various packets like ptse, ptse acks, and dbsum. This is an internal error.

Possible Solution **-** Informational message.

ROUT20: Error in setting

This indicates an error in the setting of some variables like link parameters, pnni_link_set_sigch_params functions asserts link, node and ablink and calls ablink_set_sigch_params which returns error only when ablink->sig_type=ab_trunk_group because the VP trunk group is not yet implemented. This is an internal error.

Possible Solution - Informational message.

ROUT21: Failed to send

This indicates a failure to send the specified packets like hello, dbsum, ptse, ptse ack, ptsp. This is an internal error.

Possible Solution - Informational message.

ROUT22: Failed to add

This indicates a failure to add; e.g., adding ptse handle to peer's rxmt list,req list, and ack list. This is an internal error.

Possible Solution - Informational message.

ROUT23: Failed to recv or error in receiving

This indicates a failure to receive the specified packet. This is an internal error.

Possible Solution - Informational message.

ROUT24: Failed to drop

This indicates a failure to drop the specified packets. This is an internal error.

Possible Solution - Informational message.

ROUT25: Failed to clean

This indicates a failure to clean the specified objects. This is an internal error.

Possible Solution - Informational message.

ROUT26: Error in

This indicates an error in the specified event. This is a very generic error used to indicate various event errors or failures.

Possible Solution - Informational message.

ROUT27: Null

This indicates the specified variable or structure is empty. This is a generic and widely used message type.

Possible Solution - Generally, an assert takes care of these situations.

ROUT28: Empty

This indicates the specified variable is Empty or NULL. This is a generic and widely used message type.

Possible Solution - Informational message.

2.31 SEID Error Messages

SEID0: SecurID Configuration File Error

This indicates that the SecurID configuration file is corrupted, is an unsupported version, is an invalid format, or does not exist on the switch.

Possible Solution - Informational message.

SEID1: SecurID Server Unreachable

This indicates that the switch is unable to communicate with the SecurID server. The server is either unreachable or is not running.

Possible Solution - Informational message.

SEID2: Unknown Server Code

This indicates that the SecurID server returned an unknown code for the switch's authentication request.

Possible Solution - Informational message.

SEID3: Socket Creation Failure

This indicates that one of the calls for creating and initializing a socket for communication with the SecurID server failed. This could be due to a lack of resources.

Possible Solution - Informational message.

SEID4: No SecurID Server Information

This indicates that the switch did not find which SecurID server to use because the information was not listed in the configuration file.

Possible Solution - Informational message.

SEID5: SecurID Server Unreachable

This indicates that the switch could not send data to the SecurID server. It could be due to a network misconfiguration, an interface being down, etc.

Possible Solution - Informational message.

2.32 SNMP Error Messages

SNMP0:

This indicates that the requested object does not exist or is an unknown object.

Possible Solution - Informational message.

SNMP1:

This indicates that an invalid, inconsistent, or wrong value was specified.

Possible Solution - Informational message.

SNMP2:

This indicates that a variable which had read-only access was attempted to be modified.

Possible Solution - Informational message.

SNMP3:

This indicates some general system error occurred in processing the SNMP request.

Possible Solution - Informational message.

SNMP4:

This indicates that the specified value is the wrong type.

Possible Solution - Informational message.

SNMP5:

This indicates that the specified value is the wrong length.

Possible Solution - Informational message.

SNMP6:

This indicates that the request to create a new row in an SNMP table failed. This could happen due to specifying invalid indices, or trying to create duplicate entries.

Possible Solution - Informational message.

SNMP7:

This indicates that the processing of an SNMP request - either creating a new row, or modifying a value - failed because system resources (such as memory) were unavailable.

Possible Solution - Informational message.

SNMP8:

This indicates that the variable the user is trying to access cannot be accessed, or may be an unsupported or deprecated variable.

Possible Solution - Informational message.

SNMP9:

This indicates that the specified IOCTL to get or set something during a SNMP operation failed.

Possible Solution - Informational message.

SNMP10:

This indicates that a call to set some variable failed during an SNMP set operation.

Possible Solution - Informational message.

SNMP11:

This indicates a failure to open the indicated device.

Possible Solution - Informational message.

SNMP12:

This indicates that the SNMP operation on the requested table failed, as the table has not been initialized yet. Typically, the user will not see this error.

Possible Solution - Informational message.

SNMP13:

This indicates an attempt to open an SNMP session failed.

Possible Solution - Informational message.

SNMP14:

This is an internal error that indicates that an attempt to close an SNMP session failed.

Possible Solution - Informational message.

SNMP15:

This indicates that an attempt to open an SNMP session to the specified host failed, because the host is unknown.

Possible Solution - Informational message.

SNMP16:

This indicates an internal error while building a SNMP packet.

Possible Solution - Informational message.

SNMP17:

This indicates that the specified object identifier is invalid or has an unrecognized format.

Possible Solution - Informational message.

SNMP18:

This message indicates the occurrence of an SNMP trap. It is essentially a NOTICE to the administrator. The message gives the trapId of the trap that occurred and lists the trap variables. It also indicates if it is being transmitted to the trap destinations. If it is not being transmitted, it means that the threshold for that trap has not been reached yet.

Possible Solution - Informational message.

SNMP19:

This indicates some internal error occurred during an SNMP operation.

Possible Solution - Please record the message and contact FORE Systems' Technical Support for assistance.

SNMP20:

This indicates the SPVC reroute feature has been globally disabled or enabled.

Possible Solution - Informational message.

SNMP21:

This message is an informational message about IISP autoconfiguration. For an IISP link to automatically determine either the uni version or user/net side, or both, the peer has to support ILMI 4.0. This is because pre-ILMI4.0 specifically states that ILMI is not used over IISP links. Only ILMI 4.0 allows ILMI to be run over IISP links and defines autoconfiguration of the uni version and/or user/net side. If the peer does not support ILMI 4.0, then this interface will not come up. You will have to delete the uni and recreate it specifying both version and un side.

Possible Solution - Informational message

SNMP22:

This indicates that if the peer is a non-Fore switch, the max_vci advertised will be a number that is 1 less than a power of 2. For example, if the max_vci is configured to be 45, the value advertised will be 31 (if the peer is a non-Fore switch). Only Fore switches allow one to specify any value for max vci for vci range negotiation. This is because the ILMI spec defines the operational, negotiated maxVCI to be one less than a power of 2. If the peer is not a Fore switch, and if the value chosen by the switch is not the desired value, then the uni should be deleted and recreated with a proper value (i.e. one less than a power of 2).

Possible Solution - Informational message.

SNMP23: Notification

These notification messages are used to notify the network administrator of any important events they should know about that occur in the SNMP layer.

Possible Solution - Informational message.

2.33 SPANS Error Messages

SPAN0:

This is only an informational notice. It is generally used for printing the contents of the variables or for informing the user about the completion of a task.

Possible Solution - Informational message.

SPAN1: System error

This error condition usually reports a major error situation.

Possible Solution - Informational message.

SPAN2: Error in creating sigpath

This error could have occurred because incorrect parameters were specified when creating the signalling path or because specified resources are not available.

Possible Solution - Informational message.

SPAN3: Error in activating sigpath

This error could have occurred because incorrect parameters were specified when activating the signalling path or because specified resources are not available.

Possible Solution - Informational message.

SPAN4: Error in finding sigpath

This indicates that a signalling path does not exist for this instance of SPANS. This could be because the signalling path was not created on the particular link and VPI was created, but not inserted into the signalling path tree for SPANS.

Possible Solution - Informational message.

SPAN5: Error in creating aal

This indicates that fabric data structures were unable to be allocated. This could be because incorrect parameters were specified when creating the signalling path or because specified resources are not available.

Possible Solution - Informational message.

SPAN6: Ports are cross-linked

This indicates that SPANS routing has detected cross-linked switch ports. When a link is moved, topology information may become temporarily stale. This is a transient condition.

Possible Solution - Informational message.

SPAN7: CDB directory does not exist

This indicates that the CDB does not have either a software, spans, sigpath, or term directory.

Possible Solution - Informational message.

SPAN8: Unable to write to cdb

This indicates that there is a major error condition in the CDB.

Possible Solution - Informational message.

SPAN9: Unable to read from cdb

This indicates that there is an error condition in the CDB or that the value was not written to the CDB.

Possible Solution - Informational message.

SPAN10: Nsap router missing

This indicates that the NSAP router has not been initialized. The relevant schedulers for receiving FT-PNNI hello messages and NSAP map messages have been installed but the router itself is missing. This indicates a serious condition.

Possible Solution - Informational message.

SPAN11: Wrong link type

This indicates that the link is not a UNI link or an NNI link.

Possible Solution - Informational message.

SPAN12: Link overflow

This indicates that the number of links from a SPANS map message or an NSAP map message exceeds the maximum number of links for a port.

Possible Solution - Informational message.

SPAN13: Unable to calculate equivalent capacity

This indicates that the Quality of Service parameters are wrong or that the VBR overbooking parameters are wrong.

***Possible Solution* -** Informational message.

SPAN14: Affects both SPANS and FTPNNI

This indicates that errors which occur when creating the signalling path for SPANS would bring down the signalling path. This would seriously affect FT-PNNI because FT-PNNI uses the SPANS signalling path for its routing messages.

***Possible Solution* -** Informational message.

2.34 SPVX Error Messages

SPVX0: Information

This is used to print the values of certain important variables that give additional information to any preceding warning or error messages.

Possible Solution - Informational message.

SPVX1: Notification

If any important events happen in the SPVCC/SPVPC layer that the network administrator should know about, these notification messages are used.

Possible Solution - Informational message.

SPVX2: Warning

This indicates a potential source of a problem, that the switch may recover from. These warning messages will be helpful in diagnosing such problems.

Possible Solution - Informational message.

SPVX3: Debug

This contains debugging related information which may be useful to trace any error condition.

Possible Solution - Informational message.

SPVX4: Parameter Validation Error

To assist debugging, it is a usual practice to validate the parameters passed to a function at first. If the passed parameters or the parameters derived from them are null or invalid pointers, then this error message is printed with the parameter in question that is incorrect.

Possible Solution - These are used for debugging and should not occur normally.

SPVX5: Internal Error

If there is some inconsistency in some internal data structures of SPVCC/SPVPC layer, then this internal error is reported. Such errors may be fatal and can potentially lead to memory and/or resource leakage.

Possible Solution - Informational message.

SPVX6: Resource Unavailability Error;

This error is reported when the SPVX module finds that there is a lack of system resources like memory, link bandwidth, etc. The exact resource that is not available will be displayed. The system might be able to recover from this condition when resources become available in the future.

Possible Solution - Informational message.

SPVX7: Call Recording Error

This error will be reported when billing has been turned on for SPVCC/SPVPC calls. SPVX module invokes the billing module functions under such a situation. If the billing module encounters an error now, this message will be printed out. The exact nature of the error can be deduced from the information printed out by the billing module. Further processing depends on the nature and the severity of the error.

Possible Solution - Informational message.

SPVX8: Fabric Setup/Cleanup Error

After the allocation of switch fabric resources, the SPVX module invokes certain fabric functions to setup the actual connection in the hardware. Similarly, it invokes fabric functions to tear down the connection also. If the fabric module encounters an error during this process, the SPVX module prints out this message. The error message printed out by the fabric module should be used to determine the exact problem.

Possible Solution - Informational message. More detailed information can be obtained by turning on the debugging in SPVX module.

SPVX9: Signalling Error

The SPVX module invokes signalling module to send out messages for setting up or tearing down SPVPCs/SPVCCs. If the signalling module meets with an error condition during this process, this particular class of error messages will be printed out by the SPVX module. More detailed information on the error can be obtained from the error message printed out by the signalling module.

Possible Solution - Informational message.

SPVX10: Directed DTL Error

This error message is printed out by the SPVX module if it is unable to use the directed DTLs configured for that SPVCC due to some reason. If a SPVCC is being setup when there is a temporary change in topology then this message might appear for sometime and stop eventually when the topology gets restored. If there is an error in the DTLs that were configured, or if there are misconfigurations in routing in the network, then this error will occur persistently.

Possible Solution - When this error occurs the user can display the DTLs configured for that SPVCC using the **`configuration spvx spvcc pnni show advanced`** command and the **`configuration atmr ftpnni dtl show`** command, and verify that the DTLs and the routing parameters in the network have been configured correctly.

SPVX11: Invalid Configuration Parameters Error

This error message is printed out when the SPVX module detects that one of the configuration parameters for a SPVCC or a SPVPC is incorrect. Information on the misconfigured parameter is also printed out. The SPVPC or SPVCC in question will not be created.

Possible Solution - Create the SPVPC/SPVCC with proper values for that parameter

SPVX12: ABR Parameter negotiation error

This message is printed out if the switch detects an error in the way the ABR parameters have been negotiated in the CONNECT message that has been received for a SPVCC/SPVPC.

Possible Solution - Informational message.

SPVX13: Connection ID check Failure

In SPVX module if the switch allocates the connection identifier (VPI/VCI) before forwarding the SETUP message for a SPVPC/SPVCC out, it makes sure that the connection identifier (VPI/VCI) received in CALL PROCEEDING or CONNECT or ALERTING message is the same as the one that was previously allocated. This error is printed when a mismatch is detected.

Possible Solution - If there is any mismatch, then it means that the switch down stream has not accepted the VPI/VCI we have sent. This could be because of a misconfiguration of the user and network sides of the NNI interface especially when the interface is IISP or Public UNI.

2.35 SRVC Error Messages

SRVC0: Invalid service type

This indicates an unsupported Service Type has been found in the list of supported services. This is a result of some kind of memory corruption.

Possible Solution - Informational message.

SRVC1: Invalid address index value

This indicates a bad address index value in the object identifier of the SNMP request. Currently, values 1 through 4 are valid.

Possible Solution - Informational message.

SRVC2: Invalid port

This indicates the port number used in the object identifier of the SNMP request is not a valid port number. This port may not exist on the switch currently.

Possible Solution - Informational message.

SRVC3: Service registry splay alloc failed

This indicates failure to initialize service registry. The service registry feature does not work when this message appears.

Possible Solution - Informational message.

SRVC4: Service registry delete failed

This indicates some kind of corruption took place. The service registry entry you tried to delete is not in the splay tree.

Possible Solution - Informational message.

SRVC5: Failed to create service registry entry

This error could happen if there is not enough memory to allocate to the new entry being created or if a duplicate entry already exists.

Possible Solution - Informational message.

2.36 TASK Error Messages

TASK0: Info

Informative message.

Possible Solution **-** Informational message.

TASK1: Warning

Warning message.

Possible Solution **-** Informational message.

TASK2:Error

Error message.

Possible Solution **-** Informational message.

TASK3: Debug

Debug message usually associated with a debug flag.

Possible Solution **-** Informational message.

TASK4: Malloc failure

Failed to allocate memory.

Possible Solution **-** Informational message.

TASK5: Failed to create msgQ

Failed to create message queue.

Possible Solution **-** Informational message.

TASK6: Failed to create msgQSet

Failed to create message queue set. This message queue set is monitored by a task for the incoming messages Incoming messages for this message queue set will be dropped with any processing.

Possible Solution **-** Informational message.

TASK7: Failed to add a queue to the QSet

Failed to add the queue to the message queue set. The result of this is that the target task which monitors the set won't be able to read the messages.

***Possible Solution* -** Informational message.

TASK8: Failed to add msgQSet to the shared name DB

Failed to add the message queue set to the shared name data base. As a result of this the target task (task that monitors this message queue) won't be able to read the incoming messages if the task happen to run on a different processor.

***Possible Solution* -** Informational message.

TASK9: Failed to find msgQSet in the shared name DB

Failed to find the message queue set to the shared name data base. As a result of this the target task (task that monitors this message queue) won't be able to read the incoming messages if the task happen to run on a different processor.

***Possible Solution* -** Informational message.

2.37 UPCV Error Messages

UPCV0: UPC contract SNMP agent: invalid value passed for writing

This error indicates that an invalid value was passed into the UPC contract SNMP agent. This may indicate a user error in AMI/*ForeView*, or some more fundamental system error.

Possible Solution - Check the network management interface and ensure that all parameters to the UPC contract are valid.

2.38 UTIL Error Messages

util0: error - failed on attempt to update integer value in the CDB

This internal error indicates that switch software failed on an attempt to update an integer value in the switch Configuration Database (CDB).

Possible Solution - Informational message.

util1: error - failed on an attempt to open the cdb

This internal error indicates that switch software failed on an attempt to get a handle into the switch Configuration Database (CDB).

Possible Solution - Informational message.

2.39 VPMS Error Messages

VPMS0: Unable to allocate VCI_ANY

The switch was unable to allocate any VCI. This means that there are no more VCIs available on the path.

Possible Solution - If this error persists, you should delete and recreate the terminating and originating paths with a greater maxvci.

VPMS1: Unable to allocate specific VCI

The switch was unable to allocate a specific VCI. This means that the VCI is already in use. It could be permanently in use by a PVC or temporarily in use by an SVC.

Possible Solution - Informational message.

VPMS2: Unable to alt allocate VCI_ANY

The switch was unable to allocate any VCI. This means that there are no more VCIs available on the path.

Possible Solution - If this error persists, you should delete and recreate the terminating and originating paths with a greater maxvci.

VPMS3: Unable to alt allocate specific VCI

The switch was unable to allocate a specific VCI. This means that the VCI is already in use. It could be permanently in use by a PVC or temporarily in use by an SVC.

Possible Solution - Informational message.

2.40 VPVC Error Messages

VPVC0: The specified path already exists.

This indicates that the path that you are trying to create already exists.

Possible Solution - Informational message.

CHAPTER 3 SCP Diagnostics

The tests provided in this section are very specific diagnostics that are only to be run if you have determined that there is a problem with your i960 or Pentium-based SCP in an *ASX*-200WG, *ASX*-200BX, *ASX*-1000, *ASX*-1200, *TNX*-210, or *TNX*-1100.

Currently, the SCP self-test diagnostics mentioned in this chapter are not available for the *ASX*-4000.

NOTE This chapter does not apply to the *ESX*-3000, LE25 and LE155 switches.

3.1 SCP Diagnostics

If you have determined that there is a hardware problem on a switch control processor (SCP), run the SCP diagnostics that are available by connecting a terminal device to that SCP's serial port and accessing the SCP Monitor mode.

NOTE The diagnostics will only test the SCP, not the switch fabric.

NOTE All AMI sessions should be closed before these tests are run.

NOTE It is recommended that you back up your CDB before running any tests that check the FLASH and/or the SRAM. The chip configuration is saved before testing each one and then restored. However, if a power failure occurs or if the switch rebooted during the test, some of the data may not be restored properly.

3.1.1 Accessing the SCP Monitor Mode

To access the SCP Monitor mode on an SCP, perform the following steps:

1. Boot the SCP by pressing the RESET button on the front panel of the SCP. Because the RESET button was designed to avoid accidental resets, you will need to use a straightened paper clip to push the RESET button.
2. Press and release the SELECT button on the front panel of the SCP. The display LED will cycle through the following parameters:

```
- ASXP5[1]
- 12:00 a.m.
- TTY Test
- DRAM 00-15 MB[1]
- DRAM OK
- Timer T
- Clock T
- TEST BUS
- FLASH?
```

3. When the display LED shows FLASH?, press the NEXT button. ETHERNT? will be shown on the display LED.
4. Press the NEXT button again so that MONITOR? is shown on the display LED.
5. Press the SELECT button. The ? will disappear from MONITOR on the display LED, indicating that MONITOR has been chosen. The terminal device will indicate that the user is in the SCP Debug Monitor mode.
6. Press the RETURN key on your terminal device's keyboard to get to the => prompt.
7. At the => prompt, type **?** and press the RETURN key. A list of available debugging and hardware test commands will display.

---

1. This line displays for a Pentium-based SCP only.

3.1.2 Running the Hardware Tests

Table 3.1 lists the test commands and the SCP type for which it is available:

Table 3.1 - SCP Test Commands

Command	Description	SCP Type
test-clock	test Real Time Clock	all i960 and Pentium types
test-dram	test the DRAM using both address and pattern tests	all i960 and Pentium types
test-dl	test DRAM in a longer, more robust test	i960HA and Pentium only
test-dc <bank> <chip>	test DRAM chip # <chip> in bank <bank>	i960CF and i960HA only
test-ethernet	test Ethernet	all i960 and Pentium types
test-flash	test Flash	all i960 and Pentium types
test-fc <chip>	test Flash chip <chip>	all i960 and Pentium types
test-serial	test Serial Port	all i960 and Pentium types
test-sram	test SRAM	all i960 and Pentium types
test-timer	test Timer	all i960 and Pentium types
test-sdb	test SDB	i960HA and Pentium only
test-all	test all devices, except Flash and SRAM	all i960 and Pentium types
test-manufact	test all devices	all i960 and Pentium types
test-sim <simm>	test DRAM SIMM # <simm>	i960HA only
march-data <addr>	test the integrity of the data bus	i960HA only
march-address <addr>	test the integrity of the address bus	i960HA only

Type the test command at the prompt to run the individual test. A test that completes correctly will be reported as “OK” on both the terminal connected to the serial port and on the display LED on the front panel of the SCP. A test that is not successful will be reported as “failure” on the terminal connected to the serial port and as “BAD” on the display LED. If any of the tests fail, contact FORE Systems’ TAC using one of the methods listed in the Preface of this manual.

The following subsections depict an example of how to perform each test through the serial port and the SCP's confirmation message to the terminal connected to the serial port that the test was successful. The user input is in **`bold courier`** font and the SCP's response is shown in `courier` font.

3.1.2.1 Clock Test

This test checks the real time clock to verify that it is ticking correctly. It takes about two seconds to run. This test is available for all i960 and Pentium types.

```
=>test-clock
Clock: OK
```

3.1.2.2 DRAM Test

This test checks the DRAM's functionality using address and pattern tests. It takes about 30 seconds to run. This test is available for all i960 and Pentium types.

```
=>test-dram
64MB EDO DRAM detected[1]
DRAM: OK
```

3.1.2.3 Complete DRAM Test

This test checks the DRAM's functionality using a longer, more robust test. It takes about ten minutes to run. This test is only available for the i960HA and Pentium SCPs.

```
=>test-dl
64MB EDO DRAM detected[1]
DRAM: OK
```

3.1.2.4 DRAM Chip Test

This test checks the functionality of a DRAM chip. It takes about two seconds to run. This test is only available for the i960 SCP types.

```
=>test-dc a
DRAM chip: OK
```

---

1. This line is specific to the Pentium-based SCPs only.

3.1.2.5 Ethernet Test

This test check the functionality of the Ethernet chip by running an internal loopback test. It takes about one second to run. This test is available for all i960 and Pentium types.

```
=>test-ethernet
Ethernet: OK
```

3.1.2.6 FLASH Test

This test checks the functionality of each FLASH chip. It takes about 20 minutes to run. This test is available for all i960 and Pentium types.

NOTE

It is recommended that you back up your CDB before running this test. The chip configuration is saved before testing each one and then restored. However, if a power failure occurs or if the switch rebooted during the test, some of the data may not be restored properly.

```
=>test-flash
Flash Test
Save Chip 0

Erase Chip
Pattern 0

Erase Chip
Pattern 1

Erase Chip
Pattern 2

Erase Chip
Pattern 3
.
.
.
Erase Chip
Pattern 1

Erase Chip
Pattern 2

Erase Chip
Pattern 3
Flash: OK
```

3.1.2.7 FLASH Chip Test

This test checks the functionality for a specific FLASH chip. It takes about one and a half minutes to run. This test is available for all i960 and Pentium types.

