Avaya

User's Guide

Avaya M770 Multifunction Switch
ATM Switch

Software Version 2.3

Catalog No. 130075 Rev.C: October, 2001

Contents

List of Commands in the Command-line Interface

Note: Commands marked ’ * ’ are available in the Master Agent module only.

Chapter 1

Introduction

This chapter provides information about the Avaya M770 ATM Switch, and the features that this software release supports.

Note: This User Guide describes only the ATM functionality of the Avaya M770 chassis.

- Information about the Avaya M770 chassis' safety considerations, architecture, main chassis control panel, M-SPV/M-SPX/M-SPS supervisor modules, power supplies and fans is available in the Avaya M770 User Guide.
- Detailed information about the 10M/100M/1Gigabit Ethernet, M-SPV/M-SPX/M-SPS supervisor, and M-MLS multilayer module can be found in their respective Installation Guides

About the Avaya M770 ATM Switch

The M770 ATM switch is a high-performance distributed Asynchronous Transfer Mode (ATM) switch that is designed for building and campus backbone applications, high-performance centralized servers, and power-user environments. Its advanced architecture can support very high traffic loads with no data loss or breaks in communication. The M770 ATM Switch also implements LAN Emulation (LANE) components. LANE enables legacy LAN applications to use a transparent ATM transport medium. In this way, end-stations on existing LANs can communicate with ATM end-stations.

The M770 ATM Switch supports a range of option modules that enable you to customize the switch to fulfil applications that are appropriate to your networking requirements. It is designed as a software-upgradeable product. Therefore, you can expand the functionality of the switch by downloading new software.

Master Agent and Sub Agent

The M770 ATM Switch is a fully distributed ATM switch. Each module has its own switching and CPU power. In order to present the switch as a single and united entity, one module is automatically elected as a Master Agent while the other modules are Sub Agents. The Master Agent status is shown by the Network Management Agent (NMA) LED.

The Master Agent is the module hosting the Management LEC with all its functionality: IP address and switch-wide information. The Master Agent is also a regular module with all the functionality of a Sub-Agent such as controlling the physical ports, virtual ports and download.

The Master and Sub Agents have slightly different CLI options. For example, the Master Agent has the “ip” command and the “access” command which will enable you to access a Sub Agent from the Master Agent. A simple way to find out whether you are currently communicating with a Master Agent is to type `help` at the command line and check whether there is an “access” command option.

All the information configured to the Master Agent (IP, ATM Prefix) is backed up by all the Sub Agents, so if the Master Agent is removed, another module will be elected and all previous configuration settings will be kept.

Related Documents

- Installation Guide of each module
- Avaya M770 ATM Switch Manager application within the CajunView™ software suite
- Avaya M770 M-SPS Installation Guide

Supported Modules

Avaya M770 ATM Switch Software Version 2.3 supports the following ATM modules:

- M15-155F/SF/MS module: 15 OC-3 Multimode or Multimode/Single-mode fiber ports
- M3-622F/SF module: 3 OC-12 Multimode, Single-mode or Multimode/Single-mode fiber ports
- M4-DS3 module: 4 DS3 ports with traffic shaping capabilities

Features List

Hardware Features

- Dual 40 Gbps passive backplane switch
- Low Cell Transfer Delay through the switch is 20 µsec (in port to out port)
- Low Cell Delay Variation through the switch is 5 µsec (in port to out port)
- Clock Synchronization (Generation / Propagation) of clock to all other ports
- Supports CBR, VBR-rt, VBR-nrt, ABR, UBR Classes of Service
- Supports AAL1, AAL2, AAL3 / 4 and AAL5 classes
- Cell Loss Priority (CLP) discard
- Early Packet Discard (EPD) and Partial Packet Discard (PPD) for AAL5
- ABR with EFCI Tagging
- Hot swapping of modules
- Line Indication LEDs: Link (LNK), Transmit (Tx), Receive (Rx), Loss of Signal (LOS), Remote Defect Indicator (RDI)
- Idt R4650 (100 MIPS) RISC processor, 32M RAM and 4M Flash on each module for fast call set up and protocol processing

M15-155F/SF/MS module features

- 32K cells per slot output buffers
- 16K cells per slot input buffers
- 120K Virtual Channels per module
- 32K Virtual Channels per port

M3-622F/SF module features

- 32K cells per slot output buffers
- 16K cells per slot input buffers
- 168K Virtual Channels per module
- 56K Virtual Channels per port

M4-DS3 module features

- Supports a line distance of up to 137 meters of coaxial cable
- Supports Vport (Virtual Port) traffic shaping on DS3 ports
  For more information see Chapter 6, “Managing Virtual Ports“
- 30K Virtual Channels per module for both Permanent and Switched Virtual Circuits
- 16K cells per slot input buffers
- 32K cells per slot output buffers
- Additional 256K cells per slot output buffers for traffic shaping

Software Features

- ATM Forum PNNI (Private Network-Network Interface) protocol for routing within large ATM networks
- Support for ATM Forum hierarchical PNNI, including all 4 base subsets of configurations:
  - — Mimimum function (single peer group)
  - — Boarder node
  - — PGL/LGN
  - — Boarder with LGN peer support.
- Support for optional ATM Forum PNNI features:
  - — Exterior addresses
  - — Alternate routing
  - — ATM traffic descriptors negotiating.
- ATM Forum IISP (Interim Inter-switch Signalling Protocol) for signalling between switches and static routing across the ATM network
- ATM Forum ILMI, UNI 3.0, UNI 3.1and UNI 4.0 signalling, selectable on a per-port basis, supporting point-to-point and point-to-multipoint Virtual Circuits
- Translation between UNI 3.0, UNI 3.1 and UNI 4.0 signalling
- Statistics for each Virtual Channel
- Virtual ports for Virtual Path (VP) tunnelling
- Virtual Path (VP) Switching capability (both PVP and SVP)
- Centralized PVC configuration
- Point-to-Multipoint PVCs
- Up to 1K of PVCs per module
- SNMP Network Management using LANE Client
- Command line Interface (CLI) management available remotely by using Telnet and/or directly by using the serial RS-232 port on the module front panel.
- Trivial File Transfer Protocol (TFTP) for software and configuration download and for configuration uploads (stores the configuration in a server)
- Full LAN Emulation (LANE) suite consisting of a LECS (LAN Emulation Configuration Server), a combined LES (LAN Emulation Server) and BUS (Broadcast Unknown Server), and a management LEC (LAN Emulation Client)
- ATM Forum LUNI 2.0 protocol
- Proprietary Resilient LECS
- Proprietary Resilient and Distributed LAN Emulation Services
- Multiple LES/BUS per module (up to 16)
- LECS support of multiple ELANs (up to 64)
- LECS ELAN client mapping (for secure ELANs)
- Efficient Point-to-Multipoint support using a minimal duplication scheme (patented)
- Up to 1K Point-to-Multipoint roots per module

- Up to 5460 Point-to-Multipoint branches or leaves per module
- Up to 210 OC-3 ports in a single switch
- Up to 42 OC-12 ports in a single switch
- Up to 56 DS3 ports in a single switch
- Signaling performance of 130 setups/sec with PNNI running per Module. Performance improves as you add modules
- Signaling security (access control)
- Support for Single-domain and Dual-domain M770 ATM switch Upper Backplanes
- SNMP (Simple Network Management Protocol) management over IP over LAN emulation, using the following MIBs (Management Information Bases):
    - MIB II (RFC 1213)
    - Interface MIB (RFC 2233)
    - ATM MIB, ATM-2 MIB (RFC 1695)
    - SONET/SDH MIB (RFC 1595)
    - PNNI MIB
    - LEC MIB
    - LANE Server MIB
    - Private MIB
    - DS3 MIB (RFC 2496)

Supported Standards

Operational Standards

Safety Standards	
UL1950	(United States)
CSA-C22.2 No.950	(Canada)
EN60950	(Europe)
AS3260, AUSTEL TS001	(Australia)
EMI	
FCC Part15, Class A	(United States)
EN55022, Class A and B	(Europe)
VCCI Type 1	(Japan)
EMS	
IEC801-2, ESD up to 8kV	•
IEC801-3, RFI 3V/m	•
IEC801-4, Electrical Fast Transients, level 2	•
Power & Environmental Conditions	
IEC555-2, Power Factor Correction	•
IEC555-3, Ac Input Transients	•
Audible noise IS07779 paragraph 7, max. 50dBA	•

ATM Forum Standards

Approved ATM Forum Specs.	Specifications
Physical Layer	
155.52 Mbps SONET/SDH STS-3c Physical Layer	af-uni-0010.002 (Issued as part of UNI 3.1
622.08 Mbps Physical Layer	af-phy-0046.000
User-Network Interface (UNI)	
ATM User-Network Interface Specification V3.0	af-uni-0010.001
ATM User-Network Interface Specification V3.1	af-uni-0010.002
UNI Signaling 4.0	af-sig-0061.000
ILMI (Integrated Layer Management Interface)	
ILMI 4.0	af-ilmi-0065.000
Traffic Management	
Traffic Management 4.0	af-tm-0056.000
PNNI	
Interim Inter-Switch Signaling Protocol	af-pnni-0026.000
PNNI V1.0	af-pnni-0055.000
LAN Emulation:	
LAN Emulation over ATM 1.0	af-lane-0021.000
LANE v2.0 LUNI Interface	af-lane-0084.000

Chapter 2

Getting Started

This chapter describes how to get started with an Avaya M770 ATM Switch. This includes an overview of the management and configuration tasks that you should perform soon after installation.

Powering up the Avaya M770 ATM Switch

During the system startup of an Avaya M770 ATM Switch, the switch automatically performs a number of self-tests on its internal hardware.

The startup process is documented in each module’s Installation Guide which includes information about the self-tests that are carried out and how the LED indicators on the switch indicate the status of the self-tests.

If any non-critical hardware self-test fails then the Boot Loader will be entered. From the Boot Loader you may be able to diagnose and remedy the problem. For more information on how to use the Boot Loader, see Appendix B Using BOOT Loader.

If the M770 ATM Switch passes all the self-tests, it will load the main image from flash memory and you can manage the M770 ATM Switch.

Managing an Avaya M770 ATM Switch

The M770 ATM Switch can be configured and managed using the following management methods:

- Management from a local or remote console using the command-line interface.
- Management from a network management station using SNMP and the Avaya M770 Manager which is an easy-to-use, graphical management application.

Management from a local or remote console

You can manage the M770 ATM Switch using the following methods:

- Out-of-band console management by means of a VT100-compatible terminal connected to the serial port (labelled Console) of the M770 ATM module.
- Remote console management using a terminal using Telnet over TCP/IP
- Out-of-band console management using a VT100-compatible terminal connected to the serial port (labelled Console) of the M-SPV/M-SPX/M-SPS Supervisor module.

For information about connecting a terminal device to the serial interfaces, refer to each module’s Installation Guide.

Management from a network management station

You can manage the M770 ATM Switch using SNMP management running over UDP/IP over an Emulated LAN (ELAN).

- Connect the management station to the ELAN that the management LEC is connected to, or make sure it can communicate with that ELAN.
- Set the IP address of the M770 ATM Switch management LEC, and make sure the management station is either on the same subnet or can communicate with that subnet. If the management station and management LEC are on different subnets, set the default gateway on the M770 ATM Switch so it can communicate with the management station.
- Make sure you know the SNMP community name (for both read and write access).
- Operate the Avaya M770 ATM Switch Manager on your management station as part of the CajunView package. The Avaya M770 ATM Switch Manager enables you to view the device, check the status indicators from the management station, and perform a range of management tasks. For more information about Avaya M770 ATM Switch Manager, refer to the Avaya M770 ATM Switch Manager User Guide.

Setup Procedures on an Avaya M770 ATM Switch

To install an M770 ATM Switch successfully, do the following:

- To access and manage an M770 ATM Switch remotely, an IP address must be assigned to the switch. For more information on setting up an IP address on an M770 ATM Switch, see ”Setting the IP address” on page 11.
- To access an attached device or switch, set up static routing entries to switches that do not support PNNI and to any attached devices that do not support ILMI. For more information on setting up a routing table on an M770 ATM Switch, see Chapter 9, “Managing Static Routing”.
- To enable an attached device or switch to communicate, you may need to configure ports. For more information on configuring ports on an M770 ATM Switch, see ”ATM Port Configuration” on page 12.
- To enable communication over the network - LAN Emulation must be set up on the switch. For more information on setting up LAN Emulation on an M770 ATM Switch, see “Setting up LAN Emulation” on page 16.

Setting the IP address

To access and manage an M770 ATM Switch remotely, for example using Telnet or SNMP, an IP address must be set for the switch.

You will need to decide whether the M770 ATM Switch will use BOOTP to acquire its IP address or whether you wish to set it manually.

If you plan to use BOOTP, make sure a BOOTP server is on the same ELAN as the M770 ATM Switch management LEC, or there is a route from a BOOTP server to the ELAN. For more information about managing the Management LEC, see Chapter 11. You will need to set the IP address of the M770 ATM Switch to BOOTP (this is the default IP setting for a new M770 ATM Switch). The M770 ATM Switch will then attempt to learn its IP address using the BOOTP protocol.

If you plan to set the IP address manually, first ensure that the terminal or terminal emulator is connected to the serial interface of the Master Agent. The IP address of the switch can only be seen on the Master Agent (the Master Agent module's "NMA" LED will light ON). For example, if you want to set the IP address to be 149.49.46.61 with a subnet mask 255.255.255.0, and a gateway IP address 149.49.46.150, you should perform the following steps:

```
M15-155s8:/>ip address 149.49.46.61 255.255.255.0
M15-155s8:/>ip gateway 149.49.46.150
```

For more information about setting IP addresses, see "Configuring the Avaya M770 ATM Switch Address Information" on page 31.

Note: Changing the IP address commands will take effect immediately, and will disrupt IP traffic (for example, Telnet or SNMP) that is going to the M770 ATM Switch.

ATM Port Configuration

Setting the virtual port to its default configuration

If you are attaching an end-station or an edge device that supports ILMI to an Avaya M770 then you must ensure that the virtual port on the M770 ATM Switch is using its default configuration. For a list of the default port settings, see Appendix A, “Default Settings on a New Avaya M770 ATM Switch”. For example, to set vport 8.4.0 to its default settings type:

```
M15-155s8:/>vport disable 8.4.0
M15-155s8:/>vport reset all 8.4.0
M15-155s8:/>vport enable 8.4.0
```

This will enable ILMI to automatically configure the virtual port so that it can communicate with the attached device. For more information on resetting the parameters on the virtual port, see “Resetting Virtual Port Parameters” on page 75.

Connecting to a device, supporting ILMI

If you are attaching an end-station, edge device or another ATM switch which supports ILMI then the M770 ATM Switch will automatically configure the virtual port to communicate with the attached device.

Ensure that ILMI is enabled on all devices and the ports have been set to their default port configuration before attaching the device. ILMI will not alter any parameters that have been manually configured by the administrator. If a parameter has been automatically configured for a port, using ILMI, the parameter will be displayed with an asterisk “*” next to it.

Connecting to a device *not* supporting ILMI

If you are attaching an end-station, edge device or another ATM switch that doesn’t support ILMI to an Avaya M770, then you must disable ILMI on the M770 ATM Switch port that connects the two devices.

You should then verify that the following virtual port parameters on the M770 ATM Switch are the same as the parameters on the attached device:

- The port profile must be set to either “network” or “user” (the opposite to the configuration on the remote device).
- The signalling stack type must be set to either UNI 3.0, UNI 3.1, UNI 4.0, IISP 3.0, IISP 3.1 or PNNI 1.0 (according to the configuration on the remote switch).
- Other signalling parameters on the M770 ATM Switch to match the remote device like VPI and VCI range.

For example, if you are connecting an Avaya M400 Gate Switch LSA+ module which does not support ILMI, to port 8.4.0 on the M770 ATM Switch, you should configure port 8.4.0 on the M770 ATM Switch by performing the following steps:

```
M15-155s8:/>vport disable 8.4.0
M15-155s8:/>vport disable 8.4.0 ILMI
M15-155s8:/>vport set stacktype 8.4.0 UNI 3.0
M15-155s8:/>vport set vpirange 8.4.0 [0..0]
M15-155s8:/>vport set vcirange 8.4.0 [32..1023]
M15-155s8:/>vport enable 8.4.0
```

Routing Configuration

PNNI Configuration

When you configure your network you have to decide whether you're going to use a single peer group (flat) configuration or multiple peer groups (hierarchy) configuration. In case you have devices that do not support PNNI, please refer to Section Connecting to another ATM switch which doesn’t support PNNI.

Flat PNNI Configuration

Connecting to another ATM switch which *supports* PNNI

If you are attaching another ATM switch that *supports* PNNI ensure that the following conditions exist:

- All switches should have a different ATM prefix (although the network will work even if some have the same prefix). To check this in the ATM switch type: ‘`address prefix`’ (on the Master Agent modules).
- All switches must have a different node_id. By default it will be taken from the switch address.
- All switches, in the same peer group, must have the same pg_id
- All switches in the same peer group must have the same level.
  To check the PNNI and ATM addresses of the switch, type one of the following commands:

  ```
  M15-155s8:/> summary info
  ```

  or

  ```
  M15-155s8:/> route pnni config show
  ```

Note: Changing the PNNI ‘level’ also changes the first byte of the Node ID and the Peer Group ID.

Connecting to another ATM switch which *doesn't* support PNNI

If you are attaching another ATM switch that doesn't support PNNI, you must configure a route to that switch.

For example, if you are connecting a Collage 740 to port 8.5.0 on the M770 ATM Switch, you should configure the static routing table by performing the following steps:

(assume that the partial ATM prefix of the Collage 740 is 39.04)

```
M15-155s8:/>route add 39.04. 8.5.0
```

Configuring Hierarchical PNNI

The following steps will help you in configuring your network into a hierarchy of peer groups. You will need a basic knowledge of PNNI.

- Create a drawing of the network you want to achieve while completing the following steps:
    1. Decide how many level of hierarchy you need.
    2. Divide your switches into different peer groups.
    3. Decide how many peer groups are grouped together in to the next level of hierarchy.
    4. On each peer group, decide which node will be the Peer Group Leader (PGL). Or better, configure all switches to be capable of becoming a Peer Group Leader (assuming their software version supports this). The PNNI's Peer Group Leader Election protocol will determine the active PGL.
    5. Repeat the steps 3 &4, until all peer groups of all switches are organized in the hierarchy.
    6. Decide the level scopes of the different level, in the range of 1-104. A lower level should have a greater number.

Note: In the CLI, levels are numbered 1,2,3…. where 1 indicates the lower level (the physical level in which the node resides), 2 indicates the next level in the hierarchy and so on.

    7. Determine the switches' prefixes so they will match the organization into peer groups and the specified levels. There is an algorithm that can help you in determining the prefixes to match the hierarchy (see Appendix).

- Configure all switches' ATM Address prefixes as determine in step 7, and force their node IDs to match the prefix. The configuration is done on the Master Agent using the command:

```
M15-155s8:/>/address prefix <prefix> node_id
```

- For the switches that are capable of becoming PGLs (as determine in step 4) do the following:

  1 Configure the level scope as determine in step 6 for all levels (1-5) using the command:

```
M15-155s8:/>/route pnni config level set <level (1-5)> <level scope (1-
104)>
```

  2 Configure the leadership priority of the node in the lower level to a value greater than 0.

```
M15-155s8:/>/route pnni config pgle set <level-x (1-4)> 1 <leadership
priority (1-205)>
```

  3 Configure the Administrative Status of the node in the next higher level to Up

```
M15-155s8:/>/route pnni config admin set <level-x+1(2-5)> up
```

- Repeat the last step for all levels you have in the hierarchy.

Connecting to an end-station or edge device *not* supporting ILMI

If you are attaching an end-station or edge device that does not support ILMI then you must configure a route to that device. For example, if you are connecting an Avaya M400 Gate Switch LSA+ module to port 8.4.0 on the M770 ATM Switch, you should configure the static routing by performing the following steps:

[assume that the ATM address of the LSA+ is 39.01.00.00.00.00.00.00.00.00.00.00.00.00.40.od.64.02.de.00]

```
M15-155s8:/>route add
39.01.00.00.00.00.00.00.00.00.00.00.00.00.40.od.64.02.de 8.4.0
```

Note: The ATM address should not include the selector.

Setting up LAN Emulation

Each module in the Avaya M770 ATM Switch can host one LECS and multiple combined LES and BUS. This means that on one switch, there can be several resilient LECS, and for one ELAN, several distributed LES. The Avaya M770 ATM Switch LES does not have to reside in the same device as the LECS. The module that is elected as the Master will host the Management LEC.

The following steps should be performed for each M770 ATM Switch module to ensure correct LANE configuration:

1 Determine what type of LECS is to be hosted on this module (local or remote).

By default the module is configured to seek a remote LECS at WKA (Well-Known Address).

For information about the different types of LECS that can be hosted on the M770 ATM Switch, see Chapter 14, Managing the LECS.

2 If you are using resilient LECS, configure one of the LECS to have the highest priority.

For information about changing a LECS priority on the M770 ATM Switch, see Chapter 14, Managing the LECS.

3 If the M770 ATM Switch is to host a local LECS then you will need to consider the ELANs that the LECS will coordinate.

Note: To ensure that a standby LECS can smoothly take over the running of the network, should the active elected LECS fail, it must be configured with the same LANE services information as the active elected LECS.

There is no checking of database consistency between modules that are hosting the resilient LECS.

4 Determine what ELANs this switch will host and create LESes to host the required ELANs.

For information about configuring local ELANs, see Chapter 16 Managing an ELAN.

For information about configuring the local LES, see Chapter 15 Managing the LES/BUS.

— By default the M770 ATM Switch hosts the following default ELANs:

	ELAN name	ELAN LES name
Default Ethernet ELAN	default	default

Note: Ensure that the number of modules hosting a specific LES / BUS (e.g. default) does not exceed the maximum number of LESes per ELAN as defined in: `lan elan maxles` (default 5, maximum 10).

5 Determine if secure “Closed” ELANs are required. If required then you will need to set-up an ELAN client database in the Avaya M770.

For information about setting up ELAN clients, see Chapter 16 Managing ELAN Clients.

— By default when ELANs are created they are set-up as “Open” ELANs.

Recommended Redundant LANE Services Setup

You have the ability to setup redundant LANE services on every module. On each M770 ATM switch that contains N modules, you have the flexibility to configure N resilient LECS hosting ELANs that can be redundant N times. LANE redundancy is not just switch wide, but network wide. Each module in every switch can host redundant LANE services. We do not recommend that you place redundant LANE services on every module. In the event that you want to investigate where clients are registered and to look at the LECS, you need to look at every module in his network. The Cajun LaneMaster application helps you configure your redundant LANE services. To help you decide where to put the LANE services and to minimize configuration time, we recommend the following:

LECS: Setup 2 resilient LECS on two different switches. One of the LECS should have a higher priority than the other.

LES: Setup 5 distributed LESs for each ELAN. Configure each LES on a separate switch and if there are less than 5 switches, configure a LES on multiple modules in each switch.

Example for LANE Configuration

The default LANE configuration of the Avaya M770 ATM Switch:

ELAN:	Ethernet ELAN named default
LES / BUS:	Ethernet LES named default
LECS:	Remote at the well known address (wka)
LEC:	Configured to join the Ethernet ELAN default

Following is a simple configuration example, which will enable you to start working with the LANE services and to connect a network management station which uses SNMP and CajunView Management.

1 You need to decide where you want the LECS. The following command creates a local resilient LECS with priority 0 which advertises the well known address, on the module (while the LECS priority is 0 it will not be elected as active):

```
M15-155s8:/>lane lecs priority 0
```

To see all of the resilient LECS on the network type the following:

```
M15-155s8:/>lane lecs resilient show
```

If the location of the LECS is resident on a different switch or module at the wka, change the location of the LECS to be remote at the wka using the following command:

```
M15-155s8:/>lane lecs location remote wka
```

2 If your management station is on an ELAN different than default, you might need to create a new ELAN. In order to create a new ELAN, two things must be performed. First, an entry for the ELAN must be defined in the LECS table, and a LES/BUS pair must be defined for the ELAN.

To create an ELAN named elan1, you need to first define an entry for elan1 in the LECS table, typing the following command, at the module which holds the LECS:

```
M15-155s8:/>lane elan create elan1 auto ethernet
```

3 After all of the ELANs have been defined, in the ELAN database, you need to change the priority of the LECS to a priority higher than 0, so that it can participate in the LECS election. If you will be using more than one resilient LECS, configure one of the LECS to have a higher priority to the others using the following command (this example changes the LECS priority to 200):

```
M15-155s8:/>lane lecs priority 200
```

Then you need to define a distributed LES/BUS for elan1. To create a LES/BUS, that will use the selectors a1 and b1 for their ATM addresses, type the following command:

```
M15-155s8:/>lane les create elan1 distributed ethernet a1 b1
```

To Check if the LES registered its address with the LECS type:

```
M15-155s8:/>lane elan show
```

To check if any Clients registered with the LES elan1 type:

```
M15-155s8:/>lane les show
```

4 In order to manage the M770 ATM Switch, the Management LEC must register with the same ELAN as the NMS or there should be a router between the ELANs. By default the Management LEC is configured to join the Ethernet ELAN default. If you want to change the ELAN which the Management LEC will join, for example to elan1, type the following command:

```
M15-155s8:/>lane lec elan elan1
```

After changing the E LAN for the management LEC to join, you must restart the management LEC by typing:

```
M15-155s8:/>lane lec restart
```

To check with which ELAN the management LEC is currently registered type:

```
M15-155s8:/>lane lec show
```

Support for LUNI 2.0

From M770 ATM Switch embedded S/W Version 2.1 and higher, the LES supports LUNI 2.0. The first LES registered to an ELAN determines the LUNI 2.0 capability of the entire ELAN. A LUNI 1.0 client (LEC) can still register to a LUNI 2.0 server (LES) since the LUNI 2.0 LES can send LUNI 1.0 frames. However, a LUNI 2.0 client cannot register to a LUNI 1.0 server.

How to Use the Command-line Interface

This chapter explains how to get management access to the Avaya M770 ATM Switch command-line interface and how to use the command-line interface to manage the switch.

Getting Connected

You can access the Avaya M770 ATM Switch command-line interface by one of the following methods:

- Direct connection to an ATM module using a serial interface, using a VT100 terminal or a PC running a terminal emulation program. For information about the serial interface, refer to the module's Installation Guides.
- Telnet connection, using a standard Telnet program to the ATM module.
- Direct Connection or Telnet Connection via the M-SPV/M-SPX/M-SPS (S/W Ver 2.5 or higher). For more information, see to the M-SPS Installation Guide.

When a terminal is connected to the command-line interface, the M770 ATM Switch displays a welcome message on the terminal screen and logs the user directly into the root of the command-line interface. You can set a password for serial and telnet connections into the switch. For more information about setting up a password, see Setting passwords for local/remote connections in Chapter 4, Managing Miscellaneous Commands.

Note: You can access the command-line interface using Telnet directly to the ATM module only if the M770 ATM Switch's management LEC is currently joined to an ELAN that is accessible from the network management station, and the IP address of the switch has been set. However, you can access the M770 ATM Switch via Telnet to the M-SPV/M-SPX/M-SPS (using an Ethernet connection).

How the Command-line Interface Works

The command-line interface provides a set of commands that you can use to configure the M770 ATM Switch. The commands are arranged in a hierarchy such that related commands are grouped together in a single functional group. A functional group can also contain one or more functional groups, and so forth. When you login to the command-line interface, you will be placed at the root of the hierarchy. To perform an operation using a command, you will need to specify the full hierarchical path followed by the command. For example:

```
M15-155s8:/>route show
```

This command shows routes in the routing table and is contained in the `route` functional group. Alternatively, you can descend the hierarchy by typing:

```
M15-155s8:/>route
```

This will cause the prompt to change, displaying the position in the hierarchy:

```
M15-155s8:/route>
```

You can now perform the command simply by typing `show`, as follows:

```
M15-155s8:/route>show
```

The advantage of descending the hierarchy is that you can perform multiple related commands without having to type them out in full (that is, specifying their full hierarchical path).

Note: You do not need to enter all the letters of a command: you need only enter sufficient letters to uniquely identify it from other commands in the directory. For example, instead of typing `route show` you could just enter `r s` in the command-line interface. You can also use the TAB key to complete the full command.

Table 3.1 lists the commands that are used to navigate the hierarchy.

Table 3.1 Navigational commands

Command	Description
`top`	Returns you to the root of the hierarchy.
`up`	Returns you to the previous level in the hierarchy.

Note: If you press the RETURN key immediately after the prompt, it has the same effect as entering the `up` command.

If you are at a particular point in the hierarchy and you need to perform a command elsewhere in the hierarchy, you must enter the slash symbol (/) followed by the full hierarchical path followed by the command. For example:

```
M15-155s8:/route>/vport show
```

This command will list information about virtual ports while you are in the `route` functional group. After the command has been executed you will still be in the `route` functional group.

Note: After resetting a module, some of the CLI commands may not be available immediately. Wait a few seconds until all the software has initialized.

Master Agent and Sub Agent Commands

The Master Agent and Sub Agent have slightly different CLI options. For example, the Master Agent has the “ip” command and the “access” command which will enable you to access a Sub Agent from the Master Agent. A simple way to find out whether you are currently communicating with a Master Agent is to type “help” at the command line and check whether there is an “access” command option.

All the information configured to the Master Agent (IP, Permanent Managers) is backed up by the Sub Agent, so if the Master Agent is removed, another module will be elected and all previous configuration settings will be kept.

Command hierarchy

The hierarchy of the commands in the Command Line Interface (CLI) can be obtained at any time by typing `tree`. The `tree` command can be used at the prompt of any functional group to view the sub-commands of the group.

For example, the output of the `tree` command from the `pport` functional group prompt is:

Command: `M15-155s8:/pport>tree`

Output:

```
pport
+-disable -- Disable a physical port
+-enable -- Enable a physical port
+-reset -- Reset all settable parameters on a physical port to their defaults
+-set -- Set a physical port parameter
| +-framing -- Specify the framing
| +-payloadscrambling -- Specify whether payload scrambling is on or off
| `-txrate -- Specify port transmit rate in Kbits/sec
+-show -- Show information about all physical ports
| `-counters -- Show counter information for a physical port
```

Note: Certain functional groups in the hierarchy are also commands in their own right. For example, the `vport show` functional group is also a command when entered on its own.

Conventions used to describe commands

Throughout this chapter the following conventions are used:

- All command examples are given in relation to the root of the hierarchy. That is, this is how you would enter the command if you were at the root of the hierarchy.
- The syntax of commands are described using the symbols displayed in Table 3.2.

Table 3.2 Symbols used to describe command syntax

Syntax	Description
[ ]	Characters surrounded by square brackets denote optional arguments.
{ }	Characters surrounded with braces denote a selection list. When there are several argument selections surrounded by braces and separated by a vertical bar (|) then one of the arguments must be included in the command.
< >	Characters surrounded by angle brackets denote information that you must provide.

Using the on-line help

On-line help is always available and can be obtained at any time by typing `help`. The following information will be displayed:

- All commands and functional groups available at the current position in the hierarchy, in alphabetical order.
- The universal commands. These are commands that are independent of the hierarchy. They can be executed irrespective of where you are in the hierarchy.

The help output from the root is shown below.

Command:

```
M15-155s8:/>help
```

Output:

```
Commands:-
access         -- Display or Access other modules in the
                switch
                  (master agent option only)
address        -- ATM address info
cac            -- Connection Admission Control (CAC)
                management
                  (master agent option only)
event          -- Event message commands
flash          -- Flash management commands
hardware       -- Hardware commands
ilmi           -- ILMI information
ip             -- IP configuration commands (master agent
                option
                  only)
lane           -- LANE configuration commands
password       -- sets the remote/local console password
pport          -- Physical Port management
pvc            -- Management of Permanent Virtual
                Connections
                  (PVCs)
route          -- Routing table management
script         -- Management of script files
snmp           -- Console network management
summary        -- Summary information
system         -- System wide commands
td             -- Traffic Descriptor Management
terminal       -- Terminal settings
version        -- Display build version number
vport          -- Virtual Port management

Universal commands:-
?, exit, help, retstatus, top, tree, up.
```

Help is also available for individual commands. To obtain help on a command, type `help` followed immediately by the full command. As an example, the help output for the `address esi` command is:

Command:

```
M15-155s8:/>help address esi
```

Output:

```
esi            -- Display the module ESI address
                 Syntax: address esi ... to display
                 current esi
NOTE: the esi is burnt in and cannot be changed!
```

Note: If there is a discrepancy between the information in the on-line help and the information in this manual, always follow the advice in the on-line help, as it is the most current information available.

Chapter 4

Managing Miscellaneous Commands

This chapter describes how to use the command-line interface to set passwords, address information, and CAC information.

For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Setting passwords for local / remote connections

To protect the Avaya M770 ATM Switch from accidental or unauthorized configuration from a local (via the serial port) or remote end-station (via Telnet), you may want to set a password for the switch.

The following sequence shows you how to set a password for the switch for the first time. Because no password exists, the M770 ATM Switch does not prompt for the old password.

Command:

```
M15-155s8:/>password
```

Output:

```
M15-155s8:/>There is no password at the moment.
M15-155s8:/>Enter the new password (does not echo): ********
[ENTER]
M15-155s8:/>Enter the new password again (does not echo):
******** [ENTER]
M15-155s8:/>Password changed.
```

Once you have set a password, the CLI will ask you to enter the password each time you connect to the switch.

To terminate a session and prevent other from configuring the switch use the `exit` command.

Once you have enabled password protection there is a timeout period of 15 minutes before the CLI session is terminated.

To delete a password

Enter the old password and press “Enter” for the new password.

Managing the Sub Agents

The `access` command displays or accesses other modules in the switch. It opens a telnet session to the module located in slot <slot_number>. If <slot_number> is not entered, all modules in the switch will be listed.

To return to the Master Agent use the `exit` command.

Command:

```
M15-155s8:/>access [<slot_no>]
```

Output:

```
List of modules found in the switch
===================================
M15-155F in slot 13     (Master Agent)
M15-155F in slot 14

M15-155s8:/>access 13
Welcome to the M770 ATM Switch command line interface
M15-155s13:/>exit
M15-155s8:/>
```

Switch Summary Information

The `summary info` command displays system information for the current ATM switching module:

Command:

```
M15-155s8:/>summary info
```

Output:

```
System Information:

Module Type         : M15-155F - 15 atm ports (OC-3, MMF)
Serial Number       : 0000000
C/S Version         : 0.0
Slot number         : 6 (Master Agent)
Upper Backplane     : Single Domain
Boot ROM Version    : 1.1.2
Boot Loader Version : 2.0.18
SW Version          : 2.0.18
Build Time          : Sun Dec 26 21:13:21 IST 1999

MAC Address         : 00.40.0D.87.00.0D
IP Address          : 149.49.34.121
IP Subnet Mask      : 255.255.255.0
IP Gateway Address  : 149.49.34.5
LEC State           : OPERATIONAL
LEC ELAN Name       : default
LEC LES Address     :
39.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00

Current ATM prefix  :
39.00.00.00.00.00.00.00.40.0D.87.00.0D
Current Node Id     :
38.A0.39.00.00.00.00.00.00.00.40.0D.87.00.0D.00.00.00.00.00.00.00
Current PG Id       :
38.39.00.00.00.00.00.00.00.00.00.00.00.00
Current Level       : 56
```

The `summary lane` command displays LECS location, an ELAN list, LES list and a list of all Selectors currently in use:

Command:

```
M15-155s8:/>summary lane
```

Output:

```
lecs location:
--------------
The local resilient LECS is active.
It is advertising the ATM Forum well-known address.
The elected LECS is at the ATM Forum well-known address.

elan list:
----------
Name                               Security  Type
    LES Mode and Address(es)
    Maximum Number of LESs         LES address formula
-----------------------------------------------------------
default                            Open      Ethernet
    Distributed
      1 LES(s) using LES group address
      at 39.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
    5                              Group address

Global                             Open      Ethernet
    Distributed
      (No les is registered)

ELAN_3                             Open      Ethernet
    Distributed
      at 39.00.00.00.00.00.00.00.40.0D.87.00.0D.00.40.0D.87.00.0D.8A
    5                              Round robin

ELAN_Generic                       Open      Ethernet
    Distributed
      (No les is registered)

ELAN_Global                        Open      Ethernet
    Distributed
      at 39.00.00.00.00.00.00.00.40.0D.87.00.0D.00.40.0D.87.00.0D.82
    5                              Round robin

les list:
---------
                                                         Selectors
Name                            Type           Enabled  LES  BUS  Clnts
ELAN_Global                      Ethernet       Yes      82   83   0
ELAN_5                           Ethernet       Yes      88   89   0
ELAN_3                           Ethernet       Yes      8A   8B   0
default                          Ethernet       Yes      20   21   5

List of all selectors now in use:
(20) (21) (7F) (80) (81) (82) (83) (88) (89) (8A) (8B)
```

Configuring the Avaya M770 ATM Switch Address Information

Setting the Avaya M770 ATM Switch IP address, subnet mask, and gateway

An M770 ATM Switch will need an IP address so that it can be managed remotely. You must decide whether the M770 ATM Switch will use BOOTP to acquire its IP address or whether the address must be set manually.

If you plan to use BOOTP, make sure the BOOTP server is on the same ELAN as the M770 ATM Switch management LEC, or there is a route from the BOOTP server to the ELAN. You will need to set the IP address of the M770 ATM Switch to BOOTP (this is the default IP setting for a new M770 ATM Switch). The M770 ATM Switch will then attempt to learn its IP address using the BOOTP protocol.

Note: IP address configuration commands will take effect immediately and may disrupt IP traffic (for example, Telnet or SNMP) going to the M770 ATM Switch.

To set the M770 ATM Switch's IP address and subnet mask, enter the `ip address` command:

Command: `M15-155s8:/>ip address <ip_address> [<netmask>]`

Example: `M15-155s8:/>ip address 192.32.220.61 255.255.255.0`

Parameters:

`<ip_address>` A unique IP address that is to be assigned to the M770 ATM Switch.
If you set the address to BOOTP, the M770 ATM Switch will attempt to learn its IP address using the BOOTP protocol.

`<netmask>` A valid IP subnet mask.
0.0.0.0 indicates that the default subnet mask should be determined from the IP address.
If a value is not supplied for the netmask, the default value of 255.255.00.00 will be used.

To enable remote access to the M770 ATM Switch from a different IP subnet, you must identify the IP address of a default gateway. The gateway must be on the same IP subnet as the M770 ATM Switch.

To set the gateway IP address, use the `ip gateway` command.

Command: `M15-155s8:/>ip gateway <ip_address>`

Example: `M15-155s8:/>ip gateway 192.32.220.8`

Parameters:

`<ip_address>` A valid IP address for the gateway.

Viewing Avaya M770 ATM Switch IP address information

You can display IP address information for the M770 ATM Switch. For information about changing the IP address information, see “Setting the Avaya M770 ATM Switch IP address, subnet mask, and gateway” on page 31.

To view the IP address information, use the `ip show` command. The message “initializing” indicates that the LEC has not yet joined the ELAN.

Command: `M15-155s8:/>ip show`

Output:

```
IP address: 192.32.220.61 (The address was obtained
using BOOTP.)

IP subnet mask: 255.255.255.0

IP gateway address: 192.32.220.8

MAC address: <valid address> (or initializing)

Layer 2: ok (or initializing)
```

Viewing the End System Identifier (ESI)

The End System Identifier (ESI), also referred to as the Burnt-In Address (BIA), is the factory-assigned world-wide unique address for the switch. If the management LEC on the M770 ATM Switch is joined to an Ethernet ELAN, its MAC address will default to the ESI (Ethernet format).

To display the BIA (ESI) of the M770 ATM Switch, use the `address esi` command.

Command: `M15-155s8:/>address esi`

Output:

```
Switch ESI Address (Ethernet Format): 00.40.0D.07.00.0e
```

Note: The ESI cannot be changed. However, in the case of LANE, a Locally Administered Address (LAA) can be defined. For more information see “Managing the ELAN for the management LEC” on page 165.

Viewing or changing the switch prefix

When a M770 ATM Switch with a blank EEROM is powered up, a default prefix is generated and stored in the EEROM.

The default prefix is 39.00.00.00.00.00.00.xx.xx.xx.xx.xx.xx where x is the MAC address of the switch.

Note that the first byte of all switch prefixes must start with one of the following:

- 39. An ATM Forum Identifier (AFI) for the Data Country Code (DCC). This is allocated and assigned to countries and administered by the ISO member for that country.
- 47. An AFI for the International Code Designator (ICD). This is allocated and assigned to countries, and administered by an ISO registration authority for that country, for example the British Standards Institute (BSI).
- 45. An AFI for E.164 encapsulated. This is useful for organizations who wish to use the existing number plan used in public networks.
- 49. The local AFI that defines a structure that can be used by anyone within a private network.

To display the current switch prefix, use the `address prefix` command.

Command: `M15-155s8:/>address prefix`

Output: `Current Prefix: 39.00.00.00.00.00.00.00.40.0d.87.00.2c`

If you have an ATM network that uses its own block of ATM addresses, you can make the M770 ATM Switch conform to this scheme by changing the default switch prefix. Any end-stations directly connected to the M770 ATM Switch will only obtain their new prefix if they re-register over ILMI.

To change the switch prefix for the M770 ATM Switch, use the `address prefix` command.

Command: `M15-155s8:/>address prefix <prefix> [node_id] [pg_id]`

Parameters:		
	`<prefix>`	The new switch prefix. The prefix must be a 13-byte address and expressed as 13 two-digit hexadecimal numbers separated by periods. (39.00.01.02.03.04.05.06.07.08.09.aa.bb) is an example of a switch prefix address. The first byte of the switch prefix address must be 39, 45, 47 or 49. For more information see text in the introduction to this section.
	`[node_id]`	Optional parameter that indicates that the PNNI node ID shall be changed according to the new prefix
	`[pg_id]`	Optional parameter that indicates that the PNNI peer group ID shall be changed according to the new prefix

Note: You must reboot the switch before the above command will take affect. You must update all the other affected switches' static routing table entries with the new switch prefix. If you are using PNNI routing then the affected routing entries will be updated automatically.

Resetting the saved switch prefix

You can reset the saved switch prefix to current address. This prevents the current address from changing even after a reset.

To reset the saved switch prefix, use the `address reset` command.

Command:

```
M15-155s8:/>address reset
```

Setting the switch prefix to its default value

The default prefix is 39.00.00.00.00.00.00.xx.xx.xx.xx.xx.xx where x is the MAC address of the switch master agent module.

To change the switch prefix for the M770 ATM Switch to its default value, use the `address default` command.

Command:

```
M15-155s8:/>address default
```

Output:

```
Done.
```

Note: You must reboot the switch before the above command will take affect. You must update all the other affected switches' static routing table entries with the new switch prefix. If you are using PNNI routing then the affected routing entries will be updated automatically.

Viewing or changing the IP time server address

A time server is a server that provides the date and time, as specified by RFC 868, such as a UNIX machine running 'timed' to the M770 ATM Switch. You must provide the M770 ATM Switch with the IP address of a time server or set the M770 ATM Switch to discover the server on the network by broadcasting requests. To view the time received from the time server, use the `system time` command (refer to Chapter 17, "Managing System Commands" for details). To view the current time server, use the `ip timeserver` command.

Command:

```
M15-155s8:/>ip timeserver
```

Output:

```
The M770 is requesting the time from a server at
192.16.1.14
The M770 will use the first time server that responds to a
broadcast request.
```

To set or change the time server, use the `ip timeserver` command.

Command:

```
M15-155s8:/>ip timeserver [<address> | discover]
```

Parameters:

`<address>`	This enables you to specify the IP address of the time server.
`discover`	This enables the M770 ATM Switch to discover the server by broadcasting requests.

Using PING

The M770 ATM Switch allows you to PING an IP address. The M770 ATM Switch will send one Internet Control Message Protocol (ICMP) echo request to the address each second until you press CTRL-C. Whenever the remote device responds, the time taken to respond is displayed in milliseconds.

To PING an IP address, use the `ip ping` command.

Command:

```
M15-155s8:/>ip ping <address>
```

Example:

```
M15-155s8:/>ip ping 192.32.220.5
```

Parameters: `<address>` The IP address for the remote device.

Output:

```
PING: target address is 192.32.220.5
Type Control+C to stop the ping sequence
Response from 192.32.220.5: seq 0, delay 5 ms
Response from 192.32.220.5: seq 1, delay 2 ms
Response from 192.32.220.5: seq 2, delay 2 ms
Response from 192.32.220.5: seq 3, delay 1 ms
Response from 192.32.220.5: seq 4, delay 1 ms
Ping of 192.32.220.5
        Packets sent:      5
        Packets received: 5
```

Note: The command will continue to PING. To interrupt it, press CTRL-C.

Managing the IP Cache

This section explains how to view the IP and route ARP cache of the M770 ATM Switch and how to delete entries in the ARP cache.

Listing the contents of the Avaya M770 ATM Switch’s IP ARP cache

When listing the contents of the M770 ATM Switch’s IP ARP cache, the destination IP and MAC addresses are shown. Also displayed is whether or not the ARP process has completed for each destination IP address in the IP ARP cache.

An entry in the cache becomes aged out 30 minutes from the last time it was used.

To display the contents of the M770 ATM Switch’s IP ARP cache, use the `ip arpcache show` command.

Command:

```
M15-155s8:/>ip arpcache show
```

Output:

```
IP ARP cache entries
--------------------------------
192.32.220.5- 00.00.F6.1A.3C.62 (complete)
196.32.220.4- 00.00.F6.09.18.59 (complete)
196.32.220.8- 00.00.F6.09.44.3F (complete)
196.32.220.19- incomplete
```

Deleting an entry from the Avaya M770 ATM Switch’s IP ARP cache

When you delete an entry from a M770 ATM Switch IP ARP cache that still has IP traffic on it, there will be a short delay while the ARP process finds the remote host and the IP address is added to the ARP cache again.

Note: If an IP address is moved on the network then you should delete the entry in the IP ARP cache to force the M770 ATM Switch to locate the new MAC address.

To delete an entry from the M770 ATM Switch’s IP ARP cache, use the `ip arpcache delete` command.

Command:

```
M15-155s8:/>ip arpcache delete <address>
```

Parameters:

`<address>`	A standard IP address that is to be removed from the ARP cache.

Listing the contents of the Avaya M770 ATM Switch’s IP route cache

The destination IP address, the router address, and the network mask are displayed for each entry in the IP route cache. The default router address is also displayed. This uses the M770 ATM Switch’s IP gateway address.

To display the contents of the M770 ATM Switch’s IP route cache, use the `ip routecache` command.

Command:

```
M15-155s8:/>ip routecache
```

Output:

```
IP route cache entries
--------------------------------
Destination   Mask            Router       Interface
127.0.0.0     255.0.0.0       (local)      m-spv
149.49.34.0   255.255.255.0   (local)      lec
default       *               149.49.34.5  lec
```

Connection Admission Control (CAC)

The M770 ATM Switch carries out Connection Admission Control (CAC) on both the input and output ports to ensure that there is enough bandwidth to allow the call to be accepted.

Bandwidth is reserved in the following manner for the different service categories:

- CBR -Bandwidth equal to Peak Cell Rate (PCR) requested will be allocated, if available.
- VBR -Bandwidth allocation will use the Simple Generic CAC (SGCAC) algorithm described in PNNI 1.0. This is based on PCR and SCR (Sustainable Cell Rate) requested.
- UBR -UBR calls will always be accepted (assuming the limit on active VCs has not been reached).

Note: If you have any rate limit set on a port then CAC will not allow you to set up connections which could exceed the set limit.

All new circuits through the switch are allocated according to the SGCAC, this provides the optimum usage of the bandwidth through your switch.

Allocating VBR bandwidth according to the SGCAC algorithm

To allocate VBR bandwidth according to SGCAC algorithm method, use the `cac sgcac` command.

Command: `M15-155s8:/>cac sgcac`

Output: `VBR bandwidth now allocated according to SGCAC.`

Allocating VBR bandwidth according to the PCR

To allocate VBR bandwidth according to PCR method, use the `cac pcr` command.

Command: `M15-155s8:/>cac pcr`

Output: `VBR bandwidth now allocated according to PCR.`

Viewing VBR bandwidth allocation method

To view the VBR bandwidth allocation method currently being used, use the `cac show` command.

Command: `M15-155s8:/>cac show`

Output: `VBR bandwidth allocated according to SGCAC.`

Managing Physical Ports

This chapter describes how to use the command-line interface to manage and configure physical ports. For information about how to access and use the M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Listing Information About All Physical Ports

You can view information about all of the physical ports. When a module is installed in the M770 ATM Switch, default physical ports are created for all of its ports. Each of these default physical ports is assigned a physical port id. The physical port id consists of the slot number in which the module is installed and the port number.

To display information for all physical ports, enter the `pport show` command.

Command: `M15-155s8:/>pport show`

Output:

```
Physical Port Information
Port Admin  Oper  Speed  Framing  VPI     VPC VPI      VCI
Id   State  State Kbps   Mode      Range  Range
8.0   Up    Up    ---    ---     [0..0]  [0..4095]    [0..1023]
8.1   Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.2   Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.3   Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.4   Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
.
.
.
8.13  Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.14  Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.15  Up    Down  155520 Sonet   [0..7]    ---        [0..1023]
8.16  Up    Down  155520 Sonet   [0..7]    ---        [0..65535]


Port  Cell        Payload       Media   Media  Last
Id    Mode        Scrambling    Type    Mode   Change
8.0   Unassigned  On            ---     UP    ---
8.1   Unassigned  On            MMF     LRDI   0:00:00:15.0
8.2   Unassigned  On            MMF     UP     0:00:00:54.4
8.3   Unassigned  On            MMF     LRDI   0:00:00:22.8
8.4   Unassigned  On            MMF     UP     0:00:00:63.4
.
.
8.11  Unassigned  On            MMF     UP    0:00:00:06.7
8.12  Unassigned  On            MMF     UP    0:00:00:12.1
8.13  Unassigned  On            MMF     UP    0:00:00:30.1
8.14  Unassigned  On            MMF     UP    0:00:00:19.9
8.15  Unassigned  On            MMF     UP    0:00:00:27.4
8.16  Unassigned  Off           ---     ---    ---
```

Note: In the Table above, Port 0 is the CPU port and Port 16 is the Backplane port.

Note: When you enter M4-DS3s8:/> pport show for the DS3 module you will see all of the parameters displayed in the Table above, with information at the bottom of the table for several additional Physical Port parameters displayed only for DS3 modules. See the Table below.

Command:

```
M4-DS3s8:/>pport show
```

Output:

```
Physical Port Information
Port   Cell    Line   Cable        Tx      Loop
Id     Mapping Code   Length       Clock   Back
8.0    ---     ---    ---          ---     ---
8.1    PLCP    B8ZS   >225 feet    Local   None
8.2    ADM     B8ZS   0-225 feet   Local   None
8.3    ADM     B8ZS   0-225 feet   Local   None
8.4    PLCP    B8ZS   0-225 feet   Local   None
8.5    ---     ---    ---          ---     ---
```

Note: In the Table above, Port 0 is the CPU port and Port 5 is the Backplane port.

The `pport show` command displays the information described in Table 5.1.

Table 5.1 Output from the pport show command

Field	Description
Port Id	The physical port number. This is displayed in the format <slot>.<port number>.
Admin State	The administrative state of the physical port. If the state is UP then this physical port is enabled. If the state is DOWN then this physical port is disabled. This will occur when you disable the physical port using the command-line interface or use SNMP.
Oper State	The operational state of the physical port. If the state is UP then this physical port is functional. If the state is DOWN then this physical port is not functional. This could be due to a problem with the physical connection.
Speed (kbps)	The speed for a physical port in kbps.
Framing Mode	The physical layer framing for a physical port. For fiber the value is either Sonet or SDH. The default setting is Sonet. For DS3 the value is either C-bit or M23. The C-bit framing mode for DS3 reserves the C-bits for application-specific uses. The M23 framing mode for DS3 uses the C-bits to indicate the presence or absence of stuffing bits. The default setting is C-bit. The CPU port will always display “_ _ _” and the Backplane port will always display “_ _ _”.

Table 5.1 Output from the pport show command

Field	Description
VPI Range	The VPI range assigned to a physical port.
VPC VPI Range	The VPC VPI range used for VPCs (Virtual Path Connections).
VCI Range	The VCI range assigned to a physical port.
Cell Mode	The empty cell generation mode for a physical port. This can be either Idle or Unassigned. The default setting is Unassigned.
Payload Scrambling	The payload scrambling mode for a physical port. This can be enabled or disabled. The default setting is set to On.
Media Type	The media type for a physical port. MMF (Multi-Mode Fiber) cable. SMF (Single-Mode Fiber) cable. UTP (Unshielded Twisted Pair) cable. Coaxial (BNC) cable.
Media Mode	The Media Mode shows the status of the physical port, which is normally UP.
Last Change	The Last Change shows the time when the port entered it's current state. The time format dd:hh:mm:ss:ds
Cell Mapping (DS3 only)	The Cell Mapping shows the mapping mode used for the transport of ATM cells over DS3. The Mapping mode is either ADM (ATM Direct Mapping) or PLCP (Physical Layer Convergence Protocol). The default setting is ADM.
Line Code (DS3 only)	The supported Line Code is always B8ZS.
Cable Length (DS3 only)	The BNC coaxial cable length can be either 0-225 feet or 225-450 feet. The default setting is 225-450 feet.
Tx Clock (DS3 only)	The transmit clock source is either local (derives the clock internally), or loop (derives the clock from the received signal). The default setting is local.
Loopback (DS3 only)	Loopback is either line loopback (the receiver loops back the received line signal), or payload loopback (the receiver loops back the received payload), or none. The default setting is none.

Displaying Counter Information for a Physical Port

You can view general counter information for all physical ports by using the command: `pport show counters`.

There are two additional counter commands available only for DS3 modules that will display DS3-specific counter information:

- `pport show ds3counters`
- `pport show plcpcounters`

Displaying counter information for all physical ports

To display counter information for all physical ports, enter the `pport show counters` command.

Command: `M4-DS3s8:/>pport show counters`

Output:

```
Physical Port Counters
----------------------
Port                Tx      Rx       Tx       Rx      Rx
ID               Cells   Cells   Discar   Discar  Errors
                                      ds       ds
8.0             151971  128993        0        0       0
8.1                  0       0        0        0       0
8.2                  0       0        0        0       0
8.3             279163  101045        0        0       0
8.4             310163  131011        0        0       0
(Port 5 = Backplane, Port 0 = Cpu)
```

The `pport show counters` command displays the information described in Table 5.2.

Table 5.2 Output from the pport show counters command

Field	Description
Port Id	The physical port. This is displayed in the format <slot>.<port>
Tx Cells	The number of cells that have been transmitted through the physical port.
Rx Cells	The number of cells that have been received through the physical port.
Tx Discards	The number of transmitted cells that have been discarded.
Rx Discards	The number of received cells that have been discarded.

Table 5.2 Output from the pport show counters command

Field	Description
Rx Errors	The number of cell errors that have been received through the physical port.

Displaying counter information for DS3 physical ports

You can view counter information specific only to DS3 modules by entering the command: `pport show ds3counters`. The information this command displays will not appear when you enter the command: `pport show counters.`

DS3 Counter information is accumulated in 15 minute completed intervals for the last 24 hours the system was up. Fewer than 96 intervals of information will be available if the module has been restarted within the last 24 hours.

There are 96 (15 minute) intervals numbered 1-96 with interval 0 always the current interval, interval 1 the interval most recently completed, and interval 96 the earliest possible interval. As soon as the current 15 minute interval ends, a new current interval 0 starts.

`The pport show ds3counters current` command displays counter information only for the current interval. The `pport show ds3counters interval` command displays a historical record of the counters for the completed intervals (up to 96 completed intervals) during the last 24 hours the system was up.

Note: The `pport show ds3counters` command displays counter information specific only to DS3 modules.

Command: `M4-DS3s8:/>pport show ds3counters [ne|fe] [current|total|interval [<pport id>]]`

Example: `M4-DS3s8:/>pport show ds3counters ne current`

Parameters:

ne	To specify that the counter information is supplied from the near end.
fe	To specify that the counter information is supplied from the far end.
current	To specify that the ne/fe counter information is supplied from the current interval for all ports.
total	To specify that the ne/fe counter information is supplied for the last 24 hours for all ports.
interval [pport id]	To specify that the ne/fe counter information is supplied in all intervals (up to 96) for all ports. If the physical port identifier is entered, only the interval counters for the specified DS3 port are displayed. If no value is specified, then the interval counters for all DS3 ports are displayed.

Note: The `pport show ds3counters` command displays several parameters for near end (ne) counter information (PESS, PSESS, LCVS, PCVS, LESS) that are not displayed for far end (fe) counter information.

To display DS3 counter information for all near end DS3 physical ports for the current interval, use the `pport show ds3counters ne current` command.

Command:
```
M4-DS3s8:/>pport show ds3counters ne current
```

Output:
```
Link near end current counters
----------------------
Port   PESS  PSES  UASS  LCVS  PCVS  LESS  CCVS  CESS  CSES
ID           S                                         S
8.1       0     0     0     0     0     0     0     0     0
8.2       0     0     0     0     0     0     0     0     0
8.3       0     0     0     0     0     0     0     0     0
8.4       0     0     0     0     0     0     0     0     0
```

The `pport show ds3counters ne current` command displays the information described in Table 5.3.

Table 5.3 Output from the pport ds3show ne current counters command

Field	Description
Port Id	The physical port. This is displayed in the format <slot>.<port>
PESS	The number of P-bit errored seconds.
PSESS	The number of P-bit severely errored seconds.
UASS	The number of unavailable seconds.
LCVS	The number of line coding variations.
PCVS	The number of P-bit coding variations.
LESS	The number of line errored seconds.
CCVS	The number of C-bit coding violations.
CESS	The number of C-bit errored seconds.
CSESS	The number of C-bit severely errored seconds.

To display DS3 counter information for all far end DS3 physical ports for the current interval, use the `pport show ds3counters fe current` command.

Command: `M4-DS3s8:/>pport show ds3counters fe current`

Output:

```
Link far end curent counters
----------------------
Port   CESS  CSES  CCVS  UASS
ID             S
8.1       0     0     0     0
8.2       0     0     0     0
8.3       0     0     0     0
8.4       0     0     0     0
```

Note: The `pport show ds3counters` command displays several parameters for near end (ne) counter information (PESS, PSESS, LCVS, PCVS, LESS) that are not displayed for far end (fe) counter information.

To display DS3 counter information for all near end DS3 physical ports in all intervals, use the `pport show ds3counters ne interval` command.

Command: `M4-DS3s8:/>pport show ds3counters ne interval`

Output:

```
Link near end interval counters for
port 8.1
----------------------
Intvl  PESS  PSES  UASS  LCVS  PCVS  LESS  CCVS  CESS  CSES
                S                                          S
1         0     0     0     0     0     0     0     0     0
2         0     0     0     0     0     0     0     0     0
3         0     0     0     0     0     0     0     0     0
4         0     0     0     0     0     0     0     0     0
5         0     0     0     0     0     0     0     0     0


Link near end interval counters for
port 8.2
----------------------
Intvl  PESS  PSES  UASS  LCVS  PCVS  LESS  CCVS  CESS  CSES
                S                                          S
1         0     0     0     0     0     0     0     0     0
2         0     0     0     0     0     0     0     0     0
3         0     0     0     0     0     0     0     0     0
4         0     0     0     0     0     0     0     0     0
5         0     0     0     0     0     0     0     0     0
```

```
Link near end interval counters for
port 8.3
----------------------
Intvl  PESS  PSES  UASS  LCVS  PCVS  LESS  CCVS  CESS  CSES
                S                                         S
1         0     0     0     0     0     0     0     0     0
2         0     0     0     0     0     0     0     0     0
3         0     0     0     0     0     0     0     0     0
4         0     0     0     0     0     0     0     0     0
5         0     0     0     0     0     0     0     0     0


Link near end interval counters for
port 8.4
----------------------
Intvl  PESS  PSES  UASS  LCVS  PCVS  LESS  CCVS  CESS  CSES
                S                                         S
1         0     0     0     0     0     0     0     0     0
2         0     0     0     0     0     0     0     0     0
3         0     0     0     0     0     0     0     0     0
4         0     0     0     0     0     0     0     0     0
5         0     0     0     0     0     0     0     0     0
```

To display far end DS3 counter information for a specific DS3 physical port (for example port 8.3), use the `pport show ds3counters fe interval pport.id` command.

Command: `M4-DS3s8:/>pport show ds3counters fe interval 8.3`

Output:

```
Link far end interval counters for
port 8.3
----------------------
Intvl  CESS  CSES  CCVS  UASS  LCVS  PCVS
                S
1         0     0     0     0     0     0
2         0     0     0     0     0     0
3         0     0     0     0     0     0
4         0     0     0     0     0     0
5         0     0     0     0     0     0
```

Displaying PLCP counter information for DS3 physical ports

You can view PLCP (Physical Layer Convergence Protocol) counter information for physical ports on DS3 modules that have their mapping mode set to PLCP. To view PLCP counter information use the command: `pport show plcpcounters`.

Note: The `pport show plcpcounters` command does not display PLCP counter information for DS3 ports that have their mapping mode set to ADM.

To display DS3 counter information for all DS3 physical ports, enter the `pport show plcpcounters` command.

Command:

```
M4-DS3s8:/>pport show plcpcounters
```

Output:

```
Physical port plcp counters
----------------------

Port       BIP   FERR   FEBE
ID
8.1          0      0      0
8.2          0      0      0
8.3          0      0      0
8.4          0      0      0
```

The `pport show counters` command displays the information described in Table 5.4.

Table 5.4 Output from the pport show plcpcounters command

Field	Description
BIP	Bit interleaved errors (B1).
FERR	Framing Pattern Octet Errors and Path Overhead Identification Octet Errors.
FEBE	Far End Block Errors.

Disabling a Physical Port

Before any physical port parameters can be changed, cleared, or reset, you must disable the physical port. To disable a physical port, use the `pport disable` command.

Command:	`M15-155s8:/>pport disable <pport id>`	
Example:	`M15-155s8:/>pport disable 8.1`	
Parameter:	`<pport id>`	The physical port identifier in the form <slot>.<port number>

Enabling a Physical Port

To enable a physical port, use the `pport enable` command.

Command:	`M15-155s8:/>pport enable <pport id>`	
Example:	`M15-155s8:/>pport enable 8.1`	
Parameter:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.

Setting Physical Port Parameters

You can set individual parameters for a physical port. Once a physical port parameter has been set, ILMI will not override the parameter when the physical port is re-enabled.

You can set the following parameters for all physical ports:

- payload scrambling
- framing mode
- transmit rate limit

You can set the following parameters only for physical DS3 ports:

- cable length
- mapping mode
- loopback type
- Tx clock source

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To set a parameter for a physical port, you must perform the following steps:

1. Disable the physical port.
2. Set the parameter for the disabled physical port, as required.
3. Enable the physical port.