NOTE

It is recommended that you back up your CDB before running this test. The chip configuration is saved before testing each one and then restored. However, if a power failure occurs or if the switch rebooted during the test, some of the data may not be restored properly.

```
=>test-fc 1
Save Chip 1

Erase Chip
Pattern 0

Erase Chip
Pattern 1

Erase Chip
Pattern 2

Erase Chip
Pattern 3
Flash: OK
```

3.1.2.8 Serial Port Test

This test checks the serial port's internal paths. It takes about one second to run. This test is available for all i960 and Pentium types.

```
=>test-serial
Serial: OK
```

3.1.2.9 SRAM Test

This test checks the SRAM's functionality. It takes about one second to run. This test is available for all i960 and Pentium types.

NOTE It is recommended that you back up your CDB before running this test. The SRAM is saved before testing and then restored. However, if a power failure would occur or if the switch were rebooted during the test, some of the data may not be restored properly.

```
=>test-sram
SRAM: OK
```

3.1.2.10 Timer Test

This test checks to see if the timer is counting correctly. It takes about one second to run. This test is available for all i960 and Pentium types.

```
=>test-timer
Timer: OK
```

3.1.2.11 SDB Test

This test checks for access to the switch fabric. It takes about one second to run. This test is only available for the i960HA and Pentium SCPs.

```
=>test-sdb
SDB test passed
```

3.1.2.12 Hardware Test

This series of tests checks the functionality of all of the hardware devices in the SCP, except the FLASH chips and SRAM. It takes about fifteen seconds to run. This test is available for all i960 and Pentium types.

```
=>test-all
Clock: OK
64MB EDO DRAM detected[1]
DRAM: OK
Ethernet: OK
Timer: OK
Serial: OK
```

1. This line is specific to the Pentium SCPs only.

3.1.2.13 Complete Hardware Test

This series of tests checks the functionality of all of the hardware devices in the SCP including the FLASH chips and SRAM. It takes about six minutes to run. This test is available for all i960 and Pentium types.

NOTE

It is recommended that you back up your CDB before running this test. The chips are saved before testing each one and then restored. However, if a power failure would occur or if the switch were rebooted during the test, some of the data may not be restored properly.

```
=>test-manufact
Clock: OK
DRAM: OK
Ethernet: OK
Timer: OK
}Serial: OK
SRAM: OK
Flash Test
.
.
.
Erase Chip
Pattern 1

Erase Chip
Pattern 2

Erase Chip
Pattern 3
Flash: OK
```

3.1.2.14 DRAM SIMM Test

This test checks the functionality of a specific DRAM SIMM. It takes about one second to run. This test is only available for the i960HA SCP.

```
=>test-sim 1
DRAM SIMM: OK
```

3.1.2.15 Data Bus Integrity Test

This test checks the integrity of the data bus. It takes about one second to run. This test is only available for the i960HA SCP.

```
=>march-d 0x500000
Data BUS OK at location 0x00500000
```

3.1.2.16 Address Bus Integrity Test

This test checks the integrity of the address bus. It takes about one second to run. This test is only available for the i960HA SCP.

```
=>march-a 0x500000
Address BUS OK for address 0x00500000
```

CHAPTER 4 Loopback Modes

This chapter contains information about network module loopback modes, which are useful when checking for network connectivity. Loopback modes are available in AMI at the **configuration port** level. The port level is broken down by interface type, such as **configuration port ds1 loopback**. Please see the *ATM Management Interface (AMI) Manual* for information about logging in to AMI.

NOTE

Loopbacks cannot be established on ports that are in-service (on-line).

Network modules used in the *ASX*-4000 and *ESX*-3000 are referred to as port cards.

4.1 Overview

When a port is down, all signalling and communication is disabled. This allows you to perform loopbacks for the particular port. The **configuration port admin** AMI command lets you change the state of a port. Log in to AMI and enter the following parameters:

configuration port admin *<port>* (**up | down**)

The *<port>* variable indicates the port that is to be modified and the (**up | down**) variable indicates whether the specified port is on-line (up) or off-line (down).

All ports are capable of loopback modes of varying types, depending on the interface. Check the options available for each interface in AMI to be sure the loopback test you wish to perform is supported by the hardware.

NOTE

Loopback tests require equipment capable of sending, receiving and analyzing a data stream. Testing is done link by link (no switching of the data stream) between any two points. If any switching is required between the source and destination, the VPI/VCI of the outgoing cells must be such that it will return to the source.

4.2 Configuring SONET Loopback

To facilitate testing of the SONET ports and depending on the type of network module or port card, there are four different loopback configurations available: `line`, `diagnostic`, `path`, and `both`. When a SONET port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a SONET port, log in to AMI and enter the following parameters:

configuration port sonet loopback *<port>* (**line**|**diag**|**path**|**both**|**none**)

The *<port>* variable indicates the SONET port that is to be modified and the (**line |diag |path | both | none**) variable indicates the type of loopback to be used on the specified port. The default loopback setting is `none` which means that no loopback takes place on that port. If there are no SONET ports on the switch, then this option is not valid.

After entering the loopback command through AMI, the SCP configures the port hardware for the appropriate loopback and enters the information into the CDB so that the change is put into effect every time the switch control software starts on that particular SCP.

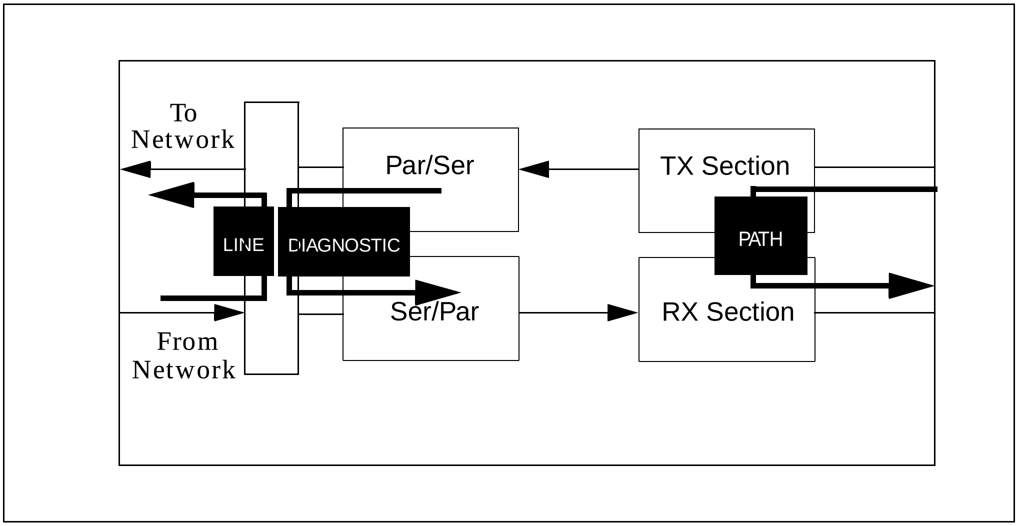

Figure 4.1 - SONET Single Port Loopback Diagram

4.2.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the fiber is retransmitted back out to the fiber. In line loopback, the port acts as if it were an optical repeater. Cells generated by the SCP to this port are not sent over the fiber. This option is valid for all SONET network modules.

NOTE

This option is not supported for Series 1 OC-48c port cards on an *ASX*-4000. To perform a line loopback, the both loopback should be used.

4.2.2 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The SONET stream being transmitted by the SCP to a port is looped back to the SCP. The stream is still transmitted over the fiber, but the incoming stream is ignored. This option is valid for all SONET network modules, except for Series C OC-12 network modules.

4.2.3 Path Loopback

Path loopback is another form of diagnostic loopback in which the path block transmitter is connected to the path block receiver. This option is valid ONLY for Series C OC-12 network modules.

4.2.4 Both Loopback

Both loopback lets you perform both diagnostic and line loopback on a particular port.

NOTE

This loopback is only applicable to the Series 1 OC-48c/STM-16c port card in an *ASX*-4000. If this loopback is attempted on a network module or port card that is not an OC-48c/STM-16c, an error message displays indicating that this particular loopback is not supported for the network module or port card type.

4.3 Configuring DS3 Loopback

To facilitate testing of the DS3 ports, there are four different loopback configurations available: `cell`, `payload`, `diagnostic`, and `line`. When a DS3 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a DS3 port, log in to AMI and enter the following parameters:

conf port ds3 loopback *<port>* (**cell | payload | diag | line| none**)

The *<port>* variable indicates the DS3 port that is to be modified and the `(cell|payload|diag|line|none)` variable indicates the type of loopback to be used on the specified port. The default loopback setting is `none`, which means that no loopback takes place on that port. If there are no DS3 ports on the switch, then this option is disabled.

After entering the loopback command through AMI, the SCP configures the port hardware for the appropriate loopback and enters the information into the CDB so that the change is put into effect every time the switch control software starts on that particular SCP.

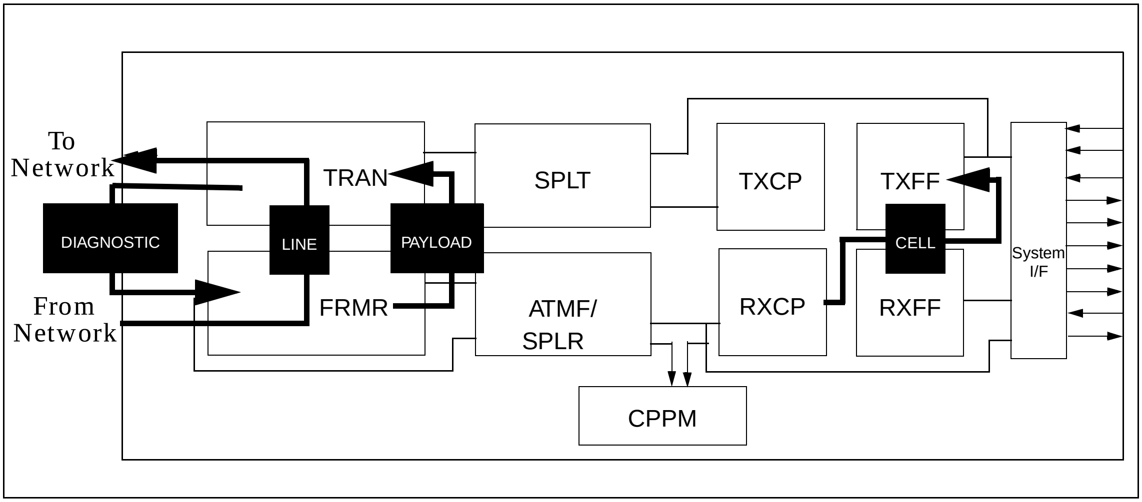

Figure 4.2 - DS3 Single Port Loopback Diagram

4.3.1 Cell Loopback

When enabled, the DS3 stream is received from the network, unframed into ATM cells, reframed, and then transmitted back to the network.

4.3.2 Payload Loopback

When enabled, the DS3 stream is received from the network, has the DS3 overhead bits re-inserted, and is retransmitted to the network.

4.3.3 Diagnostic Loopback

This connects the transmitter to the receiver. The DS3 stream transmitted by the switch to a port is looped back to the switch. The DS3 stream is still transmitted to the network, but the incoming DS3 stream is ignored.

4.3.4 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the switch to this port are not sent over the line.

4.4 Configuring DS1 Loopback

To facilitate testing of the DS1 ports, there are three different loopback configurations available: `line`, `payload`, and `diagnostic`. When a DS1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a DS1 port, log in to AMI and enter the following parameters:

configuration port ds1 loopback *<port>* (**line | payload | diag | none)**

The *<port>* variable indicates the DS1 port that is to be modified and the `(line|payload|diag|none)` variable indicates the type of loopback to be used on the specified port. The default loopback setting is `none`, which means that no loopback takes place on that port. If there are no DS1 ports on the switch, then this option is disabled.

After the loopback state is modified on a DS1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file so that the change is put into effect every time the switch control software starts on that particular SCP.

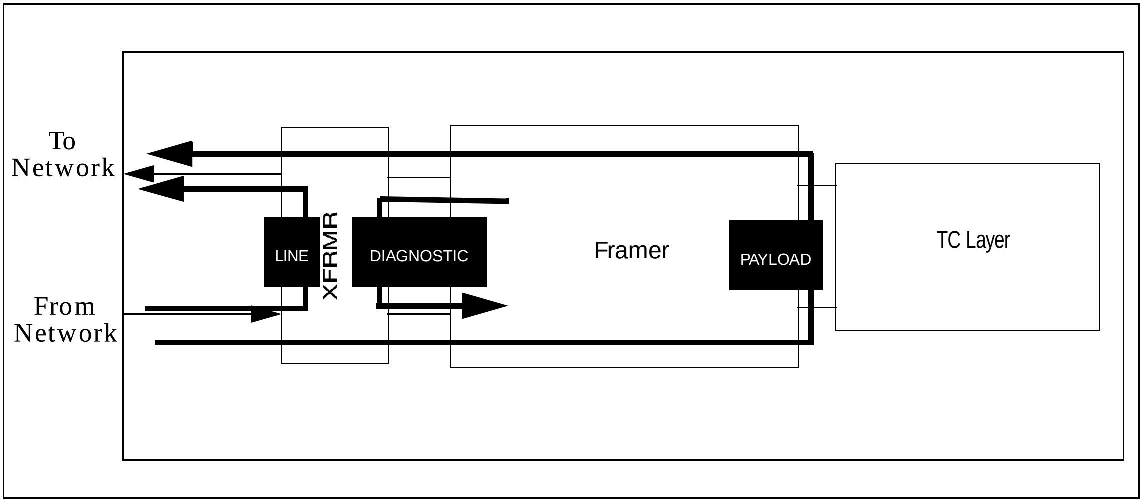

Figure 4.3 - DS1 Single Port Loopback Diagram

4.4.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the switch to this port are not sent over the line.

4.4.2 Payload Loopback

When enabled, the DS1 stream received from the network has the DS1 overhead bits re-inserted and the stream is retransmitted to the network.

4.4.3 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The DS1 stream transmitted by the switch to a port is looped back to the switch. The DS1 stream is still transmitted to the network, but the incoming DS1 stream is ignored.

4.5 Configuring CESDS1 Loopback

To facilitate testing of the CESDS1 ports, line loopback is available. When a CESDS1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a CESDS1 port, log in to AMI and enter the following parameters:

configuration port cesds1 loopback *<port>* (**line | none)**

The *<port>* variable indicates the CESDS1 port that is to be modified and the (line|none) variable indicates the type of loopback to be used on the specified port. The default loopback setting is none, which means that no loopback takes place on that port. If there are no CESDS1 ports on the switch, then this option is disabled.

After the loopback state is modified on a CESDS1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file so that the change is put into effect every time the switch control software starts on that particular SCP.

4.5.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the switch to this port are not sent over the line.

4.6 Configuring IWFDS1 Loopback

To facilitate testing of the Frame Relay/FUNI interworking function (IWF) DS1 ports, line loopback and other loopback are available. When an IWFDS1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on an IWFDS1 port, long in to AMI and enter the following parameters:

configuration port iwf ds1 loopback *<port>* **(line | diag | none)**

The *<port>* variable indicates the IWFDS1 port that is to be modified and the `(line|diag|none)` variable indicates the type of loopback to be used on the specified port. The default loopback setting is `none`, which means that no loopback takes place on that port. If there are no IWFDS1 ports on the switch, then this option is disabled.

After the loopback state is modified on an IWFDS1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file so that the change is put into effect every time the switch control software starts on that particular SCP.

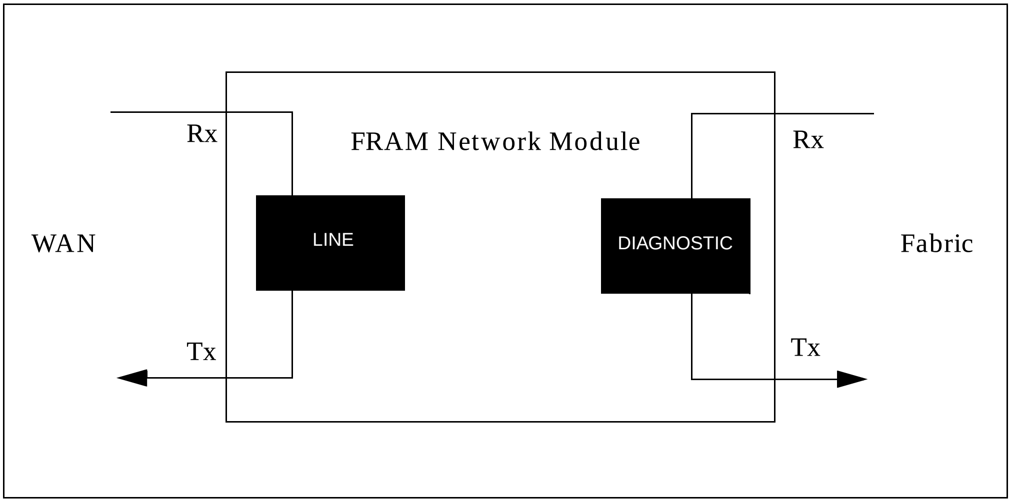

Figure 4.4 - IWFDS1 Loopback Diagram

4.6.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the switch to this port are not sent over the line.

In remote line loopback, the received signal will be transmitted without any modification of the information. Received frames will be disabled from reaching the switch fabric.

In local loopback mode, transmitted cells from the fabric will be returned to the switch fabric. The loopback point will be chosen to exercise as much of the network module circuitry as possible.

The internal loopback ensures error detection circuits are operating properly.

4.6.2 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The DS1 stream transmitted by the switch to a port is looped back to the switch. The DS1 stream is still transmitted to the network, but the incoming DS1 stream is ignored.

4.7 Configuring E3 Loopback

To facilitate testing of the E3 ports, there are four different loopback configurations available: `cell`, `payload`, `diagnostic`, and `line`. When an E3 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on an E3 port, log in to AMI and enter the following parameters:

conf port e3 loopback *<port>* (**cell** | **payload** | **diag** | **line**| **none**)

The *<port>* variable indicates the E3 port that is to be modified and the `(cell|payload|diag|line|none)` variable indicates the type of loopback on the port. The default loopback setting is `none` which means that no loopback takes place on that port. If there are no E3 ports on the switch fabric, then this option is disabled.

After entering the loopback command through AMI, the SCP configures the port hardware for the appropriate loopback and enters the information into the CDB so that the change is put into effect every time the switch control software starts on that particular SCP.

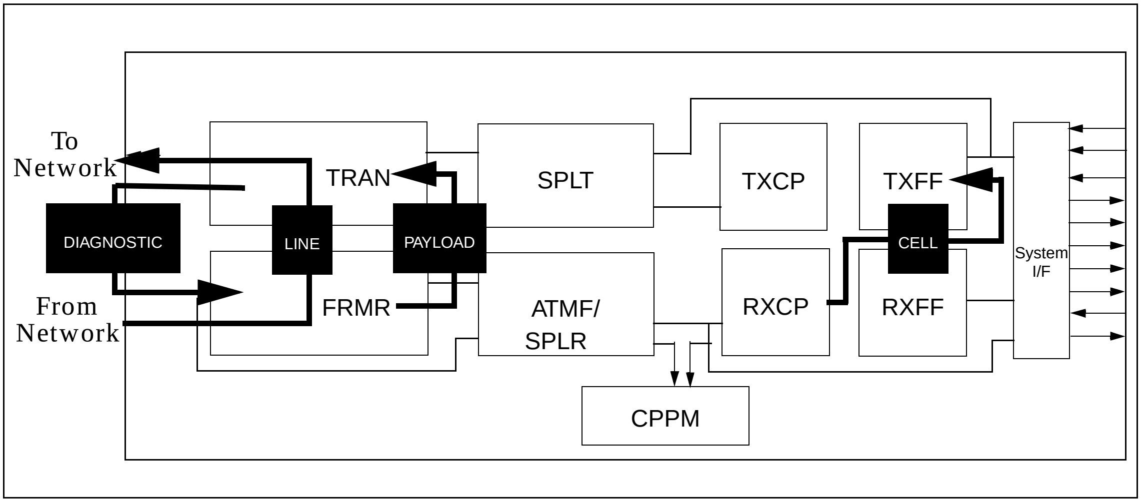

Figure 4.5 - E3 Single Port Loopback Diagram

4.7.1 Cell Loopback

When enabled, the E3 stream received from the network is unframed into ATM cells. The cells are then reframed and transmitted back to the network.

4.7.2 Payload Loopback

When enabled, the E3 stream received from the network has the E3 overhead bits re-inserted and is retransmitted to the network.

4.7.3 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The E3 stream transmitted by the SCP to a port are looped back to the SCP. The E3 stream is still transmitted to the network, but the incoming E3 stream is ignored.

4.7.4 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the SCP to this port are not sent over the line.

4.8 Configuring E1 Loopback

To facilitate testing of the E1 ports, there are three different loopback configurations available: `line`, `payload`, and `diagnostic`. When an E1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on an E1 port, log in to AMI. Enter the following parameters:

configuration port e1 loopback *<port>* (**line** | **payload** | **diag** | **none**)

The *<port>* variable indicates the E1 port that is to be modified and the `(line|payload|diag|none)` variable indicates the type of loopback on the port. The default loopback setting is `none` which means that no loopback takes place on that port. If there are no E1 ports on the switch fabric, then this option is disabled.

After the loopback mode is modified on an E1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file on the SCP so that the change is put into effect each time the switch control software starts on that particular SCP.

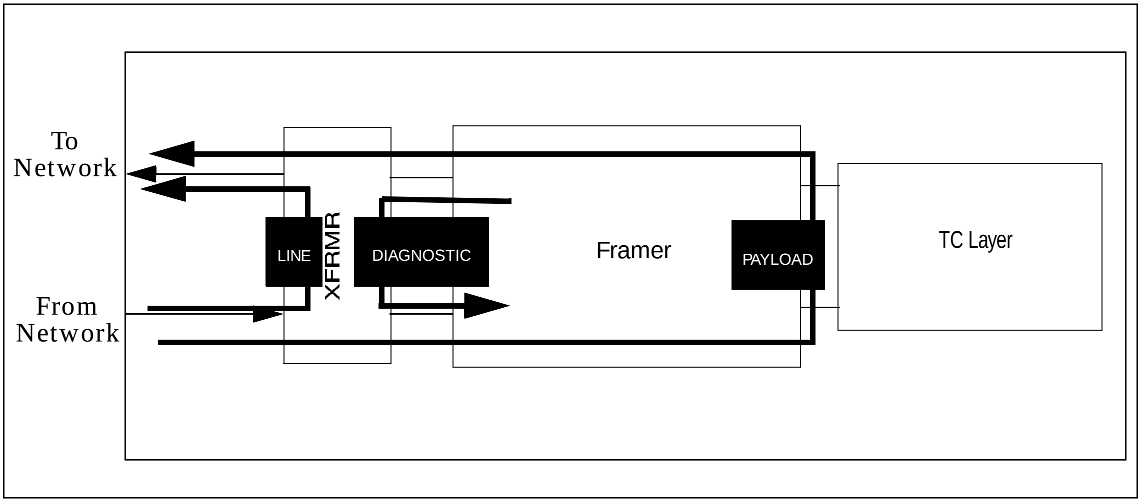

Figure 4.6 - E1 Single Port Loopback Diagram

4.8.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the SCP to this port are not sent over the line.

4.8.2 Payload Loopback

When enabled, the E1 stream received from the network has the E1 overhead bits re-inserted and is retransmitted to the network.

4.8.3 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The E1 stream transmitted by the SCP to a port is looped back to the SCP. The E1 stream is still transmitted to the network, but the incoming E1 stream is ignored.

4.9 Configuring CESE1 Loopback

To facilitate testing of the CESE1 ports, line loopback is available. When a CESE1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a CESE1 port, log in to AMI. Enter the following parameters:

configuration port cese1 loopback *<port>* (**line | none**)

The *<port>* variable indicates the CESE1 port that is to be modified and the `(line|none)` variable indicates the type of loopback on the port. The default loopback setting is `none` which means that no loopback takes place on that port. If there are no CESE1 ports on the switch fabric, then this option is disabled.

After the loopback mode is modified on a CESE1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file on the SCP so that the change is put into effect each time the switch control software starts on that particular SCP.

4.9.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the SCP to this port are not sent over the line.

4.10 Configuring IWFE1 Loopback

To facilitate testing of the Frame Relay / FUNI interworking function (IWF) E1 ports, line loopback and other loopback are available. When an IWFE1 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on an IWFE1 port, log in to AMI. Enter the following parameters:

configuration port iwf e1 loopback *<port>* (**line** | **diag** | **none**)

The *<port>* variable indicates the IWFE1 port that is to be modified and the (line|diag|none) variable indicates the type of loopback on the port. The default loopback setting is none which means that no loopback takes place on that port. If there are no IWFE1 ports on the switch fabric, then this option is disabled.

After the loopback mode is modified on a IWFE1 port, the SCP immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the CDB file on the SCP so that the change is put into effect each time the switch control software starts on that particular SCP.

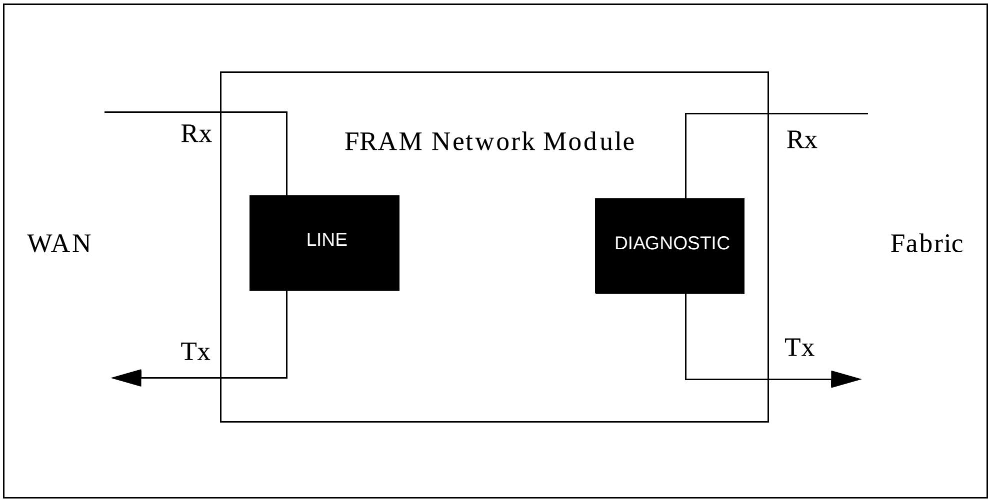

Figure 4.7 - IWFE1 Loopback Diagram

4.10.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the SCP to this port are not sent over the line.

4.10.2 Diagnostic Loopback

Diagnostic loopback results in an internal local loopback within the network module which allows traffic received off the internal fabric to be looped back onto the fabric.

4.11 Configuring J2 Loopback

To facilitate testing of the J2 ports, there are two different loopback configurations available: `line` and `diagnostic`. When a J2 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a J2 port, log in to AMI and enter the following parameters:

`configuration port j2 loopback` *`<port>`* `(`**`line`** `|` **`diag`** `|` **`none`**`)`

The *`<port>`* variable indicates the J2 port that is to be modified and the `(line|diag|none)` variable indicates the different types of loopback. The default setting is `none` which means that no loopback takes place on that port. If there are no J2 ports on the switch, this option is disabled.

After entering the loopback command through AMI, the SCP configures the port hardware for the appropriate loopback and enters the information into the CDB so that the change is put into effect every time the switch control software starts on that particular SCP.

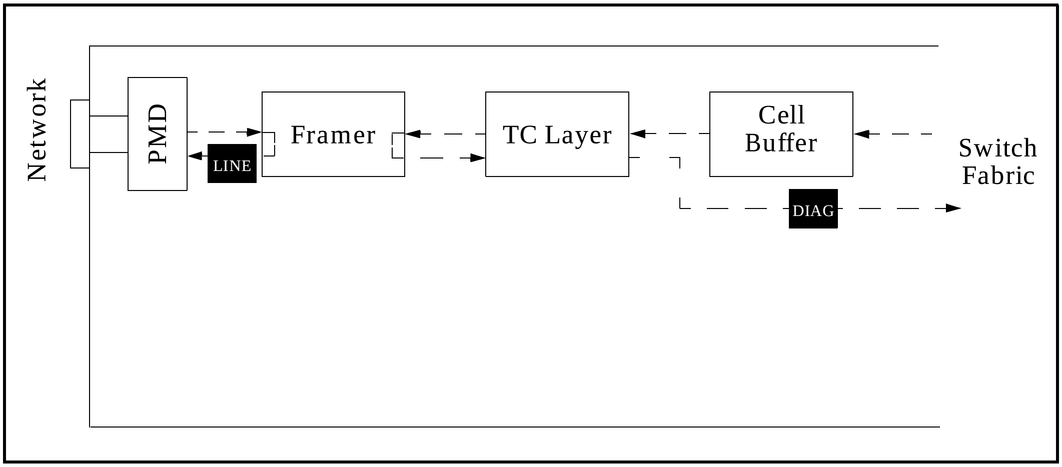

Figure 4.8 - J2 Single Port Loopback Diagram

4.11.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the coaxial cable is retransmitted back out to the line. Cells generated by the SCP to this port are not sent over the line.

4.11.2 Diagnostic Loopback

Diagnostic loopback connects the transmitter to the receiver. The J2 stream being transmitted by the SCP to a port is looped back to the SCP. The stream is still transmitted over the line, but the incoming stream is ignored.

4.12 Configuring TP25 Loopback

To facilitate testing of the TP25 ports, a line loopback configuration is available. When a TP25 port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a TP25 port, log in to AMI and enter the following parameters:

configuration port tp25 loopback *<port>* (**line | none**)

The *<port>* variable indicates the TP25 port that is to be modified and the `(line|none)` variable indicates the type of loopback on the port. The default loopback setting is `none` which means that no loopback takes place on that port. If there are no TP25 ports on the switch, then this option is disabled.

After entering the loopback command through AMI, the SCP configures the port hardware for the appropriate loopback and enters the information into the CDB so that the change is put into effect every time the switch control software starts on that particular SCP.

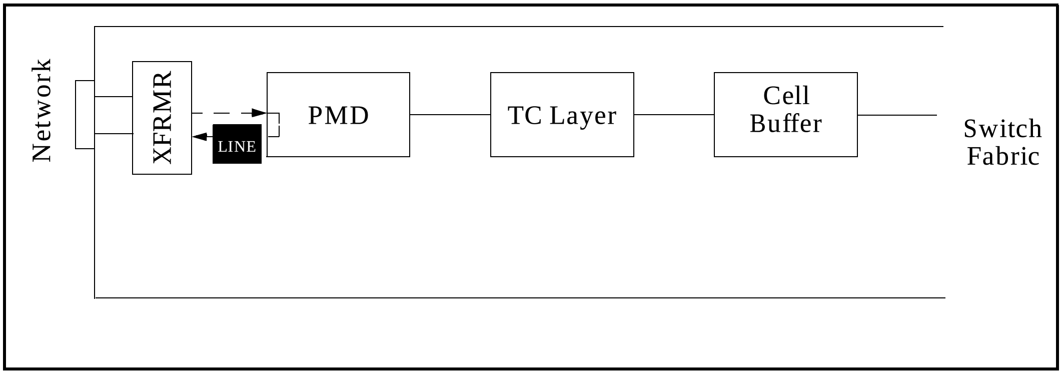

Figure 4.9 - TP25 Single Port Loopback Diagram

4.12.1 Line Loopback

Line loopback connects the receiver to the transmitter. The data stream received from the line is retransmitted back out to the line. Cells generated by the switch to this port are not sent over the line.

4.13 Configuring TAXI Loopback

To facilitate testing of the TAXI ports, a diagnostic loopback configuration is available. When a TAXI port is in loopback mode, it no longer passes normal traffic.

To change the loopback type on a TAXI port, log in to the ATM Management Interface (AMI) and enter the following parameters:

configuration port taxi loopback *<port>* (**diag | none**)

The *<port>* variable indicates the TAXI port that is to be modified and the (diag|none) variable indicates the type of loopback to be used on the specified port. The default loopback setting is none, which means that no loopback takes place on that port. If there are no TAXI ports on the switch fabric, then this option is disabled.

After the loopback state is modified on a TAXI port, the switch control processor (SCP) immediately puts that change into effect on that switch fabric. At the same time, that information is entered into the configuration database file on the SCP so that the change is put into effect every time the switch control software starts on that particular SCP.

4.13.1 Diagnostic Loopback

The diagnostic loopback connects the transmitter to the receiver. The TAXI stream transmitted by the fiber to a port is looped back to the fiber. The stream is still transmitter over the fiber, but the incoming stream is ignored.

CHAPTER 5 Debugging PNNI

This chapter describes methods for troubleshooting the most common configuration problems in a network based on ATM Forum PNNI (hereafter referred to as PNNI) routing. This chapter assumes that you are already familiar with the configuration of a PNNI network. If you are not familiar with PNNI, please read Chapter 6, *ATM Forum PNNI*, in the *ATM Switch Network Configuration Manual*.

Before contacting FORE Systems' Technical Assistance Center, perform the methods outlined in this chapter to correct or at least pinpoint the problem. If you need to contact the Technical Assistance Center, please have the results of these steps ready, as well as a sketch of your network, when reporting your problem.

The following topics are discussed in this chapter:

5.1 Performing Basic PNNI Debugging

There are several things to check while debugging your PNNI network:

- Default Routing Protocol of the Default Domain
- Operational Status of the PNNI Node
- PNNI Links
- Hello State of the PNNI Links
- Peer State

These topics are all described in detail in the following subsections.

5.1.1 Default Routing Protocol of the Default Domain

Verify that you have configured PNNI on your switch by looking at the default routing protocol for your switch.

1. Use the **`conf atmr domain show`** command and look at the `Defproto` field. This field shows one of the following:
   - `ftpnni` - This switch is running FT-PNNI.
   - `pnni` - This switch is running PNNI. This switch has up to four PNNI nodes. If it has multiple PNNI nodes, it is a split switch (it connects up to four PNNI peer groups).
   - `gateway` - This switch has one FT-PNNI node and one PNNI node.

   Your switch should either say `pnni` or `gateway`. If it does, move on to Section 5.1.2 in this chapter. If it says `ftpnni`, perform step 2.
2. If your switch says `ftpnni`, change the default routing protocol using the **`conf atmr domain modify`** command.

   a. If this switch is within a PNNI peer group, change it to `pnni`.

   b. If this switch is in a PNNI peer group, but is connecting the PNNI peer group to a FT-PNNI peer group, change it to `gateway`.

5.1.2 Operational Status of a PNNI Node

If the default routing protocol is configured properly, then check the operational status of each PNNI node to see if the node is active (up).

1. Use **conf atmr pnni node show** to display all PNNI nodes that are configured on the switch. (There must be at least one PNNI node configured on the switch.)
2. On each node, ensure that both the node's operational status and administrative status are up, in the OperStat and AdminStat fields, respectively. If the administrative status is down, configure it up using **conf atmr pnni node admin up**. (Doing this enables the operational status as well.)
3. Check for PNNI Topology State Elements (PTSEs) in each node's topology database (TDB) by using **display atmr ptse**. If a node does not have any PTSEs, or if it has only one or two (these must be its nodal information and internal reachability PTSE), then it does not have any PNNI links attached to it.

To check the PNNI links, use the steps outlined in Section 5.1.3.

5.1.3 PNNI Links

Ensure that the PNNI links have been automatically configured to type PNNI by looking at the SigProto field under **conf atmr show**. If they have not, you can change the type manually as follows:

1. Delete the signalling channel using **conf sig delete**.
2. Re-create it using **conf sig new** with the **-version** as **pnni10** and the **-type** as **privateNNI**.
3. Run **conf sig show** and look at the Interface field to ensure that the type is now PNNI.
4. Run **conf atmr show** and verify that the SigProto field reflects PNNI for each link. Also, verify that the Node field is set to a valid index for a PNNI node.

If the links are configured properly, use the method in Section 5.1.4 to check the Hello state of each link.

5.1.4 Hello State of the PNNI Links

Once the links are configured as PNNI, the Hello Protocol begins on the links. This protocol discovers and verifies the identity of neighbor nodes and determines the status of the logical links to those nodes.

Verify the state of the Hello protocol as follows:

1. Look at the `HelloState` field under **`display atmr pnni link`**.

```
myswitch::> display atmr pnni link
 Node Port VPI PortId     HelloState    Version        LinkType
 1    1C3  0   0x10000012 commonOutside version1point0 outsideLinkAndUplink
      RmtNodeId                                           RmtPortId
      80:160:47.000580ffe1000000f21b0050.ff1a2d0f0001.00  0x10000008
      UpNodeId                                            DerAggrTk
      72:80:47.000580ffe1000000f2000000.ff1a2d0f0002.00   0
      UpnodeAtmAddress                            CommonPGID
     47.000580ffe1000000f21b0050.ff1a2d0f0002.00 72:47.000580ffe100000000000000
```

2. The `Node` field indicates the index number of the PNNI node to which this PNNI link has been attached. If the node on the far side of this link belongs to the same peer group as the local node, and everything is working properly, the Hello protocol reaches a final state of `twoWayInside`.
3. In *ForeThought* 6.x, outside links (links between nodes in different peer groups) are supported. The `HelloState` finally becomes `commonOutside`. In *ForeThought* 5.x outside links (links between nodes in different peer groups) are not supported. In this case, the protocol remains in its initial `HelloState` of `Attempt`. If the link was not meant to be an outside link, and if the protocol is still in `Attempt` state, then examine the Hello messages as described in Section 5.1.4.1.

5.1.4.1 Hello Messages

Examine the Hello Messages as follows:

1. Check the number of Hello Messages received and transmitted by looking at the `RcvHellos` and `XmtHellos` fields, respectively, under **`stat atmr pnni link`**.
2. If the number of Received Messages received for this link is zero, debug the remote switch instead of the switch you are currently debugging. If the number is greater than zero, check the peer group IDs as described in Section 5.1.4.2.

5.1.4.2 Peer Group IDs

The peer group ID may be improperly configured for either of the two nodes connected by this link. Check the peer group ID as follows:

1. Run **`conf atmr pnni node show`** on both the local and the remote switch to ensure that the `PeerGroupID` field lists the appropriate peer group ID on each switch.
2. Turn on PNNI debugging using **`debug trace atmr pnni basic on`** and **`debug atmr pnni enhanced on`**. If the peer group IDs are not matched, the switch prints the following message repeatedly to the console:

```
tAsx[X]:    INFO: nodix= 2, pnni_hello_rx_hello: outside case
```

   If the peer group IDs are configured properly, examine the peer state as shown in Section 5.1.5.

5.1.5 Peer State

If the link successfully reaches a `twoWayInside` Hello state, the PNNI nodes begin a database exchange. During this process, the two nodes update each other with the latest copies of all PTSEs known between them and they synchronize their two TDBs. Once this process is complete, the two nodes set each other's peer state to `full`.

To verify the peer state, do the following:

1. Use **`display atmr pnni peer`** and look at the `PeerRemoteNodeId` field. If the remote node is not listed as one of the peers of the local node, then go back and make sure that the Hello State (under **`display atmr pnni link`**) is still in `twoWayInside`.
2. If the `State` field shows anything other than `full`, then the nodes may still be in the process of exchanging their databases, but this state should not persist for long. If it does, turn PNNI debugging on (under **`debug trace atmr pnni>`**) and watch for warning or error messages.

5.2 Debugging Multiple Node Switches

Using *ForeThought* 6.x, up to four PNNI nodes can be operational in a switch simultaneously. Using *ForeThought* 5.x, up to two PNNI nodes can be operational in a switch simultaneously. If there are multiple PNNI nodes in a switch, it is a split switch. See Section 5.2.1 for additional debugging techniques for split switches. If each of the PNNI nodes on a split switch reside in different routing domains, see Section 5.2.2.

If one node is a FT-PNNI node and the other node is a PNNI node, it is a gateway switch. See Section 5.2.3 for additional debugging techniques for gateway switches.

5.2.1 Debugging Split Switches

A split switch has two (or more) PNNI nodes and connects two (or more) adjacent PNNI peer groups. Using several split switches, many peer groups can be connected in a single network. Each peer group in a network is called an *area* in the FORE hierarchy. Each area must be given a unique area ID and a level in the FORE hierarchy.

In a split switch, the links that belong to each of the two peer groups must be attached to the node that is configured with the peer group ID of that peer group. All of the PNNI interfaces attach to node 1 by default.

To move the links in a split switch, do the following:

1. To attach a link to a specific node, use **`conf atmr pnni interface modify`** *`<port>`* *`<vpi>`* **`-nodeix`** *`<nodeix>`*. This changes the node index associated with the interface.
2. After attaching the interfaces to the correct node, look at the `SigProto` and the `Node` fields, respectively, under **`conf atmr show`** to ensure that each PNNI link has the correct type (PNNI) and the correct node index associated with it.
3. Use the method described in Section 5.1.4 to debug the individual PNNI links.

5.2.2 Debugging Split Switches in Multiple Routing Domains

Split switches can also be configured so that the two (or more) nodes reside in two (or more) different routing domains. In this case, no dynamic routing occurs between these domains. Inter-domain static routes must be configured manually using the **conf atmr pnni address** menu to enable routing between these domains. A new domain can be created using **conf atmr domain new**. When using multiple domains, by default, all signalling interfaces are created in domain 1, which is the default domain.

To debug a split switch that resides in different domains, check the following:

1. If there are any signalling interfaces (both UNI and NNI) that do not belong to the default domain, delete and re-create them in the correct domain using the **conf sig** menu.
2. After you have moved the interfaces, use **conf atmr show** to ensure all of the interfaces have the correct domain ID, correct node index, and correct type by looking at the `Domain`, `Node`, and `SigProto` fields, respectively.

5.2.3 Debugging Gateway Switches

A gateway switch has one FT-PNNI node and one PNNI node. It connects a FT-PNNI peer group to a PNNI peer group. To debug a gateway switch, check the following:

1. Use **conf atmr show** and look at the `SigProto` field to ensure that all of the NNI links have either auto-configured or have been hard-coded to the correct type (either FT-PNNI or PNNI).
2. Verify that the `Node` field is set to the node index of the correct node. The FT-PNNI interface displays the node index as `ftpnni (65535)`.
3. Use the method described in Section 5.1.4 to debug the individual PNNI links.

5.3 Reading the Prefix Table

The prefix table is the data structure that stores all of the reachable addresses in a given routing domain. There is one prefix table for each domain. Use **`dis atmr ptab`** to view the prefix table.

In a simple network that only contains a single PNNI peer group, there are three types of entries in the prefix table:

- locally reachable addresses (such as ILMI-registered addresses and static routes)
- summary reachable addresses derived from the above entries advertised by the local node(s)
- summary reachable addresses advertised by other nodes in the peer group

By default, every PNNI node in the network advertises one 13-byte prefix as an internal reachable address. This prefix is the same as the one displayed in the `Prefix` field under **`conf atmr domain show`**. By default, all ILMI registered addresses and addresses of the control port (LEC, CLIP address, etc.) share this 13-byte prefix. Therefore, this prefix effectively summarizes all reachable addresses at this node.

The following is an example of a prefix table:

```
myswitch::> display atmr ptab
Domain Prefix                                      Len  Flags      TimeStamp
 1      47.000580ffe1000000f21b1a29.000000000000   104  0x0        34c7a58a
        OwnerLevel OwnerProtocol  OwnerPathFlags
        5          pnni           0x0
        PTEs:
        ProtoId ProtoHndl Protocol PathFlags Level Area  Scope SrcArea  Type
         1     0xe38dc     pnni      0x0      5     5    0     0         1
Domain Prefix                                      Len  Flags      TimeStamp
 1      47.000580ffe1000000f21c3d7d.000000000000   104  0x2        34c61ad7
        OwnerLevel OwnerProtocol  OwnerPathFlags
        0          bogus          0x0
        PTEs:
        ProtoId ProtoHndl Protocol PathFlags Level Area  Scope SrcArea  Type
        1       0xeb094    pnni      0x1      5     5     0    0        1
Domain Prefix                                      Len  Flags      TimeStamp
 1      47.000580ffe1000000f21c3d7d.0020481c3d7d   152  0x0        34c61ad7
        OwnerLevel OwnerProtocol  OwnerPathFlags
        255        ilmi           0x0
        PTEs:
        ProtoId ProtoHndl Protocol PathFlags Level Area  Scope SrcArea  Type
        0       0xe28b8   ilmi       0x0      255   0     0     0        1
```

The prefix table is organized as follows:

- Each prefix that is reachable in the domain is listed. Under each prefix, is a list of entries called Prefix Table Entries (PTEs). For each prefix that is known to be reachable, there may be one or more protocols that are advertising this reachability information. Each protocol registers a PTE under that particular prefix.

  For example, the third prefix in the example table has a single PTE listed under it, which has been registered by ILMI. In this case, the address belongs to the control port of the switch and this address is registered as an ILMI address.

- Entries that are derived from other entries have the least significant bit of the `PathFlags` field set. For example, the second prefix in the example table has a single PTE registered by PNNI. This PTE is a summarization of the third prefix and has been registered by PNNI. Since this PNNI entry is a derived entry, the least significant bit of the `PathFlags` field is set.
- The first prefix in the example table has one PTE registered under it. This PTE has been registered by PNNI as a result of a reachability advertisement received from a remote PNNI node residing on another switch.

Use the prefix table to find out if a given address is reachable in the PNNI network. For example, suppose a LANE client is trying to route to the LAN Emulation Client Server (LECS) well-known address (WKA). If the client is unable to connect to the LECS, enable (turn on) the following debug commands: **debug trace sig q93b q93b**, **debug trace sig q93b call_fwd** and **debug trace atmr pnni>**. This may show one of the following:

- The LECS WKA is not registered in this PNNI network. If there is no prefix table entry corresponding to this address, this is the problem. Go to the switch on which the LECS WKA address is configured and make sure that the address is, indeed, registered.
- The address is registered, but PNNI path computation does not work. In this case, the WKA address has been registered correctly and there is an entry in the prefix table, but PNNI cannot compute a path to this destination. Use the method described in Section 5.4 to debug the PNNI path computation.
- The address is registered and PNNI path computation works, but the call does not go through for some other reason. In this case, PNNI successfully computes a path and the SETUP message gets forwarded, but a RELEASE message comes back and clears the call.

  This may be caused by problems such as VCI depletion at a downstream switch. In this case, use the `cause` value in the RELEASE message as an indication to what the problem is. You may have to trace the call through a series of switches before you find out the exact cause at the switch where the RELEASE is originated.

5.4 Reading the PNNI Path Computation Profile Table

ForeThought 5.x and *ForeThought* 6.x implement several value-added features beyond what is required by the ATM Forum PNNI Specification. One of these important features is path computation profiles.

The PNNI path computation (PC) module maintains profiles of call SETUPs which are given in terms of their QoS values and traffic parameters. These profiles can be either cached profiles or user-specified profiles. Cached profiles are profiles of call SETUPs previously seen by this switch and dynamically created as a result. User-specified profiles are those that are manually configured by the user through AMI.

To do fast calculations of Designated Transit Lists (DTLs) when a call SETUP arrives, the PNNI PC module pre-computes the shortest path trees for each known PC profile. If the call SETUP matches one of the known profiles, then the pre-computed tree for that profile is used to construct the DTL. If the call SETUP does not match any of the profiles, then a new profile is created and the shortest path is computed on demand.