Configuring payload scrambling

You can configure payload scrambling on or off. The default setting on.

When payload scrambling is enabled, the transmitted data will be passed through a self-synchronizing scrambler with the polynomial $x^{43}+1$. This provides security against false cell and frame delineation.

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To configure payload scrambling for a physical port, use the `pport set payloadscrambling` command.

Command:	`M15-155s8:/>pport set payloadscrambling <pport> [on | off]`	
Example:	`M15-155s8:/>pport set payloadscrambling 8.3 on`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.
	`[on | off]`	To specify the whether payload scrambling is on or off.

Specifying the framing mode for a port

You can specify that the framing mode used for a physical fiber optic port is either Sonet or SDH. The default setting is Sonet. For DS3 modules you can specify that the framing mode used for a DS3 physical port is either CBIT or M23. The default setting for DS3 ports is CBIT.

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To specify framing for a physical fiber optic port, use the `pport set framing` command.

Command:	`M15-155s8:/>pport set framing <pport> [sonet | SDH]`	
Example:	`M15-155s8:/>pport set framing 8.1 SDH`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.
	`Sonet`	Sets the framing mode for the physical port to Sonet. The default setting is Sonet.
	`SDH`	Sets the framing mode for the physical port to SDH.

To specify framing for a DS3 physical port, use the `pport set framing` command.

Command:	`M4-DS3s8:/>pport set framing <pport> [CBIT | M23]`	
Example:	`M4-DS3s8:/>pport set framing 8.2 CBIT`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.
	`CBIT`	Sets the framing mode for the physical port to CBIT. The default setting is CBIT.
	`M23`	Sets the framing mode for the physical port to M23.

Configuring transmit rate limit for the M15-155 module

This command is supported only by M15-155 ATM modules.

The M770 ATM Switch hardware enables you to configure the peak output cell rate of any port to be restricted, to control congestion on the network. This feature is used for traffic shaping, mainly when you have a WAN connection.

For example, if a 155Mbps port is connected to another service at a lower rate (<155Mbps), then this will require the data cell rate (ignoring idle cells) to be rate limited at the output port of the switch.

The outcome of this command can be seen in “pport show” in the speed column.

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To configure Tx rate limiting for a physical port, use the `pport set txrate` command.

Command:	`M15-155s8:/>pport set txrate <pport> <rate>`	
Example:	`M15-155s8:/>pport set txrate 8.3 100`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.
	`<rate>`	To specify the port transmit rate in Kbits per second. You can set the minimum rate capping to 64K bit per second.

Note: The M770 ATM Switch CAC feature is aware of any rate limit set on a port and will not allow connections to be setup which could exceed the current limit. All UBR connections are accepted as usual, however these may suffer cell loss if the total traffic rate exceeds the current rate limit.

Specifying a cable length for a DS3 port

You can specify the coaxial (BNC) cable length for a DS3 port. The coaxial cable length is up to these numbers in feet:

- 225: 0-225 feet, 0-68 meters.
- 450: 225-450 feet, 68-137 meters.

The default cable length is 225 (i.e. 0-225 feet).

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To configure the coaxial cable length for a DS3 port, use the `pport set length` command.

Command:	`M4-DS3s8:/>pport set length <<slot>.<port>> [225|450]`	
Example:	`M4-DS3s8:/>pport set length 8.1 225`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port number>.
	`225`	Sets the allowable coaxial cable length to: 0-225 feet, 0-68 meters.
	`450`	Sets the allowable coaxial cable length to: 225-450 feet, 68-137 meters.

Specifying a mapping mode for a DS3 port

You can specify for a DS3 port the mapping mode used for the transport of ATM cells over DS3. The mapping mode is either ADM or PLCP. The default mapping mode is ADM.

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To set the mapping mode for a DS3 port, use the `pport set mapping` command.

Command:	`M4-DS3s8:/>pport set mapping <<slot>.<port>> [adm	plcp]`	
Example:	`M4-DS3s8:/>pport set mapping 8.2 plcp`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port.number>.
	`adm`	Sets the mapping mode to ADM. The default setting is ADM.
	`plcp`	Sets the mapping mode to PLCP.

Specifying loopback type for a DS3 port

You can specify loopback type for a DS3 port. Loopback is either line loopback (the receiver loops back the received line signal), or payload loopback (the receiver loops back the received payload), or none (no loopback). The default loopback is none (no loopback).

Note: In order to start/stop loopback using the `set loopback` command both the Admin state and Oper state of the port must be UP. Another method of stopping loopback is to disable the port. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To set the loopback type for a DS3 port, use the `pport set loopback` command.

Command:	`M4-DS3s8:/>pport set loopback <<slot>.<port>>[payload|line|none]`	
Example:	`M4-DS3s8:/>pport set loopback 8.1 line`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port.number>.
	`payload`	Sets the loopback type to payload.
	`line`	Sets the loopback type to line.
	`none`	Sets the loopback type to none.

Specifying the Tx Clock source for a DS3 port

You can specify the transmit clock source for a DS3 port. The transmit clock source is either local (derives the clock internally), or loop (derives the clock from the received signal). The default setting is local.

To set the Tx clock source for a DS3 port, use the `pport set txClock` command.

Command:	`M4-DS3s8:/>pport set txClock <<slot>.<port>>[local|loop]`	
Example:	`M4-DS3s8:/>pport set loopback 8.1 line`	
Parameters:	`<pport id>`	The physical port identifier in the form <slot>.<port.number>.
	`local`	Sets the transmit clock source to local.
	`loop`	Sets the transmit clock source to loop.

Resetting Parameters on a Physical Port

You can reset all configurable parameters for a specific physical port to their default values.

Note: You must disable the physical port before you can change, clear or reset any physical port parameters. For more information about how to disable a physical port, see Disabling a Physical Port on page 49.

To reset all configurable parameters on a physical port to their default values, use the `pport reset` command.

Command:	`M15-155s8:/>pport reset <pport id>`	
Parameter:	`<pport id>`	The physical port number in the form <slot>.<port number>

Chapter 6

Managing Virtual Ports

This chapter describes how to use the command-line interface to manage virtual ports.

- For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.
- For more information about virtual ports, see “Virtual Ports” in Appendix F, “Routing and Signalling Concepts”.

Showing Virtual Port Information

Listing information about virtual ports

You can view information about all of the virtual ports on the M770 ATM Switch. When a module is installed in the M770 ATM Switch, default virtual ports are created for the ports. Each of these default virtual ports is assigned a virtual port id of zero.

Any virtual port information that is marked with an asterisk (*) has been learned by the M770 ATM Switch during the ILMI dialogue with the remote device. Information that is not marked with an asterisk has been either configured by the user or is the default setting for the virtual port.

To view configuration information about all of the virtual ports, use the `vport show command` with the following parameters.

Command:

```
M15-155s8:/>vport show [config | status | vpivciranges]
```

Parameter:	`When no parameter is entered.`	This will display the link configuration information about all virtual ports on a module.
	`config`	This will display the link configuration information for all of the virtual ports on a module. For more information see Listing the link configuration information for all virtual ports later in this chapter.
	`status`	This will display the link status information for all of the virtual ports on a module. For more information see Listing the status information for all virtual ports later in this chapter.
	`vpivciranges`	This will display the VPI and signalling VCI ranges for all of the virtual ports on a module. For more information see Listing the VPI and VCI range information for all virtual ports later in this chapter.

To view information about all virtual ports, use the `vport show` command.

Command:

```
M15-155s8:/>vport show
```

Output:

```
Virtual Port Information
Virtual AdminOperStackUserQ.SAALVPISig VCIILMI
Port Id StateStateType/NetStateRangeRangeState

8.0.0   UpUp   InternalUserUp[0..0][32..1023]Disabled
8.1.0   UpDown UNI 3.0NetDown[0..7][32..1000]Inactive
8.2.0   UpDown PNNI-1NetDown[0..7][32..1000]Inactive
8.3.0   UpDown PNNI-1NetDown[0..7][32..1000]Inactive
8.4.0   UpDown PNNI-1NetDown[0..7][32..1000]Inactive
8.5.0   UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.6.0   UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.7.0   UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.8.0   UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.9.0   UpUp   UNI 3.1*NetUp[0..0]*[32..1023]*Ready
8.10.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.11.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.12.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.13.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.14.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.15.0  UpDown PNNI-1NetDown[0..7][32..1023]Inactive
8.16.0  UpUp   PNNI-1*User*Up[0..0][32..65535]*InterSwitch
8.16.1  UpDown PNNI-1NetDown[1..1][32..65535]CStartSent
8.16.2  UpDown PNNI-1NetDown[2..2][32..65535]CStartSent
8.16.3  UpDown PNNI-1NetDown[3..3][32..65535]NoContact
8.16.4  UpDown PNNI-1NetDown[4..4][32..65535]NoContact
8.16.5  UpDown PNNI-1NetDown[5..5][32..65535]NoContact
8.16.6  UpDown PNNI-1NetDown[6..6][32..65535]NoContact
8.16.7  UpDown PNNI-1NetDown[7..7][32..65535]NoContact
8.16.8  UpUp   PNNI-1*Net*Up[8..8][32..65535]*InterSwitch
8.16.9  UpUp   PNNI-1*User*Up[9..9][32..65535]*InterSwitch
8.16.10 UpUp   PNNI-1*User*Up[10..10][32..65535]*InterSwitch
8.16.11 UpUp   PNNI-1*User*Up[11..11][32..65535]*InterSwitch
8.16.12 UpUp   PNNI-1*User*Up[12..12][32..65535]*InterSwitch
8.16.13 UpUp   PNNI-1*User*Up[13..13][32..65535]*InterSwitch
8.16.14 UpUp   PNNI-1*User*Up[14..14][32..65535]*InterSwitch
```

The `vport show` command displays the information described in Table 6.1.

Note: In the above Table “*” indicates that the information was obtained from ILMI protocol. Port 0 is the CPU port and Port 16 is the Backplane port.

Table 6.1 Output from the vport show command

Field	Description
Virtual Port Id	The virtual port. This is displayed in the format <slot>.<port>.<virtual port number>.
Admin State	The administrative state of the virtual port. If the state is UP then this virtual port is enabled. If the state is DOWN then this virtual port is disabled. This will occur when you disable the virtual port using the command-line interface or via management.
Oper State	The operational state of the virtual port. If the state is UP then this virtual port is functional. If the state is DOWN then this virtual port is not functional. This could be due to a problem with ILMI or ILMI has been disabled due to a problem with the physical connection.
Stack Type	The type of signalling used. This can be UNI 3.0, UNI 3.1, UNI 4.0, IISP 3.0, IISP 3.1 or PNNI 1.0.
User / Net	The signalling profile of the virtual port. This can be either “user” or “network”. For more information on which signalling profile should be used, refer to ATM Port Configuration in Chapter 2 Getting Started.
Q.SAAL State	The state of the signalling data-link layer (Q.SAAL-SSCOP).
VPI Range	The VPI range assigned to the virtual port.
VCI Range	The VCI range assigned to the virtual port.

Table 6.1 Output from the vport show command (Continued)

Field	Description
ILMI State	The ILMI state of the virtual port. The possible ILMI states are: Inactive — The virtual port is disabled or the physical layer is down. NoContact — The physical layer is up but the remote ILMI entity is not responding. CStartSent — The M770 ATM Switch is attempting to start an ILMI dialogue (a cold start trap has been sent). GNTimeout — The M770 ATM Switch has received no response to a getnext request from the ILMI prefix table of the remote device. GetRemoteInfo — The M770 ATM Switch is interrogating the remote device to determine link characteristics. SwDoRegPrefix — The M770 ATM Switch telling the remote device about the switch prefix of the M770 ATM Switch. SwWaitAddress — The M770 ATM Switch has set the prefix and is waiting to receive the address from the remote device. SwHaveAddress — The M770 ATM Switch has received the address from the user side. SwToSwPause — There is a pause in the ILMI dialogue between two switches. Ready — ILMI is up on an UNI link (not between two switches). InterSwitch — ILMI is up on a link between two switches. NoPrefixes — ILMI has tried repeatedly to tell the remote device its prefix without success. It will try to bring signalling up but remains in this state. Disabled — ILMI is disabled on this port. ShuttingDown(Disabled) — Port is in the process of disabling ILMI on this port.

Listing the link configuration information for all virtual ports

You can view the link configuration information for all virtual ports on a module or for a specific virtual port.

Any virtual port information that is marked with an asterisk (*) has been learned by the M770 ATM Switch during the ILMI dialogue with the remote device. Information that is not marked with an asterisk has either been configured by the user or is the default setting for the virtual port.

To view the link configuration information about all virtual ports, use the `vport show config` command.

Command: `M15-155s8:/>vport show config [<vport id>]`

Parameter: `<vport id>` The virtual port.
This is displayed in the format <slot>.<port>.<virtual port number>
If a <virtual port number> parameter is not supplied then the link configuration summary information is displayed for all virtual ports.

Example: `M15-155s8:/>vport show config`

Output:

```
Virtual Port Configuration Information
Virtual Admin  OperILMIPollMultiStrictSig. SSCOPWait for
Port Id State  StateEnabledModeRegAALRx. WindowPeer SSCOP
8.0.0  Up     UpNo   DisabledOnOffDefaultNo
8.1.0  Down   DownYesNoneOn  OffDefault  No
8.2.0  Up     UpYes  Port + ESIOnOffDefaultNo
8.3.0  Up     DownYesNoneOn  OffDefault  No
8.4.0  Down   DownYesNoneOn  OffDefault  No
```

The `vport show config` command displays the information described in Table 6.2.

Table 6.2 Output from the vport show config command

Field	Description
Virtual Port Id	The virtual port. This is displayed in the format <slot>.<port>.<virtual port number>.
Admin State	The administrative state of the virtual port. If the state is UP then this virtual port is enabled. If the state is DOWN then this virtual port is disabled. This will occur when you disable the virtual port using the command-line interface or via Management.
Oper State	The operational state of the virtual port. If the state is UP then this virtual port is functional. If the state is DOWN then this virtual port is not functional. This could be due to a problem with ILMI or ILMI has been disabled due to a problem with the physical connection.
ILMI Enabled	Whether or not ILMI is enabled on the virtual port.

Table 6.2 Output from the vport show config command

Field	Description
Poll Mode	ILMI polling is used to verify that the same end-station remains attached at a given port. There are two methods that can be used: • check the ESI has not changed. This is referred to as “Port + ESI”. • check that the system up-time has not changed by a significant amount. This is referred to as “SysUpTime”.
Multi Reg	This specifies whether multiple ILMI registration is enabled or not on the virtual port.
Strict AAL Trans.	This specifies whether the translation of the AAL parameter, that is between UNI 3.0, IISP 3.0, UNI 3.1 and IISP 3.1 should be OFF, Normal or Strict.
Sig. SSCOP Rx. Window	This parameter is reserved for future use. All ports are set to the default parameter.
Wait for Peer SSCOP	This specifies whether this vport will wait indefinitely for an incoming QSAAL connection.

Listing the status information for all virtual ports

You can view the status information for all virtual ports on a module or for a specific virtual port.

Any virtual port information that is marked with an asterisk (*) has been learned by the M770 ATM Switch during the ILMI dialogue with the remote device. Information that is not marked with an asterisk has either been configured by the user or is the default setting for the virtual port.

To view the virtual port status, enter the `vport show status` command.

Command: `M15-155s8:/>vport show status [<vport id>]`

Parameter: `<vport id>` The virtual port.
This is displayed in the format <slot>.<port>.<virtual port number>.
If a <vport number> parameter is not supplied then the link status summary information is supplied for all virtual ports.

Example: `M15-155s8:/>vport show status`

Output:

```
Virtual Port Status Information
Virtual AdminOperStackUserQ.SAALQ.2931PNNI-HelloILMIILMI
Port Id StateStateType/NetStateStateStateVerState
8.0.0   UpUp   InternalUserUpUpDown4.0Disabled
8.1.0   UpDown PNNI 1.0NetDownDownDown4.0Inactive
8.2.0   UpUp   UNI 3.1*Net*UpUpDown3.x*Ready
8.3.0   UpUp   UNI 4.0*Net*UpUpDown4.0*Ready
8.4.0   UpUp   PNNI 1.0*Net*UpUpUp4.0* InterSwitch
```

The `vport show status` command displays the information described in Table 6.3.

Table 6.3 Output from the vport show status command

Field	Description
Virtual Port Id	The virtual port. This is displayed in the format <slot>.<port>.<virtual port number>.
Admin State	The administrative state of the virtual port. If the state is UP then this virtual port is enabled. If the state is DOWN then this virtual port is disabled. This will occur when you disable the virtual port using the command-line interface or the Avaya M770 ATM Switch Manager.
Oper State	The operational state of the virtual port. If the state is UP then this virtual port is functional. If the state is DOWN then this virtual port is not functional. This could be due to a problem with ILMI or ILMI has been disabled due to a problem with the physical connection.
Stacktype	The type of signalling used. This can be UNI 3.0, UNI 3.1, UNI 4.0, IISP 3.0, IISP 3.1 or PNNI 1.0.
User / Net	The signalling profile of the virtual port. This can be either “user” or “network”. For more information on which signalling profile should be used, refer to ATM Port Configuration in Chapter 2 Getting Started.
Q.SAAL State	The state of the signalling data-link layer (SAAL).
Q.2931 State	The state of the signalling layer (Q.2931).
ILMI Ver	The version of ILMI running on this virtual port.
ILMI State	The ILMI state of the virtual port. For a list of the different ILMI states, see Table 6.1, “Output from the vport show command,” earlier in this chapter.

Listing the VPI and VCI range information for all virtual ports

You can view the VPI and signalling VCI range information for all virtual ports on a module or for a specific virtual port.

Any virtual port information that is marked with an asterisk (*) has been learned by the M770 ATM Switch during the ILMI dialogue with the remote device. Information that is not marked with an asterisk has either been configured by the user or is the default setting for the virtual port.

To view VPI and signalling VCI range information about the virtual ports, use the `vport show vpivciranges` command.

Command:

```
M15-155s8:/>vport show vpivciranges [<vport id>]
```

Parameter: `<vport id>` The virtual port.
This is displayed in the format <slot>.<port>.<virtual port number>.
If a <vport number> parameter is not supplied then the VPI and signalling VCI ranges are supplied for all virtual ports.

Example:

```
M15-155s8:/>vport show vpivciranges
```

Output:

```
Virtual Port VPI and VCI Ranges
VirtualVPISig VpciSig VCISig Vpci
Port IdRangeRangeRangeBase
8.0.0  [0..0][0..0][32..1023]0
8.1.0  [0..7][0..7][32..1023]0
8.2.0  [0..0]*[0..0]*[32..1023]*0
8.3.0  [0..7][0..7][32..1023]0
8.4.0  [0..7][0..7][32..1023]0
```

The `vport show vpivciranges` command displays the information described in Table 6.4.

Table 6.4 Output from the vport show vpivciranges command

Field	Description
Virtual Port Id	The virtual port. This is displayed in the format <slot>.<port>.<virtual port number>.
VPI Range	The VPI range assigned to the virtual port.
Sig VPCI Range	The signalling VPCI range assigned to the virtual port.
Sig VCI Range	The signalling VCI range assigned to the virtual port.
Sig VPCI Base	The signalling VPCI base on a non-root virtual port.

Listing bandwidth information for all virtual ports

To view bandwidth information for all virtual ports on a module, use the `vport show bandwidth command.`

DS3 modules use traffic shaping on virtual ports. Traffic is shaped based on the total bandwidth assigned to each virtual port. The bandwidth assigned can be seen as Total BW. For more information see “Traffic shaping for DS3 virtual ports“ on page 64.

On non-DS3 modules there is no rate limit shaping. Therefore the maximum transmit rate for a vport is limited by the capacity of the physical port and not by the total bandwidth assigned to the vport. .

Command: `M4-DS3s8:/>vport show bandwidth status (cells/sec)`

Output:

```
Virtual Port Bandwidth status (cells/sec)
----------------------
                Total BW    Alloc BW     Curr       Curr

Virtual       In    Out    In    Out  PVPC  PVCC  SVPC  SVCC
Port ID
8.0.0      34732  34732     0     0     0     0     0     0
               1      1
8.1.0      90118  90118     0     0     0     0     0     0

8.1.3       2358   2358     0     0     0     0     0     0

8.1.5      11792  11792     0     0     0     0     0     0

8.2.0      43980  43980     0     0     0     0     0     0

8.2.3      47168  47168     0     0     0     0     0     0

8.2.4      13120  13120     0     0     0     0     0     0

8.3.0      10426  10426     0     0     0     0     0     0
               8      8
8.4.0      10426  10426     0     0     0     0     0     0
               8      8
```

Configuring Virtual Ports

Creating a virtual port

Note: Before you can create a new virtual port you must assign a VPI range. To do this you must first reduce the VPI range of the root virtual port. For more information about setting the VPI range for a virtual port, see Setting Virtual Port Parameters later in this chapter on page 69.

To control shaping use the `vport create` command.

Command: `M4-DS3s8:/>vport create <vport id> <VPI> [<bandwidth>]`

Example: `M4-DS3s8:/>vport create 1.2.3 4 2358`

Parameters:

`<vport id>` The new virtual port identifier is an integer which isn’t yet used to represent a virtual port on this physical port. The virtual port is in the form <slot>.<port>.<virtual port number>.

`<vpi>` The virtual path to be associated with this virtual port. This virtual path must already exist on physical port <slot>.<port>

`[<bandwidth>]` Applicable for DS3 modules only. An optional parameter to set the bandwidth pool. The default value is root max bandwidth/ max number of vports per port. The bandwidth is measured in CPS.

Traffic shaping for DS3 virtual ports

The M4-DS3 module supports traffic shaping (rate limit shaping) on its virtual ports. You can use shaping only on non-root virtual ports.

All aggregated traffic (SVCs, PVCs etc.) going out of the vport is shaped to the Peak Cell Rate (PCR) which is configured by the user for that vport. Rate limit shaping means that the DS3 module will adjust the transmitted traffic to a rate no higher than the user defines as the PCR for the vport. The DS3 module uses a 256k buffer to allow bursty traffic to be accumulated in the switch and then be sent out later.

In order to control shaping you use the `vport create` command. The `bandwidth` parameter defines the Peak Cell Rate (PCR) allowed on a vport and is defined in Cells Per Second (Cells / sec).

If you do not define a bandwidth value, then a default rate is assigned to that vport. The default rate is calculated as follows: the actual maximum bandwidth of the port divided by the maximum number of vports that can be defined on a port. The actual maximum bandwidth of a ports takes into account the overhead associated with the different cell mappings (ADM / PLCP). The maximum number of vports per port depends on the number of vpi bits configured for the module.

For example, if the number of VPI bits is 3 and we are using ADM then the default bandwidth assigned for a vport is 104268 CPS divided by 8. However, if we were using PLCP, the default bandwidth would be 95990 CPS divided by 8.

Deleting a virtual port

To delete a virtual port, use the `vport delete` command.

Command:	`M15-155s8:/>vport delete <vport id>`	
Example:	`M15-155s8:/>vport delete 8.1.4`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Disabling a virtual port

Before any virtual port parameters can be changed or reset you will have to disable the virtual port.

To disable a virtual port, use the `vport disable` command.

Command:	`M15-155s8:/>vport disable <vport id>`	
Example:	`M15-155s8:/>vport disable 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Enabling a virtual port

To enable a virtual port, use the `vport enable` command.

Command:	`M15-155s8:/>vport enable <vport id>`	
Example:	`M15-155s8:/>vport enable 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Managing ILMI

Disabling ILMI on a virtual port

If an attached device does not support ILMI, you will need to disable ILMI on the virtual port. Note that if the remote device is an end-station then address registration will not take place automatically and a static route will need to be added for the attached device.

To disable ILMI on a virtual port, use the `vport disable` command.

Command:	`M15-155s8:/>vport disable <vport id> ilmi`	
Example:	`M15-155s8:/>vport disable 8.1.0 ilmi`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`ilmi`	ILMI is a protocol used by a switch to learn about an attached device.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

Disabling ILMI polling on a virtual port

If an attached end-station does not support ILMI polling, the M770 ATM Switch will not poll to ensure the integrity of the link. However, if the end-station does support ILMI polling but is not responding to polls in time, the virtual port will not become operational at all or be intermittent. Before the virtual port can become operational, you will need to disable ILMI polling.

To disable ILMI polling on a virtual port, use the `vport disable` command.

Command:	`M15-155s8:/>vport disable <vport id> poll`	
Example:	`M15-155s8:/>vport disable 8.1.0 poll`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`poll`	ILMI polling is a mechanism used by the M770 ATM Switch to ensure that the same end-station is still attached to it. Since ILMI polling is an enhancement to ILMI, when ILMI is disabled, polling is also disabled.

Disabling ILMI multiple registration

Disables the registration of the same address via ILMI, on multiple ports.

To disable ILMI registration on multiple ports, use the `vport disable` command.

Command:	`M15-155s8:/>vport disable <vport id> ilmimultireg`
Example:	`M15-155s8:/>vport disable 8.1.0 ilmimultireg`

Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`ilmimultireg`	ILMImultireg is an enhancement to ILMI, when ILMI is disabled, ILMImultireg is also disabled. By default `ilmimultireg` is enabled on a M770 ATM Switch.

Enabling ILMI on a virtual port

To enable ILMI on a virtual port, use the `vport enable` command.

Command:
```
M15-155s8:/>vport enable <vport id> ilmi
```
Example:
```
M15-155s8:/>vport enable 8.1.0 ilmi
```

Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`ilmi`	ILMI is a protocol used by a switch to learn about an attached device.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

Enabling ILMI polling on a virtual port

To enable ILMI polling on a virtual port, use the `vport enable` command.

Command:
```
M15-155s8:/>vport enable <vport id> poll
```
Example:
```
M15-155s8:/>vport enable 8.1.0 poll
```

Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`poll`	ILMI polling is a mechanism used by the M770 ATM Switch to ensure that the same device is still attached. Since ILMI polling is an enhancement to ILMI, ILMI must already be enabled.

Enabling ILMI multiple registration

A given address can be registered via ILMI on multiple ports.

To enable ILMI registration on multiple port, use the `vport enable` command.

Command:
```
M15-155s8:/>vport enable <vport id> ilmimultireg
```
Example:
```
M15-155s8:/>vport enable 8.1.0 ilmimultireg
```

Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`ilmimultireg`	ILMImultireg is an enhancement to ILMI, when ILMI is disabled, ILMImultireg is also disabled. By default `ilmimultireg` is enabled.

Setting the ILMI version on a virtual port

This parameter changes the ILMI version used on this vport. By default, this parameter is ILMI 4.0 which is backwards compatible with devices using ILMI 3.1.

To set the ILMI version on the virtual port use the `vport set ilmiver` command.

Command:	`M15-155s8:/>vport set ilmiver <vport id> [31 | 40]`	
Example:	`M15-155s8:/>vport set ilmiver 8.1.0 31`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`[31 | 40]`	Changes the ILMI Version to ILMI 3.1 or 4.0

Resetting the ILMI version on a virtual port

If you reset the virtual port’s ILMI version parameter, the port will re-learn the ILMI version when it is enabled and a remote device is connected.

To reset the ILMI version on the virtual port, use the `vport reset ilmiver` command.

Command:	`M15-155s8:/>vport reset ilmiver <vport id>`	
Example:	`M15-155s8:/>vport reset ilmiver 8.1.0`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Setting Virtual Port Parameters

You can set individual parameters for a virtual port. Once a virtual port parameter has been set, ILMI will not override the parameter when the virtual port is re-enabled. If you want ILMI to override a set parameter, you must disable the virtual port and clear the parameter. You must then re-enable the virtual port.

You can set the following virtual port parameters using the `vport set` command:

- Signalling profile
- Signalling stack type
- Signalling VPCI range
- Signalling VPCI base
- Signalling VCI range
- VPI range on a root virtual port
- ILMI version
- Waiting for incoming Q.SAAL connection

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

To set a parameter for a virtual port, you must perform the following steps:

1. Disable the virtual port.
2. Set the parameter for the disabled virtual port, as required.
3. Enable the virtual port.

Setting the signalling profile parameter

You can set the signalling profile on a virtual port to either "user" or "network". One side of the link must be set to "user" and the other side to "network". If ILMI is enabled, then normally end-stations are always the "user" side of a link. For more information on which signalling profile should be used for an attached device, see ATM Port Configuration on page 12.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

To set the signalling profile for a virtual port, use the `vport set profile` command.

Command:
```
M15-155s8:/>vport set profile <vport id> [user | network]
```

Example:	`M15-155s8:/>vport set profile 8.1.0 user`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`user`	During signalling the virtual port will act as the user side of the connection.
	`network`	During signalling the virtual port will act as the network side of the connection. The default signalling profile is “network”. However, on an inter-switch link, using IISP, one side of the link will have to be configured to “user” side. This does not apply when 2 M770 ATM Switches are connected together which will automatically configure one side of the link to “user”.

Setting the stack type parameter

You can set the signalling stack type for a virtual port. The default signalling stack type is PNNI 1.0.

The signalling stack type can be:

- UNI 3.0
- UNI 3.1

  Note, straight “IISP” is by default based on UNI 3.1 signalling.
- UNI 4.0
- IISP 3.0
- IISP 3.1
- PNNI 1.0

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To set the signalling stack type for a virtual port, use the `vport set stacktype` command.

Command:	`M15-155s8:/>vport set stacktype <vport id> <value>`	
Example:	`M15-155s8:/>vport set stacktype 8.1.0 UNI 3.1`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`<value>`	Selects the type of signalling stack that will be used for the virtual port.

Setting the signalling VPCI range

You can set a signalling VPCI range for a virtual port. This range can only be changed on the root virtual port.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To set a signalling VPCI range for a virtual port, use the `vport set sigvpcirange` command.

Command:	`M15-155s8:/>vport set sigvpcirange <vport id> <range>`	
Example:	`M15-155s8:/>vport set sigvpcirange 8.1.0 [0..2]`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`<range>`	Selects the signalling VPCI range that will be used for the virtual port.

Setting the signalling VPCI base

You can set a signalling VPCI Base for a non-root virtual port. This command enables the switch to interoperate with switches that use the VPI value for the VPCI in the setup signalling message. The default VPCI value is ‘0’.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To set a signalling VPCI base for a virtual port, use the `vport set sigvpcibase` command.

Command:	`M15-155s8:/>vport set sigvpcibase <vport id> 0|vpi`	
Example:	`M15-155s8:/>vport set sigvpcibase 8.1.2 vpi`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>
	`<0|vpi>`	Selects the signalling VPCI base that will be used for the virtual port. To interoperate with another M770 ATM Switch, set it to ‘0’. This is the default setting.

Setting the signalling VPC VPI range

On a root virtual port (which may have several VPIs associated with it) there is an option of signalling virtual paths connections. Therefore, the user should identify the range of VPIs that are associated with Signaled Virtual Paths (SVPs) and the rest are associated with Permanent Virtual Paths (PVPs).

Note: Before setting up PVPs, or preparing the virtual port for SVPs, the module hardware has to be configured to accept Virtual Paths connection. This is done using the command “hardware vpcvpirnage” in which the user identifies the range of VPIs that are associated with VP switching. For more information refer to “Managing VPI range for VP switching” on page 99.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To set the signalling VPC VPI range used for SVPs on a root virtual port use the `vport set sigvpcvpirange` command:

Command:

```
M15-155s8:/> vp set sigvpcvpirange <root vport id> <range>
```

Example: Defining one vpi (6) to be used for SVPs on this virtual port (2.15.0):

```
M15-155s8:/>vp set sigvpcvpirange 2.15.0   [6..6]
```

Parameters:

`<root vport id>`	Virtual port identifier in the form <slot>.<port>.0
`<range>`	in the form: [<lower bound>..<upper bound>] <lower bound> must be the minimum VPI number for VP switching as defined by “hardware vpcvpirange”

In this example, if the hardware was configured to have 4 bits for VPIs and 11 bits for VCIs (“Managing the number of VPI and VCI bits” on page 98). And the VPIs for VP switching was configured to be in the range of [6..15] (refer to “Managing VPI range for VP switching” on page 99). Then the range of VPIs that is left for PVPs is [7..15].

Setting the signalling VCI range

You can set the signalling VCI range used for SVCs on a virtual port. Usually the VCI range is reduced in order to create PVCs on these VCs. To increase the VPI range or vice versa, please see the command `hardware vpivcibits` on page 98.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To set a signalling VCI range for a virtual port, use the `vport set vcirange` command.

Command: `M15-155s8:/>vport set vcirange <vport id> <range>`

Example: `M15-155s8:/>vport set vcirange 8.1.0 [32..800]`

Parameters:

`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
`<range>`	Selects the signalling VCI range that will be used for the virtual port. The range must be in the form [x..y] where x > 32 and y < maximum vci as defined by the number of VCI bits.

Note: Do not reduce the lower limit of the signalling VCI range below 32. All values below 32 are reserved for signalling protocol.

Setting the VPI range on a root virtual port

The VPI range set for the root virtual port cannot be greater than the VPI range of the physical port.

Note: Before you can create a new virtual port you must reduce the VPI range of the root virtual port. For more information about creating a virtual port, see “Creating a virtual port” on page 64.

To set a VPI range for a root virtual port, use the `vport set vpirange` command.

Command: `M15-155s8:/>vport set vpirange <vport id> <range>`

Example: `M15-155s8:/>vport set vpirange 8.1.0 [0..3]`

Parameters:

`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
`<range>`	Selects the VPI range that will be used for the virtual port. The upper range can be 0, 1, 3 or 7.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

Setting the QSAAL wait parameter on a virtual port

This parameter changes this vport to wait indefinitely for an incoming QSAAL connection. By default, this parameter is disabled.

To set the waitqsaal parameter on the virtual port use the `vport set waitqsaal` command.

Command:	`M15-155s8:/>vport set waitqsaal <vport id> [on|off]`	
Example:	`M15-155s8:/>vport set waitqsaal 8.1.0 on`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.
	`[on|off]`	Turns waitqsaal parameter On or Off.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

Resetting Virtual Port Parameters

You can reset a virtual port parameter so that the value returns to the default value. When the virtual port is re-enabled ILMI will, where possible, attempt to learn a value for the parameter through its dialogue with the remote device. If ILMI cannot discover a value for the parameter, the parameter remains at the default setting.

You can reset the following virtual port parameters using the `vport reset` command:

- Signalling profile
- Stack type
- Signalling VPCI range
- Signalling VCI range
- VPI range on a root virtual port.
- ILMI version
- Waitqsaal.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To clear a parameter for a virtual port, you must perform the following steps:

1 Disable the virtual port.
2 Reset the parameter for the disabled virtual port.
3 Enable the virtual port.

Resetting the signalling profile parameter

If you reset the virtual port’s signalling profile parameter, the port will re-learn what is on the other end of the link when it is enabled and a remote device is connected. For more information about this parameter, see “Setting the signalling profile parameter” on page 69.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To reset the profile parameter for a virtual port, use the `vport reset profile` command.

Command:	`M15-155s8:/>vport reset profile <vport id>`	
Example:	`M15-155s8:/>vport reset profile 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Resetting the stack type parameter

If you reset the virtual port's stack type parameter, the port will re-learn the stack type when it is enabled and a remote device is connected. For more information about this parameter, see "Setting the stack type parameter" on page 69.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

To reset the stack type parameter for a virtual port, use the `vport reset stacktype` command.

Command:	`M15-155s8:/>vport reset stacktype <vport id>`	
Example:	`M15-155s8:/>vport reset stacktype 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Resetting the signalling VPC VPI range

To reset the VPC VPI range that was previously assigned for Switched Virtual Paths, use the following command:

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

Command:	`M15-155s8:/>vport reset sigvpcvpirange <vport id>`	
Example:	`M15-155s8:/> M15-155Fs2:/> vport reset sigvpcvpirange 2.15.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.0

Output

```
Clearing sigvpcvpcirange value...
Done!
```

Resetting the signalling VPCI range

For more information about this parameter, see ”Setting the signalling VPCI range” on page 71.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To reset the signalling VPCI range for a virtual port, use the `vport reset sigvpcirange` command.

Command:	`M15-155s8:/>vport reset sigvpcirange <vport id>`	
Example:	`M15-155s8:/>vport reset sigvpcirange 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Resetting the signalling VCI range

If you reset the virtual port’s signalling VCI range, the port will re-learn the signalling VCI range supported by the remote device when it is enabled and a remote device is connected. For more information about this parameter, see “Setting the signalling VPC VPI range” on page 72.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65.

To reset the signalling VCI range for a virtual port, use the `vport reset vcirange` command.

Command:	`M15-155s8:/>vport reset vcirange <vport id>`	
Example:	`M15-155s8:/>vport reset vcirange 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>.

Resetting the VPI range

If you reset the virtual port's VPI range and the remote device is an end-station, the port will re-learn the VPI range supported by the end-station when it is enabled and a remote device is connected. For more information about this parameter, see Setting the VPI range on a root virtual port earlier in this chapter.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

To reset the VPI range for a virtual port, use the `vport reset vpirange` command.

Command:	`M15-155s8:/>vport reset vpirange <vport id>`	
Example:	`M15-155s8:/>vport reset vpirange 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Resetting the Waitqsaal parameter

For more information about this parameter, see Setting the QSAAL wait parameter on a virtual port earlier in this chapter.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see "Disabling a virtual port" on page 65.

To reset Waitqsaal for a virtual port, use the `vport reset waitqsaal` command.

Command:	`M15-155s8:/>vport reset waitqsaal <vport id>`	
Example:	`M15-155s8:/>vport reset waitqsaal 8.1.0`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Resetting all configurable parameters on a specific virtual port

You can reset all configurable parameters for a specific virtual port to their default values.

Note: You must disable the virtual port before you can change or reset any virtual port parameters. For more information about how to disable a virtual port, see “Disabling a virtual port” on page 65

To reset all configurable parameters on a disabled virtual port to their default values, use the `vport reset all` command.

Command:	`M15-155s8:/>vport reset all <vport id>`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Managing the Probe Method

Setting the managing probe method for proprietary features

You can set the method of probing that the switch will use to find proprietary features on a remote device. This can be either via the “mib” or the “sysobject id” library. By default the method of probing is set to “mib”. You will need to change the method of probing to “sysobjectid”, if your remote device does not allow probing of its “mib”.

To set the method of probing for a virtual port, use the `vport probe` command.

Command:	`M15-155s8:/>vport probe <vport id> [mib | sysobjectid]`	
Parameters:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>
	`[mib | sysobjectid]`	Sets the method of probing for proprietary features on a virtual port either via the mib or the sysobject id library.

Displaying the method of probing for proprietary features

To display the method of probing for a virtual port, use the `vport probe` command.

Command:	`M15-155s8:/>vport probe <vport id>`	
Output:	`Method of probing for proprietary features: MIB`	
Parameter:	`<vport id>`	The virtual port in the form <slot>.<port>.<virtual port number>

Virtual Port Signalling Information

Virtual port signalling information

To display signalling information for a virtual port, enter the `vport sig stats` command.

Command:	`M15-155s8:/>vport sig stats <vport id> [all]`	
Example:	`M15-155s8:/>vport sig stats 8.3.0`	
Parameters:	`<vport id>`	The virtual port identifier is displayed as <slot>.<port>.<virtual port number>.
	`[all]`	Displays all protocol statistics for the virtual port (see Table 6.5). If `all` is omitted, only high-level statistics are displayed (see Table 6.5).

The `vport sig stats` command displays the high-level statistics (see Table 6.5).

The `vport sig stats all` command displays all protocol statistics for the virtual port (see Table 6.6).

Table 6.5 High-level statistical output from the vport sig stats command

Field	Description
Statistics Info.	The number of times signalling has been started and stopped on the virtual port.
Stack up count	The number of times signalling has come up since it was last started on the virtual port.
Stack down count	The number of times signalling has gone down since it was last started on the virtual port.
Number of restarts	The number of times signalling has been restarted since it was last started on the virtual port.
Q.SAAL up count	The number of times Q.SAAL (data link protocol) has established a link to its peer since it was last started on the virtual port.
Q.SAAL down count	The number of times Q.SAAL (data link protocol) has lost the connection to its peer since it was last started on the virtual port.
Signalling type	The signalling version on this virtual port (i.e., UNI 3.1)
Signalling side	The signalling profile on this virtual port (i.e., Network)

Table 6.5 High-level statistical output from the vport sig stats command (Continued)

Field	Description
Signalling Messages	The number of signalling messages transmitted or received on this virtual port
Setup Attempts	The number of Setup messages transmitted or received on this virtual port
Setup Retransmissions	The number of Setups that were retransmitted to or from this virtual port
Errors detected in the contents of received messages	Errors detected in the contents of received messages
Active Calls	The number of incoming and outgoing active VCs on this virtual port
Active Incoming Point-to-Point Calls	The number of incoming Point-to-Point VCs on this virtual port
Active Outcoming Point-to-Point Calls	The number of outgoing Point-to-Point VCs on this virtual port
Active Incoming Point-to-Multipoint Calls	The number of incoming Point-to-Multipoint VCs on this virtual port
Active Outcoming Point-to-Multipoint Calls	The number of outgoing Point-to-Multipoint VCs on this virtual port
Active Point-to-Multipoint Leaves	The number of Point-to-Multipoint leaves on this virtual port

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Signalling Statistics:	
Statistics Info.	The number of times signalling has been started and stopped on the virtual port.
Stack up count	The number of times signalling has come up since it was last started on the virtual port.
Stack down count	The number of times signalling has gone down since it was last started on the virtual port.
Number of restarts	The number of times signalling has been restarted since it was last started on the virtual port.
Q.SAAL up count	The number of times Q.SAAL (data link protocol) has established a link to its peer since it was last started on the virtual port.
Q.SAAL down count	The number of times Q.SAAL (data link protocol) has lost the connection to its peer since it was last started on the virtual port.
Signalling type	The signalling version on this virtual port (i.e., UNI 3.1)
Signalling side	The signalling profile on this virtual port (i.e., Network)
SSCOP Connection Events	This counts the sum of: • number of TNO_RESPONSE timeouts • number of establishment failures (maximum number of TCC expiries or receipt of BGREJ) • number re-establishment attempts - receipt of BGN or RS PDUs
SSCOP Errored PDUs	This counts the sum of: • invalid PDUs - incorrect length, invalid PDU type or not 32 bit aligned • PDUs resulting in MAA error codes A-M and Q-T and are discarded.

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Setup Attempts	• Count of call SETUP messages transmitted and received • not including retransmissions.
Note: For the following fields, cause values received and transmitted on RELEASE, RELEASE_COMPLETE, ADD_PARTY_REJECT or STATUS messages are counted (does not apply to RELEASE_COMPLETE received in response to RELEASE with the same cause). The Causes are detailed in the UNI 3.1 ATM Forum Specification.	
Unavailable Routes	Causes: 1, 2, 3, 88
Unavailable Resources	Causes: 35, 37, 38, 41, 45, 47, 49, 51, 58, 63, 92
Called Party Events	Causes: 17, 18, 21, 22, 23, 27, 31
Message Errors	Causes: 10, 36, 81, 82, 89, 96, 97, 99, 100, 101, 104, 111 Also includes: • call reference length errors • all reference flag incorrectly set to 1 on received SETUP • call reference unknown on received RELEASE COMPLETE • SETUP received for call already in progress • message too short
Calling Party Events	Causes: 28, 43, 57, 65, 73, 78, 91, 93
Timer Expired	• Cause: 102 received • Any network timer expiry • Local timer expiries
Restarts	RESTART receptions and transmissions
Active Calls	Number of active switched calls - incoming and outgoing

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Q93B Statistics: The following 13 rows show errors detected in the contents of received messages	
Protocol Discriminator Errors	The number of messages received with invalid protocol Discriminator (either an unrecognized value, or a value that did not match the protocol type in use on the signalling stack).
Call Reference Length Errors	The number of messages received with call reference length errors.
Call Reference Flag Bad on Setup	SETUP messages received with call reference flag incorrectly set to 1.
Call Reference Errors	The number of messages received with a call reference that was invalid. This includes invalid use of the dummy and global call reference and incorrect call reference direction flags on these call references.
Message Passed along Requests	The number of unrecognized messages received with the pass along request bit set.
Unrecognized Message Errors	The number of unrecognized messages received and discarded.
Message Length Errors	The number of messages received with incorrect message length fields.
Mandatory IE missing Errors	The number of mandatory IE missing from message errors.
Unrecognized IE Errors	The number of unrecognized IEs received.
General IE Errors	The number of general IE errors (this includes coding standard errors and IE length errors).
Mandatory IE Content Errors	The number of mandatory IE content errors.
Non Mandatory IE Content Errors	The number of non-mandatory IE content errors.
IE Passed along Requests	The number of unrecognized IEs received with pass along indicator set.

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Cause Values for STATUS/RELEASE/RELEASE_COMPLETE/ ADD_PARTY_REJECT: Counters for tracking received and transmitted cause values. The categories are defined by the AToM MIB and are only relevant for UNI3.0 and UNI 3.1.	
Uncounted	This is included to count those cause values that are not in any of the counted categories - this includes invalid cause values and UNI4.0/PNNI cause values.
The groups defined by the AToM MIB are as follows:	
Unavailable Routes	Causes: 1, 2, 3, 88
Unavailable Resources	Causes: 35, 37, 38, 41, 45, 47, 49, 51, 58, 63, 92
Called Party Events	Causes: 17, 18, 21, 22, 23, 27, 31
Message Errors	Causes: 10, 36, 81, 82, 89, 96, 97, 99, 100, 101, 104, 111 Also includes: • call reference length errors • call reference flag incorrectly set to 1 on received SETUP • call reference unknown on received RELEASE COMPLETE • SETUP received for call already in progress • message too short
Calling Party Events	Causes: 28, 43, 57, 65, 73, 78, 91, 93
Timer Expired	• Cause: 102 received • Any network timer expiry • Local timer expiries
Counters of signals sent to/ received from SSCS (including retransmissions)	Counts the messages send to/received from SSCS

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Count of currently active calls and parties:	
Active Incoming Point-to-Point Calls	The number of incoming Point-to-Point VCs on this virtual port
Active Outcoming Point-to-Point Calls	The number of outgoing Point-to-Point VCs on this virtual port
Active Incoming Point-to-Multipoint Calls	The number of incoming Point-to-Multipoint VCs on this virtual port
Active Outcoming Point-to-Multipoint Calls	The number of outgoing Point-to-Multipoint VCs on this virtual port
Active Point-to-Multipoint Leaves	The number of Point-to-Multipoint leaves on this virtual port
AAL Resets	Counts of Signalling AAL resets.
AAL Releases	Counts of Signalling AAL releases.
Status Mismatches	Count of number of ATG_STATUS messages received with incompatible call states
Message Type Sequence Errors	Count of number of messages received in an invalid state
Endpoint Reference Errors	Counts of number of endpoint reference errors
Unknown Call Reference on RELEASE_COMPLETE	Number of RELEASE_COMPLETE message received for an unknown call Reference (this is included in the atmSigDetectMsgErrors AToM MIB object)
Timer Expired for signals	Local timers expired list, sorted by type
Restart Ack Mismatches	Count of received ATG_RESTART_ACKNOWLEDGEs with restart_class, vpci or vci that do not match those on the outgoing ATG_RESTART
Setup Retransmissions	Number of SETUP retransmissions sent and received

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
QSAAL Statistics: SSC SSCOP Statistics:	
BEGIN	• Tx/Rx - Number of Begin PDUs transmitted and received. • Retr-Tx/Retr-Rx - Number of Begin PDUs retransmissions transmitted and received. • Ack-Tx/Ack-Rx - Number of Begin PDUs acknowledgements transmitted and received. • Rej-Rx/Rej-Tx - Number of Begin PDUs rejections received and transmitted.
RESYN	The fields for Resynchronization PDUs are the same as for the Begin PDUs except that the rejection count fields are not used.
E.REC	The fields for Error Recovery PDUs are the same as for the Begin PDUs except that the rejection count fields are not used.
END	The fields for End PDUs are the same as for the Begin PDUs except that the rejection count fields are not used.
POLL	The number of POLL PDUs that were received (rx) or transmitted (tx).
STAT	The number of STAT PDUs that were received (rx) or transmitted (tx).
USTAT	The number of USTAT PDUs that were received (rx) or transmitted (tx).
Sequenced Data Messages Transmitted (not including retransmissions)	Number of sequenced data messages transmitted
Sequenced Data Messages Retransmitted	Number of sequenced data messages retransmitted
Sequenced Data Messages Acked	Number of sequenced data messages acknowledged

Table 6.6 All protocol statistics displayed by the vport sig stats all command

Field	Description
Sequenced Data Messages Received	Number of sequenced data messages received
Sequenced Data Messages Delivered from SSCS to Signalling	Number of sequenced data messages delivered
Sequenced Data Messages Duplicated	Number of retransmission requests sent and received
Retransmission Request Sent	The number of retransmission requests sent
Retransmission Request Received	The number of retransmission requests received
Transmission Window Empty	Number of times we have run out of credit to send SD PDUs.
Has SSCS credit to send SD PDUs?	Indication of whether we Currently have Credit to send SD PDUs.
MAA Errors Encountered	Number of MAA errors encountered (protocol Errors in received PDUs).
Number of times the TNO_RESPONSE has expired	Number of TNO_RESPONSE pops
Number of times the TCC timer has reached maximum value	Number of times the TCC timer has reached it's maximum number of Expiries while waiting for a response to BGN.
Number of Invalid PDU's (bad length, alignment or type)	Number of PDUs that could not be processed due to incorrect length, alignment or type.
Number of Invalid PDU's (content errors or while state not valid)	Number of PDUs that contained content errors or were received in an invalid state.

Resetting signalling statistics

To clear signalling counter for a virtual port, use the `vport sig resetstats` command:

Command: `M15-155s8:/>vport sig   resetstats <vport id>`

Example: `M15-155s8:/>vport sig   resetstats   2.9.0`

Parameter: `<vport id>` The virtual port identifier is displayed as <slot>.<port>.<virtual port number>

Output: `Done!`

Managing Connections

Listing all virtual circuits

To list the details of all virtual circuits, use the `vport connections all` command.

Command: `M15-155s8:/>vport connections all`

The `vport connections all` command displays all SVCs, PVCs, and internal virtual circuits such as ILMI signalling that are set up on the M770 ATM Switch. Information displayed in the output is described in Table 6.7.

Listing switched virtual circuits

To list the details of all SVCs, use the `vport connections svcs` command.

Command:
```
M15-155s8:/>vport connections svcs [nomesh] [addr] [td]
[<vport id>] [src|dst] [<vportid>] [dir]
```

Example: `M15-155s8:/>vport connections svcs nomesh addr 8.1.0`

Parameters:

[nomesh]	Lists SVCs passing through the vport (except for LANE mesh SCVs)
[addr]	Lists the ATM addresses where available
[td]	Displays the ATM Traffic Descriptor
[<vport id>]	Lists all SVCs passing through the vport
[<vport id>] [src|dst]	Lists the incoming/outgoing SVCs from/to the vport
[<vport id>] [<vport id>]	Lists all SVCs between the two vports
[<vport id>] [<vport id>] dir	Lists all SVCs from the 1st vport to the 2nd vport

The `vport connections svcs` command displays the information described in Table 6.7.

Listing permanent virtual circuits

To list the details of all PVCs, enter the `vport connections pvcs` command.

Command:

```
M15-155s8:/>vport connections pvcs [td] [<vport id>]
[<vport id>]
```

Example:

```
M15-155s8:/>vport connections pvcs 8.2.0
```

Parameters:

`[td]`	Displays the ATM Traffic Descriptor
`[<vport id>]`	Lists all PVCs passing through the vport
`[<vport id>]` `[<vport id>]`	Lists all PVCs between the two vports.

Note: When the above command is used both PVCs that are enabled and disabled will be listed.

The `vport connections pvcs` command displays the information described in Table 6.7.

Table 6.7 Output from the vport connections command

Field	Description
slot.port.vpi.vci	The physical port, VPI, and VCI that are assigned to the connection. For a PVC, this is the Virtual Circuit Link (VCL).
rXcount	The number of cells received on this connection.
PD	Indicates whether or not packet discard is enabled. “N” indicates that it is not enabled.
SCAT	The service category that is used for the virtual circuit.
Up Time	Indicates how long the virtual circuit has been active in days, hours, minutes, seconds, and hundredths of a second.

Table 6.7 Output from the vport connections command (Continued)

Field	Description
Type	The type of connection. PP: Point-to-Point SVC. PMP: Point-to-Multipoint SVC. PVC:PP: Point-to-Point PVC. PVC:PMP: Point-to-Miltipoint PVC RES: Reserved circuit. DD_802.5: LANE Data Direct Token-Ring VC DD_802.3: LANE Data Direct Ethernet VC MC_802.5: LANE Multicast Token-Ring VC MC_802.3: LANE Multicast Ethernet VC CONTROL: LANE Control VC LES_MESH: Distributed LES SVC mesh BUS_MESH: Distributed BUS SVC mesh DIAGNSTIC: Diagnostic ILMI: ILMI SIG: Signalling.

Viewing ILMI information for a virtual port

To display ILMI MIB information for the remote end of a virtual port, use the `ilmi show` command.

Command: `M15-155s8:/>ilmi show [<vport id>]`

Parameters: `<vport id>` The virtual port is displayed in the format: <slot>.<port>.<virtual port number>. If no virtual port id is entered then ILMI information is displayed for all virtual ports.

The `ilmi show` command displays the information described in Table 6.8.

Table 6.8 Output from the ILMI show command for a specific virtual port

Field	Description
Stack Type	The Stack Type that the remote device uses for signalling. This can be UNI 3.0, UNI 3.1, UNI 4.0, IISP 3.0, IISP 3.1 or PNNI 1.0
Private / Public	The UNI type that is used. This is either Private or Public.
IP address	The IP address of the remote device attached to the virtual port.

Table 6.8 Output from the ILMI show command for a specific virtual port (Continued)

Field	Description
OSI NSAP address	The Open Systems Interconnection (OSI) Network Service Access Point (NSAP) address. An OSI NSAP address is an address to which a management station can send network management protocol messages to access network management information about the operation of the ATM device local to this UNI Management Entity (UME).
IfName	The textual name of this interface.
MaxVpiBits	The maximum VPI bits. This, together with the MaxVpc, determines the limits of the VPI range that can be supported.
MaxVciBits	The maximum VCI bits. This, together with the MaxVcc, determines the limits of the signalling VCI range that can be supported.
MaxVpc	The maximum Virtual Path Connections (VPCs) that the remote device can support.
MaxVcc	The maximum Virtual Circuit Connections (VCCs) that the remote device can support.
SysObjectId	The value for the SysObjectId in RFC 1213 MIB.
SysUpTime	The number of days, hours, minutes, and seconds that the remote device has been on-line.
SysName	The administratively-assigned name for this node.
LECS address	The ATM address of the LECS.
Probe MIB	The probe is used to locate proprietary features on the remote device. If the probe is not supported on the remote device then remaining fields in ILMI show command will be displayed has “Not Available”.
Min Interop	Specifies the minimum interoperability version supported on the remote device.
IISP Admin State	Specifies the administration preference state supported by the remote device when setting up an IISP link.
IISP Oper State	Specifies the operational preference state supported by the remote device when setting up an IISP link.

Table 6.8 Output from the ILMI show command for a specific virtual port (Continued)

Field	Description
LECS Election	Specifies if LECS redundancy is supported on the remove device.

Note: The above information, except for the SysUpTime, is only retrieved when ILMI comes up on the link and therefore, it will not be “current”. This is only a problem when the ILMI MIB information is changed for the remote device.

Chapter 7

Managing Module Hardware

This chapter describes how to use the command-line interface to manage modules installed in an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3 How to Use the Command-line Interface.

Managing Modules

This section describes the commands that allow you to manage the modules installed in the Avaya M770 ATM Switch.

Viewing the Clock Source Ports

You can display the source of the ATM module's clock by the `hardware clock show` command. Only M770 ATM switches that have an M-SPS installed have the ability to synchronize its clock. If the M770 Supervisory Module is the M-SPX, the module will always use its local clock.

Command: `M15-155s8:/>hardware clock show`

Output:

From a module whose port is **not** being used to synchronize the ATM Switch

```
Clock synchronization information of slot 8
=============================================
The ports on this module are using a clock from the M-SPS.
No ports on this module are driving clock source ATM A or
B.
```

From a module whose port **is** being used to synchronize the ATM Switch

```
Clock synchronization information of slot 8
=============================================
The ports on this module are using a clock from the M-SPS.
Port 1 is assigned as clock source ATM B.
```

From a module which cannot be used to synchronize the ATM Switch

```
Clock synchronization information of slot 8
=============================================
The ports on this module are using a local clock.
No ports on this module are driving clock source ATM A or
B.
```

Note:

- **OC-3 Modules (M15-155F/SF/MS):**
  In order to provide DEFINITY support, all the OC-3 modules in the chassis must be C/S 2.0 or higher. The C/S of the module can be located on the unit's box or on the module itself. If the module is already inserted in the M770 switch, type the command `summary info` from the ATM module's Command Line Interface to see the C/S version.
- Only ports 1 and 2 can be used by the M-SPS to synchronize its clock. All ATM ports can be used to connect the DEFINITY to the M770 ATM Switch.
- **OC-12 Modules (M3-622F/SF):**
  Currently the DEFINITY does not support OC-12 connections, however the M3-622 module may be used as backbone links between ATM switches. Only M3-622 modules with C/S 2.0 or higher can provide clock synchronization to the network or deliver clock to the switch. Newer and older C/S's of the modules can be mixed in the same chassis, but the older modules will not be synchronized to the rest of the ATM network.
- All ports (of C/S 2.0 modules) can be used by the M-SPS to synchronize its clock.

Managing Packet Discard Thresholds for a Module

There are two packet discard thresholds for each module, called Early Packet Discard (EPD), and Partial Packet Discard (PPD). By default, both thresholds have a set limit (see below) and are enabled.

The M770 ATM Switch uses EPD to discard entire AAL5 frames for UBR traffic (rather than random cells from different frames), when it determines that it is about to become congested. The M770 ATM Switch still passes through the last cell of each AAL5 frame so that end-stations are aware of the discard that has taken place. You can configure a threshold at which the EPD will be invoked. The threshold is a percentage of the overall shared buffer space. The default for EPD is set at 80% of the buffer fill.

PPD works similarly to EPD, but it is generally invoked at higher levels of congestion. The difference is that, while with EPD the M770 ATM Switch can wait for the start of a suitable frame, PPD is involved when congestion is too serious to wait that long. Therefore, packet discarding will start in the middle of the frame. The value for PPD threshold cannot be set by the user. It is higher than the default for EPD. Under normal circumstances, EPD would deal with the congestion before the buffer capacity is reached, and PPD should never be invoked.

Note: Under normal circumstances, the early packet discard threshold should not be changed. Before attempting to change the thresholds, contact Avaya Technical Support.

The Cell Loss Priority (CLP) mechanism allows low priority cells (with CLP set to 1) to be discarded first. The CLP threshold cannot be set by the user.

Displaying the packet discard threshold for modules

To display the current packet discard thresholds for all modules, use the `hardware packetdiscard` command.

Command: `M15-155s8:/>hardware packetdiscard`

Output:

```
EPD 80%
```

The information displayed is the percentage threshold that is currently set for Early Packet Discard (EPD). The default EPD threshold is 80%. When the switch's buffers are more full than the EPD threshold then the switch module will discard NEW AAL5 frames on UBR circuits.

Changing the packet discard thresholds for modules

You can change the default thresholds for packet discard.

- Decreasing the percentage will cause packets to be discarded at an earlier stage during congestion.
- Increasing the percentage will cause the congestion to reach a higher level before the packet discard threshold is reached and packets are discarded.
- To disable packet discard enter 0 for EPD.

Note: Under normal circumstances, the packet discard thresholds should not be changed. Before attempting to change the thresholds, contact Avaya Technical Support.

To change the packet discard thresholds for an module, use the `hardware packetdiscard <epd%>` command.

Command: `M15-155s8:/>hardware packetdiscard <epd%>`

Example: `M15-155s8:/>hardware packetdiscard 70`

Parameters: `<epd%>` The new percentage threshold for EPD.

Managing the speed for the serial port

To display the current speed for the serial interface port, use the `hardware serial speed` command.

Command:
```
M15-155s8:/>hardware serial speed
```

Output:
```
M15-155s8:/>9600
```

To set up the speed for the serial interface port, use the `hardware serial speed` command and type the desired speed after the command as shown:

Command:
```
M15-155s8:/>hardware serial speed [4800|9600|19200|38400]
```

Example:
```
M15-155s8:/>hardware serial speed  9600
```

Parameters:

`[4800|9600|19200|38400]`	Select the speed at which the serial interface port will communicate.

Managing the number of VPI and VCI bits

You can configure the number of VPI and VCI bits that will be used for the VPI and VCI ranges on all the physical ports for this module. To display and/or change the VPI/VCI bits for the ATM module, use the `hardware vpivcibits` command.

Use the `hardware vpivcibits` command to display the maximum number of VPI and VCI bits that are used for all ports on the module:.

Command:
```
M15-155s8:/>hardware vpivcibits
```

Output:
```
Configured number of vpi bits:  3,     vci bits:  12
Current number of vpi bits:     3,     vci bits:  12
```

Use the `hardware vpivcibits <vpibits> <vcibits>` command to change the maximum number of VPI and VCI bits that will be used for all ports on the module. It takes effect only after the next reboot.

Command:
```
M15-155s8:/>hardware vpivcibits <vpibits> <vcibits>
```

Example:
```
M15-155s8:/>hardware vpivcibits 4 11
```

Parameters:

`<vpibit>`	The maximum number of VPI bits for all ports on the module
`<vcibits>`	The maximum number of VCI bits for all ports on the module

The number of bits that can be used varies with each ATM module. See the table below on the allowed parameters..

Table 7.1 Allowed Parameters for the `hardware vpivcibits` *command*

Parameters	M15-155 Modules	M3-622 Modules
Total Number of VPI/VCI bits	15	16
VPI bit Range	0 – 6	0 – 7
VCI bit Range	9 – 15	9 – 16

Managing Trunk ID range for P2MP PVCs

When the you wish to set a P2MP PVC, you need to assign trunk ID to the P2MP call manually. The trunk ID is used as a unique identifier for the P2MP call, on both the ingress module (on which the root of the call is connected), and on the egress modules (on which the leaves of the call are connected). Trunk IDs are defined on a module basis using the following commands. They are used in the PVC setup, for more details see Chapter 8, “Permanent Virtual Connections (PVCs and PVPs)”.

Use the `hardware trunkidrange` command to display the current configuration of Trunk ID range:

Command:

```
M15-155s8:/>hardware trunkidrange
```

Output:

```
Allowed reserved Trunk Id range:        0..895
Configured reserved Trunk Id range:     0..0
Current reserved Trunk Id range:        0..0
```

Use the `hardware trunkidrange <maxTrunkId> | disable` command to set the Truck ID range:.