The PNNI PC profile table can be displayed using **conf atmr pnni profile show**. The following is an example of a PC profile table:

```
myswitch::configuration atmroute pnni profile> show
 Node Profile Service MinFwdCR MinRevCR FwdClpType  RevClpType FwdCLR  RevCLR
 1    2       cbr     1000     1000     clpEqual0    clpEqual0  8      8
 State     ProfileType LoadBal VPOnly OptCTD OptCDV OptAdmWt NumAvd NumPref
 computed  mgmtEntry   false   false  true    true   aw      N/A      N/A

 Node Profile Service MinFwdCR MinRevCR FwdClpType   RevClpType   FwdCLR  RevCLR
 1    10      ubr     N/A      N/A      clpEqual0    clpEqual0    N/A     N/A
 State    ProfileType LoadBal VPOnly OptCTD OptCDV OptAdmWt NumAvd NumPref
 computed  cacheEntry   true  false  false  false   aw     0    0
```

There are two PC profiles in this table. The first one is a user-specified profile (the `ProfileType` field shows `mgmtEntry`), and the other is a cached profile (the `ProfileType` field shows `cacheEntry`).

Each profile could result in the computation of up to three shortest path trees (SPTs). Each one of the three trees minimizes one of the three additive metrics: Cell Transit Delay (CTD), Cell Delay Variation (CDV), and Administrative Weight. The administrative weight tree is always computed for all profiles. The CTD and CDV trees are optional and are specified when a profile is created.

The state of the profile can be one of the following:

- inactive - The SPTs have not been calculated for this tree.
- computing - The SPTs are in the process of being computed.
- computed - This profile is valid and the SPTs are computed.

Profile entries for multicast connections look different from those for unicast connections. Each multicast connection results in a new profile which defines all of the links that make up the multicast connection as preferred links.

Every time a new link is added to this multicast connection, a new profile is created with the new link included in the set of preferred links. The preferred links of a profile can be displayed using the **advanced** option for **conf atmr pnni profile show**. The following is an example of a multicast profile:

```
myswitch::configuration atmroute pnni profile> show 1 11 advanced
 Node Profile Service MinFwdCR MinRevCR FwdClpType   RevClpType   FwdCLR  RevCLR
 1    11       ubr     N/A      N/A      clpEqual0    clpEqual0    N/A      N/A
 State     ProfileType  LoadBal VPOnly OptCTD OptCDV OptAdmWt NumAvd NumPref
 computed  cacheEntry    true   false  false  false    aw      0      1
      No avoided link information for this profile
      List of preferred links for multicast:
 Index PreferNodeId                                      PreferPortId
 1     80:160:47.000580ffe1000000f21b1a29.ff1b1a290001.00 0x10000001
 RemoteNodeId                                        PreferLinkType
 80:160:47.000580ffe1000000f21c3d7d.ff1c3d7d0001.00  normalLink
```

The profile in this example belongs to a multicast connection with one preferred link. Preferred links are used by multicast connection profiles for two reasons. First, they ensure that when a new leaf joins the multicast connection, only a minimal number of new links are added to the tree by taking the existing tree into consideration. Second, they ensure that the addition of new links do not introduce loops in the tree.

Debugging PNNI

5.5 Reading the PNNI Map and PC Map Tables

The PNNI map and the PC map can be used for debugging a PNNI network. The PNNI map is discussed in detail in Section 5.5.1 and the PC map is discussed in Section 5.5.2.

5.5.1 Reading the PNNI Map

To display the list of all PNNI links known to this switch, use **display atmr pnni map**. Each entry in this mapping table is a uni-directional link. Therefore, each physical link in this network contributes two entries to this table. The following is an example of a PNNI map:

```
myswitch::display atmroute pnni> map
Node OriginatingNodeId                                  OrigPortId Index
 1   80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  0x10000020 1
 Type           PeerGroupId                    AggrToken  RmtPortId
 horizontalLink 80:47.000580ffe1000000f2000000 0          0x10000023
 RemoteNodeId                                        VpCap PTSEId     MTag
 80:160:47.000580ffe1000000f21c3d7d.ff1c3d7d0001.00  FALSE 0x10000020 0
 Category Dir       AdmWt  MCR      ACR      CTD  CDV    CLR0 CLR0+1 CRM  VF
 cbr      outgoing  5040  5660377   5660377  0    0      8    8      0    0
 rtvbr    outgoing  5040  5660377   5660377  0    0      8    8      0    0
 nrtvbr   outgoing  5040  5660377   5660377  0    0      8    8      0    0
 ubr      outgoing  5040  5660377   5660377  0    0      8    8      0    0
 Node OriginatingNodeId                                  OrigPortId  Index
 1    80:160:47.000580ffe1000000f21c3d7d.ff1c3d7d0001.00  0x10000023   1
 Type           PeerGroupId                      AggrToken RmtPortId
 horizontalLink 80:47.000580ffe1000000f2000000   0         0x10000020
 RemoteNodeId                                        VpCap PTSEId     MTag
 80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  FALSE 0x10000023   0

 Category Dir       AdmWt  MCR      ACR      CTD  CDV    CLR0 CLR0+1 CRM  VF
  cbr     outgoing  5040  5660377   5660377  0    0      8    8      0    0
  rtvbr   outgoing  5040  5660377   5660377  0    0      8    8      0    0
  nrtvbr  outgoing  5040  5660377   5660377  0    0      8    8      0    0
  ubr     outgoing  5040  5660377   5660377  0    0      8    8      0    0
```

The map in this example was taken from a simple network of two switches connected by a single physical link. There are two PNNI nodes in this network and there are two PNNI links connecting them, one in each direction.

If PNNI path computation does not work, use this map to ensure that all the links that are supposed to exist, indeed, exist.

5.5.2 Reading the PC Map

The PNNI PC mapping table contains information pertaining to the SPTs computed for each of the known PC profiles. To display this map, use **display atmr pnni pcmap**. The following is an example of a PC map, which corresponds to the PC profile table shown in Section 5.4. This example network consists of three switches connected in a triangle using three links, with one link between each pair of switches.

```
myswitch::display atmroute pnni> pcmap
 Node Profile Tree MapNodeId
 1    2       0   80:160:47.000580ffe1000000f21b1a29.ff1b1a290001.00
     ParentNodeId                                        LocalPort
     80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  10000003
     AdmWt MCR    ACR    CTD(usec)  CDV(usec) CLR0   CLR0+1 CRM  VF
     5040  353207 352367 745        725        8      8     0    0
 Node Profile Tree MapNodeId
 1    2       0    80:160:47.000580ffe1000000f21c3d7d.ff1c3d7d0001.00
     ParentNodeId                                        LocalPort
     80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  10000023
     AdmWt MCR    ACR     CTD(usec)  CDV(usec) CLR0   CLR0+1 CRM  VF
     5040 5660377 5660377 0          0          8      8     0    0
Node Profile Tree MapNodeId
 1   10      0    80:160:47.000580ffe1000000f21b1a29.ff1b1a290001.00
     ParentNodeId                                        LocalPort
     80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  10000003
     AdmWt MCR    ACR     CTD(usec)  CDV(usec) CLR0   CLR0+1 CRM  VF
     5040  353207 352367  745        725        8      8     0    0
Node Profile Tree MapNodeId
1    10      0    80:160:47.000580ffe1000000f21c3d7d.ff1c3d7d0001.00
     ParentNodeId                                        LocalPort
     80:160:47.000580ffe1000000f21c0687.ff1c06870001.00  10000023
     AdmWt MCR     ACR     CTD(usec)  CDV(usec) CLR0   CLR0+1 CRM  VF
     5040  5660377 5660377 0          0          8      8     0    0
```

Each PNNI node computes up to three SPTs for each PC profile. The SPTs are spanning trees that are rooted at the PNNI node, which compute the SPT and contain only those links that satisfy the QoS, service category, and traffic requirements for its profile. In this example, the first two entries constitute one SPT for profile 2 (a UBR cached profile) and the last two entries constitute one SPT for profile 10 (a CBR user-defined profile).

Each entry in this example table is a link in the SPT to which it belongs. Each entry indicates a MapNodeId and the ParentNodeID (which shows the parent of this MapNodeId in the SPT). Typically, an SPT has an entry for each PNNI node in the network, except the PNNI node at which the SPT is computed (since this is the root of the tree and does not have a parent). Therefore, in a network of *n* nodes, there are *n-1* entries in each SPT. Exceptions to this rule arise only when there are one or more nodes in the network that cannot be reached from the local PNNI node without violating the QoS requirements.

APPENDIX A Hardware Addressing Schemes

This appendix outlines the hardware addressing scheme used by the enterprise Management Information Base (MIB) to reference ports on an *ASX*-200WG, *ASX*-200BX, *ASX*-1000, *ASX*-1200, *ASX*-4000, *TNX*-210, *TNX*-1100, LE 25, LE 155, and *ESX*-3000. This information is useful when interpreting debug messages and performing SNMP queries.

There are two main SNMP indexing schemes used: software port indices and hardware port indices. Software port indices are single numbers starting at 0 for the first port, incrementing 8 ports per module. For example, port A1 has a software port index of 0. Port C3 has a software port index of 18, or 8 * 2 + 2.

Hardware port indices are of the form {board}.{network module}.{port} or bnp notation. They start at 0.0.0 for the first port and increment across boards, network modules, and ports. For example, port C3 is hardware port 0.2.2.

A.1 *ASX*-200WG, ASX-200BX, *TNX*-210, LE 25, and LE 155 Port Numbering

Table A.1 summarizes the port numbering conventions and related SNMP indexing format used for an *ASX*-200WG, *ASX*-200BX, *TNX*-210, LE 25, and LE 155.

Table A.1 - *ASX*-200WG, *ASX*-200BX, *TNX*-210, LE 25, and LE 155 Port Numbering

Port Name	Software Port Number	Board-Netmod-Port Index	Port Name	Software Port Number	Board-Netmod-Port Index
Board 1 (CTL = 56) 0.7.0					
A1	0	0.0.0	C1	16	0.2.0
A2	1	0.0.1	C2	17	0.2.1
A3	2	0.0.2	C3	18	0.2.2
A4	3	0.0.3	C4	19	0.2.3
A5	4	0.0.4	C5	20	0.2.4
A6	5	0.0.5	C6	21	0.2.5
A7	6	0.0.6	C7	22	0.2.6
A8	7	0.0.7	C8	23	0.2.7
B1	8	0.1.0	D1	24	0.3.0
B2	9	0.1.1	D2	25	0.3.1
B3	10	0.1.2	D3	26	0.3.2
B4	11	0.1.3	D4	27	0.3.3
B5	12	0.1.4	D5	28	0.3.4
B6	13	0.1.5	D6	29	0.3.5
B7	14	0.1.6	D7	30	0.3.6
B8	15	0.1.7	D8	31	0.3.7

A.2 *ASX*-1000, *ASX*-1200, and *TNX*-1100 Port Numbering

Table A.2 shows the numbering conventions that are referred to in the MIBs for ports on board 1 on an *ASX*-1000, *ASX*-1200, and T*NX*-1100. Boards 2, 3, and 4 use the same numbering scheme as board 1. This fact is important when interpreting debug messages.

Table A.2 - *ASX*-1000, *ASX*-1200, and *TNX*-1100 Board 1 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Board 1 (CTL = 56)			
1a1	0	1c1	16
1a2	1	1c2	17
1a3	2	1c3	18
1a4	3	1c4	19
1a5	4	1c5	20
1a6	5	1c6	21
1a7	6	1c7	22
1a8	7	1c8	23
1b1	8	1d1	24
1b2	9	1d2	25
1b3	10	1d3	26
1b4	11	1d4	27
1b5	12	1d5	28
1b6	13	1d6	29
1b7	14	1d7	30
1b8	15	1d8	31
1e1	N/A	1e3	34
1e2	33	1e4	35

Table A.3 shows the numbering conventions that are referred to in the MIBs for ports on board 2 on an *ASX*-1000, *ASX*-1200, and *TNX*-1100.

Table A.3 - *ASX*-1000, *ASX*-1200, and *TNX*-1100 Board 2 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Board 2 (CTL = 113)			
2a1	57	2c1	73
2a2	58	2c2	74
2a3	59	2c3	75
2a4	60	2c4	76
2a5	61	2c5	77
2a6	62	2c6	78
2a7	63	2c7	79
2a8	64	2c8	80
2b1	65	2d1	81
2b2	66	2d2	82
2b3	67	2d3	83
2b4	68	2d4	84
2b5	69	2d5	85
2b6	70	2d6	86
2b7	71	2d7	87
2b8	72	2d8	88
2e1	89	2e3	91
2e2	N / A	2e4	92

Table A.4 shows the numbering conventions that are referred to in the MIBs for ports on board 3 on an *ASX*-1000, *ASX*-1200, and *TNX*-1100.

Table A.4 - *ASX*-1000, ASX-1200, and *TNX*-1100 Board 3 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Board 3 (CTL = 170)			
3a1	114	3c1	130
3a2	115	3c2	131
3a3	116	3c3	132
3a4	117	3c4	133
3a5	118	3c5	134
3a6	119	3c6	135
3a7	120	3c7	136
3a8	121	3c8	137
3b1	122	3d1	138
3b2	123	3d2	139
3b3	124	3d3	140
3b4	125	3d4	141
3b5	126	3d5	142
3b6	127	3d6	143
3b7	128	3d7	144
3b8	129	3d8	145
3e1	146	3e3	N / A
3e2	147	3e4	149

Table A.5 shows the numbering conventions that are referred to in the MIBs for ports on board 4 on an *ASX*-1000, *ASX*-1200, and *TNX*-1100.

Table A.5 - *ASX*-1000, *ASX*-1200, and *TNX*-1100 Board 4 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Board 4 (CTL = 227)			
4a1	171	4c1	187
4a2	172	4c2	188
4a3	173	4c3	189
4a4	174	4c4	190
4a5	175	4c5	191
4a6	176	4c6	192
4a7	177	4c7	193
4a8	178	4c8	194
4b1	179	4d1	195
4b2	180	4d2	196
4b3	181	4d3	197
4b4	182	4d4	198
4b5	183	4d5	199
4b6	184	4d6	200
4b7	185	4d7	201
4b8	186	4d8	202
4e1	203	4e3	205
4e2	204	4e4	N / A

A.3 ESX-3000 Port Numbering

Table A.14 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 1 on an *ESX*-3000. The backplane ports are not addressable and there is only one switch control processor port. These facts are important when interpreting debug messages.

Table A.6 - *ESX*-3000 Port Card Slot 1 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 1 Switch Control Port (CTL= 512)							
1a1	0	1b1	16	1c1	32	1d1	48
1a2	1	1b2	17	1c2	33	1d2	49
1a3	2	1b3	18	1c3	34	1d3	50
1a4	3	1b4	19	1c4	35	1d4	51
1a5	4	1b5	20	1c5	36	1d5	52
1a6	5	1b6	21	1c6	37	1d6	53
1a7	6	1b7	22	1c7	38	1d7	54
1a8	7	1b8	23	1c8	39	1d8	55
1a9	8	1b9	24	1c9	40	1d9	56
1a10	9	1b10	25	1c10	41	1d10	57
1a11	10	1b11	26	1c11	42	1d11	58
1a12	11	1b12	27	1c12	43	1d12	59
1a13	12	1b13	28	1c13	44	1d13	60
1a14	13	1b14	29	1c14	45	1d14	61
1a15	14	1b15	30	1c15	46	1d15	62
1a16	15	1b16	31	1c16	47	1d16	63

Table A.15 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 2 on an *ESX*-3000.

Table A.7 - *ESX*-3000 Port Card Slot 2 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 2 Switch Control Port (CTL = 512)							
2a1	64	2b1	80	2c1	96	2d1	112
2a2	65	2b2	81	2c2	97	2d2	113
2a3	66	2b3	82	2c3	98	2d3	114
2a4	67	2b4	83	2c4	99	2d4	115
2a5	68	2b5	84	2c5	100	2d5	116
2a6	69	2b6	85	2c6	101	2d6	117
2a7	70	2b7	86	2c7	102	2d7	118
2a8	71	2b8	87	2c8	103	2d8	129
2a9	72	2b9	88	2c9	104	2d9	120
2a10	73	2b10	89	2c10	105	2d10	121
2a11	74	2b11	90	2c11	106	2d11	122
2a12	75	2b12	91	2c12	107	2d12	123
2a13	76	2b13	92	2c13	108	2d13	124
2a14	77	2b14	93	2c14	109	2d14	125
2a15	78	2b15	94	2c15	110	2d15	126
2a16	79	2b16	95	2c16	111	2d16	127

Table A.16 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 3 on an *ESX*-3000.

Table A.8 - ESX-3000 Port Card Slot 3 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 3 Switch Control Port (CTL = 512)							
3a1	128	3b1	144	3c1	160	3d1	176
3a2	129	3b2	145	3c2	161	3d2	177
3a3	130	3b3	146	3c3	162	3d3	178
3a4	131	3b4	147	3c4	163	3d4	179
3a5	132	3b5	148	3c5	164	3d5	180
3a6	133	3b6	149	3c6	165	3d6	181
3a7	134	3b7	150	3c7	166	3d7	182
3a8	135	3b8	151	3c8	167	3d8	183
3a9	136	3b9	152	3c9	168	3d9	184
3a10	137	3b10	153	3c10	169	3d10	185
3a11	138	3b11	154	3c11	170	3d11	186
3a12	139	3b12	155	3c12	171	3d12	187
3a13	140	3b13	156	3c13	172	3d13	188
3a14	141	3b14	157	3c14	173	3d14	189
3a15	142	3b15	158	3c15	174	3d15	190
3a16	143	3b16	159	3c16	175	3d16	191

Table A.17 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 4 on an *ESX*-3000.

Table A.9 - ESX-3000 Port Card Slot 4 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 4 Switch Control Port (CTL = 512)							
4a1	192	4b1	208	4c1	224	4d1	240
4a2	193	4b2	209	4c2	225	4d2	241
4a3	194	4b3	210	4c3	226	4d3	242
4a4	195	4b4	211	4c4	227	4d4	243
4a5	196	4b5	212	4c5	228	4d5	244
4a6	197	4b6	213	4c6	229	4d6	245
4a7	198	4b7	214	4c7	230	4d7	246
4a8	199	4b8	215	4c8	231	4d8	247
4a9	200	4b9	216	4c9	232	4d9	248
4a10	201	4b10	217	4c10	233	4d10	249
4a11	202	4b11	218	4c11	234	4d11	250
4a12	203	4b12	219	4c12	235	4d12	251
4a13	204	4b13	220	4c13	236	4d13	252
4a14	205	4b14	221	4c14	237	4d14	253
4a15	206	4b15	222	4c15	238	4d15	254
4a16	207	4b16	223	4c16	239	4d16	255

Table A.18 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 5 on an *ESX*-3000.

Table A.10 - ESX-3000 Port Card Slot 5 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 5 Switch Control Port (CTL = 512)							
5a1	256	5b1	272	5c1	288	5d1	304
5a2	257	5b2	273	5c2	289	5d2	305
5a3	258	5b3	274	5c3	290	5d3	306
5a4	259	5b4	275	5c4	291	5d4	307
5a5	260	5b5	276	5c5	292	5d5	308
5a6	261	5b6	277	5c6	293	5d6	309
5a7	262	5b7	278	5c7	294	5d7	310
5a8	263	5b8	279	5c8	295	5d8	311
5a9	264	5b9	280	5c9	296	5d9	312
5a10	265	5b10	281	5c10	297	5d10	313
5a11	266	5b11	282	5c11	298	5d11	314
5a12	267	5b12	283	5c12	299	5d12	315
5a13	268	5b13	284	5c13	300	5d13	316
5a14	269	5b14	285	5c14	301	5d14	317
5a15	270	5b15	286	5c15	302	5d15	318
5a16	271	5b16	287	5c16	303	5d16	319

Table A.19 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 6 on an *ESX*-3000.

Table A.11 - ESX-3000 Port Card Slot 6 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 6 Switch Control Port (CTL = 512)							
6a1	320	6b1	336	6c1	352	6d1	368
6a2	321	6b2	337	6c2	353	6d2	369
6a3	322	6b3	338	6c3	354	6d3	370
6a4	323	6b4	339	6c4	355	6d4	371
6a5	324	6b5	340	6c5	356	6d5	372
6a6	325	6b6	341	6c6	357	6d6	373
6a7	326	6b7	342	6c7	358	6d7	374
6a8	327	6b8	343	6c8	359	6d8	375
6a9	328	6b9	344	6c9	360	6d9	376
6a10	329	6b10	345	6c10	361	6d10	377
6a11	330	6b11	346	6c11	362	6d11	378
6a12	331	6b12	347	6c12	363	6d12	379
6a13	332	6b13	348	6c13	364	6d13	380
6a14	333	6b14	349	6c14	365	6d14	381
6a15	334	6b15	350	6c15	366	6d15	382
6a16	335	6b16	351	6c16	367	6d16	383

Table A.20 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 7 on an *ESX*-3000.

Table A.12 - ESX-3000 Port Card Slot 7 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 7 Switch Control Port (CTL = 512)							
7a1	384	7b1	400	7c1	416	7d1	432
7a2	385	7b2	401	7c2	417	7d2	433
7a3	386	7b3	402	7c3	418	7d3	434
7a4	387	7b4	403	7c4	419	7d4	435
7a5	388	7b5	404	7c5	420	7d5	436
7a6	389	7b6	405	7c6	421	7d6	437
7a7	390	7b7	406	7c7	422	7d7	438
7a8	391	7b8	407	7c8	423	7d8	439
7a9	392	7b9	408	7c9	424	7d9	440
7a10	393	7b10	409	7c10	425	7d10	441
7a11	394	7b11	410	7c11	426	7d11	442
7a12	395	7b12	411	7c12	427	7d12	443
7a13	396	7b13	412	7c13	428	7d13	444
7a14	397	7b14	413	7c14	429	7d14	445
7a15	398	7b15	414	7c15	430	7d15	446
7a16	399	7b16	415	7c16	431	7d16	447

Table A.21 shows the numbering conventions that are referred to in the MIBs for ports on port card slot 8 on an *ESX*-3000.

Table A.13 - ESX-3000 Port Card Slot 8 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number	Port Name	Software Port Number
Port Card 8 Switch Control Port (CTL = 512)							
8a1	448	8b1	464	8c1	480	8d1	496
8a2	449	8b2	465	8c2	481	8d2	497
8a3	450	8b3	466	8c3	482	8d3	498
8a4	451	8b4	467	8c4	483	8d4	499
8a5	452	8b5	468	8c5	484	8d5	500
8a6	453	8b6	469	8c6	485	8d6	501
8a8	454	8b8	470	8c8	486	8d8	502
8a8	455	8b8	471	8c8	487	8d8	503
8a9	456	8b9	472	8c9	488	8d9	504
8a10	457	8b10	473	8c10	489	8d10	505
8a11	458	8b11	474	8c11	490	8d11	506
8a12	459	8b12	475	8c12	491	8d12	507
8a13	460	8b13	476	8c13	492	8d13	508
8a14	461	8b14	477	8c14	493	8d14	509
8a15	462	8b15	478	8c15	494	8d15	510
8a16	463	8b16	479	8c16	495	8d16	511

A.4 *ASX*-4000 Port Numbering

On an *ASX*-4000, the link number is the software port number assigned to a specific port. This link number is what the MIB refers to for ports on port cards. On an *ASX*-4000, link numbers range from 0 to 1024 where link 0 refers to 1A1 (port card 1, interface group A, port 1) and link number 1024 refers to the control port (5CTL). There are 64 links reserved for each interface group on a port card. For example, link 64 refers to 1B1, link 128 refers to 1C1, and so on.