Command:

```
M15-155s8:/>hardware trunkidrange <maxTrunkId> | disable
```

Parameters:

`<maxTrunkId>`	Maximum trunk ID for P2MP PVCs on all ports of the module
`disable`	The trunk ID reservation will be disabled after the next reboot, i.e., the new range will be 0..0

Note: Changes to the Trunk ID range applies to all ports of the module, and they take effect only after the next reboot of the module.

Managing VPI range for VP switching

When the user wishes to configure Virtual Path (VP) switching, the VPI range has to be set to meet this need. By default, all VPIs are used for VC switching, therefore, the default configuration is:

Command:

```
M15-155s8:/>hardware vpcvpirange
```

Output:

```
Configured VPC VPI     VP Switching is disabled
range
Current VPC VPI range  VP Switching is disabled
```

To change the default VPI range for Virtual Path Connections (VPC) use the `hardware vpcvpirange` command:

Command:

```
M15-155s8:/>hardware vpcvpirange <minVpcVpi>
```

Note: These changes take effect only after the next reboot of the module

Note: T least one VPI has to be reserved for the signalling VPC.

After the next reboot, the VPC VPI configuration would look like this::

Command:

```
M15-155s8:/>hardware vpcvpirange
```

Output:

```
Configured VPC VPI     6..7
range
Current VPC VPI range  6..7
```

At this point, the user can configure Permanent Virtual Paths (PVPs). For more details about PVPs, please refer to Chapter 8, “Permanent Virtual Connections (PVCs and PVPs)”.

Permanent Virtual Connections (PVCs and PVPs)

This chapter describes how to use the command-line interface to manage PVC connections in an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Managing Permanent Virtual Connections (PVCs and PVPs)

Managing PVC connections

Not all ATM equipment currently supports UNI signalling. Therefore, you may need to manually establish a virtual circuit to make a connection between two ATM endpoints over an ATM network. These connections are referred to as Permanent Virtual Circuits (PVCs).

A PVC is a concatenation of Virtual Circuit Links (VCLs), where each VCL is bi-directional.

Figure 8.1 illustrates the terms VCL and PVC.

Figure 8.1 A breakdown of a PVC connection

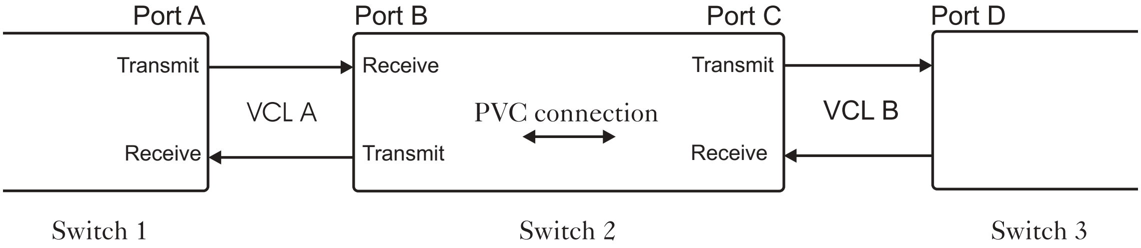


Figure 8.1 shows a PVC, consisting of two VCLs that span three switches. A VCL is a bi-directional link between two entities, such as two switches or a switch and an end-station. With respect to switch 2, VCL A is identified by specifying the physical port (port B) and the VPI/VCI used at that port. Similarly, with respect to switch 1, VCL A is identified by specifying the physical port (port A) and the VPI/VCI used at that port. Note that the VPI/VCI in the same switch, is the same at both ports. The PVC connection could be between 2 ports on the same module or between 2 modules on the same switch (through the backplane). This means that port B and port C can be on one module or on 2 different modules on the same switch.

Note: Before you attempt to set up a PVC you will need to reduce the signalling VCI range, for a virtual port, that is used for SVCs.
Do not use a VCI in the range [0...31] as these are reserved by the ATM Forum. To reduce the VCI range, see Setting Virtual Port Parameters in Chapter 6 Managing Virtual Ports.

Since a VCL is bi-directional, a traffic descriptor needs to be defined for the transmit and receive data paths belonging to the VCL. For VCL A, the traffic descriptor for the receive data path at port B should be the same as the traffic descriptor for the transmit data path at port A. Similarly, the traffic descriptor for the transmit data path at port B should be the same as the traffic descriptor for the receive data path at port A. For more information about managing traffic descriptors, see Managing Traffic Descriptors later in this chapter.

Creating a PVC connection

PVC connections will be re-established automatically when the M770 ATM Switch powers up. You can have up to 1k (1024) PVC connections on a module.

Creating a Point-to-Point (PP) PVC connection

To set up a PP PVC with uni-directional traffic on one module, you must set up a bi-directional PP PVC that has a Peak Cell Rate (PCR) of zero in one direction. To set up a bi-directional PVC between 2 ports on different modules (on the same switch) you must type the command on the CLI of each module.The appropriate order of the VCL and the td1, td2 should switch places (rx-td in one module should be the tx-td in the other module).

The command described below will setup a VCL on each <slot.port.vpi.vci> and a PVC connection joining the two. The PVC connection will be automatically assigned an id.

Traffic descriptors do not have to be specified. If they are not, UBR traffic will be assumed and an existing UBR traffic descriptor will be used. If no such traffic descriptor exists, one will be automatically set up for UBR traffic. If any other type of traffic is required, you must first set up the traffic descriptors in the usual way (using the command `td setup`). on the required modules.

If one of the specified VCLs already exists, this VCL's traffic descriptors will be used in preference to any other VCLs specified by the user. If both VCLs already exist, their traffic descriptors must be compatible (that is the transmit and receive traffic descriptor identifiers) for the command to succeed.

To create a PVC connection, use the `pvc setup pp` command:

Command:

```
M15-155s8:/>pvc setup pp <vcl1index> <vcl2index> [<td1> [<td2>]]
```

Example1: Setting up a PP PVC between 2 ports on the same module:

```
M15-155s8:/>pvc setup pp 8.1.0.1001 8.2.0.1002 6 2
```

Example2: Setting up a PP PVC between 2 ports on different modules but on the same switch:

```
M15-155s8:/>On module 8: M15-155s8:/>pvc setup pp 8.1.0.1001
9.1.0.1002 6 2
M15-155s8:/>On module 9: M15-155s9:/>pvc setup pp 9.1.0.1002
8.1.0.1001 2 6
```

Parameters:

`<vcl1index>` The first VCL for the PVC connection in the format <slot.port number.vpi.vci>.

`<vcl2index>` The second VCL for the PVC connection in the format <slot.port number.vpi.vci>.

`td1` This refers to the transmit traffic descriptor of the first VCL and the receive traffic descriptor of the second VCL on the PVC connection.

`td2` This refers to the receive traffic descriptor of the first VCL and the transmit descriptor of the second VCL on the PVC connection. *Note:* if td2 is omitted then it defaults to the same as td1.

Creating a Point-to-Multipoint (PMP) PVC connection

Note: Before you set up a PMP PVC you have to identify the Trunk ID range that can be used by the module that holds the root of the call. Trunk IDs are used for associating different branches of the same PMP PVC call to its root. There may be up to 895 Trunk IDs on each module that holds roots of PMP PVC calls. By default, no Trunk IDs are defined. Refer to Chapter 7, “Managing Module Hardware” for instructions on how to change that definition.

For PMP PVC calls, the optional traffic descriptor parameter indicates the traffic on the forwarding direction, i.e. from the root to the branches. The backward (reverse) direction is always zero.

To set up a PMP PVC between ports on different modules (on the same switch) you must type the command on the CLI of each module. The order of the VCLs should NOT switch places. The root VCL is the first, and the branch VCLs come second.

The command described below will setup a VCL on each <slot.port.vpi.vci> and a PMP PVC connection joins the root to its branches. The PMP PVC connection will be automatically assigned an id.

Traffic descriptor does not have to be specified. If they are not, UBR traffic will be assumed and an existing UBR traffic descriptor will be used. If no such traffic descriptor exists, one will be automatically set up for UBR traffic. If any other type of traffic is required, you must first set up the traffic descriptors in the usual way (using the command td setup) on all required modules.

If one of the specified VCLs already exists, this VCL's traffic descriptors will be used in preference to any other VCLs specified by the user. If both VCLs already exist, their traffic descriptors must be compatible for the command to succeed.

To create a PMP PVC connection, use the `pvc setup pmp` command:

Command:

```
M15-155s8:/>pvc setup pmp <vci1index> <vci2index>...<vciNindex>
<trunkId> [<fwd td>]
```

Example1: Setting up a PMP PVC between 2 ports on the same module:

```
M15-155s8:/> pvc setup pmp 2.15.0.801 2.15.0.802 2.200 3
```

Example2: Adding a branch to the same PMP call (same trunk ID) on a different module:

On module 2: `M15-155s2:/> pvc setup pmp 2.15.0.803 9.2.0.803 9.2.0.804 2.200 3`

On module 9: `M15-155s9:/> pvc setup pmp 2.15.0.803 9.2.0.803 9.2.0.804 2.200 3`

Parameters:

`<vci1index>` The first VCL for the PVC connection in the format <slot.port number.vpi.vci>.

`<vci2index>...<vcNindex>` The branch VCLs (until the *N*th branch) for the PMP PVC connection in the format <slot.port.vpi.vci>

`<trunkId>` The identifier of the PMP call, but be the same on both the root module and the branch module. The format is <slot>.<index>. Must be in the range of trunk IDs are determined by the module that holds the root.

`<fwd td>` Index of traffic descriptor for the forwarding direction (rx for the root VCL, and tx for the branch VCLs).

Freeing a PVC connection

To free a PVC connection and associated VCLs, use the `pvc free` command:

Command:

```
M15-155s8:/>pvc free {<vcl_index>|<all>}
```

Use: Either

```
M15-155s8:/>pvc free <vclindex>
```

`<vclindex>` Index is one of the VCLs of the PVC connection
Note: If PP PVC - the PVC and associated VCLs are free.
If P2MP PVC
if <vclindex> = Root VCL, the all PMP tree
PVCs and their associated VCLs are free.
If <vclindex> = Branch VCL, the designated PVC
and it'sassociated Branch is free,
If last Branch PVC then Root VCL is free too.

Or

```
M15-155s8:/>pvc free all
```

to free all PVC connections and associated VCLs.

In order to free a PVC connection between two modules, you must type the command (example above) in the CLI of each module. Type the appropriate vcl_id for each module.

Listing the current PVC connections

To list all current PVC connections which are set up on the M770 ATM Switch, use the `pvc show` command.

Command: `M15-155s8:/>pvc show`

Output:

```
----ID--  -----VCL1--- -----VCL2--- Admin Oper Type Trunk
--|       --|          --|          |     |    |    Id
27000042  9.2.0.801    9.2.0.802    UP    UP   P2P  N/A
2 |       |            |            |     |    |
27000045  2.15.0.803   9.2.0.803    UP    UP   P2MP 2.200
6 |       |            |            |     |    |
27000045  9.2.0.803    9.2.0.804    UP    UP   P2MP 2.200
6 |       |            |            |     |    |
```

The `pvc connection show` command displays the information described in Table 8.1.

Table 8.1 Output from the pvc connection show command

Field	Description
ID	Unique identifier for the PVC connection, assigned by the switch.
VCL1	The transmitting VCLs for a PVC connection.
VCL2	The receiving VCLs for a PVC connection.
Admin	The management state of the PVC connection. • If the state is “UP” then this PVC connection is enabled. • If the state is “DOWN” then this PVC connection is disabled. This will occur if you have disabled the PVC connection using the command-line interface.

Table 8.1 Output from the pvc connection show command

Field	Description
Oper	The operational state of the PVC connection. • If the state is “UP” then this PVC is functional. • If the state is “DOWN” then this PVC is not functional. This may be because either the PVC is disabled or a port (on this switch) used by the PVC is down.
Type	Indicates whether this is a Point-to-Point PVC (PP) or a Point-to-Multipoint (P2MP) PVC.
TrunkId	The trunk id that is used by the PMP call. New branches to existing calls can be added using the existing trunk ID. The format is <slot>.<index> where <slot> is the slot number of the module that holds the root of the call.

Disabling a PVC connection

To temporarily disable an established PVC connection, use the `pvc disable` command.

Command: `M15-155s8:/>pvc disable <vclindex>`

Example: `M15-155s8:/>pvc disable 9.2.0.805`

Parameter: `<vclindex>` Index is one of the VCLs of the PVC connection

Note: If PP PVC - the PVC is disabled.

If P2MP PVC -

If the VCL is Root VCL, the entire PMP tree and associated VCLs are disabled.

If the VCL Branch VCL, the designated PVC and it's associated VCLs are disabled.

Enabling a PVC connection

To enable a disabled PVC connection, use the `pvc enable` command.

Command: `M15-155s8:/>pvc enable <vclindex>`

Example: `M15-155s8:/>pvc enable 9.2.0.805`

Output `PMP PVC 270000002 (Branch VCL 9.2.0.805): admin up`

Parameter: `<vclindex>` Index is one of the VCLs of the PVC connection

Note: If PP PVC - the PVC is enabled.
If P2MP PVC -
If the VCL is Root VCL, the entire PMP tree and associated VCLs are enabled.
If the VCL Branch VCL, the designated PVC and it's associated VCLs are enabled.

Listing all the VCLs

To list details of all VCLs, use the `pvc vcl show` command.

Command: `M15-155s8:/>pvc vcl show`

Output:

```
----VCL_ID--  -       -       ---Xid--  Oper  LastChan  Type
--|           TD_RX-  TD_TX-  -|        |     ge|
              |       |
9.2.0.801                     27000000  |UP   0:00:34
|             3|      3|      1|        |               p2p
9.2.0.802                     27000000  |UP   0:00:34
|             3|      3|      1|        |               p2p
9.2.0.803                     27000000  |UP   0:00:34   p2mple
|             0|      3|      2|        |               af
9.2.0.804                     27000000  |UP   037:33    p2mple
|             0|      3|      2|        |               af
9.2.0.805                     27000000  |UP   0:40:48   p2mple
|             0|      3|      2|        |               af
2.15.0.803                    27000000  |UP   0:00:34   p2mpro
|             3|      0|      2|        |               ot
```

The `pvc vcl show` command displays the information described in Table 8.2.

Table 8.2 Output from the pvc vcl show command

Field	Description
VCL ID	The unique VCL identifier is displayed.
TD-RX	The receive traffic descriptor identifier.
TD-TX	The transmit traffic descriptor identifier.
Xid	The PVC connection that is using this VCL, if there is one.

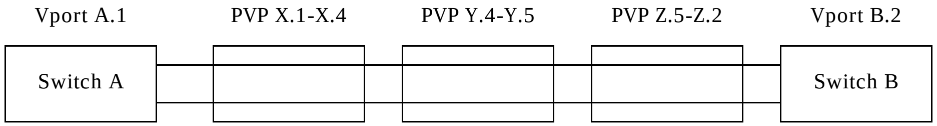
Table 8.2 Output from the pvc vcl show command

Field	Description
Oper	The operational state of the corresponding PVC connection. If the state is “UP” then the PVC is functional. If the state is “DOWN” then the PVC is not functional. This may be because either the PVC is disabled or a port (on this switch) used by the PVC is down. If the state is “NULL” then the VCL in question has no PVC associated with it.
LastChange	Indicates when the operational state of the VCL last changed. This is displayed as hours, minutes, and seconds. At power up, `0:0:0` is displayed.
Type	The type of the VCL. • p2p indicates it is a VCL of a Point-to-Point PVC, • p2mpRoot indicates it's the root VCL of a Point-to-Multipoint PVC. • p2mpLeaf indicates it's a leaf (or a branch) of a Point-to-Multipoint PVC.

Managing PVP Connections

Managing PVP Connections

In some network configurations there may be a need to configure a Permanent Virtual Path (PVP) which is sometimes called Tunneling. The PVP or the Tunnel is created to cross as many ATM switches as needed, so the remote ends would see each other as if they are adjacent. This is done by creating Virtual Ports on the remote switches using a specified VPI, and this VPI is switches through out the ATM network.



The above example shows a direct connection between switches A and B. Two vports were created, A.1 (vport on switch A using VPI 1) and B.2 (vport on switch B using VPI 2). The Virtual Path Connection (VPC) between the two switches is constructed using 3 PVPs in switches X, Y, and Z: X.1 - X.4, Y.4 - Y.5, and Z.5 - Z.2 respectively. In this example, a letter (A, B, X, Y, Z) represents a switch port. The number after the decimal is the VPI that is used. Note that if there is no other vport between A and X, or B and Z (i.e vports A.0 and B.0 are disabled), then switches A and B would not know that switches X, Y, and Z exist.

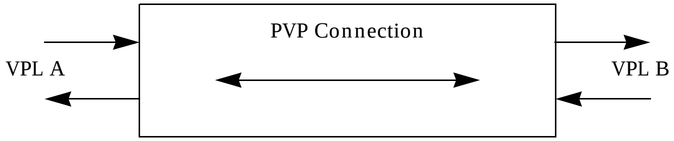
Note: Before you attempt to set up a PVP you will need to configure two things:

1. Define the VPI range that is used for VP switching. By default, all VPIs are used for VC switching, and VP switching is disabled. For configuring VPC VPI range refer to “Managing VPI range for VP switching” on page 99.
2. Define the VPIs that are used to Signalled VPs, and the rest are used for Permanent VPs. For configuring signaled VPC VPI range refer to “Setting Virtual Port Parameters” on page 69.

Creating a PVP connection

A PVP is created by constructing two VPLs. The VPLs describe the edges of the PVP, see Figure 8.2. Refer also to “Creating PVPs” on page 293.

Figure 8.2 A PVP Connection



PVP connections will be re-established automatically when the M770 ATM Switch powers up. You can have up to 64 PVP connections on a module. To set up a bi-directional PVP between 2 ports on different modules (on the same switch) you must type the command on the CLI of each module.

The command described below will setup a VPL on each <slot.port.vpi> and a PVP connection joining the two. The PVP connection will be automatically assigned an ID.

To create a PVP connection, use the `pvp setup` command:

Command:

```
M15-155s6:/>pvp setup <vpl1index> <vpl2index> [<td1>] [<td2>]
```

Example 1: Setting up a PVP between two ports on the same module with default traffic descriptors:

```
M15-155s6:/>pvp setup 6.2.8 6.3.8
```

Example 2: Setting up a PVP between 2 ports on different modules on the same switch, with traffic descriptors:

```
M15-155s6:/>pvp setup 6.3.7 9.1.7 3
M15-155s9:/>pvp setup 6.3.7 9.1.7 3
```

Parameters:

`<vpl1index>`	The first VPL for the PVP connection in the format `<slot.port number.vpi>`.
`<vpl2index>`	The first VPL for the PVP connection in the format `<slot.port number.vpi>`.
`td1`	Index of rx td for vpl1 (= tx td for vpl2)
`td2`	<td2> = index of tx td for vpl1 (= rx td for vpl2)

Freeing a PVP connection

To free a PVP connection, use the `pvp free` command:

Command: `M15-155s8:/>pvp free <pvp-id>|all`

Parameters:

`<pvp-id>`	The index of the PVP connection
`all`	All configured PVPs.

In order to free a PVP connection between 2 modules, you must type the command in the CLI of each module.

Listing the current PVP connections

To list all current PVP connections which are set up on the M770 ATM Switch use the `pvp show` command.

Command: `M15-155s8:/>pvp show`

Output:

```
PVP ID     VPL1  | VPL 2 | FWD TD| REV TD| ADMIN
|
===================================================
===========
270047153  9.1.7 | 6.3.7 | 1     | 1     | UP
|
```

The `pvp show` command displays the information described in Table 8.3

Table 8.3 Output from the pvp show command

Field	Description
ID	Unique identifier for the PVP connection assigned by the switch
VPL1	One VPL for a PVP connection
VPL2	The second VPL for a PVP connection
FWD TD	Traffic descriptor for the forwarding direction (from VPL1 to VPL2)
REV TD	Traffic descriptor for the reverse direction (VPL2 to VPL1)
Admin	The management state of the PVP connection

Disabling a PVP connection

To temporarily disable an established PVP connection, use the `pvp disable` command.

Command: `M15-155s8:/>pvp disable <pvp-id>`

Example: `M15-155s8:/>pvp disable enable 270047153`

Parameters: `<pvp-id>` PVP connection index

Enabling a PVP connection

To enable an established PVP connection, use the `pvp enable` command.

Command: `M15-155s8:/>pvp enable <pvp-id>`

Example: `M15-155s8:/>pvp enable 270047153`

Parameters: `<pvp-id>` PVP connection index

Listing all the VPLs

To list all the VPLs, use the `pvp vpl show` command:

Command: `M15-155s8:/>pvp vpl show`

Output:

```
VPL   |  X CONNECT ID  FWD TD   REV TD   STATE
         |            |        |
=================================================
============
6.3.7    270047153    1        1        UP
|        |            |        |
9.1.7    270047513    1        1        UP
|        |            |        |
```

The `pvp vpl show` command displays the information described in Table 8.4

Table 8.4 Output from the pvp vpl show command

Field	Description
VPL	The unique VPL identifier in terms of slot.port.vpi
X CONNECT ID	The PVP connection that is using this VPL.
FWD TD	The forward traffic descriptor identifier
REV TD	The reverse traffic descriptor identifier
State	The management state of the corresponding PVP connection

Managing Traffic Descriptors

A Traffic Descriptor defines the service category that will be used to transport traffic and the bandwidth that is required. Each service category has its own set of parameters. The M770 ATM Switch can support up to 32 different user configured traffic descriptors for the creation of PVCs.

The M770 ATM Switch supports three service categories:

- Constant Bit Rate (CBR) traffic, such as uncompressed voice or video.

  For CBR traffic you will need to specify the dedicated Peak Cell Rate (PCR) per second. Bandwidth for CBR traffic is guaranteed for the duration of the connection.
- Variable Bit Rate (VBR) traffic, such as compressed voice or video.

  For VBR traffic you will need to specify a dedicated Peak Cell Rate (PCR), a Sustainable Cell Rate (SCR), and a Maximum Burst Size (MBS). Bandwidth for VBR traffic is guaranteed for the duration of the connection.
- Unspecified Bit Rate (UBR) traffic, such as broadcasts frames.

  UBR connections will always be accepted but bandwidth will not be guaranteed. This is also referred to as “best effort” traffic.

Note: When creating traffic descriptors all cell rates are specified as cells per second.

If the CLP bit is not set in the ATM cell header, it indicates high priority traffic.

Creating a CBR traffic descriptor

To create a CBR traffic descriptor, use the `td setup CBR` command.

Command:
```
M15-155s8:/>td setup CBR <td_id> pcr0+1=<pcr0+1> [pcr0=<pcr0>]
```

Example:
```
M15-155s8:/>td setup CBR 2 pcr0+1=64000 pcr0=48000
```

Parameters:

`<td_id>`	An unique identifier for this traffic descriptor.
`<pcr0+1>`	The combined PCR for all cells regardless of whether the CLP (Cell Loss Priority) bit is set in the ATM cell header.
`<pcr0>`	An optional PCR for cells where the CLP bit is not set in the ATM cell header. This PCR must be less than, or equal to, the combined PCR.

Creating a UBR traffic descriptor

To create a UBR traffic descriptor, use the `td setup UBR` command.

Command: `M15-155s8:/>td setup UBR <td_id>`

Example: `M15-155s8:/>td setup UBR 1`

Parameter: `<td_id>` An unique identifier for this traffic descriptor.

Creating a VBR traffic descriptor

There are three types of VBR traffic descriptors that can be created.

To create a VBR traffic descriptor, use one of the three methods described in this section, use the `td setup VBR` command:

1st Method

Command: `M15-155s8:/>td setup VBR <td_id> pcr0+1=<pcr0+1> [pcr0=<pcr0>]`

Example: `M15-155s8:/>td setup VBR 3 pcr0+1=64000 pcr0=48000`

Parameters:

`<td_id>` An unique identifier for this traffic descriptor.

`<pcr0+1>` The combined PCR for all cells regardless of whether the CLP bit is set in the ATM cell header.

`<pcr0>` An optional PCR for cells where the CLP bit is not set in the ATM cell header. This PCR must be less than, or equal to, the combined PCR.

2nd Method

Command:

```
M15-155s8:/>td setup VBR <td_id> pcr0+1=<pcr0+1>
scr0+1=<scr0+1> mbs0+1=<mbs0+1>
```

Example: `M15-155s8:/>td setup VBR 4 pcr0+1=128000 scr0+1=64000 mbs0+1=1000`

Parameters:

`<td_id>` An unique identifier for this traffic descriptor.

`<pcr0+1>` The combined PCR for all cells regardless of whether the CLP bit is set in the ATM cell header.

`<scr0+1>` The SCR for all cells regardless of whether the CLP bit is set in the ATM cell header.

`<mbs0+1>` The MBS for all cells regardless of whether the CLP bit is set in the ATM cell header.

3rd Method

Command: `M15-155s8:/>td setup VBR <td_id> pcr0+1=<pcr0+1> scr0=<scr0> mbs0=<mbs0>`

Example: `M15-155s8:/>td setup VBR 4 pcr0+1=128000 scr0=48000 mbs0=800`

Parameters: `<td_id>` An unique identifier for this traffic descriptor.

`<pcr0+1>` The combined PCR for all cells regardless of whether the CLP bit is set in the ATM cell header.

`<scr0>` The SCR for cells where the CLP bit is not set.

`<mbs0>` The MBS for cells where the CLP bit is not set.

Removing a traffic descriptor

To remove a traffic descriptor, use the `td free` command:

Command: `M15-155s8:/>td free <td_id>`

Example: `M15-155s8:/>td free 1`

Parameter: `<td_id>` An identifier for the traffic descriptor.

Note: A traffic descriptor that is in use cannot be freed. First, you will need to free the VCLs that are using the traffic descriptor.

Listing the traffic descriptors

To list all traffic descriptors, use the `td show` command:

Command: `M15-155s8:/>td show`

Output:

```
--ID--  --Count---SRC-  ---Quality of Service----
   1       7      Int   UBR=UBR(Unknown): Best Effort Traffic
   2       0      Int   No service!
   3       7      Auto  UBR(Best-Effort): PCR0+1=127
   4       3      Auto  UBR(Best-Effort): PCR0+1=255
   5       4      Auto  UBR(Unknown): PCR0+1=3532
```

The `td show` command displays the information described in Table 8.5.

Table 8.5 Output from the td show command

Field	Description
ID	The traffic descriptor identifier.
Count	The number of times the traffic descriptor is used by VCLs.

Table 8.5 Output from the td show command

Field	Description
SRC	Indicates the source of the traffic descriptor. Internal - traffic descriptors created internally by the switch. Auto - traffic descriptors created automatically when setting up SVCs. User - traffic descriptors created manually for setting up PVCs.
Quality of Service	The service category of the traffic descriptor as well as the PCR, SCR, and MBS values (where applicable).

Chapter 9

Managing Static Routing

This chapter describes how to use the command-line interface to setup and manage static routes in an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3 “How to Use the Command-line Interface”.

Setting up routing entries

This chapter describes the commands that allow you to configure static routes in the routing table in the Avaya M770 ATM Switch. For more examples about setting up routing entries for an attached device, see “Routing Configuration” on page 13.

Static routing is needed when connecting to an ATM host which does not support ILMI, and when connecting to another switch which supports only IISP and not PNNI.

Adding a new routing entry to the routing table

To add a new routing entry to the routing table, enter a partial prefix, followed by one or more virtual ports. A 19-byte ATM address is usually composed by combining the switch network prefix with the End-Station Identifier (ESI) of the attached device.

Note: Static routing should be configured on the module through which the route is performed e.g. if you want to add a route to virtual port 8.4.0 you need to configure this in module number 8.
The static routes shown in module 8 will be only the routes of module 8.

To add a new routing entry to the routing table, use the `route add` command access the module where you want this route to be added.

Command:

```
M15-155s8:/>route add <address> <vport id> [<vport id>...]
```

Examples:

```
M15-155s8:/>route add
39.00.00.00.00.00.00.00.01.f6.e0.00.21.11.31.6f.00.28.01  8.1.0
M15-155s8:/>route add
39.00.00.00.00.00.00.00.01.f6.e0.00.22  8.2.0 8.2.3
M15-155s8:/>route add 39.00  8.4.0
```

Parameters:

`<address>` ATM address to be added to the routing table.
<hex-byte>[.<hex-byte>[.<hex-byte>...]]
eg. 12.ab.CD.de.ad.00 (up to 19 hex-bytes)

`<vport id>` ID of the virtual port which is to be used to route towards the specified ATM address

`<org scope>` The organizational scope of the address <1..15> if not specified default to 15 (global scope)

The organizational scope is a UNI scope translated to PNNI advertisement scope according to Table 9.1 below (extracted from the PNNI standard). The PNNI advertisement scope indicates how far in the hierarchy this address should be advertised.

Table 9.1 Default UNI Scope to PNNI Level Mapping

UNI Scope	PNNI Routing Level Indicator
1-3	96
4-5	80
6-7	72
8-10	64
11-12	48
13-14	32
15 (global)	0

Note: All ATM addresses that are entered in the routing table must begin with the AFI that is supported by the switch. The current AFIs supported by a M770 ATM Switch are 39, 47, and 45. For more information about these AFIs, see Viewing or changing the switch prefix in Chapter 4, “Managing Miscellaneous Commands”.

Once routes have been added, you can view them using the `route show` command. For more information about displaying the routes in a routing table, see “Listing the routing entries in a routing table” on page 120.

Deleting a routing entry from the routing table

When you delete a routing entry that is currently being used for an established connection, this connection will not be affected. The deletion will take effect next time you set up the connection.

To delete a route from the routing table, use the `route delete` command.

Command:	`M15-155s8:/>route delete <address> <vport id> [<vport id>...]`	
Examples:	`M15-155s8:/>route delete 39.00.00.00.00.00.00.00.01.f6.e0.00.21.11.31.6f.00.28.01  8.1.0`	
Parameters:	`<address>`	This can be either the 19-byte hexadecimal address or a partial.
	`<vport id>`	A virtual port that was used to route to the specified ATM address.

Note: It is not recommended that you delete routes that were added dynamically by ILMI.

Note: Internal routes that have been added to the routing table by an entity that is internal to the switch (for example, by LANE services) cannot be deleted.

Listing the routing entries in a routing table

To list the routing table of a specific module, including routes that have been disabled, use the `route show` command.

Command:

```
M15-155s8:/>route show
```

Output:

```
Port   ATM Prefix                                                     Status
Origin
Scope
----   ----------                                                     ----
-- ------
6.0.0  39.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00 Up
Internal
15 -
6.0.0  39.00.00.00.00.00.00.00.40.0D.87.00.0D.00.40.0D.87.00.0D Up
Internal
15 -
6.0.0  47.00.79.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01 Up
Internal
15 -
6.10.0 39.00.00.00.00.00.00.00.40.0D.87.00.0D.00.40.0D.63.01.F5 Up
ILMI
15 -
```

The `route show` command displays the information described in Table 9.2.

Table 9.2 Output from the route show command

Field	Description
ATM Prefix	The full ATM address or a truncated ATM address.
Port	The virtual port to route through.
Status	The status of the entry. UP indicates that the route is functional. DOWN indicates that the route is non-functional. This could be because the port is down or disabled by the user.
Origin	The origin of the routing entry. Static- The routing entry has been manually entered. ILMI- The routing entry has been learned using ILMI. Such entries are added by the M770 ATM Switch for end-stations that are attached to it and are using the ILMI protocol. Internal- The routing entry was added by an entity that is internal to the switch (for example, by LANE services).
Scope	The UNI scope with which this address was registered. The UNI scope is translated to PNNI advertisement scope according to Table 9.1. The PNNI level indicates the hierarchy scope up to which the address is advertised. The default UNI scope is 15 (the address is advertised throughout the entire PNNI domain).

Chapter 10

Managing PNNI Routing

This chapter describes how to use the command-line interface to manage the PNNI routing in an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3 How to Use the Command-line Interface.

PNNI (Private Network-Network Interface)

The description in this chapter assumes basic knowledge of the PNNI protocol. For more information regarding the PNNI standard, refer to the ATM Forum publication (af-pnni-0055.000).

Hierarchical PNNI

Hierarchical PNNI is supported from M770 ATM Switch Embedded S/W Version 2.1 and above. You can now configure your ATM network into a hierarchy of peer groups, with multiple peer groups at each level. A single M770 ATM Switch can operate as both a physical and a logical node. There may be up to four logical nodes in four heirarchy levels in the same switch. The physical node represents the switch itself, while a logical node in a higher level peer group represents a lower level peer group.

In the following sections describing PNNI, the 'level' parameter in a command refers to the instance of the PNNI node within the switch, level = 1 is the physical node, and level = 2 is the first logical node.

PNNI Implementation in the Avaya M770 ATM Switch

The architecture of the M770 ATM Switch is a distributed one, i.e. no single point of failure. All cards implement full PNNI, and at the same time share the information received and produced by each other. Information generated by an individual card is shared by all other cards and accepted as if it is self-originated. All switch cards share the same node ID and peer group ID, so to other switches in the peer group it looks like one unified switch.

When Hierarchical PNNI configurtion is used, the Master Agent module of the Avaya M770 ATM switch (the PDC or PNNI Designated Card) has a special role. This is the module that advertises the switch as willing to become a PGL (Peer Group Leader). If it is elected as PGL, the next higher level node the LGN (Logical Group Node) resides in the PDC module. Therefore, commands that are applicable only PGL or LGN can be performed only on the PDC.

PNNI Global Topology Information

General topology information

To show the global topology information, use the following command:

Command: `M15-155s2/>route pnni topology general`

Output:

```
Global PNNI topology information
+------------------+-------------------+--------------------+-------+
| Horizontal Links |  Nodes            | Reachable Addresses| Ptses |
+--------+---------+---------+---------+---------+----------+-------+
|        |Not      |         |Not      |         |          |       |
|Routable|Routable |Reachable|Reachable| Internal|Exterior  |       |
+--------+---------+---------+---------+---------+----------+-------+
|       2|       0 |        4|       0 |        9|         3|     22|
+--------+---------+---------+---------+---------+----------+-------+
```

The output of this command provides tabular general information about the entire PNNI domain: number of horizontal links, nodes and reachable addresses, and the number of PTSEs in the local database. It distinguishes between horizontal links that are routable and those that are not routable. A horizontal link is a bi-directional connection between two adjacent PNNI nodes. The information about a link is derived from two Horizontal Link PTSEs which represent the two uni-directional connections. A link may be non-routable if:

- The paired link (the link on the other direction) doesn’t exist, i.e. a Horizontal Link PTSE describing the other direction doesn’t appear in the local database.
- The remote node doesn’t appear in the local database (it’s Nodal Info PTSE was not received).

Note: In heirarchical PNNI configuration, uplinks known to this node are not shown in the output above. To see Uplinks information, see the Global Topology Uplink command on page 130.

In addition, the table distinguishes between nodes that are reachable, and those that are not reachable. Reasons for a node to be non-reachable are:

- One or more PTSEs generated by this node were received at the local node, but the Nodal Info PTSE of that node was not one of them.
- The Nodal Info PTSE of that node was received, however, there is no valid route to that node. A route may be non-valid if one or more links on that route are non-routable.
- A node may be non-reachable if one of the nodes on the path is a non-transit node.

Reachable addresses are grouped to Internal and Exterior Reachable Addresses (RAs). Internal RAs are ATM addresses that are part of the PNNI domain. The switches learned them using ILMI and advertised them in Internal RA IGs. Exterior RAs are ATM addresses that are not part of the PNNI domain. They were learned by the switch using a private protocol or manually configured, and advertised using Exterior RA IGs. Finally, the total number of different PTSEs received at this node is displayed.

Topology hierarchy list

Use the following command to display the hierarchy list of the PNNI network:

Command:

```
M15-155s8:/>route pnni topology hlist
```

Output:

```
Hlist:
Level=1. Scope=56
nodeId:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.1
6.00
atmAddr:
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.81
pgId:    38.39.04.00.00.00.00.00.00.00.00.00.00.00
PGL:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.1
6.00

Level=2. Scope=48
nodeId:
30.38.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.0
0.00
atmAddr:
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.82
pgId:    30.39.00.00.00.00.00.00.00.00.00.00.00.00
PGL:     -----
Done!
```

The hierarchy list represents the hierarchy of peer groups as it is seen from this switch (physical node).

As described in the ATM Forum PNNI protocol, each node sees its peer group, and the peer groups that are directly above it. It doesn't see neighboring peer groups, their content or their internal information.

The output example above represents a network with 2 levels of hierarchy. Level 1 represents the lowest level, where the physical node resides. The Level 1 output displays the following:

- Level scope (56)
- nodeID
- ATM Address
- Peer group ID for the physical node
- The nodeID of the Peer Group Leader (PGL) of this peer group (if it exists)

The next level in the hierarchy, the Level 2 output, displays the following :

- Level scope (48)
- nodeID
- ATM address

- Peer group ID of this (logical) node
- Peer Group Leader (if it exists)

In this example, there is no PGL, and therefore, there are no additional peer groups in the hierarchy.

Global topology links

Use the following command to display the global topology links:

Command: `M15-155s8:/>route pnni topology link [<level>]`

Output:

```
Node Id:
38.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.00
.20.00
                                            Port: 11.03.00
<---+
                                                          |
                                            Port: 08.07.00
<---+
Node Id:
38.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.00
.21.00
```

This represents the fact that 2 Horizontal Links PTSEs for 2 routable uni-directional links exist in the node topology database. The link is identified by the node ID and the port number of its ends.

If the link does not exist, an ‘X’ will be displayed on the vertical line.

If the optional <level> parameter is used, only the horizontal links of that level shall be displayed.

Global Topology Nodes

Use the following command to show the global topology nodes in a tabular form.

Command:

```
M15-155s8:/>route pnni topology node [<level>]
```

Output:

```
Orig    Leade   Restri  Represen  Restri  Non-      Reachabl
Node    r       ctTran  t         ct      Transit   e
Id              sit               Branch  for PGL
-----------------------------------------------------------
--------------
        No      No      Simple    No      No        Yes

60.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.0
0.21.00
        No      No      Simple    No      No        Yes

60.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.0
0.20.00
```

The information in this table is derived from Nodal Info PTSEs received from the nodes in the domain.

If the optional <level> parameter is used, only the nodes of that level shall be displayed.

Table 10.1 Output from the topology nodes show command

Field	Description
Orig Node Id	This is the 22 bytes of the node ID.
Leader	Indicates whether the node thinks it is a Peer Group Leader (PGL).
Restrict Transit	Indicates if the node advertises itself as restricted transit. If a node is restricted transit, no routes can go through that node. However, setups to/from end systems connected to that node are valid.
Representation	Indicates the way the node is represented. For LGNs, the representations may be either ‘simple’ or ‘complex’.
Restrict Branching	Indicates whether the node can branch point-to-multipoint calls. This attribute is resource related.
Non-transit for PGL Election	Indicates whether the node is ignored when computing connectivity in the PGL Election algorithm. The node is non-transit for PGLE when it is operating in overload state.
Reachable	Indicates whether the node is reachable. Reasons for a node to be unreachable are indicated in “General topology information” on page 124.

Global Topology PTSEs

The following command displays the database of PTSEs.

Command:
```
M15-155s8:/>route pnni topology ptse [<index>]
```

Parameter:
```
<index> - Index of specific ptse (0 for all)
This is optional parameter to show the ptse in full format
mode.
```

Example:
```
M15-155s8:/>route pnni topology ptse
```

Output:
```
Ptse table:
Orig
Node Id:
60.a0.39.84.0f.80.01.bc.61.de.81.00.00.40.00.00.00.6f.00.00.40
.00
Slot Index: 0
Index Ptse Id           Type        Seq NumLife TimeCheckSum
----- ------          --------------------------------------
--------
1 0x00000001          nodalInformation6696756137
2 0x02000003          internalReachableAddress10265655917
3 0x02000005          internalReachableAddress6696751421

Orig
Node Id:
60.a0.39.84.0f.80.01.bc.61.de.81.00.00.40.00.00.00.6f.00.00.40
.00
Slot Index: 3
Index Ptse Id           Type  Seq NumLife TimeCheckSum
----- ------          --------------------------------------
--------
4 0x34000008          horizontalLinks111056758

Orig
Node Id:
60.a0.39.84.0f.80.01.bc.61.de.81.00.00.40.00.00.00.6f.00.00.60
.00

Index Ptse Id           Type        Seq NumLife TimeCheckSum
----- ------          --------------------------------------
--------
5 0x00000001          nodalInformation211066922
6 0x02000003          internalReachableAddress1108416206
7 0x94000007          horizontalLinks111066918
Done!
```

This command lists all the PTSEs in the local database. It organizes them by their originator, and then according to their PTSE-ID (for the local node there is a distinction between different slots originating PTSEs). In this table only summary information about the PTSEs is presented, for more information about a specific PTSE, use the optional `<index>` parameter in the command.

Global Topology Reachable Addresses

For displaying the global topology reachable addresses, use the following command:

Command: `M15-155s8:/>route pnni topology ra`

Examples:

```
Ra: Len = 104 bits
    Prefix = 39.84.0f.80.01.bc.61.de.81.00.00.20.00
    Orig Node Id  Type       Reachable  Scope
    -----------------------------------------
               Internal   Yes        0

60.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.0
0.20.00

Ra: Len    = 152 bits
    Prefix =
47.00.79.00.00.00.00.00.00.00.00.00.00.00.a0.3e.00.00.01
    Orig Node Id  Type       Reachable  Scope
    -----------------------------------------
               Internal   Yes        0

60.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.0
0.20.00
```

The output is a list of Reachable Addresses, with the following information about it:

Field	Description
Len	This is the length of the reachable address in bits.
Prefix	The prefix indicates, that all addresses that start with this prefix can be reached directly from the advertising node.
Orig Node Id	This is the 22 bytes of the node that advertises direct reachability to this address.
Type	Indicates whether the address is advertised as internal or exterior to the advertising node.
Reachable	Indicates whether the node advertising the address is reachable. If it is not reachable, there is an incorrect connection in the network.

Field	Description
Scope	This field indicates the scope of advertisement of the address. The scope value indicates up to which hierarchical level the address will be advertised. The lower the value is, the wider the domain that gets the address. Value of 0 indicates that the address will be advertised through out the entire PNNI domain. The advertisement scope is mapped from the UNI scope. For more details refer to the Static Routing chapter.

Global Topology Uplink

Use the following command to display the global topology uplinks in the network:

Command:

```
M15-155s8:/>route pnni topology uplink [<level>]
```

Output:

```
Node Id:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
                       Aggregation Token: 0    Uplink Port:
02.12.00.00-->-+

|
Node Id:
30.38.39.00.00.00.00.00.00.00.00.00.00.00.00.00.00.F6.00.00.0E.00
<---+

Node Id:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
                       Aggregation Token: 0    Uplink Port:
09.13.00.00-->-+

|
Node Id:
30.38.39.00.00.00.00.00.00.00.00.00.00.00.00.00.00.F6.00.00.0E.00
<---+
```

The first node is the originating node, its level scope is lower in the hierarchy than the destination upnode. The first byte of the Node ID holds the level scope in which the node resides (in hex). In this example, the uplink's originating node resides in level 56 (0x38) and the upnode resides in level 48 (0x30).

The Aggregation Token is a 4-byte integer that marks whether different uplinks to the same upnode shall be aggregated to the same higher-level horizontal link.

If the optional <level> parameter is used, only uplinks originating at that level will be displayed.

PNNI Local Topology Information

Local PNNI Links

The PNNI Local Links command gives information about the links on which the Hello protocol, and possibly the Database Synchronization (DBS) take place. On the physical level, these links would be local to the module. On a logical level, these links would be local to the LGN, i.e. the PDC slot (MA) on the switch that acts as PGL/LGN.

The following command displays the state of the local PNNI links:

Command:
```
M15-155s8:/>route pnni local link <level>
```

Output for:
```
             ------------------------------------------------------------------
Physical     Port       Hello       Nbr   Link   Activ Remote           Remot
Level                                            e     Port             e
                        State       Stat  Statu  Time                   Node
                                    e     s                             ID
             ------------------------------------------------------------------
Inside       13.02.00.  twoWayInsi  full  <----  33478 05.02.00.00
             00         de                >      8
              38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.0
                                                                              0

Outside      09.13.00.  commonOuts  ----  -----  14037 01.13.00.00
             00         ide         -     --
              38.A0.39.01.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.4E.0
                                                                              0
             ------------------------------------------------------------------

             Port       Hello       Nbr   Svc    Link   Activ Remote    Remot
                                                        e               e
                        State       Stat  State  Statu  Time  Port      Node
                                    e            s                      ID
Logical      00.02.00.  twoWay      full  open   <----  14065 00.02.00.
Level        00                                  >            01
              38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.0
                                                                              0
             ------------------------------------------------------------------
```

The output in a tabular format includes the following information:

Field	Description	
Port	The local port number.	
Hello State	The state of the Hello protocol on this link.	
	“twoWayInside”	An inside link (within the peer group). The node on the other side was discovered correctly.
	“commonOutside”	An outside link (to a node on a different peer group). The node on the other side was discovered correctly and a common parent peer group was identified
	“twoWay”	A logical link. The logical node on the other side was discovered correctly.
Nbr State	Indicates the state of the Neighboring Peer FSM that is used for database synchronization. The state ‘full’ indicates that the nodes’ databases are in-synch. The state ‘remote’ indicates that the synchronization protocol is not yet performed on this link. However, it could be that there is a parallel link from a different slot of this switch going to the same neighbor, and the synchronization is done over that link. This field is not applicable for outside links, as database synchronization is not performed between peer groups.	
Link Status	Indicates the status of the link between this node and its neighbor. A uni-directional link indicates that the Nbr State is not full. This could be due to another parallel link to the same neighbor (and the synchronization is done over that link), or due to a problem in the synchronization protocol. This field is not applicable for outside links, as database synchronization is not performed between peer groups.	
Active Time	For an Inside Link or Logical Link, this indicates the time in seconds that the neighbor’s database is synchronized (i.e. the Nbr State is ‘full’). For an Outside Link, it indicates the time in seconds since the Hello reached a “commonOutside” state.	
Remote Port	This is the port ID at the other end.	
Remote Node	The 22 bytes node ID of the remote node.	

Field	Description
Svc State	This field is applicable only for logical links, in which the Hello protocol runs over an SVC-RCC. It indicate the SVC-RCC state. If the state is 'open' it means that the PNNI control channel between LGNs was opened correctly, and now the PNNI protocols should get to their final states.

Local Memory Information

The following command displays the PNNI memory usage:

Command:
```
M15-155s8:/>route pnni local memory
```

Examples:
```
Pnni   alloc memory:         65824 bytes (  0 %)
Switch alloc memory:         14094808 bytes ( 84 %)
Switch free  memory:         2682408 bytes ( 15 %)
Switch total memory:         16777216 bytes
Note: Switch alloc memory include the pnni alloc memory
```

Field	Description
Pnni alloc memory	The number of bytes that are allocated for PNNI. In parenthesis is the percentage of the PNNI allocation from the entire switch memory.
Switch alloc memory	Includes all memory, including PNNI that is currently allocated.
Switch free memory	The number of bytes, and percentage of memory that is still free.
Switch total memory	Include both the memory available in RAM and in SIMMs.

Local Peer Neighbors

The following command displays inofmration regarding synchronization protocol with the neighbors to this module.

Command:
```
M15-155s8:/>route pnni local nbr <level>
```

Examples:

```
Peer Nbr:
=========
Remote Node Id:
38.a0.39.84.0f.80.01.bc.61.de.81.00.00.20.00.00.00.6f.00.00.20.00
Nbr                          Active
State                        Time
------------------
full                         1513

Total number of ports:               1
Number of received DBS packets:      2
Number of transmitted DBS packets:   4
Number of received PTSPs:            808
Number of transmitted PTSPs:         341
Number of received PTSE requests:    1
Number of transmitted PTSE requests: 1
Number of received PTSE acks:        334
Number of transmitted PTSE acks:     729

Nbr Ports:
==========
Local                        Remote       Hub   Flood
Port                         Port         Slot  Status
08.07.00.00                  12.03.00.00  8      True

Peer Nbr:
=========
Remote Node Id:
38.A0.39.00.00.00.00.00.00.00.00.00.00.00.00.02.D0.80.7
E.C0.01.00
Nbr         Active
State       Time
------------------
full         21140

Total number of ports:               1
Number of received DBS packets:      2
Number of transmitted DBS packets:   2
Number of received PTSPs:            25
Number of transmitted PTSPs:         146
Number of received PTSE requests:    1
Number of transmitted PTSE requests: 0
Number of received PTSE acks:        134
Number of transmitted PTSE acks:     24


Nbr Ports:
==========
Local                        Remote       Hub   Flood
Port                         Port         Slot  Status
08.07.00.00                  14.02.00.00  8      True
```

The output of this command shows the neighbors to this node and their state.

Field	Description
Peer Node Id	The 22-bytes node ID of the peered neighbor.
Nbr State	Indicates the state in the Neighboring Peer state machine for this neighbor. The state ‘full’ indicates that the two nodes completed database synchronization.
Active Time	The amount of seconds since the databases became synchronized, and this link is advertised.
SvcHello State	This field is applicable for logical neighboring relationship. Between LGNs all PNNI control protocols run over SVC-based RCC. This field indicates the state of the SVC-based RCC Hello protocol.The state of 'twoWay' indicates that the remote node was discovered correctly.
Total number of ports	The number of parallel links that go to the same neighbor node.
Number of received DBS packets	The number of Database Summary packets that were received from the neighboring peer (part of the PNNI database synchronization phase).
Number of transmitted DBS packets	The number of Database Summary packets that were transmitted to the neighboring peer (part of the PNNI database synchronization phase).
Number of received PTSPs	The number of PNNI Topology State Packets (PTSP) that were received from the neighboring peer.
Number of transmitted PTSPs	The number of PTSPs that were transmitted to the neighboring peer.
Number of received PTSE requests	The number of received PNNI Topology State Element (PTSE) requests (during PNNI Database synchronization phase).

Field	Description
Number of transmitted PTSE requests	The number of transmitted PTSE requests (during PNNI Database synchronization phase).
Number of received PTSE acks	The number of PTSE acknowledgments that were received from the neighboring peer.
Number of transmitted PTSE acks	The number of PTSE acknowledgments that were transmitted to the neighboring peer.
Nbr Port	Provides a table* with information about all the ports on the physical node that are connected to the same neighbor. The local ports may be from any slot on the switch. *This table is applicable to physical level neighbors.
Local Port	The identification (slot.port) of the local end of the link to the neighbor.
Remote Port	The identification of the remote end (slot.port).
Hub Slot	The slot on which the local end of the link resides.
Flood Status	A true/false value indicating which of the parallel links is used for flooding of PTSEs. In case there is only one link to a neighbor that link will be used for flooding of PTSEs.

Local Reachable Addresses

To show local reachable addresses (RAs), use the following command:

Command:

```
M15-155s8:/>route pnni local ra
```

Examples:

```
Local Ra: Len   = 152 bits
          Prefix =
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.5C
          Port                Type           Scope
          -----------------------------------------
          08.00.00.00   Internal       0
```

The output of this command displays a list of all local Reachable Addresses. For each address it shows the following information:

Field	Description
Len	The address length in bits. The maximum length would be 152 bits, as ATM routing is done for only 19 bytes addresses. The last byte of the ATM address (the selector) has local significance only, and does not affect routing.
Prefix	The ATM address prefix (up-to 19 bytes) that is known to PNNI.
Port Type and Scope Table	Provide a table of all the local ports that this address is registered on. For each port it provides the Port Type and Scope.
Type	The address type for each port it can be either Internal address or Exterior address.
Scope	This field indicates the scope of advertisement of the address. The scope value indicates up to which hierarchical level the address will be advertised. The lower the value, the wider the domain that gets the address. Value of 0 indicates that the address will be advertised through out the entire PNNI domain. The advertisement scope is mapped from the UNI scope. For more details refer to the Static Routing chapter.

Port 0 on the local slot indicates the CPU. Addresses registered on the CPU port indicates services that are registered on the local module, for example, the LECS address as appears in the above example.

PNNI Local Switch Information

The following commands show information for the entire switch.

Local Switch links

This command displays all PNNI uplinks that were advertised by any module in the switch. Uplinks are advertised for Outside links (links to other peer groups) that their Hello protocol had reached the final state of 'commonOutside'..

Command:

```
M15-155s8:/>route pnni local switch link
```

Output:

```
Node Id:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
                                             Port: 11.03.00.00-
                                    ->-+
                                                |
                                                      Port: 11.03.00.00-
                                                ->-+
                Node Id:
                38.A0.39.04.02.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.20.00
```

This represents the fact that 2 Horizontal Links PTSEs for 2 routable uni-directional links exist in the local node database. The link is identified by the node ID and the port number of its ends.

If the link does not exist, an ‘X’ will be displayed on the vertical line.

Note: In hierarchical PNNI, local switch links include all logical and physical horizontal links that are directly connected to this switch (including all its nodes).

Local Switch Reachable Addresses

This command displays the 19-byte address of end stations directly connected to the switch. These addresses were either learned via ILMI or added manually in the static route table. The addresses here are all of the addresses seen in each of the modules using the `route pnni local ra` command. To show local switch reachable addresses (RAs), use the following command:

Command: `M15-155s8:/>route pnni local switch ra`

Examples:

```
Local Ra: Len    = 152 bits
          Prefix =
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.5C
Port          Type         Scope
--------------------------------
06.00.00.00   Internal     0

Local Ra: Len    = 152 bits
          Prefix =
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8
Port          Type         Scope
--------------------------------
02.00.00.00   Internal     0

Local Ra: Len    = 152 bits
          Prefix =
39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.64.03.EA
Port          Type         Scope
--------------------------------
02.15.00.00   Internal     0
09.13.00.00   Exterior     32

Local Ra: Len    = 152 bits
          Prefix =
47.00.79.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01
Port          Type         Scope
--------------------------------
06.00.00.00   Internal     0
```

The output of this command displays a list of all local switch Reachable Addresses. For each address it shows the following information:

Field	Description
Len	The address length in bits. The maximum length would be 152 bits, as ATM routing is done for only 19 bytes addresses. The last byte of the ATM address (the selector) has local significance only, and does not affect routing.
Prefix	The ATM address prefix (up to 19 bytes, 152 bits) that is known to PNNI.
Port, Type and Scope Table	Provide a table of all the local ports that this address is registered on. For each port it provides the port type and scope.
Type	The address type may be either Internal or Exterior (to the PNNI domain). An exterior ATM address is an address that was set statically using static routes.
Scope	This field indicates the scope of advertisement of the address. The scope value indicates up to which hierarchical level the address will be advertised. The lower the value, the wider the domain that gets the address. Value of 0 indicates that the address will be advertised through out the entire PNNI domain. The advertisement scope is mapped from the UNI scope. For more details refer to the Static Routing chapter.

Port 0 on the local slot indicates the CPU. Addresses registered on the CPU port indicates services that are registered on the local switch, for example, the LECS address as appears in the above example.

Local Switch Uplinks

This command displays all PNNI uplinks that were advertised by any module in the switch. Uplinks are advertised for Outside links (links to other peer groups) that their Hello protocol had reached the final state of 'commonOutside'.

Command:

```
M15-155s8:/>route pnni local switch link
```

Output:

```
Node Id:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
          Aggregation Token: 0           Uplink Port:
                                      02.04.00.00-->-+

                                      |
Node Id:
30.00.39.04.02.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
<---+


Node Id:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
          Aggregation Token: 0           Uplink Port:
                                      09.13.00.00-->-+

                                      |
Node Id:
30.38.39.02.00.00.00.00.00.00.00.00.00.00.00.00.00.F6.00.00.09.00
<---+
```

PNNI Configuration Commands

In Hierarchical PNNI, there is a need to configure the nodes separately on different levels. Therefore, there is an additional parameter to indicate the level that is currently being configured. You may omit this parameter for the configuration show commands. In this case, the command would refer to all levels.

Showing all PNNI configured variables

To show important 1st level PNNI variables use the following command:

Command:

```
M15-155s8:/>route pnni config show [<level>]
```

Output:

```
Level 1 -
=========
Level Scope:  Configure [Current]: 56 [ 56 ]
Admin Status: Up    Oper Status:   Up    Restricted Transit:
No
Node id:      Configure [Current]
38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00
[
38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00  ]
Atm Addr:
39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.81
PG id:        Configure [Current]
38.39.03.00.00.00.00.00.00.00.00.00.00.00
[ 38.39.03.00.00.00.00.00.00.00.00.00.00.00 ]
```

Note: Configuration of the first level requires a switch reset. Therefore, the output of the 'Show' command gives both current values (in brackets) and configured value (as currently stored in the NVRAM).

To show PNNI variables for all levels use the same command with no level parameter:

Command:

```
M15-155s8:/>route pnni config show
```

Output

```
Level 1 -
=========
Level Scope:  Configure [Current]: 56 [ 56 ]
Admin Status: Up    Oper Status: Up    Restricted Transit: No
Node id:      Configure [Current]
38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.00
[ 38.A0.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.00  ]
Atm Addr:     39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.81
PG id:      Configure [Current]
38.39.03.00.00.00.00.00.00.00.00.00.00.00
[ 38.39.03.00.00.00.00.00.00.00.00.00.00.00 ]

Level 2 -
=========
Level Scope:  48
Admin Status: Up    Oper Status: Down  Restricted Transit: No
Node ID:
30.00.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00
Atm Addr:
39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.82
PgId : 28.39.00.00.00.00.00.00.00.00.00.00.00.00

Level 3 -
=========
Level Scope:  40
Admin Status: Down  Oper Status: Down  Restricted Transit: No
Node ID:
28.00.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00
Atm Addr:
39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.83
PgId : 28.39.00.00.00.00.00.00.00.00.00.00.00.00

Level 4 -
=========
Level Scope:  32
Admin Status: Down  Oper Status: Down  Restricted Transit: No
Node ID:
20.00.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00
Atm Addr:
39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.84
PgId : 28.39.00.00.00.00.00.00.00.00.00.00.00.00

Level 5 -
=========
Level Scope:  24
Admin Status: Down  Oper Status: Down  Restricted Transit: No
Node ID:
18.00.39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.2
3.00
Atm Addr:
39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.8
PgId : 28.39.00.00.00.00.00.00.00.00.00.00.00.00
```

Due to the internal PNNI implementation in Avaya M770 ATM switch, the Master Agent module has the role of PDC (PNNI Designated Card). The PDC is the module that advertises the switch Nodal Information PTSE, and in hierarchical PNNI, this is the module that acts as PGL/LGN (in case the switch was elected Peer Group Leader). As a result, when the user uses the `/route pnni config show` command on a sub-agent module, some configuration parameters would be unknown to the sub-agent module. Those parameters would appear as dashed line. The parameters for the Logical Levels are:

- Operational status of a level
- Node ATM address

All above configuration variables are explained in subsequent chapters.

PNNI Administrative Status

Each PNNI node has an administrative (admin) status. This parameter indicates whether this node has to be administratively up or down. The physical node (on the 1st level) admin status is always up. The admin status of a higher level node (logical node) is determined by the user. It shall be up if the user wants the logical node to be active.

Note: The admin status of a logical node is important when you want the switch to become a Peer Group Leader, and an Logical Group Node at the higher level. In order to achieve that you'll have to set both the Leadership Priority of the node at the lower level to a value greater than 0, and the admin status of the next higher level to 'up'.

Showing PNNI node admin status

To show the admin status of a node use the following command:

Command:

```
M15-155s8:/>route pnni config admin show 1
```

Output:

```
Admin Status:
Level 1 - Up
```

To show the admin status of all levels, use the following command:

Command:

```
M15-155s8:/>route pnni config admin show
```

Output:

```
Admin Status:
Level 1 - Up
Level 2 - Up
Level 3 - Down
Level 4 - Down
Level 5 - Down
```

Setting PNNI node admin status

Use the following command to set pnni node admin status. It takes effect only for logical levels (greater than 1).

Command:

```
M15-155s8:/>route pnni config admin set <level> <up | down>
```

PNNI ATM addresses

The following command displays the ATM address of the PNNI node. The PNNI node's ATM address is advertised in Nodal Information PTSE and is important when the node is a PGL/LGN. In this case, an SVC-RCC shall be opened between LGNs, i.e., between the PNNI node's ATM addresses.

Command:

```
M15-155s8:/>route pnni config atm_addr show [<level>]
```

Output:

```
Atm address:
Level 1 -    39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.81
Level 2 -    39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.82
Level 3 -    39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.84
Level 4 -    39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.85
Level 5 -    39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.86
```

Setting PNNI defaults for all parameters

Use the following command to set PNNI configuration with default parameters.

Command:

```
M15-155s8:/>route pnni config default <level>
```

This request will set defaults for all configurable variables: PNNI node level, node id, peer group id, restrict transit flag, pgle parameters, svce parameters and all the timers for the pysical level. Changes won't take effect until the next reboot, except for timers, restrict transit flag and PGLE parameters.

For logical levels, changes will take place immediately.

Note: Make sure the admin status of that level is down when you use this command on the logical level.

PNNI Interfaces

Showing all PNNI interfaces

Use the following command to display the current configuration of the PNNI interfaces:

Command:
```
M15-155s8:/>route pnni config interfaces show
```

Examples:
```
Port  Interfac  PNNI Port Aggr  VP           Admin Weight
Id    e Index             Toke  Cap
                          n
                                      CBR  RtVB NrtVB  ABR  UBR
                                           R    R
--------------------------------------------------------------
-------------
1     6148      06.01.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
2     6150      06.02.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
3     6152      06.03.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
4     6154      06.04.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
5     6156      06.05.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
6     6158      06.06.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
7     6160      06.07.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
8     6162      06.08.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
9     6164      06.09.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
10    6166      06.10.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
11    6168      06.11.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
12    6170      06.12.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
13    6172      06.13.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
14    6174      06.14.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
15    6176      06.15.00. 0     True  504  5040 5040   504  504
                00                    0                0    0
```

Here you can see the ATM interface on the switch slot. For every interface you find the following information:

Field	Description
Interface Index	This is the ifIndex for this port.
Pnni Port	This is the port ID as known to PNNI.
Aggr Token	This is the aggregation token for the link if exists. The Aggregation Token is used by the network administrator to indicate to the PGL how to aggregate multiple uplinks into higher-level horizontal links.
VP Cap	Indicates whether the interface is capable of carrying VPCs or not.
Admin Weight	Indicates the administered weight that is currently assigned for the link for different Classes of Services: CBR (Constant Bit Rate), RtVBR (Real Time Variable Bit Rate), NrtVBR (Non-real time VBR), ABR (Available Bit Rate), and UBR (Unspecified Bit Rate). The default value is 5040 for all administered weights. Administered Weights are used during routes calculation. When different routes to the destination are available, the one with the lowest cost is taken. The cost of the route is calculated as the summation of all admin. weight along the path.