Table A.14 shows the numbering for ports on port card 1. The backplane ports are not addressable and there is only one control port. This is important when interpreting debug messages. In the interest of space, ports 1a16 through 1a63 and 1b16 through 1b63 are not shown here.

Table A.14 - *ASX*-4000 Port Card 1 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 1 Switch Control Port (5CTL = 1024)			
1a1	0	1b1	64
1a2	1	1b2	65
1a3	2	1b3	66
1a4	3	1b4	67
1a5	4	1b5	68
1a6	5	1b6	69
1a7	6	1b7	70
1a8	7	1b8	71
1a9	8	1b9	72
1a10	9	1b10	73
1a11	10	1b11	74
1a12	11	1b12	75
1a13	12	1b13	76
1a14	13	1b14	77
1a15	14	1b15	78
:	:	:	:
1a64	63	1b64	127

Table A.15 shows the numbering conventions that are referred to in the MIBs for ports on port card 2 on an *ASX*-4000. In the interest of space, ports 1c16 through 1c63 and 1d16 through 1d63 are not shown here.

Table A.15 - *ASX*-4000 Port Card 2 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 2 Switch Control Port (5CTL)= 1024)			
1c1	128	1d1	192
1c2	129	1d2	193
1c3	130	1d3	194
1c4	131	1d4	195
1c5	132	1d5	196
1c6	133	1d6	197
1c7	134	1d7	198
1c8	135	1d8	199
1c9	136	1d9	200
1c10	137	1d10	201
1c11	138	1d11	202
1c12	139	1d12	203
1c13	140	1d13	204
1c14	141	1d14	205
1c15	142	1d15	206
:	:	:	:
1c64	191	1d64	255

Table A.16 shows the numbering conventions that are referred to in the MIBs for ports on port card 3 on an *ASX*-4000. In the interest of space, ports 2a16 through 2a63 and 2b16 through 2b63 are not shown here.

Table A.16 - *ASX*-4000 Port Card 3 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 3 Switch Control Port (5CTL)= 1024)			
2a1	256	2b1	320
2a2	257	2b2	321
2a3	258	2b3	322
2a4	259	2b4	323
2a5	260	2b5	324
2a6	261	2b6	325
2a7	262	2b7	326
2a8	263	2b8	327
2a9	264	2b9	328
2a10	265	2b10	329
2a11	266	2b11	330
2a12	267	2b12	331
2a13	268	2b13	332
2a14	269	2b14	333
2a15	270	2b15	334
:	:	:	:
2a64	319	2b64	383

Table A.17 shows the numbering conventions that are referred to in the MIBs for ports on port card 4 on an *ASX*-4000. In the interest of space, ports 2c16 through 2c63 and 2d16 through 2d63 are not shown here.

Table A.17 - *ASX*-4000 Port Card 4 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 4 Switch Control Port (5CTL = 1024)			
2c1	384	2d1	448
2c2	385	2d2	449
2c3	386	2d3	450
2c4	387	2d4	451
2c5	388	2d5	452
2c6	389	2d6	453
2c7	390	2d7	454
2c8	391	2d8	455
2c9	392	2d9	456
2c10	393	2d10	457
2c11	394	2d11	458
2c12	395	2d12	459
2c13	396	2d13	460
2c14	397	2d14	461
2c15	398	2d15	462
:	:	:	:
2c64	447	2d64	511

Table A.18 shows the numbering conventions that are referred to in the MIBs for ports on port card 5 on an *ASX*-4000. In the interest of space, ports 3a16 through 3a63 and 3b16 through 3b63 are not shown here.

Table A.18 - *ASX*-4000 Port Card 5 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 5 Switch Control Port (5CTL = 1024)			
3a1	512	3b1	576
3a2	513	3b2	577
3a3	514	3b3	578
3a4	515	3b4	579
3a5	516	3b5	580
3a6	517	3b6	581
3a7	518	3b7	582
3a8	519	3b8	583
3a9	520	3b9	584
3a10	521	3b10	585
3a11	522	3b11	586
3a12	523	3b12	587
3a13	524	3b13	588
3a14	525	3b14	589
3a15	526	3b15	590
:	:	:	:
3a64	575	3b64	639

Table A.19 shows the numbering conventions that are referred to in the MIBs for ports on port card 6 on an *ASX*-4000. In the interest of space, ports 3c16 through 3c63 and 3d16 through 3d63 are not shown here.

Table A.19 - *ASX*-4000 Port Card 6 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 6 Switch Control Port (5CTL = 1024)			
3c1	640	3d1	704
3c2	641	3d2	705
3c3	642	3d3	706
3c4	643	3d4	707
3c5	644	3d5	708
3c6	645	3d6	709
3c7	646	3d7	710
3c8	647	3d8	711
3c9	648	3d9	712
3c10	649	3d10	713
3c11	650	3d11	714
3c12	651	3d12	715
3c13	652	3d13	716
3c14	653	3d14	717
3c15	654	3d15	718
:	:	:	:
3c64	703	3d64	767

Table A.20 shows the numbering conventions that are referred to in the MIBs for ports on port card 7 on an *ASX*-4000. In the interest of space, ports 4a16 through 4a63 and 4b16 through 4b63 are not shown here.

Table A.20 - *ASX*-4000 Port Card 7 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 7 Switch Control Port (5CTL = 1024)			
4a1	768	4b1	832
4a2	769	4b2	833
4a3	770	4b3	834
4a4	771	4b4	835
4a5	772	4b5	836
4a6	773	4b6	837
4a7	774	4b7	838
4a8	775	4b8	839
4a9	776	4b9	840
4a10	777	4b10	841
4a11	778	4b11	842
4a12	779	4b12	843
4a13	780	4b13	844
4a14	781	4b14	845
4a15	782	4b15	846
:	:	:	:
4a64	831	4b64	895

Table A.21 shows the numbering conventions that are referred to in the MIBs for ports on port card 8 on an *ASX*-4000. In the interest of space, ports 4c16 through 4c63 and 4d16 through 4d63 are not shown here.

Table A.21 - *ASX*-4000 Port Card 8 Port Numbering

Port Name	Software Port Number	Port Name	Software Port Number
Port Card 8 Switch Control Port (5CTL = 1024)			
4c1	896	4d1	960
4c2	897	4d2	961
4c3	898	4d3	962
4c4	899	4d4	963
4c5	900	4d5	964
4c6	901	4d6	965
4c7	902	4d7	966
4c8	903	4d8	967
4c9	904	4d9	968
4c10	905	4d10	969
4c11	906	4d11	970
4c12	907	4d12	971
4c13	908	4d13	972
4c14	909	4d14	973
4c15	910	4d15	974
:	:	:	:
4c64	959	4d64	1023

Acronyms

The networking terms in the following list are defined in the Glossary of this manual. Glossary items are listed alphabetically according to the full term.

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACM	Address Complete Message
ACR	Allowable Cell Rate
ADPCM	Adaptive Differential Pulse Code Modulation
AHFG	ATM-attached Host Functional Group
AIMUX	ATM Inverse Multiplexing
AIS	Alarm Indication Signal
AMI	Alternate Mark Inversion
AMI	ATM Management Interface
ANSI	American National Standards Institute
APCM	Adaptive Pulse Code Modulation
API	Application Program Interface
APP	Application Program
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATDM	Asynchronous Time Division Multiplexing
ATM	Asynchronous Transfer Mode
AUI	Attachment User Interface
B8ZS	Bipolar 8 Zero Substitution
BCOB	Broadband Connection Oriented Bearer
BCOB-A	Bearer Class A
BCOB-C	Bearer Class C
BCOB-X	Bearer Class X
BECN	Backward Explicit Congestion Notification
BER	Bit Error Rate
BES	Bursty Errored Seconds
BGP	Border Gateway Protocol
B-ICI	B-ISDN Inter-Carrier Interface.
BIP	Bit Interleaved Parity
B-ISDN	Broadband Integrated Services Digital Network
B-ISUP	Broadband ISDN User’s Part

BITS	Building Integrated Timing Supply
BNC	Bayonet-Neill-Concelman
BPDU	Bridge Protocol Data Unit
bps	Bits per Second
BPV	Bipolar Violation
B-TE	Broadband Terminal Equipment
BUS	Broadcast and Unknown Server
CAC	Connection Admission Control
CAS	Channel Associated Signaling
CBDS	Connectionless Broadband Data Service
CBR	Constant Bit Rate
CCITT	International Telephone and Telegraph Consultative Committee
CCS	Common Channel Signaling
CDV	Cell Delay Variation
CE	Connection Endpoint
CEI	Connection Endpoint Identifier
CES	Circuit Emulation Service
CGA	Carrier Group Alarm
CIP	Carrier Identification Parameter
CIR	Committed Information Rate
CLIP	Classical IP
CLP	Cell Loss Priority
CLR	Cell Loss Ratio-1-15
CLS	Connectionless service
CMIP	Common Management Interface Protocol
CMR	Cell Misinsertion Rate
CPE	Customer Premise Equipment
CRA	Cell Rate Adaptation
CRC	Cyclic Redundancy Check
CRS	Cell Relay Service
CS	Controlled Slip, **or** Convergence Sublayer
CSU	Channel Service Unit
CTD	Cell Transfer Delay
CTS	Clear To Send
DACS	Digital Access and Cross-Connect System
DARPA	Defense Advanced Research Projects Agency
DCC	Data Country Code
DCE	Data Communications Equipment
DCS	Digital Cross-connect System
DES	Destination End Station
DFA	DXI Frame Address
DLCI	Data Link Connection Identifier

DNS	Domain Naming System
DSn	Digital Standard n (n=0, 1, 1C, 2, and 3)
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
EEPROM	Electrically Erasable Programmable Read Only Memory
EFCI	Explicit Forward Congestion Indication
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
EISA	Extended Industry Standard Architecture
ELAN	Emulated Local Area Network
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read Only Memory
EQL	Equalization
ER	Explicit Rate
ES	End System, **or** Errored Second
ESF	Extended Super Frame
ESI	End System Identifier
EXZ	Excessive Zeroes (Error Event)
FC	Face Contact
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FEBE	Far End Block Error
FEC	Forward Error Correction
FECN	Forward Explicit Congestion Notification
FERF	Far End Receive Failure
FIFO	First-In, First-Out
FRS	Frame-Relay Service
FTP	File Transfer Protocol
FT-PNNI	*ForeThought* PNNI
FUNI	Frame-Based UNI
GCAC	Generic Connection Admission Control
GCRA	Generic Cell Rate Algorithm
GFC	Generic Flow Control
HDB3	High Density Bipolar
HDLC	High Level Data Link Control
HEC	Header Error Control
HIPPI	High Performance Parallel Interface
HSSI	High-Speed Serial Interface
ICMP	Internet Control Message Protocol

IDU	Interface Data Unit
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILMI	Interim Local Management Interface
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IS	Intermediate system
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU-T	International Telecommunication Union Telecommunication
IWF	Interworking Function
IXC	Interexchange Carriers
JPEG	Joint Photographic Experts Group
Kbps	Kilobits per second
LAN	Local Area Network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LATA	Local Access and Transport Area
LBO	Line Build Out
LCV	Line Code Violations
LE_ARP	LAN Emulation Address Resolution Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LLC	Logical Link Control
LOF	Loss Of Frame
LOP	Loss Of Pointer
LOS	Loss Of Signal
LSB	Least Significant Bit
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Media Attachment Unit
MBS	Maximum Burst Size
MCDV	Maximum Cell Delay Variance
MCLR	Maximum Cell Loss Ratio
MCR	Minimum Cell Rate
MCTD	Maximum Cell Transfer Delay
MIB	Management Information Base
MIC	Media Interface Connector
MID	Message Identifier
MMF	Multimode Fiber Optic Cable
MPEG	Motion Picture Experts Group
MPOA	Multiprotocol over ATM

MSB	Most Significant Bit
MTU	Maximum Transmission Unit
NM	Network Management Entity
NML	Network Management Layer
NMS	Network Management Station
NNI	Network-to-Network Interface or Network Node Interface
NPC	Network Parameter Control
NRZ	Non Return to Zero
NRZI	Non Return to Zero Inverted
NSAP	Network Service Access Point
NTSC	National TV Standards Committee
OAM	Operation and Maintenance Cell
OC-n	Optical Carrier level-n
OID	Object Identifier
OOF	Out-of-Frame
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First Protocol
OUI	Organizationally Unique Identifier
PAD	Packet Assembler Disassembler
PAL	Phase Alternate Line
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PDN	Public Data Network
PDU	Protocol Data Unit
PHY	Physical Layer
ping	Packet Internet Groper
PLCP	Physical Layer Convergence Protocol
PLP	Packet Level Protocol
PM	Physical Medium
PMD	Physical Medium Dependent
PNNI	Private Network Node Interface or Private Network-to-Network Interface
PPP	Point-to-Point Protocol
PROM	Programmable Read-Only Memory
PRS	Primary Reference Source
PSN	Packet Switched Network
PT	Payload Type
PVC	Permanent Virtual Circuit (or Channel)
PVCC	Permanent Virtual Channel Connection
PVPC	Permanent Virtual Path Connection
QD	Queuing Delay
QoS	Quality of Service

RD	Routing Domain
RFCs	Requests For Comment
RFI	Radio Frequency Interference
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RTS	Request To Send
SA	Source Address
SA	Source MAC Address
SAP	Service Access Point
SAR	Segmentation And Reassembly
SC	Structured Cabling, **or** Structured Connectors, **or** Stick and Click
SCR	Sustainable Cell Rate
SCSI	Small Computer Systems Interface
SDLC	Synchronous Data Link Control
SDU	Service Data Unit
SEAL	Simple and Efficient Adaptation Layer
SECAM	Systeme En Coleur Avec Memoire
SEL	Selector
SES	Severely Errored Seconds
SF	Super Frame
SGMP	Simple Gateway Management Protocol
SIR	Sustained Information Rate
SLIP	Serial Line IP
SMDS	Switched Multimegabit Data Service
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAP	SubNetwork Access Protocol
SNI	Subscriber Network Interface
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPANS	Simple Protocol for ATM Network Signalling
SPARC	Scalable Processor Architecture Reduced instruction set Computer
SPE	Synchronous Payload Envelope
SPVC	Smart PVC
SS7	Signaling System No. 7
SSCOP	Service Specific Connection Oriented Protocol
SSCS	Service Specific Convergence Sublayer
ST	Straight Tip, **or** Stick and Turn
STM	Synchronous Transfer Mode

STP	Shielded Twisted Pair, Spanning Tree Protocol
STS	Synchronous Transport Signal
SVC	Switched Virtual Circuit (or Channel)
SVCC	Switched Virtual Channel Connection
SVPC	Switched Virtual Path Connection
TAXI	Transparent Asynchronous Transmitter / Receiver Interface
TC	Transmission Convergence
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCR	Tagged Cell Rate
TCS	Transmission Convergence Sublayer
TDM	Time Division Multiplexing
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TM	Traffic Management
UAS	Unavailable Seconds
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UNI	User-to-Network Interface
UPC	Usage Parameter Control
UTOPIA	Universal Test & Operations Interface for ATM
UTP	Unshielded Twisted Pair
VBR	Variable Bit Rate
VC	Virtual Channel (or Circuit)
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VINES	Virtual Network Software
VLAN	Virtual Local Area Network
VP	Virtual Path
VPC	Virtual Path Connection
VPDN	Virtual Private Data Network
VPI	Virtual Path Identifier
VPL	Virtual Path Link
VPN	Virtual Private Network
VPT	Virtual Path Terminator
VS/VD	Virtual Source / Virtual Destination
VT	Virtual Tributary
WAN	Wide-Area Network
ZBTSI	Zero Byte Time Slot Interchange

Glossary

10Base-T - a 10 Mbps baseband Ethernet specification utilizing twisted-pair cabling (Category 3, 4, or 5). 10BaseT, which is part of the IEEE 802.3 specification, has a distance limit of approximately 100 meters per segment.

802.1d Spanning Tree Bridging - the IEEE standard for bridging; a MAC layer standard for transparently connecting two or more LANs (often called subnetworks) that are running the same protocols and cabling. This arrangement creates an extended network, in which any two workstations on the linked LANs can share data.

802.3 Ethernet - the IEEE standard for Ethernet; a physical-layer standard that uses the CSMA / CD access method on a bus-topology LAN.

802.5 Token Ring - the IEEE physical-layer standard that uses the token-passing access method on a ring-topology LAN.

AAL Connection - an association established by the AAL between two or more next higher layer entities.

Adapter - A fitting that supplies a passage between two sets of equipment when they cannot be directly interconnected.

Adaptive Differential Pulse Code Modulation (ADPCM) - A technique that allows analog voice signals to be carried on a 32K bps digital channel. Sampling is done at 8Hz with 4 bits used to describe the difference between adjacent samples.

Adaptive Pulse Code Modulation (APCM) - A technique that effectively reduces occupied bandwidth per active speaker by reducing sampling rates during periods of overflow peak traffic.

Address - A unique identity of each network station on a LAN or WAN.

Address Complete Message (ACM) - A B-ISUP call control message from the receiving exchange to sending exchange indicating the completion of address information.

Address Mask - a bit mask used to identify which bits in an address (usually an IP address) are network significant, subnet significant, and host significant portions of the complete address. This mask is also known as the subnet mask because the subnetwork portion of the address can be determined by comparing the binary version of the mask to an IP address in that subnet. The mask holds the same number of bits as the protocol address it references.

Address Prefix - A string of 0 or more bits up to a maximum of 152 bits that is the lead portion of one or more ATM addresses.

Address Resolution - The procedure by which a client associates a LAN destination with the ATM address of another client or the BUS.

Address Resolution Protocol (ARP) - a method used to resolve higher level protocol addressing (such as IP) into the appropriate header data required for ATM; i.e., port, VPI, and VCI; also defines the AAL type to be used.

Agent - a component of network- and desktop-management software, such as SNMP, that gathers information from MIBs.

alarm - an unsolicited message from a device, typically indicating a problem with the system that requires attention.

Alarm Indication Signal (AIS) - In T1, an all ones condition used to alert a receiver that its incoming signal (or frame) has been lost. The loss of signal or frame is detected at the receiving end, and the failed signal is replaced by all the ones condition which the receiver interprets as an AIS. The normal response to this is AIS is for the receiving end to generate a yellow alarm signal as part of its transmission towards the faulty end. (The AIS itself is sometimes called a Blue Signal).

A-Law - The PCM coding and companding standard used in Europe.

Allowable Cell Rate (ACR) - parameter defined by the ATM Forum for ATM traffic management. ACR varies between the MCR and the PCR, and is dynamically controlled using congestion control mechanisms.

Alternate Mark Inversion (AMI) - A line coding format used on T1 facilities that transmits ones by alternate positive and negative pulses.

Alternate Routing - A mechanism that supports the use of a new path after an attempt to set up a connection along a previously selected path fails.

American National Standards Institute (ANSI) - a private organization that coordinates the setting and approval of some U.S. standards. It also represents the United States to the International Standards Organization.

American Standard Code for Information Interchange (ASCII) - a standard character set that (typically) assigns a 7-bit sequence to each letter, number, and selected control characters.

AppleTalk - a networking protocol developed by Apple Computer for communication between Apple's products and other computers. Independent of the network layer, AppleTalk runs on LocalTalk, EtherTalk and TokenTalk.

Application Layer - Layer seven of the ISO reference model; provides the end-user interface.

Application Program (APP) - a complete, self-contained program that performs a specific function directly for the user.

Application Program Interface (API) - a language format that defines how a program can be made to interact with another program, service, or other software; it allows users to develop custom interfaces with FORE products.

Assigned Cell - a cell that provides a service to an upper layer entity or ATM Layer Management entity (ATMM-entity).

asxmon - a FORE program that repeatedly displays the state of the switch and its active ports.

Asynchronous Time Division Multiplexing (ATDM) - a multiplexing technique in which a transmission capability is organized into a priori, unassigned time slots. The time slots are assigned to cells upon request of each application's instantaneous real need.

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 Adaptation Layer (AAL) - the AAL divides user information into segments suitable for packaging into a series of ATM cells. AAL layer types are used as follows:

AAL-1 - constant bit rate, time-dependent traffic such as voice and video
AAL-2 - still undefined; a placeholder for variable bit rate video transmission
AAL-3/4 - variable bit rate, delay-tolerant data traffic requiring some sequencing and/or error detection support (originally two AAL types, connection-oriented and connectionless, which have been combined)
AAL-5 - variable bit rate, delay-tolerant, connection-oriented data traffic requiring minimal sequencing or error detection support

ATM Address - Defined in the UNI Specification as 3 formats, each having 20 bytes in length.

ATM Forum - an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

ATM Inverse Multiplexing (AIMUX) - A device that allows multiple T1 or E1 communications facilities to be combined into a single broadband facility for the transmission of ATM cells.

ATM Layer link - a section of an ATM Layer connection between two adjacent active ATM Layer entities (ATM-entities).

ATM Link - a virtual path link (VPL) or a virtual channel link (VCL).

ATM Management Interface (AMI) - the user interface to FORE Systems' *ForeThought* switch control software (SCS). AMI lets users monitor and change various operating configurations of FORE Systems switches and network module hardware and software, IP connectivity, and SNMP network management.

ATM Peer-to-Peer Connection - a virtual channel connection (VCC) or a virtual path connection (VPC) directly established, such as workstation-to-workstation. This setup is not commonly used in networks.

ATM Traffic Descriptor - a generic list of parameters that can be used to capture the intrinsic traffic characteristics of a requested ATM connection.

ATM User-to-User Connection - an association established by the ATM Layer to support communication between two or more ATM service users (i.e., between two or more next higher layer entities or between two or more ATM entities). The communication over an ATM Layer connection may be either bidirectional or unidirectional. The same Virtual Channel Identifier (VCI) is used for both directions of a connection at an interface.

atmarp - a FORE program that shows and manipulates ATM ARP entries maintained by the given device driver. This is also used to establish PVC connections.

ATM-attached Host Functional Group (AHFG) - The group of functions performed by an ATM-attached host that is participating in the MPOA service.

atmconfig - a FORE program used to enable or disable SPANS signaling.

atmstat - a FORE program that shows statistics gathered about a given adapter card by the device driver. These statistics include ATM layer and ATM adaptation layer cell and error counts. This can also be used to query other hosts via SNMP.

Attachment User Interface (AUI) - IEEE 802.3 interface between a media attachment unit (MAU) and a network interface card (NIC). The term AUI can also refer to the rear panel port to which an AUI cable might attach.

Auto-logout - a feature that automatically logs out a user if there has been no user interface activity for a specified length of time.

Automatic Protection Switching (APS) - Equipment installed in communications systems to detect circuit failures and automatically switch to redundant, standby equipment.

Available Bit Rate (ABR) - a type of traffic for which the ATM network attempts to meet that traffic's bandwidth requirements. It does not guarantee a specific amount of bandwidth and the end station must retransmit any information that did not reach the far end.

Backbone - the main connectivity device of a distributed system. All systems that have connectivity to the backbone connect to each other, but systems can set up private arrangements with each other to bypass the backbone to improve cost, performance, or security.

Backplane - High-speed communications line to which individual components are connected.

Backward Explicit Congestion Notification (BECN) - A Resource Management cell type generated by the network or the destination, indicating congestion or approaching congestion for traffic flowing in the direction opposite that of the BECN cell.

Bandwidth - usually identifies the capacity or amount of data that can be sent through a given circuit; may be user-specified in a PVC.

Baud - unit of signalling speed, equal to the number of discrete conditions or signal events per second. If each signal event represents only one bit, the baud rate is the same as bps; if each signal event represents more than one bit (such as a dibit), the baud rate is smaller than bps.