Setting the PNNI interface aggregation token

The aggregation token is significant in multiple peer groups configuration. When two different outside links to the same peer group has the same derived aggregation token, the PGL/LGN will aggregate them into one higher level horizontal link. However, if their derived aggregation tokens are different, two higher level horizontal links shall be advertised. This may be useful, if the network administrator has a reason to distinguish between the two links.

Note: A derived aggregation token is calculated from the configured aggregation token at both ends, using the following formula. If the configured aggregation token at both ends is the same, the derived aggregation token gets this value. If one configured aggregation token has a non-zero value and the other one is zero, the derived aggregation token gets the non-zero value. If both ends have a non-zero configured aggregation token, and these values are not the same, the derived aggregation token is zero.

Command:

```
M15-155s8:/>route pnni config interfaces aggrToken <ifIndex>
<aggrToken>
```

Parameters:

```
<ifIndex> -    Index number of the interface (or all)
<aggrToken> -  Aggr Token value
```

Setting the PNNI interface administrative weight

Use the following command to set administrative weight to PNNI interfaces:

Command:

```
M15-155s8:/>route pnni config interfaces weight <ifIndex> <type>
<value>
```

Parameters:

```
<ifIndex> - Index number of the interface (or all)
<type>    - Cbr RtVbr NrtVbr Abr Ubr all
<value>   - admin weight, range [1..16777216]
Notes: - ifIndex=all : all interfaces
type=all    : all types
```

In the following example the user configures the Administered Weight for RtVBR for interface 5124 to be 10000.

Examples:

```
M15-155s8:/>route pnni config interfaces weight 5124 RtVbr 10000
```

Set PNNI interfaces to default values

In order to set PNNI interfaces to default values, use the following command:

Command:

```
M15-155s8:/>route pnni config interfaces default <ifIndex> <cos>
```

Parameters:

```
<ifIndex> - Index number of the interface (or all)
<cos>  - Cbr RtVbr NrtVbr Abr Ubr all
Notes: - ifIndex=all : all interfaces will get default parameters
                             - cos=all : all classes of service for this
interface will
                              get default values.
```

PNNI Levels

Showing PNNI Node Level

This command shows the level scopes as configured by the user for all nodes within the switch.

Command:

```
M15-155s8:/>route pnni config level show [<level>]
```

Output:

```
Level Scope:
Level 1 - Configure [Current]: 56 [ 56 ]
Level 2 - 48
Level 3 - 40
Level 4 - 32
Level 4 - 24
```

Note: The greater the scope is in number, the lower the hierarchical level. In other words, lower level scope numbers indicates higher level nodes.

Setting PNNI Node Level

Use the following command to set PNNI node level. When setting the lowest node's level, it takes affect only after next reboot. Setting all other node's level requires that the administrative status of that node would be down. For more information about the admin status refer to `/route pnni config admin` command.

Command:

```
M15-155s8:/> route pnni config level set <level (1-5)>
<level (1-104)>
```

Parameters:

`<level (1-5)`	Internal level: 1 is the lowest physical node
`<level (1-104)>`	Level scope, has network-wide significance.

Setting PNNI Node Level to the Default Value

The following command sets the PNNI node level to its default according to the given level. Default values of the different internal levels appear in table Table 10.2

Table 10.2 Default Level Scope to PNNI Internal Levels

Internal Level	Level Scope (Decimal)	Level Scope (Hex)
1 (physical)	56	38
2	48	30
3	40	28
4	32	20
5	24	18

Note: The level scope of a node appears as the first byte of its node ID, and the first byte of its peer group ID. In addition, the 104 **-** <level> rightmost bits of the peer group ID are set to zero.

PNNI Node ID

Showing PNNI node ID

Use the following command to display the PNNI node ID of this node.

Command:

```
M15-155s8:/>route pnni config node_id show [<levvel>]
```

Output:

```
Node id:
Level 1 -    Configure [Current]:
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
[
38.A0.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.00
]
Level 2 -
30.38.39.04.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.00
Level 3 -
28.30.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.00
Level 4 -
20.28.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.00
Level 5 -
18.20.39.03.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.00
```

Setting PNNI node ID

Use the following command to set PNNI node ID. For the physical level, this takes affect only after next switch reboot. For logical levels, this change requires that the node would be administratively down before the set takes place.

Command:

```
M15-155s8:/>route pnni config node_id set <level (1-5)> <node id>
```

Parameters		
	`Level (1-5)`	Internal level number: 1 is the lowest (physical) node
	`Node id`	22 hexadecimal bytes separated by a decimal. The first byte is the level (1-104 in Hex).

Setting PNNI node ID to default value

Use the following command to set PNNI node ID to its default value. The default value is derived from the switch's ATM address and the PNNI level that is currently being configured. For the lowest level (physical), the scope level gets into the first byte of the node ID, then comes the value "160", and then the full ATM address of the switch. Further changes to the switch ATM address won't be reflected in the PNNI node ID unless specified by the `address prefix` command

For logical levels, the default value is derived from the lower level peer group ID. The level gets into the first byte of the node ID, then come 14 bytes of the lower peer group ID, (that this node would represent if it becomes LGN). Then come the ESI (6 bytes) of the physical system implementing this LGN. The last byte is zero.

Command:

```
M15-155s8:/>route pnni config node_id default <level>
```

Examples:

```
Note: This request will set default value (extracted
from ATM address) for node id.
Do you want to continue (Y/N)?
```

PNNI Operational Status

The operational status of a physical node is always 'up'. The operational status of a logical node may be either 'up' or 'down'. It will be up, if the logical node is active, i.e. the lower level node is PGL, and the logical node is LGN. This is determined by the Peer Group Leader Election (PGLE) protocol between the nodes at the lower level Peer Group.

To show the operational status of a node use the following command. If the level parameter is omitted, the operational status of all levels will be displayed.

Command:

```
M15-155s8:/>route pnni config oper show [<level>]
```

Output:

```
Admin Status:
Level 1 - Up
Level 2 - Up
Level 3 - Down
Level 4 - Down
Level 5 - Down
```

Note: The operational status cannot be set by the user. The user determines the administrative status, and the operational status is determined by the lower level PGLE protocol.

PNNI Peer Group ID

Showing PNNI peer group ID

Use the following command to display the PNNI peer group ID.

Command:

```
M15-155s8:/>route pnni config pg_id show [<level>]
```

Output:

```
Peer group id:
Level 1 -    Configure [Current]:
38.39.04.00.00.00.00.00.00.00.00.00.00.00
[ 38.39.04.00.00.00.00.00.00.00.00.00.00.00 ]
Level 2 -    30.39.00.00.00.00.00.00.00.00.00.00.00.00
Level 3 -    28.39.03.00.00.00.00.00.00.00.00.00.00.00
Level 4 -    20.39.03.00.00.00.00.00.00.00.00.00.00.00
Level 5 -    18.39.03.00.00.00.00.00.00.00.00.00.00.00
```

The PNNI peer group ID is used when the PNNI protocol constructs the peer groups in which topology databases are being synchronized. A link between two neighbors that share the same peer group ID is considered an inside link, and a link between 2 PNNI nodes that don’t have the same peer group is considered an outside link. Topology databases are synchronized only over inside links.

Setting PNNI peer group ID

Use the following command to set the PNNI peer group ID.

Command:
```
M15-155s8:/>route pnni config pg_id set <level>
< pg id >
```

Parameters

`level (1-5)`	Internal level number: 1 is the lowest (physical) node
`pg id`	14 hexadecimal bytes separated by a decimal. The first byte is the level (1-104 in Hex). 104-level rightmost bits should be zero.

Output:
```
Warning: This request will change the peer group id. It will
also change the node level and the first byte of the node id to
<level scope in hex>.
Do you want to continue (Y/N)?
```

Setting PNNI peer group ID to default value

Use the following command to set the PNNI Peer Group ID to its default value. The default value is derived from the PNNI level and the switch's prefix. The first byte of the peer group ID is the level indicator. The following bytes must be prefixes of ATM End System Addresses as defined in the PNNI specification (af-pnni-0055.000). The peer group is encoded with the 104-n rightmost bits set to zero, where n is the level.

Command:
```
M15-155s8:/>route pnni config pg_id default <level>
```

Output:
```
This request will set default value (extracted from ATM
address) for peer group id.
Do you want to continue (Y/N)?
```

PNNI PGLE Parameters

The Peer Group Leader Election (PGLE) submenu is important in hierarchical PNNI, where this protocol takes place while electing the PGL. The most important parameter here is the Leadership Priority, which indicates the priority of each node for becoming a PGL. Leadership Priority of 0 indicates that the node will not become a PGL.

Showing PNNI PGLE parameters

Command:
```
M15-155s8:/>route pnni config pgle show [<level>]
```

Output:
```
Svcc Table - Level 1:
Name                    Index    Current    Default
                                 Value      Value
---------------------------------------------------
--------
Leadership priority     1        20         20
initTimerPeriod         2        15000      15000
overrideTimerPeriod     3        30000      30000
reElectionTimerPeriod   4        15000      15000
```

Set PNNI PGLE parameters to default values

Use the following command to set the PNNI node PGLE parameters to their default values:

Command:
```
M15-155s8:/>route pnni config pgle default [<level>]
[<index>]
```

Parameters:
```
<level> - internal PNNI level number: 1 is the physical
node
<index> - the index of the timer
```

This request will set value for PGLE parameter according to the index parameter. Changes will take effect immediately.

Set PNNI PGLE Parameter

Use the following command to set the PNNI node PGLE parameters:

Command:
```
M15-155s8:/>route pnni config pgle set <level> <index>
<value>
```

Parameters:
```
<level> - internal PNNI level number: 1 is the physical
node
<index> - the index of the timer
<value> - the vlaue that the selected timer will receive
```

This request will set value for PGLE parameter according to the index parameter. Changes will take effect immediately.

PNNI Restricted Transit Flag

A PNNI node may be administered to be restricted transit. This will restrict calls from going through this node, but will not restrict calls to be set from / to endstations connected to the node directly. This feature may be used by network administrators to imply some policy over the network.

Showing PNNI node restrict transit flag

Use the following command to show pnni node restrict transit flag:

Command:
```
M15-155s8:/>route pnni config restrict_transit show [<level>]
```

Output:
```
Restricted Transit:
Level 1 - No
Level 2 - No
Level 3 - No
Level 4 - No
Level 5 - No
```

Setting PNNI node restrict transit flag

Use the following command to set the PNNI restrict_transit flag:

Command:
```
M15-155s8:/>route pnni config restrict_transit set <level> <no
| yes>
```

Parameters

Level (1-5)	Internal level number: 1 is the lowest (physical) node
No | Yes	No – indicates the node is not restricted for transit Yes – indicates that the node is restricted for transit, i.e., no Setup calls through this mode

Output:
```
Note: This request will define this switch as a transit/non-
transit switch
i.e. [no] setup call through this node
Changes will take effect immediately
```

Setting PNNI node restrict transit flag to default value

Use the following command to set the restrict transit flag to its default of ‘no’.

Command:
```
M15-155s8:/>route pnni config restrict_transit default
<level>
```

Examples:
```
Note: This request will set default value (no) for
restrict transit flag
i.e. setup call can through this node
Changes will take effect immediately
```

PNNI Summary Tables

Showing PNNI summary table

Use the following command to show the configured PNNI summary table:

Command:

```
M15-155s8:/>route pnni config summary show <level>
```

Examples:

```
Summary: Type = internal
         Len       = 104 bits
         Prefix    = 39.84.0f.80.01.bc.61.de.81.00.00.60.00
         Suppress  = false
         State     = advertising
         RowStatus = active
         Local Ra:
         Len  Prefix
-----------------------------------------------------------------

Summary: Type      = internal
         Len       = 104 bits
         Prefix    = 39.84.0f.80.01.bc.61.de.81.00.00.78.00
         Suppress  = false
         State     = advertising
         RowStatus = active
         Local Ra:
         Len  Prefix
-----------------------------------------------------------------
152  39.84.0f.80.01.bc.61.de.81.00.00.78.00.00.00.6f.00.00.40
152  39.84.0f.80.01.bc.61.de.81.00.00.78.00.00.00.6f.00.00.60
152  39.84.0f.80.01.bc.61.de.81.00.00.78.00.00.40.0d.63.01.f7
```

PNNI specification defines that each PNNI node advertises the addresses that are locally connected to it. Since it is not scalable that each node would advertise all of its local RAs, PNNI defines a way that the node advertises only summaries of addresses. For lowest level node, the ATM address of a switch is the switch default summary, as all directly connected hosts and edge devices that use ILMI for address registration get the switch prefix as the prefix to their address. For lowest level node, the address prefix of the switch is the default summary.

Note: In a well-configured network, the switches' prefixes will be organized according to their peer groups. This way, the default summaries on the default level will match the ATM prefixes of the switches. See Appendix G, “Setting Address Prefixes to Match Hierarchical PNNI” for more details about prefix assignment.

Here you can see all summaries that were defined, either manually or by default (i.e. the switch prefix).

Field	Description
Type	Indicates whether this summary applies to Internal Reachable Addresses or to Exterior Reachable Addresses. An Internal RA is an address that is internal to the PNNI domain, while an Exterior RA is an address that does not resides in the PNNI domain. It may be manually configured (or via a proprietary protocol), and may be reached over a non-PNNI link.
Len	The length of the summary in bits.
Prefix	The ‘Len’ bits long address prefix to be advertised if there are RAs that fall under this prefix.
Suppress	This can be either ‘true’ or ‘false’. If it is ‘true’ this means that the summary would not be advertised and therefore all addresses that fall under this summary would not be known in the PNNI domain. If it is ‘false’ it means that the summary would be advertised.
State	Indicates whether the summary is currently being advertised. It may be either ‘advertising’ ‘suppressing’ or ‘inactive’.
RowStatus	Indicates the status of this row in the MIB table. All values other than ‘active’ indicates that this row is not active.
Local Ra	Provides a list of local reachable addresses that fall under this summary. Each RA is displayed by its Len (length in bits) and Prefix.

Set the PNNI summary address prefix

Use the following command to set a PNNI summary address prefix.

Command:

```
M15-155s8:/>route pnni config summary set <type> <prefix> <len> <suppress>
<level>
```

Parameters:

<type>	I(nternal) or E(xterior)
<prefix>	The ATM address prefix. Each octes is in hex and is separated by a “.”
<length>	length of the prefix in bits (0-152)
<suppress>	T(rue) or F(alse)
<level>	Internal level number. 1 is the lowest (physical) node

Examples:

```
set I 39.84.0f.80.01.bc.61.de.81.00.00.60.00 104 F 1
```

Enable the PNNI summary address prefix

To enable pnni summary address prefix use the following command.

Note: When a pnni summary address is enabled summary show State = advertising and RowStatus = Active.

Command:

```
M15-155s8:/>route pnni config summary enable <type> <prefix> <len> <level>
```

Parameters:

<type>	I(nternal) or E(xterior)
<prefix>	The ATM address prefix. Each octes is in hex and is separated by a “.”
<length>	length of the prefix in bits (0-152)
<level>	Internal level number. 1 is the lowest (physical) node

Examples:

```
enable I 39.84.0f.80.01.bc.61.de.81.00.00.60.00 104 1
```

Disable the PNNI summary address prefix

To disable PNNI summary address prefix use the following command.

Note: When a PNNI summary address is disabled summary show State = inactive and RowStatus = notInService.

Command:

```
M15-155s8:/>route pnni config summary disable <type> <prefix> <len> <level>
```

`<type>`	I(nternal) or E(xterior)	`<type>`
`<prefix>`	The ATM address prefix. Each octes is in hex and is separated by a “.”	`<prefix>`
`<length>`	length of the prefix in bits (0-152)	`<length>`
`<level>`	Internal level number. 1 is the lowest (physical) node	`<level>`

Examples:
```
disable I 39.84.0f.80.01.bc.61.de.81.00.00.60.00 104 1
```

Remove the PNNI summary address prefix

To remove the PNNI summary address prefix use the following command.

Command:
```
M15-155s8:/>route pnni config summary remove <type> <prefix> <len>
<level>
```

Parameters:
```
<type>     - I(nternal) or E(xterior)
<prefix>   - The Atm address prefix
                     each octet is in hex and separate with '.'
<length>   - length of the prefix in bits (0-152)
<level>    – Internal level number. 1 is the lowest
(physical) node
```

Examples:
```
set I 39.84.0f.80.01.bc.61.de.81.00.00.60.00 104 1
```

Set the PNNI summary table to the default

Use the following command to set the PNNI summary table to its default values. For lowest-level node it is the switch’s ATM prefixs. For higher-level nodes it’s the switch prefix where its length in bits is equal to the level where it resides.

Command:
```
M15-155s8:/>route pnni config summary default <level>
```

PNNI SVCC timers

In hierarchical configuration of PNNI, after each peer group elects a PGL, and the Uplinks to remote Upnodes are advertised within the peer group, LGNs try to open connections between themselves for passing PNNI control information. These connections are called SVC-based RCC since they are used as Routing Control Channel. There are special timers that are used when the SVCCs (Switched Virtual Channel Connections) are set and maintain. These timers are handled in this submenu.

Showing PNNI SVCC timers

Command:

```
M15-155s8:/>route pnni config svcc show [<level>]
```

Output:

```
Svcc Table - Level 1:
Name              Index    Current    Default
                           Value      Value     Range
-------------------------------------------------------
---------
Init Time         1        4          4         [ 1 -
                                                30]
Retry Time        2        30         30        [ 1 -
                                                300]
Calling Integ     3        35         35        [ 1 -
Time                                            300]
Called Integ      4        50         50        [ 1 -
Time                                            400]
```

Set PNNI SVCC timers to default values

Use the following command to set the PNNI node SVCC timers to their default values:

Command:

```
M15-155s8:/>route pnni config svcc default <level> <index|all>
```

Parameters:

```
<level> - internal PNNI level number: 1 is the physical node
<index> - the index of the timer, to set all timers type 'all'
```

This request will set value for SVCC timers according to the index parameter. Changes will take effect immediately.

Set PNNI SVCC timers

Use the following command to set the PNNI node SVCC timers:

Command:

```
M15-155s8:/>route pnni config svcc set <level> <index>
<value>
```

Parameters:

```
<level> - internal PNNI level number: 1 is the physical
node
<index> - the index of the timer, to set all timers type
'all'
<value> - the value that the selected timer will receive
```

Note: This request will set value for SVCC timers according to the index parameter. Changes will take effect immediately.

PNNI Timers

Show PNNI node timers

Use the following command to show the PNNI node timers:

Command:

```
M15-155s8:/>route pnni config timers show <level>
```

Examples:

```
Timers :
Name                   Index  Current   Default
                              Value     Value    Range      Units
-----------------------------------------------------------------
PtseHoldDown           1        10        10   [  1 -  600]  100ms
HelloHoldDown          2        10        10   [  1 -  600]  100ms
HelloInterval          3        15        15   [  1 -  600]  secs
HelloInactivityFactor  4         5         5   [  1 -   20]  fctr
HlinkInactivityTime    5       120       120   [  1 -  600]  secs
PtseRefreshInterval    6      1800      1800   [ 60 - 3600]  secs
PtseLifeTimeFactor     7       200       200   [100 -  500]  %
RxmtInterval           8         5         5   [  1 -   60]  secs
RDelayedAckInterval    9        10        10   [  1 -  600]  100ms
AvcrPm                10        50        50   [  1 -   99]  %
AvcrMt                11         3         3   [  1 -   99]  %
CdvPm                 12        25        25   [  1 -   99]  %
CtdPm                 13        50        50   [  1 -   99]  %
```

The user is not expected to change any of these timers. However, if you need more information about these timers you may refer to the PNNI specification (af-pnni-0055.000), Annex E: Architectural Variables.

The <level> parameter is optional – if it is omitted, timers of all levels will be displayed.

Set PNNI node timers to default values

Use the following command to set the PNNI node timers to their default values.

Command:

```
M15-155s8:/>route pnni config timers default <index(All=99)>
<level>
```

Parameters:

```
<index> the index of the timer , to set all timers type 99
```

Output:

```
Note: This request will set value for timers , according to
the index parameter.
Changes will take effect immediately.
```

Set PNNI node timers

Use the following command to set PNNI node timers.

Command:

```
M15-155s8:/>route pnni config timers set  <index> <value>
<level>
```

Parameters:

```
<index> the index of the timer as appear in the ‘show’ screen.
<value> the value that the selected timer will get.
<level>  Internal level number: 1 is the lowest (physical)
node.
```

Examples:

```
route pnni config timers set 1 15 1
Note: This request will set value for timers , according to
the index parameter.
Changes will take effect immediately.
```

Managing the Management LEC

This chapter describes how to use the command-line interface to manage the management LEC in an Avaya M770 ATM Switch. For information about how to access and use the command-line interface, see Chapter 3 How to Use the Command-line Interface.

Avaya M770 LANE services

The Avaya M770 can host multiple LANE Servers (LECS, LES and BUS) in addition to one management LEC. For a list of all the M770 ATM Switch default LANE services settings, see Appendix A, “Default Settings on a New Avaya M770 ATM Switch”.

For information on how to manage the LANE services in an Avaya M770, see the LANE Chapters in this manual.

Configuring the Management LEC

The M770 ATM Switch has one management LEC for managing the M770 ATM Switch. It supports several high-level protocols such as:

- Telnet for a command-line interface.
- UDP for SNMP management and TFTP software upgrades.
- BOOTP for obtaining M770 ATM Switch’s IP address from a server.
- ICMP for PING inward and outward for IP network configuration diagnosis.

The management LEC resides on the module elected as the Master Agent. For information on Master Agent, see Chapter 1, ”Introduction”.

By default, the M770 ATM Switch management LEC uses the Burnt-In Address (BIA) of the Master Agent as its MAC address. This address can be overridden and a Locally Administered Address (LAA) can be assigned.
The management LEC will register this address with the LAN Emulation Server (LES) that is hosting the Emulated LAN (ELAN) the LEC wishes to join.

The M770 ATM Switch management LEC, by default, is assigned to register to an Ethernet ELAN named “default”.

Viewing information about the management LEC

To view information about the management LEC, use the `lane lec show` command.

Command:

```
M15-155s8:/>lane lec show
```

The `lane lec information` command displays the information described in Table 11.1.

Table 11.1 Output from the lane lec show command

Field	Description
BIA	The switch's BIA, which will be used as the management LEC's MAC address, if the LAA address is not set.
LAA	The LAA, which will be used as the management LEC's MAC address if set. If zeros are displayed, the management LEC will use the BIA.
LEC State	The operational state of the management LEC. • Initial State • LECS Connect • configure • join • initial Registration • bus connect • operational - This is the final state of the LEC.
ELAN name (actual)	The name of the ELAN that the management LEC is currently registered with.
ELAN name (configured)	The name of the ELAN that the management LEC will attempt to register with when it is restarted.
ELAN type (actual)	The type of ELAN that the management LEC is currently registered with.
LAN type (configured)	The type of ELAN that the management LEC will attempt to register with when the LEC is restarted.
LES address	The ATM address of the LES where the management LEC has registered its address.
Maximum frame size (bytes)	The maximum frame size that the ELAN can support. The value is obtained from the LES.

Managing the ELAN for the management LEC

You can select the ELAN that the management LEC will attempt to join. By default, the management LEC attempts to join the ELAN “default”.

You can:

- Specify the ELAN that the management LEC will attempt to join.
- Set up the LECS to dictate which ELAN the management LEC will attempt to join.
- View the current ELAN that the management LEC will attempt to join.

Note: Any changes caused by the following commands will not take effect until the M770 ATM Switch management LEC is restarted. To restart the M770 ATM Switch management LEC, use the `lane lec restart` command.

To specify the ELAN that the management LEC will attempt to join, enter the `lane lec elan` command:

Command:	`M15-155s8:/>lane lec elan <name>`	
Example:	`M15-155s8:/>lane lec elan default`	
Parameters:	`<name>`	The name of the new ELAN that the management LEC will attempt to join. The ELAN must be somewhere on the network and known to the LECS.

To leave the decision about the ELAN that the management LEC joins, to the LECS, enter the `lane lec elan` command:

Command:	`M15-155s8:/>lane lec elan -`	
Example:	`M15-155s8:/>lane lec elan -`	

Parameters:	`-`
	`(hyphen)`
		The decision about which ELAN the management LEC will attempt to join is left to the LECS.

To view the name of the ELAN that the management LEC will try to join, enter the `lane lec elan` command:

Command:	`M15-155s8:/>lane lec elan`
Output:	`The management LEC will join the default ELAN`

Managing a Locally Administered Address for the management LEC

If you have an ELAN that uses its own block of MAC addresses, you may want the management LEC’s MAC address to conform to this scheme by assigning a Locally Administered Address (LAA). When no LAA is defined, the management LEC will use the M770 ATM Switch’s Burst-In Address (BIA).

You can:

- View the currently assigned LAA for the management LEC.
- Set the LAA to cause the management LEC to use the BIA as its MAC address.
- Assign a specific LAA to the management LEC.

To view the current management LEC address, use the `lane lec laa` command.

Command:	`M15-155s8:/>lane lec laa`
Output:	`The Management LEC will use the BIA`

To change address of the LAA, use the `lane lec laa` command.

Command:	`M15-155s8:/>lane lec laa [ none | <laa> ]`	
Examples:	`M15-155s8:/>lane lec laa none`	
Example:	`M15-155s8:/>lane lec laa 51.00.00.62.6A.3E`	
Parameters:	`none`	The management LEC will use the BIA.
	`<laa>`	A MAC address in the format appropriate to the management LEC's ELAN type. A MAC address consists of 6 hexadecimal bytes. For an Ethernet ELAN, the first byte is x2, x6, xA, or xE.

Note: The change caused by the above command will not take effect until the M770 ATM Switch management LEC is restarted. To restart the M770 ATM Switch management LEC, use the `lane lec restart` command.

Restarting the management LEC

This command is used after changing the management LEC configuration.

To restart the management LEC, use the `lane lec restart` command.

Command:

```
M15-155s8:/>lane lec restart
```

Note: The above command may disrupt Telnet and SNMP management sessions.

Displaying the LANE-ARP cache

You can display the management LEC's LANE-ARP (Address Resolution Protocol) cache. This is a list of all other LECs in the ELAN that have sent specifically-addressed LAN frames to the management LEC, or that the management LEC has sent frames to. These frames include Telnet session control and data frames, SNMP requests and responses, and PING requests and responses.

There are two kinds of entries that are displayed in the LANE-ARP cache:

- MAC addresses, which are normally other nodes on the ELAN.
- Route Descriptors (RDs), which occur only in a source-routed Token Ring ELAN and show either destinations for frames that must cross a source-routing bridge, or a device that bridges from ATM to physical Token-Ring networks.

To view the LANE ARP cache, use the `lane lec arpcache` command.

Command:

```
M15-155s8:/>lane lec arpcache
```

Output:

```
Destination  00.10.5A.0A.C0.3B
   ATM address  39.84.0F.80.01.BC.61.DF.00.87.00.77.01.00.40.0D.64.02.DE.81
   DataDirect VC Vpi:0, Vci:751
Destination  00.40.0D.5A.01.4E
   ATM address  39.84.0F.80.01.BC.61.DF.00.87.00.77.01.00.40.0D.64.02.DE.81
   DataDirect VC Vpi:0, Vci:751
```

Viewing the management LEC statistics

To display statistics about the control and data planes of the management LEC, use the `lane lec statistics` command.

Command: `M15-155s8:/>lane lec statistics`

The control plane information for the `lane lec statistics` command is shown in Table 11.2.

Table 11.2 Output from the lane lec statistics command (control plane)

Field	Description	
control packets	In/Out Bad	The number of ELAN control frames that this management LEC has received and sent. The number of corrupted control frames that this management LEC has received.
arp requests	In/Out	The number of LANE-ARP requests that this management LEC has received from and sent to the LES.
arp replies	In/Out	The number of responses to LANE-ARP requests that this management LEC has received and responded to.
raw data	In/Out	The total number of control bytes received and sent.
SVCs	In Out Failure Out	The number of incoming SVCs to the management LEC. The number of outgoing SVCs from the management LEC. The number of outgoing SVCs that have failed to be set up.

The data plane information for the `lane lec statistics` command is shown in Table 11.3.

Table 11.3 Output from the lane lec statistics command (data plane)

Field	Description	
unicasts	In / Out	The number of data frames received and sent to a single destination.
multicasts	In / Out	The number of data frames received and sent to a group MAC address.
broadcasts	In / Out	The number of data frames received and sent to all MAC addresses.
packets sent to BUS	The number of packets sent to the BUS by the management LEC.	
BUS packets discarded	The number of packets sent to the BUS that have been discarded.	
errors	In Out	The number of data frames discarded, for example, due to an unrecognised MAC address or an illegal data format. The number of oversize data frames that have been discarded.
unknown protocols	The number of data frames received for unassigned Link Layer Control (LLC) protocols.	
raw data (bytes)	In/Out	The total number of data bytes received and sent.

Chapter 12

Managing SNMP

This chapter describes how to use the command-line interface to manage SNMP in the Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see “Chapter 3”, “How to Use the Command-line Interface”.

Note: The secure commands do not affect Telnet sessions access to a M770 ATM Switch. Telnet sessions use password security.

Using SNMP Commands

These commands configure SNMP information on an Avaya M770 ATM Switch.

Viewing the system group information

To display the information for the system group (sys), use the `snmp show` command.

Command:

```
M15-155s8:/>snmp show
```

Output:

```
SNMP System Group Information
-----------------------------
SysDescr : Avaya M770 ATM Switch, Software Version 1.0.17

SysObjectID : 1.3.6.1.4.1.81.17.1.16
SysContact  : keren
SysName     : oz 77
SysLocation : akko
SysUpTime (HH:MM:SS) : 1 day, 19:53:13
```

Show the list of community names

To list all the community names, use the `snmp community show` command.

Command:
```
M15-155s8:/>snmp community show
```

Example:
```
M15-155s8:/>snmp community show
```

Output:
```
Read-Only community names
=========================
1. public

Read-Write community names
==========================
1. public

Trap community name
===================
public
```

Set the read-only community name

To add a specified name to the list of read-only community names, use the `snmp community ro` command.

Command:
```
M15-155s8:/>snmp community ro add <read-only-community-
name>
```

Delete the read-only community name

To delete an element of the read-only community names' list, use the `snmp community ro delete command`.
The element is specified by its number.

Command:
```
M15-155s8:/>snmp community ro delete <entry-number>
```

Show the list of read-only community names

To list all the read-only community names, use the `snmp community ro show` command.

Command: `M15-155s8:/>snmp community ro show`

Example: `M15-155s8:/>snmp community ro show`

Output:

```
Read-Only community names
=========================
1. public
2. ron1
3. moty
3. gidi
4. nancy
5. andrew
Done!
```

Set the read-write community name

To add a specified name to the list of read-write community names, use the `snmp community rw add` command.

Command: `M15-155s8:/>snmp community rw add <read-write-community-name>`

Delete the read-write community name

To delete an element of the read-write community names' list, use the `snmp community rw delete` command .
The element is specified by its number.

Command: `M15-155s8:/>snmp community rw delete <read-number>`

Show the list of read-write community names

To list all the read-write community names, use the `snmp community rw show` command .

Command: `M15-155s8:/>snmp community rw show`

Example: `M15-155s8:/>snmp community rw show`

Output:

```
Read-Write community names
=========================
1. public
Done!
```

Set the trap community name

To set / alter the trap community name with <trap-community-name>, use the `snmp community trap set` command .

Command:

```
M15-155s8:/>snmp community trap set <trap-community-
name>
```

Show the trap community name

To show the trap community name, use the `snmp community trap show` command.