Bayonet-Neill-Concelman (BNC) - a bayonet-locking connector used to terminate coaxial cables. BNC is also referred to as Bayonet Network Connector.

Bipolar 8 Zero Substitution (B8ZS) - a technique used to satisfy the ones density requirements of digital T-carrier facilities in the public network while allowing 64 Kbps clear channel data. Strings of eight consecutive zeroes are replaced by an eight-bit code representing two intentional bipolar pulse code violations (000V10V1).

Bipolar Violation (BPV) - an error event on a line in which the normal pattern of alternating high (one) and low (zero) signals is disrupted. A bipolar violation is noted when two high signals occur without an intervening low signal, or vice versa.

B-ISDN Inter-Carrier Interface (B-ICI) - An ATM Forum defined specification for the interface between public ATM networks to support user services across multiple public carriers.

Bit Error Rate (BER) - A measure of transmission quality, generally shown as a negative exponent, (e.g., 10^{-7} which means 1 out of 10^{7} bits [1 out of 10,000,000 bits] are in error).

Bit Interleaved Parity (BIP) - an error-detection technique in which character bit patterns are forced into parity, so that the total number of one bits is always odd or always even. This is accomplished by the addition of a one or zero bit to each byte, as the byte is transmitted; at the other end of the transmission, the receiving device verifies the parity (odd or even) and the accuracy of the transmission.

Bit Robbing - The use of the least significant bit per channel in every sixth frame for signaling.

Bit Stuffing - A process in bit-oriented protocols where a zero is inserted into a string of ones by the sender to prevent the receiver from interpreting valid user data (the string of ones) as control characters (a Flag character for instance).

Border Gateway Protocol (BGP) - used by gateways in an internet connecting autonomous networks. It is derived from experiences learned using the EGP.

bps - bits per second

Bridge - a device that expands a Local Area Network by forwarding frames between data link layers associated with two separate cables, usually carrying a common protocol. Bridges can usually be made to filter certain packets (to forward only certain traffic).

Bridge Protocol Data Unit (BPDU) - A message type used by bridges to exchange management and control information.

Broadband - a service or system requiring transmission channels capable of supporting rates greater than the Integrated Services Digital Network (ISDN) primary rate.

Broadband Access - an ISDN access capable of supporting one or more broadband services.

Broadband Connection Oriented Bearer (BCOB) - Information in the SETUP message that indicates the type of service requested by the calling user.

BCOB-A (Bearer Class A) - Indicated by ATM end user in SETUP message for connection-oriented, constant bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-C (Bearer Class C) - Indicated by ATM end user in SETUP message for connection-oriented, variable bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-X (Bearer Class X) - Indicated by ATM end user in SETUP message for ATM transport service where AAL, traffic type and timing requirements are transparent to the network.

Broadband Integrated Services Digital Network (B-ISDN) - a common digital network suitable for voice, video, and high-speed data services running at rates beginning at 155 Mbps.

Broadband ISDN User's Part (B-ISUP) - A protocol used to establish, maintain and release broadband switched network connections across an SS7/ATM network.

Broadband Terminal Equipment (B-TE) - An equipment category for B-ISDN which includes terminal adapters and terminals.

Broadcast - Data transmission to all addresses or functions.

Broadcast and Unknown Server (BUS) - in an emulated LAN, the BUS is responsible for accepting broadcast, multicast, and unknown unicast packets from the LECs to the broadcast MAC address (FFFFFFFFFFFF) via dedicated point-to-point connections, and forwarding the packets to all of the members of the ELAN using a single point-to-multipoint connection.

Brouter (bridging/router) - a device that routes some protocols and bridges others based on configuration information.

Buffer - A data storage medium used to compensate of a difference in rate of data flow or time of occurrence of events when transmitting data from one device to another.

Building Integrated Timing Supply (BITS) - a master timing supply for an entire building, which is a master clock and its ancillary equipment. The BITS supplies DS1 and/or composite clock timing references for synchronization to all other clocks and timing sources in that building.

Bursty Errored Seconds (BES) - a BES contains more than 1 and fewer than 320 path coding violation error events, and no severely errored frame or AIS defects. Controlled slips are not included in determining BESs.

Bursty Second - a second during which there were at least the set number of BES threshold event errors but fewer than the set number of SES threshold event errors.

Byte - A computer-readable group of bits (normally 8 bits in length).

Call - an association between two or more users or between a user and a network entity that is established by the use of network capabilities. This association may have zero or more connections.

Carrier - a company, such as any of the “baby Bell” companies, that provide network communications services, either within a local area or between local areas.

Carrier Group Alarm (CGA) - A service alarm generated by a channel bank when an out-of-frame (OOF) condition exists for some predetermined length of time (generally 300 milliseconds to 2.5 seconds). The alarm causes the calls using a trunk to be dropped and trunk conditioning to be applied.

Carrier Identification Parameter (CIP) - A 3 or 4 digit code in the initial address message identifying the carrier to be used for the connection.

cchan - a FORE program that manages virtual channels on a *ForeRunner* or TNX switch running asxd.

Cell - an ATM Layer protocol data unit (PDU). The basic unit of information transported in ATM technology, each 53-byte cell contains a 5-byte header and a 48-byte payload.

Cell Delay Variation (CDV) - a quantification of cell clumping for a connection. The cell clumping CDV (yk) is defined as the difference between a cell's expected reference arrival time (ck) and its actual arrival time (ak). The expected reference arrival time (ck) of cell k of a specific connection is max. T is the reciprocal of the negotiated peak cell rate.

Cell Delineation - the protocol for recognizing the beginning and end of ATM cells within the raw serial bit stream.

Cell Header - ATM Layer protocol control information.

Cell Loss Priority (CLP) - the last bit of byte four in an ATM cell header; indicates the eligibility of the cell for discard by the network under congested conditions. If the bit is set to 1, the cell may be discarded by the network depending on traffic conditions.

Cell Loss Ratio - In a network, cell loss ratio is (1-x/y), where y is the number of cells that arrive in an interval at an ingress of the network; and x is the number of these y cells that leave at the egress of the network element.

Cell Loss Ratio (CLR) - CLR is a negotiated QoS parameter and acceptable values are network specific. The objective is to minimize CLR provided the end-system adapts the traffic to the changing ATM layer transfer characteristics. The Cell Loss Ratio is defined for a connection as: Lost Cells/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.

Cell Misinsertion Rate (CMR) - the ratio of cells received at an endpoint that were not originally transmitted by the source end in relation to the total number of cells properly transmitted.

Cell Rate Adaptation (CRA) - a function performed by a protocol module in which empty cells (known as unassigned cells) are added to the output stream. This is because there always must be a fixed number of cells in the output direction; when there are not enough cells to transmit, unassigned cells are added to the output data stream.

Cell Relay Service (CRS) - a carrier service which supports the receipt and transmission of ATM cells between end users in compliance with ATM standards and implementation specifications.

Cell Transfer Delay - the transit delay of an ATM cell successfully passed between two designated boundaries. See CTD.

Cell Transfer Delay (CTD) - This is defined as the elapsed time between a cell exit event at the measurement point 1 (e.g., at the source UNI) and the corresponding cell entry event at the measurement point 2 (e.g., the destination UNI) for a particular connection. The cell transfer delay between two measurement points is the sum of the total inter-ATM node transmission delay and the total ATM node processing delay.

Channel - A path or circuit along which information flows.

Channel Associated Signaling (CAS) - a form of circuit state signaling in which the circuit state is indicated by one or more bits of signaling status sent repetitively and associated with that specific circuit.

Channel Bank - A device that multiplexes many slow speed voice or data conversations onto high speed link and controls the flow.

Channel Service Unit (CSU) - An interface for digital leased lines which performs loopback testing and line conditioning.

Channelization - capability of transmitting independent signals together over a cable while still maintaining their separate identity for later separation.

Circuit - A communications link between points.

Circuit Emulation Service (CES) - The ATM Forum circuit emulation service interoperability specification specifies interoperability agreements for supporting Constant Bit Rate (CBR) traffic over ATM networks that comply with the other ATM Forum interoperability agreements. Specifically, this specification supports emulation of existing TDM circuits over ATM networks.

Classical IP (CLIP) - IP over ATM which conforms to RFC 1577.

Clear to Send (CTS) - and RS-232 modem interface control signal (sent from the modem to the DTE on pin 5) which indicates that the attached DTE may begin transmitting; issuance in response to the DTE’s RTS.

Clocking - Regularly timed impulses.

Closed User Group - A subgroup of network users that can be its own entity; any member of the subgroup can only communicate with other members of that subgroup.

Coaxial Cable - Coax is a type of electrical communications medium used in the LAN environment. This cable consists of an outer conductor concentric to an inner conductor, separated from each other by insulating material, and covered by some protective outer material. This medium offers large bandwidth, supporting high data rates with high immunity to electrical interference and a low incidence of errors. Coax is subject to distance limitations and is relatively expensive and difficult to install.

Cold Start Trap - an SNMP trap which is sent after a power-cycle (see *trap*).

Collision - Overlapping transmissions that occur when two or more nodes on a LAN attempt to transmit at or about the same time.

Committed Information Rate (CIR) - CIR is the information transfer rate which a network offering Frame Relay Services (FRS) is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time.

Common Channel Signaling (CCS) - A form signaling in which a group of circuits share a signaling channel. Refer to SS7.

Common Management Interface Protocol (CMIP) - An ITU-TSS standard for the message formats and procedures used to exchange management information in order to operate, administer maintain and provision a network.

Concatenation - The connection of transmission channels similar to a chain.

Concentrator - a communications device that offers the ability to concentrate many lower-speed channels into and out of one or more high-speed channels.

Configuration - The phase in which the LE Client discovers the LE Service.

Congestion Management - traffic management feature that helps ensure reasonable service for VBR connections in an ATM network, based on a priority, sustained cell rate (SCR), and peak cell rate (PCR). During times of congestion, bandwidth is reduced to the SCR, based on the priority of the connection.

Connection - the concatenation of ATM Layer links in order to provide an end-to-end information transfer capability to access points.

Connection Admission Control (CAC) - the procedure used to decide if a request for an ATM connection can be accepted based on the attributes of both the requested connection and the existing connections.

Connection Endpoint (CE) - a terminator at one end of a layer connection within a SAP.

Connection Endpoint Identifier (CEI) - an identifier of a CE that can be used to identify the connection at a SAP.

Connectionless Broadband Data Service (CBDS) - A connectionless service similar to Bellcore's SMDS defined by European Telecommunications Standards Institute (ETSI).

Connectionless Service - a type of service in which no pre-determined path or link has been established for transfer of information, supported by AAL 4.

Connectionless Service (CLS) - A service which allows the transfer of information among service subscribers without the need for end-to- end establishment procedures.

Connection-Oriented Service - a type of service in which information always traverses the same pre-established path or link between two points, supported by AAL 3.

Constant Bit Rate (CBR) - a type of traffic that requires a continuous, specific amount of bandwidth over the ATM network (e.g., digital information such as video and digitized voice).

Controlled Slip (CS) - a situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when the sending device and receiving device are not using the same clock.

Convergence Sublayer (CS) - a portion of the AAL. Data is passed first to the CS where it is divided into rational, fixed-length packets or PDUs (Protocol Data Units). For example, AAL 4 processes user data into blocks that are a maximum of 64 kbytes long.

Corresponding Entities - peer entities with a lower layer connection among them.

cpath - a FORE program used to manage virtual paths on a *ForeRunner* or TNX switch running asxd.

cport - a FORE program that monitors and changes the state of ports on a *ForeRunner* switch running asxd.

Cross Connection - a mapping between two channels or paths at a network device.

Customer Premise Equipment (CPE) - equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. See also point of demarcation.

Cut Through - Establishment of a complete path for signaling and/or audio communications.

Cyclic Redundancy Check (CRC) - an error detection scheme in which a number is derived from the data that will be transmitted. By recalculating the CRC at the remote end and comparing it to the value originally transmitted, the receiving node can detect errors.

D3/D4 - Refers to compliance with AT&T TR (Technical Reference) 62411 definitions for coding, supervision, and alarm support. D3/D4 compatibility ensures support of digital PBXes, M24 services, Megacom services, and Mode 3 D3/D4 channel banks at DS-1 level.

D4 Channelization - refers to compliance with AT&T Technical Reference 62411 regarding DS1 frame layout (the sequential assignment of channels and time slot numbers within the DS1).

D4 Framed/Framing Format - in T1, a 193-bit frame format in which the 193rd bit is used for framing and signaling information (the frame/framing bit). To be considered in support of D4 Framing, a device must be able to synchronize and frame-up on the 193rd bit.

Data Communications Equipment (DCE) - a definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.

Data Country Code (DCC) - This specifies the country in which an address is registered. The codes are given in ISO 3166. The length of this field is two octets. The digits of the data country code are encoded in Binary Coded Decimal (BCD) syntax. The codes will be left justified and padded on the right with the hexadecimal value “F” to fill the two octets.

Data Link - Communications connection used to transmit data from a source to a destination.

Data Link Connection Identifier (DLCI) - connection identifier associated with frame relay packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

Data Link Layer - Layer 2 of the OSI model, responsible for encoding data and passing it to the physical medium. The IEEE divides this layer into the LLC (Logical Link Control) and MAC (Media Access Control) sublayers.

Data Set Ready (DSR) - an RS-232 modem interface control signal (sent from the modem to the DTE on pin 6) which indicates that the modem is connected to the telephone circuit. Usually a prerequisite to the DTE issuing RTS.

Data Terminal Equipment (DTE) - generally user devices, such as terminals and computers, that connect to data circuit-terminating equipment. They either generate or receive the data carried by the network.

Data Terminal Ready (DTR) - an RS232 modem interface control signal (sent from the DTE to the modem on pin 20) which indicates that the DTE is ready for data transmission and which requests that the modem be connected to the telephone circuit.

Datagram - a packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram’s header.

DECnet - Digital Equipment Corporation's proprietary LAN.

Defense Advanced Research Projects Agency (DARPA) - the US government agency that funded the ARPANET.

Demultiplexing - a function performed by a layer entity that identifies and separates SDUs from a single connection to more than one connection (see *multiplexing*).

Destination End Station (DES) - An ATM termination point which is the destination for ATM messages of a connection and is used as a reference point for ABR services. See SES.

Digital Access and Cross-Connect System (DACS) - Digital switching system for routing T1 lines, and DS-0 portions of lines, among multiple T1 ports.

Digital Cross-connect System (DCS) - an electronic patch panel used to route digital signals in a central office.

Digital Standard n (0, 1, 1C, 2, and 3) (DSn) - a method defining the rate and format of digital hierarchy, with asynchronous data rates defined as follows:

DS0	64kb/s	1 voice channel
DS1	1.544Mb/s	24 DS0s
DS1C	3.152 Mb/s	2 DS1s
DS2	6.312 Mb/s	4 DS1s
DS3	44.736 Mb/s	28 DS1s

Synchronous data rates (SONET) are defined as:

STS-1/OC-1	51.84 Mb/s	28 DS1s or 1 DS3
STS-3/OC-3	155.52 Mb/s	3 STS-1s byte interleaved
STS-3c/OC-3c	155.52 Mb/s	Concatenated, indivisible payload
STS-12/OC-12	622.08 Mb/s	12 STS-1s, 4 STS-3cs, or any mixture
STS-12c/OC-12c	622.08 Mb/s	Concatenated, indivisible payload
STS-48/OC-48	2488.32 Mb/s	48 STS-1s, 16 STS-3cs, or any mixture

DIP (Dual In-line Package) Switch - a device that has two parallel rows of contacts that let the user switch electrical current through a pair of those contacts to on or off. They are used to reconfigure components and peripherals.

Domain Name Server - a computer that converts names to their corresponding Internet numbers. It allows users to telnet or FTP to the name instead of the number.

Domain Naming System (DNS) - the distributed name and address mechanism used in the Internet.

Duplex - Two way communication.

DXI - a generic phrase used in the full names of several protocols, all commonly used to allow a pair of DCE and DTE devices to share the implementation of a particular WAN protocol. The protocols define the packet formats used to transport data between DCE and DTE devices.

DXI Frame Address (DFA) - a connection identifier associated with ATM DXI packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

Dynamic Allocation - A technique in which the resources assigned for program execution are determined by criteria applied at the moment of need.

E.164 - A public network addressing standard utilizing up to a maximum of 15 digits. ATM uses E.164 addressing for public network addressing.

E1 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

E3 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers.

Edge Device - A physical device which is capable of forwarding packets between legacy interworking interfaces (e.g., Ethernet, Token Ring, etc.) and ATM interfaces based on data-link and network layer information but which does not participate in the running of any network layer routing protocol. An Edge Device obtains forwarding descriptions using the route distribution protocol.

elarp - a FORE program that shows and manipulates MAC and ATM address mappings for LAN Emulation Clients (LECs).

elconfig - a FORE program that shows and modifies LEC configuration. Lets the user set the NSAP address of the LAN Emulation Configuration Server, display the list of Emulated LANs configured in the LECS for this host, display the list of ELANs locally configured along with the membership state of each, and locally administer ELAN membership.

Electrically Erasable Programmable Read Only Memory (EEPROM) - an EPROM that can be cleared with electrical signals rather than the traditional ultraviolet light.

Electromagnetic Interference (EMI) - signals generated and radiated by an electronic device that cause interference with radio communications, among other effects.

Electronics Industries Association (EIA) - a USA trade organization that issues its own standards and contributes to ANSI; developed RS-232. Membership includes USA manufacturers.

Embedded SNMP Agent - an SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is integrated into the physical hardware and software of the unit.

Emulated Local Area Network (ELAN) - A logical network initiated by using the mechanisms defined by LAN Emulation. This could include ATM and legacy attached end stations.

End System (ES) - a system where an ATM connection is terminated or initiated (an originating end system initiates the connection; a terminating end system terminates the connection).

End System Identifier (ESI) - This identifier distinguishes multiple nodes at the same level in case the lower level peer group is partitioned.

End-to-End Connection - when used in reference to an ATM network, a connection that travels through an ATM network, passing through various ATM devices and with endpoints at the termination of the ATM network.

Enterprise - Terminology generally referring to customers with multiple, non-contiguous geographic locations.

Equalization (EQL) - the process of compensating for line distortions.

Erasable Programmable Read Only Memory (EPROM) - A PROM which may be erased and rewritten to perform new or different functions (normally done with a PROM burner).

Errored Second (ES) - a second during which at least one code violation occurred.

Ethernet - a 10-Mbps, coaxial standard for LANs in which all nodes connect to the cable where they contend for access.

Excessive Zeroes (EXZ) Error Event - An Excessive Zeroes error event for an AMI-coded signal is the occurrence of more than fifteen contiguous zeroes. For a B8ZS coded signal, the defect occurs when more than seven contiguous zeroes are detected.

Explicit Forward Congestion Indication (EFCI) - the second bit of the payload type field in the header of an ATM cell, the EFCI bit indicates network congestion to receiving hosts. On a congested switch, the EFCI bit is set to “1” by the transmitting network module when a certain number of cells have accumulated in the network module's shared memory buffer. When a cell is received that has its EFCI bit set to “1,” the receiving host notifies the sending host, which should then reduce its transmission rate.

Explicit Rate (ER) - The Explicit Rate is an RM-cell field used to limit the source ACR to a specific value. It is initially set by the source to a requested rate (such as PCR). It may be subsequently reduced by any network element in the path to a value that the element can sustain. ER is formatted as a rate.

Extended Industry Standard Architecture (EISA) - bus architecture for desktop computers that provides a 32-bit data passage and maintains compatibility with the ISA or AT architecture.

Extended Super Frame (ESF) - a T1 framing format that utilizes the 193rd bit as a framing bit, but whose Superframe is made up of 24 frames instead of 12 as in D4 format. ESF also provides CRC error detection and maintenance data link functions.

Exterior Gateway Protocol (EGP) - used by gateways in an internet, connecting autonomous networks.

Fairness - related to Generic Flow Control, fairness is defined as meeting all of the agreed quality of service requirements by controlling the order of service for all active connections.

Far End Block Error (FEBE) - an error detected by extracting the 4-bit FEBE field from the path status byte (G1). The legal range for the 4-bit field is between 0000 and 1000, representing zero to eight errors. Any other value is interpreted as zero errors.

Far End Receive Failure (FERF) - a line error asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

Far-End - in a relationship between two devices in a circuit, the far-end device is the one that is remote.

Face Contact (FC) - Designation for fiber optic connector designed by Nippon Telegraph and Telephone which features a movable anti-rotation key allowing good repeatable performance despite numerous mating. Normally referred to as Fiber Connector, FC actually stands for Face Contact and sometimes linked with PC (Point Contact), designated as FC or FC-PC.

FCC Part 68 - The FCC rules regulating the direct connection of non-telephone company provided equipment to the public telephone network.

Federal Communications Commission (FCC) - a board of commissioners appointed by the President under the Communications Act of 1934, with the authority to regulate all interstate telecommunications originating in the United States, including transmission over phone lines.

Fiber Distributed Data Interface (FDDI) - high-speed data network that uses fiber-optic as the physical medium. Operates in similar manner to Ethernet or Token Ring, only faster.

File Transfer Protocol (FTP) - a TCP/IP protocol that lets a user on one computer access, and transfer data to and from, another computer over a network. ftp is usually the name of the program the user invokes to accomplish this task.

First-In, First-Out (FIFO) - method of coordinating the sequential flow of data through a buffer.

Flag - a bit pattern of six binary “1”s bounded by a binary “0” at each end (forms a 0111 1110 or Hex “7E”). It is used to mark the beginning and/or end of a frame.

Flow Control - The way in which information is controlled in a network to prevent loss of data when the receiving buffer is near its capacity.

***ForeThought* PNNI (FT-PNNI) -** a FORE Systems routing and signalling protocol that uses private ATM (NSAP) addresses; a precursor to ATM Forum PNNI (see PNNI).

Forward Error Correction (FEC) - A technique used by a receiver for correcting errors incurred in transmission over a communications channel without requiring retransmission of any information by the transmitter; typically involves a convolution of the transmitted bits and the appending of extra bits by both the receiver and transmitter using a common algorithm.

Forward Explicit Congestion Notification (FECN) - Bit set by a Frame Relay network to inform data terminal equipment (DTE) receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow control action as appropriate.

Fractional T1 - the use of bandwidth in 64Kbps increments up to 1.544Mbps from a T1 facility.

Frame - a variable length group of data bits with a specific format containing flags at the beginning and end to provide demarcation.

Frame Check Sequence (FCS) - In bit-oriented protocols, a 16-bit field that contains transmission error checking information, usually appended to the end of the frame.

Frame Relay - a fast packet switching protocol based on the LAPD protocol of ISDN that performs routing and transfer with less overhead processing than X.25.

Frame Synchronization Error - an error in which one or more time slot framing bits are in error.

Frame-Based UNI (FUNI) - An ATM switch-based interface which accepts frame-based ATM traffic and converts it into cells.

Frame-Relay Service (FRS) - A connection oriented service that is capable of carrying up to 4096 bytes per frame.

Framing - a protocol that separates incoming bits into identifiable groups so that the receiving multiplexer recognizes the grouping.

Frequency Division Multiplexing (FDM) - a method of dividing an available frequency range into parts with each having enough bandwidth to carry one channel.

Gbps - gigabits per second (billion)

Generic Cell Rate Algorithm (GCRA) - an algorithm which is employed in traffic policing and is part of the user/network service contract. The GCRA is a scheduling algorithm which ensures that cells are marked as conforming when they arrive when expected or later than expected and non-conforming when they arrive sooner than expected.

Generic Connection Admission Control (GCAC) - This is a process to determine if a link has potentially enough resources to support a connection.

Generic Flow Control (GFC) - the first four bits of the first byte in an ATM cell header. Used to control the flow of traffic across the User-to-Network Interface (UNI), and thus into the network. Exact mechanisms for flow control are still under investigation and no explicit definition for this field exists at this time. (This field is used only at the UNI; for NNI-NNI use (between network nodes), these four bits provide additional network address capacity, and are appended to the VPI field.)

GIO - a proprietary bus architecture used in certain Silicon Graphics, Inc. workstations.

Header - protocol control information located at the beginning of a protocol data unit.

Header Error Control (HEC) - a CRC code located in the last byte of an ATM cell header that is used for checking cell header integrity only.

High Density Bipolar (HDB3) - A bipolar coding method that does not allow more than 3 consecutive zeroes.

High Level Data Link Control (HDLC) - An ITU-TSS link layer protocol standard for point-to-point and multi-point communications.

High Performance Parallel Interface (HIPPI) - ANSI standard that extends the computer bus over fairly short distances at speeds of 800 and 1600 Mbps.

High-Speed Serial Interface (HSSI) - a serial communications connection that operates at speeds of up to 1.544 Mbps.

Host - In a network, the primary or controlling computer in a multiple computer installation.

HPUX - the Hewlett-Packard version of UNIX.

Hub - a device that connects several other devices, usually in a star topology.

I/O Module - FORE's interface cards for the LAX-20 LAN Access Switch, designed to connect Ethernet, Token Ring, and FDDI LANs to *ForeRunner* or TNX ATM networks.

Institute of Electrical and Electronics Engineers (IEEE) - the world's largest technical professional society. Based in the U.S., the IEEE sponsors technical conferences, symposia & local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics & computer engineering, provides educational programs for members, and promotes standardization.

IEEE 802 - Standards for the interconnection of LAN computer equipment. Deals with the Data Link Layers of the ISO Reference Model for OSI.
IEEE 802.1 - Defines the high-level network interfaces such as architecture, internetworking and network management.
IEEE 802.2 - Defines the Logical Link Control interface between the Data Link and Network Layers.
IEEE 802.3 - Defines CSMA/CD (Ethernet).
IEEE 802.4 - Defines the token-passing bus.
IEEE 802.5 - Defines the Token Ring access methodology. This standard incorporates IBM's Token Ring specifications.
IEEE 802.6 - Defines Metropolitan Area Networks.
IEEE 802.7 - The broadband technical advisory group.
IEEE 802.8 - The fiber optics technical advisory group.
IEEE 802.9 - Defines integrated data and voice networks.

Integrated Services Digital Network (ISDN) - an emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services into a single medium or wire.

Interexchange Carriers (IXC) - Long-distance communications companies that provide service between Local Access Transport Areas (LATAs).

Interface Data - the unit of information transferred to/from the upper layer in a single interaction across a SAP. Each Interface Data Unit (IDU) controls interface information and may also contain the whole or part of the SDU.

Interface Data Unit (IDU) - The unit of information transferred to/from the upper layer in a single interaction across the SAP. Each IDU contains interface control information and may also contain the whole or part of the SDU.

Interim Local Management Interface (ILMI) - the standard that specifies the use of the Simple Network Management Protocol (SNMP) and an ATM management information base (MIB) to provide network status and configuration information.

Intermediate System (IS) - a system that provides forwarding functions or relaying functions or both for a specific ATM connection. OAM cells may be generated and received.

International Standards Organization (ISO) - a voluntary, non treaty organization founded in 1946 that is responsible for creating international standards in many areas, including computers and communications.

International Telephone and Telegraph Consultative Committee (CCITT) - the international standards body for telecommunications.

Internet - (note the capital "I") the largest internet in the world including large national backbone nets and many regional and local networks worldwide. The Internet uses the TCP/IP suite. Networks with only e-mail connectivity are not considered on the Internet.

internet - while an internet is a network, the term "internet" is usually used to refer to a collection of networks interconnected with routers.

Internet Addresses - the numbers used to identify hosts on an internet network. Internet host numbers are divided into two parts; the first is the network number and the second, or local, part is a host number on that particular network. There are also three classes of networks in the Internet, based on the number of hosts on a given network. Large networks are classified as Class A, having addresses in the range 1-126 and having a maximum of 16,387,064 hosts. Medium networks are classified as Class B, with addresses in the range 128-191 and with a maximum of 64,516 hosts. Small networks are classified as Class C, having addresses in the range 192-254 with a maximum of 254 hosts. Addresses are given as dotted decimal numbers in the following format:

nnn.nnn.nnn.nnn

In a Class A network, the first of the numbers is the network number, the last three numbers are the local host address.

In a Class B network, the first two numbers are the network, the last two are the local host address.

In a Class C network, the first three numbers are the network address, the last number is the local host address.

The following table summarizes the classes and sizes:

Class	First #	Max# Hosts
A	1-126	16,387,064
B	129-191	64,516
C	192-223	254

Network mask values are used to identify the network portion and the host portion of the address. Default network masks are as follows:

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Subnet masking is used when a portion of the host ID is used to identify a subnetwork. For example, if a portion of a Class B network address is used for a subnetwork, the mask could be set as 255.255.255.0. This would allow the third byte to be used as a subnetwork address. All hosts on the network would still use the IP address to get on the Internet.

Internet Control Message Protocol (ICMP) - the protocol that handles errors and control messages at the IP layer. ICMP is actually a part of the IP protocol layer. It can generate error messages, test packets, and informational messages related to IP.

Internet Engineering Task Force (IETF) - a large, open, international community of network designers, operators, vendors and researchers whose purpose is to coordinate the operation, management and evolution of the Internet to resolve short- and mid-range protocol and architectural issues.

Internet Protocol (IP) - a connectionless, best-effort packet switching protocol that offers a common layer over dissimilar networks.

Internetwork Packet Exchange (IPX) Protocol - a NetWare protocol similar to the Xerox Network Systems (XNS) protocol that provides datagram delivery of messages.

Interoperability - The ability of software and hardware on multiple machines, from multiple vendors, to communicate.

Interworking Function (IWF) - provides a means for two different technologies to interoperate.

IP Address - a unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in “dot” notation (e.g., 192.228.32.14).

IP Netmask - a 32-bit pattern that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in “dot” notation (e.g., 255.255.0.0).

ISA Bus - a bus standard developed by IBM for expansion cards in the first IBM PC. The original bus supported a data path only 8 bits wide. IBM subsequently developed a 16-bit version for its AT class computers. The 16-bit AT ISA bus supports both 8- and 16-bit cards. The 8-bit bus is commonly called the PC/XT bus, and the 16-bit bus is called the AT bus.

Isochronous - signals carrying embedded timing information or signals that are dependent on uniform timing; usually associated with voice and/or video transmission.

International Telecommunications Union Telecommunications (ITU-T) - an international body of member countries whose task is to define recommendations and standards relating to the international telecommunications industry. The fundamental standards for ATM have been defined and published by the ITU-T (Previously CCITT).

J2 - Wide-area digital transmission scheme used predominantly in Japan that carries data at a rate of 6.312 Mbps.

Jitter - analog communication line distortion caused by variations of a signal from its reference timing position.

Joint Photographic Experts Group (JPEG) - An ISO Standards group that defines how to compress still pictures.

Jumper - a patch cable or wire used to establish a circuit, often temporarily, for testing or diagnostics; also, the devices, shorting blocks, used to connect adjacent exposed pins on a printed circuit board that control the functionality of the card.

Kbps - kilobits per second (thousand)

LAN Access Concentrator - a LAN access device that allows a shared transmission medium to accommodate more data sources than there are channels currently available within the transmission medium.

LAN Emulation Address Resolution Protocol (LE_ARP) - A message issued by a LE client to solicit the ATM address of another function.

LAN Emulation Client (LEC) - the component in an end system that performs data forwarding, address resolution, and other control functions when communicating with other components within an ELAN.

LAN Emulation Configuration Server (LECS) - the LECS is responsible for the initial configuration of LECs. It provides information about available ELANs that a LEC may join, together with the addresses of the LES and BUS associated with each ELAN.

LAN Emulation Server (LES) - the LES implements the control coordination function for an ELAN by registering and resolving MAC addresses to ATM addresses.

LAN Emulation (LANE) - technology that allows an ATM network to function as a LAN backbone. The ATM network must provide multicast and broadcast support, address mapping (MAC-to-ATM), SVC management, and a usable packet format. LANE also defines Ethernet and Token Ring ELANs.

lane - a program that provides control over the execution of the LAN Emulation Server (LES), Broadcast/Unknown Server (BUS), and LAN Emulation Configuration Server (LECS) on the local host.

Latency - The time interval between a network station seeking access to a transmission channel and that access being granted or received.

Layer Entity - an active layer within an element.

Layer Function - a part of the activity of the layer entities.

Layer Service - a capability of a layer and the layers beneath it that is provided to the upper layer entities at the boundary between that layer and the next higher layer.

Layer User Data - the information transferred between corresponding entities on behalf of the upper layer or layer management entities for which they are providing services.

le - a FORE program that implements both the LAN Emulation Server (LES) and the Broadcast/Unknown Server (BUS).

Leaky Bucket - informal cell policing term for the Generic Cell Rate Algorithm which in effect receives cells into a bucket and leaks them out at the specified or contracted rate (i.e., PCR).

Least Significant Bit (LSB) - lowest order bit in the binary representation of a numerical value.

lecs - a FORE program that implements the assignment of individual LECs to different emulated LANs.

leq - a FORE program that provides information about an ELAN. This information is obtained from the LES, and includes MAC addresses registered on the ELAN together with their corresponding ATM addresses.

Line Build Out (LBO) - Because T1 circuits require the last span to lose 15-22.5 dB, a selectable output attenuation is generally required of DTE equipment (typical selections include 0.0, 7.5 and 15 dB of loss at 772 KHz).

Line Code Violations (LCV) - Error Event. A Line Coding Violation (LCV) is the occurrence of either a Bipolar Violation (BPV) or Excessive Zeroes (EXZ) Error Event.

Link - An entity that defines a topological relationship (including available transport capacity) between two nodes in different subnetworks. Multiple links may exist between a pair of subnetworks. Synonymous with logical link.

Link Access Procedure, Balanced (LAPB) - Data link protocol in the X.25 protocol stack. LAPB is a bit-oriented protocol derived from HDLC. See also HDLC and X.25.

Link Down Trap - an SNMP trap, sent when an interface changes from a normal state to an error state, or is disconnected.

Link Layer - layer in the OSI model regarding transmission of data between network nodes.

Link Up Trap - an SNMP trap, sent when an interface changes from an error condition to a normal state.

Load Sharing - Two or more computers in a system that share the load during peak hours. During periods of non peak hours, one computer can manage the entire load with the other acting as a backup.

Local Access and Transport Area (LATA) - Geographic boundaries of the local telephone network, specified by the FCC, in which a single LEC may perform its operations. Communications outside or between LATAs are provided by IXCs.

Local Area Network (LAN) - a data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit higher data rates.

Logical Link Control (LLC) - protocol developed by the IEEE 802 committee for data-link-layer transmission control; the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the MAC protocol; IEEE standard 802.2; includes end-system addressing and error checking.

Loopback - a troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

looptest - program that tests an interface for basic cell reception and transmission functionality, usually used for diagnostic purposes to determine if an interface is functioning properly.

Loss Of Frame (LOF) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Pointer (LOP) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Signal (LOS) - a type of transmission error that may occur in wide-area carrier lines, or a condition declared when the DTE senses a loss of a DS1 signal from the CPE for more the 150 milliseconds (the DTE generally responds with an all ones “Blue or AIS” signal).

Management Information Base (MIB) - the set of parameters that an SNMP management station can query or set in the SNMP agent of a networked device (e.g., router).

Maximum Burst Size (MBS) - the Burst Tolerance (BT) is conveyed through the MBS which is coded as a number of cells. The BT together with the SCR and the GCRA determine the MBS that may be transmitted at the peak rate and still be in conformance with the GCRA.

Maximum Burst Tolerance - the largest burst of data that a network device is guaranteed to handle without discarding cells or packets. Bursts of data larger than the maximum burst size may be subject to discard.

Maximum Cell Delay Variance (MCDV) - This is the maximum two-point CDV objective across a link or node for the specified service category.

Maximum Cell Loss Ratio (MCLR) - This is the maximum ratio of the number of cells that do not make it across the link or node to the total number of cells arriving at the link or node.

Maximum Cell Transfer Delay (MCTD) - This is the sum of the fixed delay component across the link or node and MCDV.

Maximum Transmission Unit (MTU) - the largest unit of data that can be sent over a type of physical medium.

Mbps - megabits per second (million)

Media Access Control (MAC) - a media-specific access control protocol within IEEE 802 specifications; currently includes variations for Token Ring, token bus, and CSMA/CD; the lower sublayer of the IEEE’s link layer (OSI), which complements the Logical Link Control (LLC).

Media Attachment Unit (MAU) - device used in Ethernet and IEEE 802.3 networks that provides the interface between the AUI port of a station and the common medium of the Ethernet. The MAU, which can be built into a station or can be a separate device, performs physical layer functions including conversion of the digital data from the Ethernet interface, collision detection, and injection of bits onto the network.

Media Interface Connector (MIC) - fiber optic connector that joins fiber to the FDDI controller.

Message Identifier (MID) - message identifier used to associate ATM cells that carry segments from the same higher layer packet.

Metasignalling - an ATM Layer Management (LM) process that manages different types of signalling and possibly semipermanent virtual channels (VCs), including the assignment, removal, and checking of VCs.

Metasignalling VCs - the standardized VCs that convey metasignalling information across a User-to-Network Interface (UNI).

Metropolitan Area Network (MAN) - network designed to carry data over an area larger than a campus such as an entire city and its outlying area.

MicroChannel - a proprietary 16- or 32-bit bus developed by IBM for its PS/2 computers' internal expansion cards; also offered by others.

Minimum Cell Rate (MCR) - parameter defined by the ATM Forum for ATM traffic management, defined only for ABR transmissions and specifying the minimum value for the ACR.

Most Significant Bit (MSB) - highest order bit in the binary representation of a numerical value.

Motion Picture Experts Group (MPEG) - ISO group dealing with video and audio compression techniques and mechanisms for multiplexing and synchronizing various media streams.

MPOA Client - A device which implements the client side of one or more of the MPOA protocols, (i.e., is a SCP client and/or an RDP client. An MPOA Client is either an Edge Device Functional Group (EDFG) or a Host Behavior Functional Group (HBFG).

MPOA Server - An MPOA Server is any one of an ICFG or RSFG.

MPOA Service Area - The collection of server functions and their clients. A collection of physical devices consisting of an MPOA server plus the set of clients served by that server.

MPOA Target - A set of protocol address, path attributes, (e.g., internetwork layer QoS, other information derivable from received packet) describing the intended destination and its path attributes that MPOA devices may use as lookup keys.

Mu-Law - The PCM coding and companding standard used in Japan and North America.

Multicasting - The ability to broadcast messages to one node or a select group of nodes.

Multi-homed - a device having both an ATM and another network connection, like Ethernet.

Multimode Fiber Optic Cable (MMF) - fiber optic cable in which the signal or light propagates in multiple modes or paths. Since these paths may have varying lengths, a transmitted pulse of light may be received at different times and smeared to the point that pulses may interfere with surrounding pulses. This may cause the signal to be difficult or impossible to receive. This pulse dispersion sometimes limits the distance over which a MMF link can operate.

Multiplexing - a function within a layer that interleaves the information from multiple connections into one connection (see demultiplexing).

Multipoint Access - user access in which more than one terminal equipment (TE) is supported by a single network termination.

Multipoint-to-Multipoint Connection - a collection of associated ATM VC or VP links, and their associated endpoint nodes, with the following properties:

1. All N nodes in the connection, called Endpoints, serve as a Root Node in a Point-to-Multipoint connection to all of the (N-1) remaining endpoints.
2. Each of the endpoints can send information directly to any other endpoint, but the receiving endpoint cannot distinguish which of the endpoints is sending information without additional (e.g., higher layer) information.

Multipoint-to-Point Connection - a Point-to-Multipoint Connection may have zero bandwidth from the Root Node to the Leaf Nodes, and non-zero return bandwidth from the Leaf Nodes to the Root Node. Such a connection is also known as a Multipoint-to-Point Connection.

Multiprotocol over ATM (MPOA) - An effort taking place in the ATM Forum to standardize protocols for the purpose of running multiple network layer protocols over ATM.

Narrowband Channel - sub-voicegrade channel with a speed range of 100 to 200 bps.

National TV Standards Committee (NTSC) - Started in the US in 1953 from a specification laid down by the National Television Standards Committee. It takes the B-Y and R-Y color difference signals, attenuates them to I and Q, then modulates them using double-sideband suppressed subcarrier at 3.58MHz. The carrier reference is sent to the receiver as a burst during the back porch. An industry group that defines how television signals are encoded and transmitted in the US. (See also PAL, SECAM for non-U.S. countries).

Near-End - in a relationship between two devices in a circuit, the near-end device is the one that is local.

Network Layer - Layer three In the OSI model, the layer that is responsible for routing data across the network.

Network Management Entity (NM) - body of software in a switching system that provides the ability to manage the PNNI protocol. NM interacts with the PNNI protocol through the MIB.

Network Management Layer (NML) - an abstraction of the functions provided by systems which manage network elements on a collective basis, providing end-to-end network monitoring.

Network Management Station (NMS) - system responsible for managing a network or portion of a network by talking to network management agents, which reside in the managed nodes.

Network Module - ATM port interface cards which may be individually added to or removed from any *ForeRunner* or TNX ATM switch to provide a diverse choice of connection alternatives. Network modules in an ASX-4000 ATM switch are referred to as port cards.

Network Parameter Control (NPC) - Defined as the set of actions taken by the network to monitor and control traffic from the NNI. Its main purpose is to protect network resources from malicious as well as unintentional misbehavior which can affect the QoS of other already established connections by detecting violations of negotiated parameters and taking appropriate actions. Refer to UPC.

Network Redundancy - Duplicated network equipment and/or data which can provide a backup in case of network failures.

Network Service Access Point (NSAP) - OSI generic standard for a network address consisting of 20 octets. ATM has specified E.164 for public network addressing and the NSAP address structure for private network addresses.

Network-to-Network Interface or Network Node Interface (NNI) - the interface between two public network pieces of equipment.

Node - A computer or other device when considered as part of a network.

Non Return to Zero (NRZ) - a binary encoding scheme in which ones and zeroes are represented by opposite and alternating high and low voltages and where there is no return to a zero (reference) voltage between encoded bits.

Non Return to Zero Inverted (NRZI) - A binary encoding scheme that inverts the signal on a “1” and leaves the signal unchanged for a “0”. (Also called transition encoding.)

Nonvolatile Storage - Memory storage that does not lose its contents when power is turned off.

NuBus - a high-speed bus used in Macintosh computers, structured so users can put a card into any slot on the board without creating conflict over the priority between those cards.

nx64K - This refers to a circuit bandwidth or speed provided by the aggregation of nx64 kbps channels (where n= integer > 1). The 64K or DS0 channel is the basic rate provided by the T Carrier systems.

Nyquist Theorem - In communications theory, a formula stating that two samples per cycle is sufficient to characterize a bandwidth limited analog signal; in other words, the sampling rate must be twice the highest frequency component of the signal (i.e., sample 4 KHz analog voice channels 8000 times per second).

Object Identifier (OID) - the address of a MIB variable.

Octet - a grouping of 8 bits; similar, but not identical to, a byte.

One’s Density - The requirement for digital transmission lines in the public switched telephone network that eight consecutive “0”s cannot be in a digital data stream; exists because repeaters and clocking devices within the network will lose timing after receiving eight “0”s in a row; a number of techniques are used to insert a “1” after every seventh-consecutive “0” (see Bit Stuffing).

Open Shortest Path First (OSPF) Protocol - a routing algorithm for IP that incorporates least-cost, equal-cost, and load balancing.

Open Systems Interconnection (OSI) - the 7-layer suite of protocols designed by ISO committees to be the international standard computer network architecture.

OpenView - Hewlett-Packard's network management software.

Operation and Maintenance (OAM) Cell - a cell that contains ATM LM information. It does not form part of the upper layer information transfer.

Optical Carrier level-n (OC-n) - The optical counterpart of STS-n (the basic rate of 51.84 Mbps on which SONET is based is referred to as OC-1 or STS-1).

Organizationally Unique Identifier (OUI) - Part of RFC 1483. A three-octet field in the SubNetwork Attachment Point (SNAP) header, identifying an organization which administers the meaning of the following two octet Protocol Identifier (PID) field in the SNAP header. Together they identify a distinct routed or bridged protocol.

Out-of-Band Management - refers to switch configuration via the serial port or over Ethernet, not ATM.

Out-of-Frame (OOF) - a signal condition and alarm in which some or all framing bits are lost.

Packet - An arbitrary collection of data grouped and transmitted with its user identification over a shared facility.

Packet Assembler Disassembler (PAD) - interface device that buffers data sent to/from character mode devices, and assembles and disassembles the packets needed for X.25 operation.

Packet Internet Groper (ping) - a program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply.

Packet Level Protocol (PLP) - Network layer protocol in the X.25 protocol stack. Sometimes called X.25 Level 3 or X.25 Protocol.

Packet Switched Network (PSN) - a network designed to carry data in the form of packets. The packet and its format is internal to that network.

Packet Switching - a communications paradigm in which packets (messages) are individually routed between hosts with no previously established communications path.

Payload Scrambling - a technique that eliminates certain bit patterns that may occur within an ATM cell payload that could be misinterpreted by certain sensitive transmission equipment as an alarm condition.

Payload Type (PT) - bits 2...4 in the fourth byte of an ATM cell header. The PT indicates the type of information carried by the cell. At this time, values 0...3 are used to identify various types of user data, values 4 and 5 indicate management information, and values 6 and 7 are reserved for future use.

Peak Cell Rate - at the PHY Layer SAP of a point-to-point VCC, the Peak Cell Rate is the inverse of the minimum inter-arrival time T0 of the request to send an ATM-SDU.

Peak Cell Rate (PCR) - parameter defined by the ATM Forum for ATM traffic management. In CBR transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR.

Peer Entities - entities within the same layer.

Peripheral Component Interconnect (PCI) - a local-bus standard created by Intel.

Permanent Virtual Channel Connection (PVCC) - A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell. A Permanent VCC is one which is provisioned through some network management function and left up indefinitely.

Permanent Virtual Circuit (or Channel) (PVC) - a circuit or channel through an ATM network provisioned by a carrier between two endpoints; used for dedicated long-term information transport between locations.

Permanent Virtual Path Connection (PVPC) - A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell. A PVPC is one which is provisioned through some network management function and left up indefinitely.

Phase Alternate Line (PAL) - Largely a German/British development in the late 60s, used in the UK and much of Europe. The B-Y and R-Y signals are weighted to U and V, then modulated onto a double-sideband suppressed subcarrier at 4.43MHz. The V (R-Y) signal's phase is turned through 180 degrees on each alternate line. This gets rid of NTSC’s hue changes with phase errors at the expense of de-saturation. The carrier reference is sent as a burst in the back porch. The phase of the burst is alternated every line to convey the phase switching of the V signal. The burst's average phase is -V. (see NTSC for U.S.).

Physical Layer (PHY) - the actual cards, wires, and/or fiber-optic cabling used to connect computers, routers, and switches.

Physical Layer Connection - an association established by the PHY between two or more ATM-entities. A PHY connection consists of the concatenation of PHY links in order to provide an end-to-end transfer capability to PHY SAPs.

Physical Layer Convergence Protocol (PLCP) - a framing protocol that runs on top of the T1 or E1 framing protocol.

Physical Medium (PM) - Refers to the actual physical interfaces. Several interfaces are defined including STS-1, STS-3c, STS-12c, STM-1, STM-4, DS1, E1, DS2, E3, DS3, E4, FDDI-based, Fiber Channel-based, and STP. These range in speeds from 1.544Mbps through 622.08 Mbps.

Physical Medium Dependent (PMD) - a sublayer concerned with the bit transfer between two network nodes. It deals with wave shapes, timing recovery, line coding, and electro-optic conversions for fiber based links.

Plesiochronous - two signals are plesiochronous if their corresponding significant instants occur at nominally the same rate, with variations in rate constrained to specified limits.

Point of Demarcation - the dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.

Point-to-Multipoint Connection - a collection of associated ATM VC or VP links, with associated endpoint 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 is sending information without additional (higher layer) information. (See the following note for Phase 1.)

3. The Leaf Nodes cannot communicate directly to each other with this connection type.

Note: Phase 1 signalling does not support traffic sent from a Leaf to the Root.

Point-to-Point Connection - a connection with only two endpoints.

Point-to-Point Protocol (PPP) - Provides a method for transmitting packets over serial point-to-point links.

Policing - the function that ensures that a network device does not accept traffic that exceeds the configured bandwidth of a connection.

Port Card - ATM port interface cards which may be individually added to or removed from the ASX-4000 ATM switch to provide a diverse choice of connection alternatives. Port cards are referred to as network modules for the ASX-200WG, ASX-200BX, ASX-1000, LE155, and LE25 switches.

Port Identifier - The identifier assigned by a logical node to represent the point of attachment of a link to that node.

Presentation Layer - Sixth layer of the OSI model, providing services to the application layer.

Primary Reference Source (PRS) - Equipment that provides a timing signal whose long-term accuracy is maintained at 1 x 10 -11 or better with verification to universal coordinated time (UTC) and whose timing signal is used as the basis of reference for the control of other clocks within a network.

Primitive - an abstract, implementation-independent interaction between a layer service user and a layer service provider.

Priority - the parameter of ATM connections that determines the order in which they are reduced from the peak cell rate to the sustained cell rate in times of congestion. Connections with lower priority (4 is low, 1 is high) are reduced first.

Private Branch Exchange (PBX) - a private phone system (switch) that connects to the public telephone network and offers in-house connectivity. To reach an outside line, the user must dial a digit like 8 or 9.

Private Network Node Interface or Private Network-to-Network Interface (PNNI) - a protocol that defines the interaction of private ATM switches or groups of private ATM switches

Programmable Read-Only Memory (PROM) - a chip-based information storage area that can be recorded by an operator but erased only through a physical process.

Protocol - a set of rules and formats (semantic and syntactic) that determines the communication behavior of layer entities in the performance of the layer functions.

Protocol Control Information - the information exchanged between corresponding entities using a lower layer connection to coordinate their joint operation.

Protocol Data Unit (PDU) - a unit of data specified in a layer protocol and consisting of protocol control information and layer user data.

Proxy - the process in which one system acts for another system to answer protocol requests.

Proxy Agent - an agent that queries on behalf of the manager, used to monitor objects that are not directly manageable.

Public Data Network (PDN) - a network designed primarily for data transmission and intended for sharing by many users from many organizations.

Pulse Code Modulation (PCM) - a modulation scheme that samples the information signals and transmits a series of coded pulses to represent the data.

Q.2931 - Derived from Q.93B, the narrowband ISDN signalling protocol, an ITU standard describing the signalling protocol to be used by switched virtual circuits on ATM LANs.

Quality of Service (QoS) - Quality of Service is defined on an end-to-end basis in terms of the following attributes of the end-to-end ATM connection:

Cell Loss Ratio
Cell Transfer Delay
Cell Delay Variation

Queuing Delay (QD) - refers to the delay imposed on a cell by its having to be buffered because of unavailability of resources to pass the cell onto the next network function or element. This buffering could be a result of oversubscription of a physical link, or due to a connection of higher priority or tighter service constraints getting the resource of the physical link.

Radio Frequency Interference (RFI) - the unintentional transmission of radio signals. Computer equipment and wiring can both generate and receive RFI.

Real-Time Clock - a clock that maintains the time of day, in contrast to a clock that is used to time the electrical pulses on a circuit.

Red Alarm - In T1, a red alarm is generated for a locally detected failure such as when a condition like OOF exists for 2.5 seconds, causing a CGA, (Carrier Group Alarm).

Reduced Instruction Set Computer (RISC) - a generic name for CPUs that use a simpler instruction set than more traditional designs.

Redundancy - In a data transmission, the fragments of characters and bits that can be eliminated with no loss of information.

Registration - The address registration function is the mechanism by which Clients provide address information to the LAN Emulation Server.

Relaying - a function of a layer by means of which a layer entity receives data from a corresponding entity and transmits it to another corresponding entity.

Request To Send (RTS) - an RS-232 modem interface signal (sent from the DTE to the modem on pin 4) which indicates that the DTE has data to transmit.

Requests For Comment (RFCs) - IETF documents suggesting protocols and policies of the Internet, inviting comments as to the quality and validity of those policies. These comments are collected and analyzed by the IETF in order to finalize Internet standards.

RFC1483 - Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC1490 - Multiprotocol Interconnect over Frame Relay.
RFC1577 - Classical IP and ARP over ATM.
RFC1755 - ATM Signaling Support for IP over ATM.

Robbed-Bit Signaling - In T1, refers to the use of the least significant bit of every word of frames 6 and 12 (D4), or 6, 12, 18, and 24 (ESF) for signaling purposes.

Route Server - A physical device that runs one or more network layer routing protocols, and which uses a route query protocol in order to provide network layer routing forwarding descriptions to clients.

Router - a device that forwards traffic between networks or subnetworks based on network layer information.

Routing Domain (RD) - A group of topologically contiguous systems which are running one instance of routing.

Routing Information Protocol (RIP) - a distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

Routing Protocol - A general term indicating a protocol run between routers and/or route servers in order to exchange information used to allow computation of routes. The result of the routing computation will be one or more forwarding descriptions.

SBus - hardware interface for add-in boards in later-version Sun 3 workstations.

Scalable Processor Architecture Reduced instruction set Computer (SPARC) - a powerful workstation similar to a reduced-instruction-set-computing (RISC) workstation.

Segment - a single ATM link or group of interconnected ATM links of an ATM connection.

Segmentation And Reassembly (SAR) - the SAR accepts PDUs from the CS and divides them into very small segments (44 bytes long). If the CS-PDU is less than 44 bytes, it is padded to 44 with zeroes. A two-byte header and trailer are added to this basic segment. The header identifies the message type (beginning, end, continuation, or single) and contains sequence numbering and message identification. The trailer gives the SAR-PDU payload length, exclusive of pad, and contains a CRC check to ensure the SAR-PDU integrity. The result is a 48-byte PDU that fits into the payload field of an ATM cell.

Selector (SEL) - A subfield carried in SETUP message part of ATM endpoint address Domain specific Part (DSP) defined by ISO 10589, not used for ATM network routing, used by ATM end systems only.

Semipermanent Connection - a connection established via a service order or via network management.

Serial Line IP (SLIP) - A protocol used to run IP over serial lines, such as telephone circuits or RS-232 cables, interconnecting two systems.

Service Access Point (SAP) - the point at which an entity of a layer provides services to its LM entity or to an entity of the next higher layer.

Service Data Unit (SDU) - a unit of interface information whose identity is preserved from one end of a layer connection to the other.

Service Specific Connection Oriented Protocol (SSCOP) - an adaptation layer protocol defined in ITU-T Specification: Q.2110.

Service Specific Convergence Sublayer (SSCS) - The portion of the convergence sublayer that is dependent upon the type of traffic that is being converted.

Session Layer - Layer 5 in the OSI model that is responsible for establishing and managing sessions between the application programs running in different nodes.

Severely Errored Seconds (SES) - a second during which more event errors have occurred than the SES threshold (normally 10-3).

Shaping Descriptor - *n* ordered pairs of GCRA parameters (I,L) used to define the negotiated traffic shape of an APP connection. The traffic shape refers to the load-balancing of a network, where load-balancing means configuring data flows to maximize network efficiency.

Shielded Pair - Two insulated wires in a cable wrapped with metallic braid or foil to prevent interference and provide noise free transmission.

Shielded Twisted Pair (STP) - two or more insulated wires, twisted together and then wrapped in a cable with metallic braid or foil to prevent interference and offer noise-free transmissions.

Signaling System No. 7 (SS7) - The SS7 protocol has been specified by ITU-T and is a protocol for interexchange signaling.

Simple and Efficient Adaptation Layer (SEAL) - also called AAL 5, this ATM adaptation layer assumes that higher layer processes will provide error recovery, thereby simplifying the SAR portion of the adaptation layer. Using this AAL type packs all 48 bytes of an ATM cell information field with data. It also assumes that only one message is crossing the UNI at a time. That is, multiple end-users at one location cannot interleave messages on the same VC, but must queue them for sequential transmission.

Simple Gateway Management Protocol (SGMP) - the predecessor to SNMP.

Simple Mail Transfer Protocol (SMTP) - the Internet electronic mail protocol used to transfer electronic mail between hosts.

Simple Network Management Protocol (SNMP) - the Internet standard protocol for managing nodes on an IP network.

Simple Protocol for ATM Network Signalling (SPANS) - FORE Systems' proprietary signalling protocol used for establishing SVCs between FORE Systems equipment.

Single Mode Fiber (SMF) - Fiber optic cable in which the signal or light propagates in a single mode or path. Since all light follows the same path or travels the same distance, a transmitted pulse is not dispersed and does not interfere with adjacent pulses. SMF fibers can support longer distances and are limited mainly by the amount of attenuation. Refer to MMF.

Small Computer Systems Interface (SCSI) - a standard for a controller bus that connects hardware devices to their controllers on a computer bus, typically used in small systems.

Smart PVC (SPVC) - a generic term for any communications medium which is permanently provisioned at the end points, but switched in the middle. In ATM, there are two kinds of SPVCs: smart permanent virtual path connections (SPVPCs) and smart permanent virtual channel connections (SPVCCs).

snmpd - an SMNP agent for a given adapter card.

Source - Part of communications system which transmits information.

Source Address (SA) - The address from which the message or data originated.

Source MAC Address (SA) - A six octet value uniquely identifying an end point and which is sent in an IEEE LAN frame header to indicate source of frame.

Source Traffic Descriptor - a set of traffic parameters belonging to the ATM Traffic Descriptor used during the connection set-up to capture the intrinsic traffic characteristics of the connection requested by the source.

Spanning Tree Protocol - provides loop-free topology in a network environment where there are redundant paths.

Static Route - a route that is entered manually into the routing table.

Statistical Multiplexing - a technique for allowing multiple channels and paths to share the same link, typified by the ability to give the bandwidth of a temporarily idle channel to another channel.

Stick and Click (SC) - Designation for an Optical Connector featuring a 2.5 mm physically contacting ferrule with a push-pull mating design. Commonly referred to as Structured Cabling, Structured Connectors or Stick and Click

Stick and Turn (ST) - A fiber-optic connector designed by AT&T which uses the bayonet style coupling rather than screw-on as the SMA uses. The ST is generally considered the eventual replacement for the SMA type connector.

Store-and-Forward - the technique of receiving a message, storing it until the proper outgoing line is available, then retransmitting it, with no direct connection between incoming and outgoing lines.

Straight Tip (ST) - see *Stick and Turn*.

Structured Cabling (SC) - see *Stick and Click*.

Structured Connectors (SC) - see *Stick and Click*.

Sublayer - a logical subdivision of a layer.

SubNetwork Access Protocol (SNAP) - a specially reserved variant of IEEE 802.2 encoding SNAP indicates to look further into the packet where it will fine a Type field.

Subscriber Network Interface (SNI) - the interface between an SMDS end user’s CPE and the network directly serving the end user, supported by either a DS1 or DS3 access arrangement.

Super Frame (SF) - a term used to describe the repeating 12 D4 frame format that composes a standard (non-ESF) T1 service.

Super User - a login ID that allows unlimited access to the full range of a device's functionality, including especially the ability to reconfigure the device and set passwords.

Sustainable Cell Rate (SCR) - ATM Forum parameter defined for traffic management. For VBR connections, SCR determines the long-term average cell rate that can be transmitted.

Sustained Information Rate (SIR) - In ATM this refers to the long-term average data transmission rate across the User-to-Network Interface. In SMDS this refers to the committed information rate (similar to CIR for Frame Relay Service).

Switch - Equipment used to interconnect lines and trunks.

Switched Connection - A connection established via signaling.

Switched Multimegabit Data Service (SMDS) - a high-speed, datagram-based, public data network service expected to be widely used by telephone companies in their data networks.

Switched Virtual Channel Connection (SVCC) - A Switched VCC is one which is established and taken down dynamically through control signaling. A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell.

Switched Virtual Circuit (or Channel) (SVC) - a channel established on demand by network signalling, used for information transport between two locations and lasting only for the duration of the transfer; the datacom equivalent of a dialed telephone call.

Switched Virtual Path Connection (SVPC) - a connection which is established and taken down dynamically through control signaling. A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell.

Switching System - A set of one or more systems that act together and appear as a single switch for the purposes of PNNI routing.

Symmetric Connection - a connection with the same bandwidth specified for both directions.

Synchronous - signals that are sourced from the same timing reference and hence are identical in frequency.

Synchronous Data Link Control (SDLC) - IBM's data link protocol used in SNA networks.

Synchronous Optical Network (SONET) - a body of standards that defines all aspects of transporting and managing digital traffic over optical facilities in the public network.

Synchronous Payload Envelope (SPE) - the payload field plus a little overhead of a basic SONET signal.

Synchronous Transfer Mode (STM) - a transport and switching method that depends on information occurring in regular, fixed patterns with respect to a reference such as a frame pattern.

Synchronous Transport Signal (STS) - a SONET electrical signal rate.

Systeme En Coleur Avec Memoire (SECAM) - Sequential and Memory Color Television - Started in France in the late 60s, and used by other countries with a political affiliation. This is. The B-Y and R-Y signals are transmitted on alternate lines modulated on an FM subcarrier. The memory is a one line delay line in the receiver to make both color difference signals available at the same time on all lines. Due to FM, the signal is robust in difficult terrain.

Systems Network Architecture (SNA) - a proprietary networking architecture used by IBM and IBM-compatible mainframe computers.

T1 - a specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term “T1” is used interchangeably with “DS1.”

T1 Link - A wideband digital carrier facility used for transmission of digitized voice, digital data, and digitized image traffic. This link is composed of two twisted-wire pairs that can carry 24 digital channels, each operating at 64K bps at the aggregate rate of 1.544M bps, full duplex. Also referred to as DS-1.

T3 - a specification for a transmission line, the equivalent of 28 T1 lines. T3 lines run at 44.736 Mbps. In common usage, the term “T3” is used interchangeably with “DS3.”

Tachometer - in *ForeView*, the tachometer shows the level of activity on a given port. The number in the tachometer shows the value of a chosen parameter in percentage, with a colored bar providing a semi-logarithmic representation of that percentage.

Tagged Cell Rate (TCR) - An ABR service parameter, TCR limits the rate at which a source may send out-of-rate forward RM-cells. TCR is a constant fixed at 10 cells/second.

Telephony - The conversion of voices and other sounds into electrical signals which are then transmitted by telecommunications media.

Telnet - a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections.

Terminal Equipment (TE) - Terminal equipment represents the endpoint of ATM connection(s) and termination of the various protocols within the connection(s).

Throughput - Measurement of the total useful information processed or communicated by a computer during a specified time period, i.e. packets per second.

Time Division Multiplexing (TDM) - a method of traditional digital multiplexing in which a signal occupies a fixed, repetitive time slot within a higher-rate signal.

Token Ring - a network access method in which the stations circulate a token. Stations with data to send must have the token to transmit their data.

topology - a program that displays the topology of a FORE Systems ATM network. An updated topology can be periodically re-displayed by use of the interval command option.

Traffic - the calls being sent and received over a communications network. Also, the packets that are sent on a data network.

Traffic Management (TM) - The traffic control and congestion control procedures for ATM. ATM layer traffic control refers to the set of actions taken by the network to avoid congestion conditions. ATM layer congestion control refers to the set of actions taken by the network to minimize the intensity, spread and duration of congestion. The following functions form a framework for managing and controlling traffic and congestion in ATM networks and may be used in appropriate combinations:

Connection Admission Control
Feedback Control
Usage Parameter Control
Priority Control
Traffic Shaping
Network Resource Management
Frame Discard
ABR Flow Control

Traffic Parameter - A parameter for specifying a particular traffic aspect of a connection.

Trailer - the protocol control information located at the end of a PDU.

Transit Delay - the time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

Transmission Control Protocol (TCP) - a specification for software that bundles and unbundles sent and received data into packets, manages the transmission of packets on a network, and checks for errors.

Transmission Control Protocol/Internet Protocol (TCP/IP) - a set of communications protocols that has evolved since the late 1970s, when it was first developed by the Department of Defense. Because programs supporting these protocols are available on so many different computer systems, they have become an excellent way to connect different types of computers over networks.

Transmission Convergence (TC) - generates and receives transmission frames and is responsible for all overhead associated with the transmission frame. The TC sublayer packages cells into the transmission frame.

Transmission Convergence Sublayer (TCS) - This is part of the ATM physical layer that defines how cells will be transmitted by the actual physical layer.

Transparent Asynchronous Transmitter/Receiver Interface (TAXI) - Encoding scheme used for FDDI LANs as well as for ATM; supports speed typical of 100 Mbps over multimode fiber.

Transport Layer - Layer Four of the OSI reference model that is responsible for maintaining reliable end-to-end communications across the network.

Trap - a program interrupt mechanism that automatically updates the state of the network to remote network management hosts. The SNMP agent on the switch supports these SNMP traps.

Trivial File Transfer Protocol (TFTP) - Part of IP, a simplified version of FTP that allows files to be transferred from one computer to another over a network.

Twisted Pair - Insulated wire in which pairs are twisted together. Commonly used for telephone connections, and LANs because it is inexpensive.

Unassigned Cells - a generated cell identified by a standardized virtual path identifier (VPI) and virtual channel identifier (VCI) value, which does not carry information from an application using the ATM Layer service.

Unavailable Seconds (UAS) - a measurement of signal quality. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.

UNI 3.0/3.1 - the User-to-Network Interface standard set forth by the ATM Forum that defines how private customer premise equipment interacts with private ATM switches.

Unicasting - The transmit operation of a single PDU by a source interface where the PDU reaches a single destination.

Universal Test & Operations Interface for ATM (UTOPIA) - Refers to an electrical interface between the TC and PMD sublayers of the PHY layer.

Unshielded Twisted Pair (UTP) - a cable that consists of two or more insulated conductors in which each pair of conductors are twisted around each other. There is no external protection and noise resistance comes solely from the twists.

Unspecified Bit Rate (UBR) - a type of traffic that is not considered time-critical (e.g., ARP messages, pure data), allocated whatever bandwidth is available at any given time. UBR traffic is given a "best effort" priority in an ATM network with no guarantee of successful transmission.

Uplink - Represents the connectivity from a border node to an upnode.

Usage Parameter Control (UPC) - mechanism that ensures that traffic on a given connection does not exceed the contracted bandwidth of the connection, responsible for policing or enforcement. UPC is sometimes confused with congestion management (see *congestion management*).

User Datagram Protocol (UDP) - the TCP/IP transaction protocol used for applications such as remote network management and name-service access; this lets users assign a name, such as "RVAX*2,S," to a physical or numbered address.

User-to-Network Interface (UNI) - the physical and electrical demarcation point between the user and the public network service provider.

V.35 - ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe, and is recommended for speeds up to 48 Kbps.

Variable Bit Rate (VBR) - a type of traffic that, when sent over a network, is tolerant of delays and changes in the amount of bandwidth it is allocated (e.g., data applications).

Virtual Channel (or Circuit) (VC) - a communications path between two nodes identified by label rather than fixed physical path.

Virtual Channel Connection (VCC) - a unidirectional concatenation of VCLs that extends between the points where the ATM service users access the ATM Layer. The points at which the ATM cell payload is passed to, or received from, the users of the ATM Layer (i.e., a higher layer or ATMM-entity) for processing signify the endpoints of a VCC.

Virtual Channel Identifier (VCI) - the address or label of a VC; a value stored in a field in the ATM cell header that identifies an individual virtual channel to which the cell belongs. VCI values may be different for each data link hop of an ATM virtual connection.

Virtual Channel Link (VCL) - a means of unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed.

Virtual Channel Switch - a network element that connects VCLs. It terminates VPCs and translates VCI values. The Virtual Channel Switch is directed by Control Plane functions and relays the cells of a VC.

Virtual Connection - an endpoint-to-endpoint connection in an ATM network. A virtual connection can be either a virtual path or a virtual channel.

Virtual Local Area Network (VLAN) - Work stations connected to an intelligent device which provides the capabilities to define LAN membership.

Virtual Network Software (VINES) - Banyan's network operating system based on UNIX and its protocols.

Virtual Path (VP) - a unidirectional logical association or bundle of VCs.

Virtual Path Connection (VPC) - a concatenation of VPLs between virtual path terminators (VPTs). VPCs are unidirectional.

Virtual Path Identifier (VPI) - the address or label of a particular VP; a value stored in a field in the ATM cell header that identifies an individual virtual path to which the cell belongs. A virtual path may comprise multiple virtual channels.

Virtual Path Link (VPL) - a means of unidirectional transport of ATM cells between the point where a VPI value is assigned and the point where that value is translated or removed.

Virtual Path Switch - a network element that connects VPLs, it translates VPI (not VCI) values and is directed by Control Plane functions. The Virtual Path Switch relays the cells of a Virtual Path.

Virtual Path Terminator (VPT) - a system that unbundles the VCs of a VP for independent processing of each VC.

Virtual Private Data Network (VPDN) - a private data communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Private Network (VPN) - a private voice communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Source/Virtual Destination (VS/VD) - An ABR connection may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. A virtual source implements the behavior of an ABR source endpoint. Backwards RM-cells received by a virtual source are removed from the connection. Each ABR control segment, except the last, is terminated by a virtual destination. A virtual destination assumes the behavior of an ABR destination endpoint. Forward RM-cells received by a virtual destination are turned around and not forwarded to the next segment of the connection.

Virtual Tributary (VT) - a structure used to carry payloads such as DS1s that run at significantly lower rates than STS-1s.

Warm Start Trap - an SNMP trap which indicates that SNMP alarm messages or agents have been enabled.

Wide-Area Network (WAN) - a network that covers a large geographic area.

Wideband Channel - Communications channel with more capacity (19.2K bps) than the standard capacity of a voice grade line.

X.21 - ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

X.25 - a well-established data switching and transport method that relies on a significant amount of processing to ensure reliable transport over metallic media.

Yellow Alarm - An alarm signal sent back toward the source of a failed signal due to the presence of an AIS (may be used by APS equipment to initiate switching).

Zero Byte Time Slot Interchange (ZBTSI) - A technique used with the T carrier extended superframe format (ESF) in which an area in the ESF frame carries information about the location of all-zero bytes (eight consecutive “0”s) within the data stream.

Zero Code Suppression - The insertion of a “1” bit to prevent the transmission of eight or more consecutive “0” bits. Used primarily with T1 and related digital telephone company facilities, which require a minimum “1’s density” in order to keep the individual subchannels of a multiplexed, high speed facility active.

Zero-Bit Insertion - A technique used to achieve transparency in bit-oriented protocols. A zero is inserted into sequences of one bits that cause false flag direction.

Index

T

U

V