Command:

```
M15-155s8:/>snmp community trap show
```

Example:

```
M15-155s8:/>snmp community trap show
```

Command:

```
Trap community name
===================
public
Done!
```

Using Permanent Managers Configuration Commands

This section describes how to view and set up a list of Permanent Managers. These are a list of the Network Management Stations which receive SNMP Traps.

Adding a new manager to the list

To add a new manager to the list, use the `permngr add` command.

Command:

```
M15-155s8:/>snmp permngr add <ip_addr>
```

Parameters:

```
<ip_addr> - the ip address of the manager that need to
be added to the permanent manager table.
```

Example:

```
M15-155s8:/>snmp permngr add 149.49.34.216
```

Listing all the current managers

To list all the current managers use the `permngr show` command.

Command:

```
M15-155s8:/>snmp permngr show
```

Output:

```
Permanent Managers:
-----------------------------
1 - 149.49.36.251
2 - 149.49.39.216
```

Updating an existing manager

To update an existing managers' IP address, use the `permngr update` command.

Syntax:

```
M15-155s8:/>snmp permngr update <index> <ip_addr>
```

Parameters:

```
<index> - The permanent manager table index of the
manager ip address that needs to be updated.
<ip_addr> - the updated manager ip address.
```

Example:

```
M15-155s8:/>snmp permngr update 1 149.49.34.217
M15-155s8:/>snmp permngr show
Permanent Managers:
-----------------------------
 1  - 149.49.36.217
 2  - 149.49.39.216
```

Removing a manager from the list

To remove a new manager from the list, use the `permngr remove` command.

Command:

```
M15-155s8:/>snmp permngr remove <index>
```

Parameters:

```
The permanent manager table index of the ip address
that needs to be removed
```

Example:

```
M15-155s8:/>snmp permngr remove 2
```

Secure Group Commands

This section describes the secure group commands that enable you to enable or disable security on the switch and set up a list of Network Management Station (NMS) addresses as authorized managers.

An authorized manager is any NMS that is listed in the secure allowed table. If you enable security then only authorized managers that have been specified in the security tables will be able to manage the M770 ATM Switch.

There is a limit on the number of concurrent NMSs that can manage a single M770 ATM Switch. If SNMP security is enabled then a maximum of 15 concurrent NMSs can manage the M770 ATM Switch, otherwise up to 20 concurrent NMSs can manage the switch.

Note: The secure commands do not affect Telnet sessions access to a M770 ATM Switch. Telnet sessions use password security.

Listing the status of the SNMP security

You can list all NMSs that are assigned access as authorized managers. Also displayed are the NMS's that are currently accessing the M770 ATM Switch.

For each NMS in the table the following information is displayed: an index entry number for the NMS, the address type of the NMS, the IP address of the NMS, and when the current NMS last accessed the M770 ATM Switch.

To display all the security information for the M770 ATM Switch, use the `snmp secure show` command.

Command:

```
M15-155s8:/>snmp secure show
```

Output:

```
Secure mode is currently Disabled

SNMP Security Information : currently active NMS's
------------------------------------------------------------
-----
Index    Type     IP AddressTime Since Last Access (H:M:S)
1        IP       194.32.220.1290:02:50
2        IP       194.32.220.260:02:20

Secure mode is currently Disabled
No entries specified in MStack secure allowed table
```

Viewing or changing secure current table row timeout

Timeout is the duration of time before the NMS's are removed from the secure current tables. By default timeout is set to 300 seconds.

To display or set the timeout for security information, use the `snmp secure timeout` command.

Command:	`M15-155s8:/>snmp secure timeout [<timeval>]`	
Output:	`Current table row timeout is 300 seconds`	
Parameter:	`<timeval>`	A timeout value (between 20 and 3000) seconds

Listing all current NMS's accessing the Avaya M770 ATM Switch

You can list all the NMS addresses that are currently communicating with the M770 ATM Switch.

For each NMS in the table the following information is displayed; an index entry number for the NMS, the address type of the NMS, the IP address of the NMS, and when the current NMS last accessed the M770 ATM Switch.

Note: If SNMP security is enabled then a maximum of 15 concurrent NMS's can manage the M770 ATM Switch, otherwise up to 20 concurrent NMS's can manage the switch.

To display the current security information, use the `snmp secure current` command.

Command:

```
M15-155s8:/>snmp secure current
```

Output:

```
Secure mode is currently Disabled

SNMP Security Information : currently active NMS's
-------------------------------------------------------------
Index   Type   IP AddressTime Since Last Access (H:M:S)
1       IP     194.32.220.1290:02:50
2       IP     194.32.220.260:02:20
```

Configuring Authorized Managers

This section describes how to view and set up a list of Network Management Station (NMS) addresses on the M770 ATM Switch as authorized managers.

An authorized manager is any NMS that is listed in the Secure Allowed Table. The NMS will be able to access the M770 ATM Switch by sending SNMP requests and receiving SNMP replies from the M770 ATM Switch.

If you enable security then only authorized managers that have been specified in the security tables will be able to manage the M770 ATM Switch using SNMP.

There is a limit on the number of concurrent NMS's that can manage a single M770 ATM Switch. If SNMP security is enabled then a maximum of 15 NMS's can manage the M770 ATM Switch, otherwise up to 20 NMS's can manage the switch.

Listing all authorized managers

You can list all NMS's that are set up as authorized managers in the M770 ATM Switch. For each NMS in the table the following information is displayed; an index entry number for the NMS, the address type for the NMS, and the IP address for the NMS.

To display a list of authorized managers, use the `snmp secure allowed show` command.

Command: `M15-155s8:/>snmp secure allowed show`

Output:

```
Secure mode is currently Disabled
No entries specified in mstack secure allowed table
```

Setting up an authorized manager entry

You can add up to 15 authorized managers into the Secure Allowed Table. Only these authorized managers will be able to access this M770 ATM Switch.

To add an authorized manager entry, use the `snmp secure allowed add` command.

Command: `M15-155s8:/>snmp secure allowed add <index> <ipaddress>`

Example: `M15-155s8:/>snmp secure allowed add 3 172.16.1.152`

Parameters:

`<index>`	The index number for the entry into the table. The index value must be an integer in the range 1 to 15.
`<ipaddress>`	The IP address for the NMS that is the authorized manager.

Deleting an authorized destination station

To delete an authorised manager station from the SNMP Allowed Table, use the `snmp secure allowed delete` command.

Command:
```
M15-155s8:/>snmp secure allowed delete <index>
```

Example:
```
M15-155s8:/>snmp secure allowed delete 1
```

Parameter: `<index>` The index number for the NMS that received the trap. The index value must be an integer in the range 1 to 15.

Disabling the authorized managers table

To disable the SNMP secure mode, use the `snmp secure allowed disable` command.

Command:
```
M15-155s8:/>snmp secure allowed disable
```

Note: This command takes immediate effect.

Enabling the authorized managers table

Before enabling SNMP security, you should ensure that you have up your NMS in advance, as an authorized managers in the Allowed Secure Table, otherwise you will not be able to manage the M770 ATM Switch via SNMP.

To enable the SNMP secure mode, use the `snmp secure allowed enable` command.

Command:
```
M15-155s8:/>snmp secure allowed enable
```

Output:
```
SNMP secure mode disabled
```

Chapter 13

LANE Services

This chapter describes the features of the LANE Services in an Avaya M770 ATM Switch.

LANE Components in an Avaya M770 ATM Switch

Each module in the Avaya M770 ATM Switch can host one LECS and multiple combined LES and BUS. This means that on one switch, there can be several resilient LECS, and for one ELAN, several distributed LES. The LES does not have to reside in the same device as the LECS.

The elected master module in each switch hosts the management LEC.

For a list of the factory-configured default settings for the LANE components in an M770 ATM Switch, see Appendix A “Default Settings on a New Avaya M770 ATM Switch”.

LANE configuration file config.data

A module’s LANE configuration is saved in a flash file called `config.data`. After a change is made to the module’s LANE configuration, it is written to this file. If there is not enough room in flash memory (greater than 14 files or not enough memory left) for new LANE changes to be saved, you will receive the following message:

```
There is not enough room in flash to save your latest change.
If a reset occurs, this change will be lost.
```

If this occurs, you need to delete at least one of the unused files in flash in order for the LANE configuration to be saved.

LANE 2 Capability

LANE servers in M770 ATM switch are capable of supporting LUNI 2.0. By default, each ELAN supported by the M770 LECS is configured in 'auto' mode, meaning, that the first LES that registered at the LECS for this ELAN, determines whether the ELAN would use a LUNI 1.0 or LUNI 2.0 protocol. This ELAN capability is configurable. For more details, refer to Chapter 16, “Managing an ELAN“. If the ELAN is determined to use LUNI 1.0 and a LUNI 2.0 Client tries to register, it will be told to use LUNI 1.0. However, if a LUNI 2.0 is used in the ELAN, and a LUNI 1.0 client tries to register, it will be registered, as the LES is capable of using the LUNI 1.0 protocol as well.

The LECS in an Avaya M770 ATM Switch

- By default, the M770 ATM Switch will seek a remote LECS at the WKA.
- The M770 ATM Switch pre-defines one ELAN:
  — An Ethernet ELAN named “default”. This is the ELAN name that is requested by several Avaya’s Ethernet-to-ATM Access Switches.
- The M770 ATM Switch LECS can support up to 64 ELANs.
- The M770 ATM Switch enables you to specify default ELANs that will be used when a LEC does not specify the ELAN name but does specify the type of ELAN it wishes to join. You can also define a default ELAN that will be used when a LEC does not specify both the ELAN name and the ELAN type.
- The M770 ATM Switch LECS supports a proprietary automatic LES address determination method to locate a suitable LES for an ELAN.
- All M770 LES will automatically register with the LECS. The benefit of this is that you do not have to supply the LES address when registering with a M770 LES, and if a M770 LES is re-located you do not have to re-configure the LECS with the new LES address.
- The M770 ATM Switch LECS supports a proprietary resilient algorithm to implement LECS redundancy. On failure of an elected active LECS, resilient LECSes in standby mode will elect a new active LECS. No disruption in the working of LANE services in the ATM network will be experienced, providing all resilient LECS have the same database configurations.

Proprietary resilient LECS

The proprietary resilient LECS provides automatic redundancy for the active LECS, by continuously monitoring the status of all resilient LECS.

From the list of available resilient LECSes on the network, the selection of the "active LECS" is done by a process of election. To carry out this election, all ATM switches must be M770s, and ILMI between them must be enabled.

Note: If you are not planning to use PNNI routing or want the switches in the third party environments to host resilient LECS, then you should contact Avaya Technical Support. They can provide you with further information on what manual configuration is required, depending on your third party switch, to get LECS redundancy on your M770 ATM Switches.

A proprietary protocol is used to provide automatic LECS redundancy with the following method of:

- establishing an active mesh of SVCs between the switches hosting resilient LECSes.
- discovering and advertising resilient LECSes on the network.
- propagating the address of the "active LECS" and of the resilient standby LECSes.

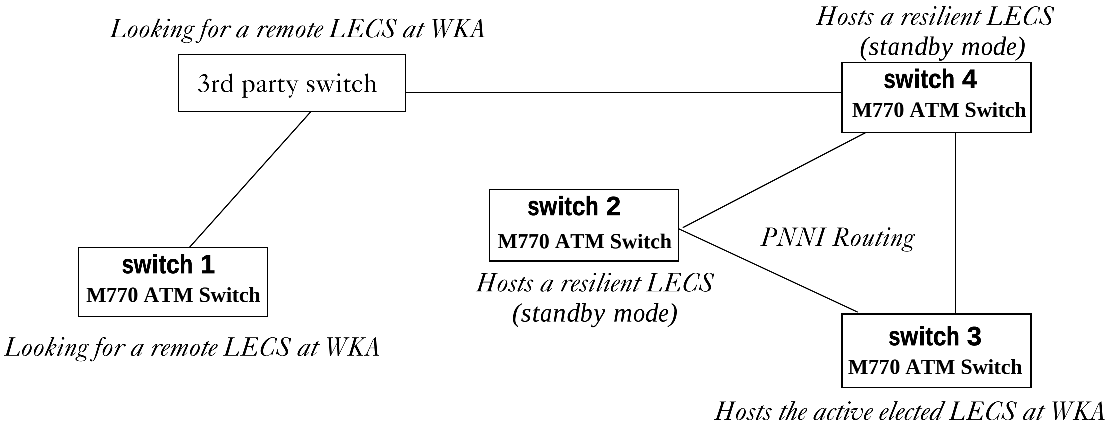
Note: To ensure that a standby LECS can smoothly take over the running of the network, should the active elected LECS fail, it must be configured with the same LANE services information as the active elected LECS.
There is no checking of database consistency between switches that are hosting resilient LECSes.

The status of the elected active LECS is continually monitored by the other resilient LECS. Should the elected active LECS fail, another election process will take place to elect a new active LECS from one of the resilient LECSes. Providing all resilient LECS have the same database configurations then there should be no disruption in the working of LANE services in the ATM network.

If your switch is hosting a local LECS then you can view the details of other resilient LECS on the network. For more information about displaying details of other resilient LECS on the network, see Displaying a resilient LECS election candidate in Chapter 14 Managing the LECS.

The example below shows the M770 ATM Switch across a third party switch. It is recommended that if you have a M770 ATM Switch connected via a third party switch, then that M770 ATM Switch should not host a resilient LECS.

Figure 13.1 M770 ATM Switches connected via third party switch


Looking for a remote LECS at WKA
3rd party switch
Hosts a resilient LECS (standby mode)
switch 4
M770 ATM Switch
switch 2
M770 ATM Switch
PNNI Routing
switch 1
M770 ATM Switch
Hosts a resilient LECS (standby mode)
Looking for a remote LECS at WKA
switch 3
M770 ATM Switch
Hosts the active elected LECS at WKA

Changing the priority of a resilient LECS

You can force the election of a resilient LECS, by placing it on a higher priority level than other resilient LECSes on the network. The higher the priority assigned to a resilient LECS, the better the chances of it winning the election. By default all resilient LECSes when created are assigned a priority of 128.

You can stop a resilient LECS being elected by assigning it a priority of zero. This enables you to configure the LANE services on a switch that is hosting a resilient LECS, without the possibility of the LECS becoming active.

Changing the priority of a LECS will trigger a new election process and the LECS with the highest priority will be elected. If two or more LECSes have the same priority level then the LECS with the higher ATM address will be elected.

Note: If the network is recovering from a failure, the election process is different. The resilient LECS with the highest up-time will remain the active LECS. This is to minimize network disruption.

Note: If you configure the priority of a resilient LECS to the highest priority (255), this will force the LECS to be elected after a network failure regardless of the LECS up-time.

For information on the commands used to change the priority of a resilient LECS, see Setting priority level for a resilient LECS in Chapter 14 Managing the LECS.

The LES and BUS in an Avaya M770 ATM Switch

Each module can provide up to 16 combined LES/BUS pairs. By default, all modules have one Ethernet LES/BUS named “default,” that will try to register with the LECS. The M770 ATM Switch LESes support a proprietary automatic LES address determination method. Therefore, all the M770 ATM Switch LESes can automatically register with an M770 ATM Switch LECS. The benefit of this is that a LES can be re-located without reconfiguring the LECS or the LECs on the ELAN hosted by the re-located LES.

The M770 ATM Switch LESes support two proprietary mechanisms for Resilient and Distributed LES/BUS services as described below. These features require that the LECS, LES and BUS will be hosted on M770 ATM Switch modules.

Note: Since by default, all modules have a LES/BUS named “default,” as soon as the number of modules in your entire network exceeds the maximum number of LESes per ELAN as defined in `lane elan max les` (default 5, maximum 10), you should start deleting or disabling servers

LUNI 2.0 capability

By default, a LES in M770 ATM switch has LUNI 2.0 capability. This means that when it registers to an M770 ATM LECS, it will try to determine that the entire ELAN will be LUNI 2.0 capable (if the LECS LUNI 2.0 was 'auto', and if this LES was registered first, it will actually determine that). When a LUNI 1.0 client tries to register to this LES, the LES will accept it. However, if the LES is not a LUNI 2.0 capable (i.e. LUNI 1.0 only), then when a LUNI 2.0 client tries to register, it will be told to work in LUNI 1.0 mode.

Proprietary resilient standby LESes

The M770 ATM Switch LECS supports a proprietary standby LESes. This will enable resiliency of the LES/BUS in case the module hosting the LES/BUS fails. You can configure up to 10 modules to host the same ELAN name (for example, “default”). Only the first LES to contact the LECS will host the “default” ELAN. All other LESes will provide standby support for the ELAN.

Should the original LES fail for any reason, one of the standby LESes will become the main LES and host the “default” ELAN. This ensures that the ELAN remains up and available to all LECs on the ELAN.

Note: Avaya *strongly recommends* that you use distributed LES/BUS services instead of resilient.

Proprietary Distributed LANE Services

The M770 ATM Switch LECS supports a proprietary system for a distributed LES/BUS in advance of implementing LANE version 2. This will enable not only resiliency of the ELAN but will also increase the number of clients (LECs) that can be supported per ELAN on multiple modules (up to 2,500 LECs per ELAN). This is achieved by allowing a single ELAN to be distributed over multiple LES/BUS pairs in several modules (up to 10 LES/BUS's per ELAN). Each client connects to a single LES/BUS as normal but it could be any of the LES/BUS pairs that are supporting the ELAN.

Virtual Channel Connection (VCC) requirements

In a single ELAN that supports the proprietary Distributed LANE Service:

- each LES has a point-to-point and a point-to-multipoint VCC mesh to each of the other LESes in the ELAN.
- each BUS has a point-to-point and a point-to-multipoint VCC mesh to each of the other BUSes in the ELAN

These connections are then used to exchange information about the registered clients in the ELAN.

Setting up Distributed LANE Services

The M770 ATM Switch module sets up distributed LANE services as follows:

1. When a distributed LES registers with the LECS, it is assigned a LEC id range and given the addresses of other distributed LESes on the ELAN.
2. The LES will then setup a point-to-point and point-to-multipoint with the other LESes on the ELAN.
3. Once connections are setup between the distributed LESes on the ELAN, the LESes will exchange information about their LECs (clients). In this way all the LESes in the ELAN will know of all other clients on the ELAN, and which LES they are attached to.
4. Each LES will also discover the address of every BUS in the ELAN. This information is then used to setup a point-to-point and point-to-multipoint VCC mesh between the BUSes.

LEC Assigned for a Distributed ELAN

When the LEC starts up, it will connect to the LECS in the usual way. If there are several different possible LESes for an ELAN, then the LECS will select which one of the distributed LES addresses to assign the LEC to.

One of the following methods can be configured:-

Round-robin.

This is the default method set when creating a new ELAN. No user configuration is required.

The LEC is assigned to the next distributed LES address in sequence (each distributed LES is used in turn). LECs assignment to the most suitable LES is left to chance.

Group address

User configuration is required.

Every distributed LES on the ELAN is assigned a group address. Note, the same group address is used by all the distributed LESes. It is this address that is returned to every LEC by the LECS, when requesting to join the ELAN. The LEC will then connect with the “nearest” distributed LES if PNNI routing is enabled (the switch that offers the least number of hops will be selected).

Longest Match with LEC address.

No user configuration is required.

The LES address supplied by the LECS is the one which best matches the ATM address of the LEC. This in practice should also provide the nearest distributed LES to the requesting LEC.

Note this may not necessarily be true, should you be using manual configured addresses or non-standard ATM addresses for M770 ATM switches that are hosting the LEC.

The Management LEC in an Avaya M770 ATM Switch

- The M770 ATM Switch has one management LEC for managing the M770 ATM Switch. It is located on the Master agent module in the switch and supports several high-level protocols such as:
  - Telnet for a command-line interface.
  - UDP for SNMP management and TFTP software upgrades.
  - BOOTP for obtaining M770 ATM Switch’s IP address from a server.
  - ICMP for PING inward and outward for IP network configuration diagnosis.
- By default, the M770 ATM Switch management LEC uses the Burnt-In Address (BIA) as its MAC address. This address can be overridden and a Locally Administered Address (LAA) can be assigned. The management LEC will register this address with the LES that is hosting the ELAN that the LEC wishes to join.
- The M770 ATM Switch management LEC, by default, requests to join an Ethernet ELAN.

Chapter 14

Managing the LECS

This chapter describes how to use the command-line interface to manage the LECS in the Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

LECS Location

Any ATM network using LANE must have one active LECS that acts as a central coordinator, making sure that all LECs join the correct ELANs, even though there may be a number of resilient (standby) LECS.

Each ATM module can host the LECS locally or look for a remote LECS. A remote LECS can be in another module, switch, or in an end-station such as a NetWare server.

The LECS type can be configured as a:

- Local Simple LECS
  This will force all local LECs to use the local LECS in the M770 ATM Switch.
- Local Resilient LECS
  This resilient LECS will enter the election and will need to be elected to become the active elected LECS. If the resilient LECS is not elected, it will become a standby LECS. For more information about the election process, see Proprietary resilient LECS in Chapter 13, “LANE Services”.
- Remote LECS
  This will force all local LECs to use a remote LECS in the network.

Advertised address of a LECS

You can specify the address that the LECS will be advertising. By default on the M770 ATM Switch the management LEC and LES/BUS will seek a remote LECS at the WKA.

For information on how to change the location of the LECS, see Changing the location of the LECS later in this chapter.

A local LECS in a M770 ATM Switch can be configured to advertise one of the following addresses:

- The WKA (Well-Known Address). The ATM Forum defines this address as 47.00.79.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01.00
- The 19 byte module address and a specific selector

If the M770 ATM Switch is looking for a remote LECS then it can be configured to use a LECS that is advertising one of the following addresses:

- The WKA
- A specific ATM address on the network.
- The address of an elected M770 ATM Switch resilient LECS.

Viewing the Location of the LECS

You can view the current location of the active LECS on the network.

Note: The output display from the following command will depend on the current location of the active LECS.

To view the location of the LECS, use the `lane lecs location` command:

Command:

```
M15-155s8:/>lane lecs location
```

- If the switch is using its own simple LECS then the following output will be displayed.

Output:

```
There is a local, simple LECS.
It is advertising the ATM Forum Well-Known Address.
Local LECS clients will use the local LECS.
```

- If the switch is using LECS redundancy and the local resilient LECS is on standby then the following output will be displayed.

Output:

```
The local resilient LECS is on standby.
It will advertise
39.84.0F.80.01.BC.61.DF.00.24.24.24.00.24.24.24.24.24.24.30
The elected LECS is at NSAP
39.84.0F.80.01.BC.61.DF.00.A4.A4.A4.00.A4.A4.A4.A4.A4.A4.30
```

- If the switch is looking for a remote LECS then the following output will be displayed.

Output:

```
There is no local LECS.
Local LECS clients will use the LECS at the ATM Forum well-known
address.
```

- If the switch is looking for a remote elected resilient LECS then the following output will be displayed.

Output:

```
There is no local LECS.
Local LECS clients will use the elected resilient LECS.
The elected LECS is at the ATM Forum well-known address.
```

Changing the location of the LECS

You can configure the LECS in a M770 ATM Switch to be either local or remote. If you configure a local LECS then you can specify it to be advertised as either a simple LECS or a resilient LECS.

If you do not specify the type of local LECS, then by default a resilient LECS is created.

Local simple LECS

When creating or changing to a local LECS:

- If a local LECS does not already exist on the switch then a local LECS is created.
- If a resilient LECS exists, then it is made simple.

Local resilient LECS

When creating or changing to a resilient LECS:

- If a local LECS does not already exist on the switch then a resilient LECS is created.
  Note, when you create a resilient LECS it will join the election process and it is this election process that will elect the “active LECS”.
  For more information about the election process, see Proprietary resilient LECS in Chapter 13, LANE Services.
- If a simple LECS exists, then it is made resilient. The address of the LECS is set as specified. The priority of the LECS is set to the default of 128.

Note: You must also ensure that all resilient LECS are configured with the same LANE services information. Should the active LECS fail, a newly elected active LECS can smoothly take over the running of the network.
No checking of database consistency between LECS is done by the switches.

Note: Changing the LECS location may disrupt all LANE connections and any change will take effect immediately.

To change the location and type of the local LECS, use the `lane lecs location local` command:

Command:	`M15-155s8:/>lane lecs location local {wka | <selector>}[{simple | resilient}]`		
Parameters :	`wka`	`simple`	An active local simple LECS is created, using the WKA. Remote clients that make requests for the WKA will be routed to this LECS via PNNI.
	`<selector>`	`simple`	An active simple LECS is created, using the modules address with the specified selector.
	`wka`	`resilient`	A resilient LECS is created. This LECS will enter the election process and if elected will be the “active LECS”. Remote clients that make requests for the WKA will be routed to this LECS via PNNI.
	`<selector>`	`resilient`	A resilient LECS is created, using the modules address with the specified selector. The created LECS will enter the election process and if elected will be the active LECS. Modules that are configured to use the elected resilient LECS will direct clients to this LECS.

Remote LECS

When creating or changing to a remote LECS:

- If a local LECS already exists on the switch then you are warned that it will be deleted and the switch will look for a LECS at the specified remote address.

To change the location of the remote LECS, use the `lane lecs remote` command:

Command:	`M15-155s8:/>lane lecs location remote {elected | wka | <address>}`		
Parameters:	`remote`	`elected`	Module will wait for notification via a proprietary protocol, of the address of the elected resilient LECS.
		`wka`	Module will seek a remote LECS, that is advertising the WKA.
		`<address>`	Module will seek a remote LECS, that is advertising the specific ATM address on the network.

Note: Changing the LECS location may disrupt all LANE connections and any change will take effect immediately.

Setting priority level for a resilient LECS

You can rig the election of a resilient LECS, by placing it on a higher priority level than other LECSes. The higher the priority assigned to a resilient LECS, the better the chances of it winning the election. By default all resilient LECSes when created are assigned a priority of 128.

Avaya recommends that you set the priority of one of the resilient LECS to have a higher priority than the others. This will ensure that this LECS will be elected as the active LECS.

You can stop a resilient LECS being elected by assigning it a priority of zero. This enables you to configure the LANE services on a switch that is hosting a resilient LECS, without the possibility of the LECS becoming active.

Changing the priority of a LECS will trigger a new election process and the LECS with the highest priority will be elected. If two or more LECSes have the same priority level then the LECS with the higher ATM address will be elected.

Note: If the network is recovering from a network failure, the election process is different. The resilient LECS with the highest up-time will remain the active LECS. This is to minimize network disruption.

To change the priority of the local LECS, use the `lane lecs priority` command:

Command:
```
M15-155s8:/>lane lecs priority <priority>
```

Parameters: `<priority>` Indicates the level of priority assigned to the resilient LECS during the election process.
0 - LECS candidate is not available for election.
1 - Lowest priority that can be assigned to a LECS.
128 - Default priority assigned to a LECS.
255 - Highest priority that can be assigned to a LECS.
This will guarantee that the LECS will be elected.

Managing Resilient LECS Candidates

Note: If you are not planning to use PNNI routing or want the M770 ATM Switch switches in the third party environments to host a resilient LECS, contact Avaya Technical Support. They can provide you with further information on what configuration is required, depending on your third party switch, to get LECS redundancy on your M770 ATM Switch switches.

For information on when to create candidates in third party environments, see Proprietary resilient LECS in Chapter 13, “LANE Services”.

Displaying a resilient LECS election candidate

To list all the resilient LECS candidates on the network that are known to the local LECS, use the `lane lecs resilient show` command:

Command:

```
M15-155s8:/>lane lecs resilient show
```

Output:

```
Mesh state is running, local LECS state is standby
Resilient LECS table
--------------------
Index   Election Protocol Endpoint AddressType
0)      39.84.0F.80.01.BC.61.DF.00.07.80.20.00.00.00.6F.07.80.20.7FPVC
1)      39.84.0F.80.01.BC.61.DF.00.07.20.9C.00.00.00.6F.07.20.9C.7FLOCAL

Index    LECS Address
0)       47.00.70.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01.00
1)       47.00.70.00.00.00.00.00.00.00.00.00.00.00.A0.3E.00.00.01.00

Index    Status   Link StatePriorityChecksumUptime
0)       standby  reachable0  8570:00:00
1)       active   reachable12885714 days, 8:28:29
```

The `lane lecs resilient show` command displays the information described in Table 14.1.

Table 14.1 Output from the lane lec resilient show command

Field	Description
Index	A unique number assigned for each resilient LECS known to this switch. Index 0 is assigned to the local LECS.
Election Protocol Endpoint Address	The full 20-byte ATM address that the resilient LECS uses to communicate with other resilient LECSes. Note all resilient LECS are assigned with selector byte of 7F.
Type	Type of resilient LECS. This can be either local, manually configured, or PVC.
LECS address	The full 20 byte ATM address of the LECS.
Status	The state of the resilient LECS. One of these should be active.
Link State	The state of the link to the resilient LECS.
Priority	The priority level assigned to the resilient LECS.
Uptime	The time in days, hours, minutes and seconds that the resilient LECS has been active.

Creating a resilient LECS election candidate

You can create a communication connection to a remote resilient LECS by specifying its election protocol end-point address. This is only necessary when using a 3rd party switch.

Note: Remote resilient LECS candidates should only be created in third party environments.

To create communication connection to a remote candidate, use the `lane lecs resilient create` command:

Command: `M15-155s8:/>lane lecs resilient create <address>`

Parameters: `<address>` This is the address the candidate uses in order to communicate with other candidates on the network.
To construct the address, you must append a selector of “7F” to the modules address.
Alternatively type the `lane lecs resilient show` command on the remote switch and use the end-point address at index 0.
Note, there should only be one election entry for each resilient LECS participating in the election.

Note: When you create a communication connection to a remote switch hosting a resilient LECS, the remote M770 ATM Switch will automatically create a respective candidate for the local LECS.

Deleting a resilient LECS election candidate

You can delete any election candidate that you manually created, using the `lane lecs resilient delete` command and specifying the endpoint address. The connection to the candidate on the remote M770 ATM Switch will be dropped which will result in the deletion of that candidate.

To delete a resilient LECS election candidate, use the `lane lecs resilient delete` command:

Command: `M15-155s8:/>lane lecs resilient delete <address>`

Specified ELAN Defaults in the LECS

Viewing default ELANs

When a LEC contacts the LECS, it usually specifies the ELAN name or the ELAN type that it wants to join. You can define up to 64 different ELAN names in an M770 ATM Switch LECS.

You can define default ELANs for switches hosting a local LECS. These are the ELANs that a LEC should join if it only specifies the ELAN type and not the name of an ELAN.

In cases where the LEC has not specified the ELAN name or the ELAN type, you can set up a default ELAN that will be used.

The following default ELAN names are defined in a M770 ATM Switch:

- **an Ethernet type ELAN:**“default”.
- **an Unspecified type ELAN:**“default”.

  The ELAN name specified here will be used when a LEC does not provide the ELAN name nor the ELAN type that it wants to join.

Note: You can only view and configure the defaults if you are using the local LECS in the M770 ATM Switch or hosting a resilient LECS.

To display the default ELANs that have been specified in the LECS, use the `lane lecs default` command:

Command:

```
M15-155s8:/>lane lecs default
```

Output:

```
No default Token Ring ELAN
Default Ethernet ELAN: default
Default ELAN for unspecified type: default
```

To change the ELAN names for the default ELAN names, see “Specifying default ELANs” on page 198.

Specifying default ELANs

For information on default ELANs, see Viewing default ELANs earlier in this chapter.

To specify a default ELAN, use the `lane lecs default` command:

Command:

```
M15-155s8:/>lane lecs default <type> <ELAN name>
```

Example:

```
M15-155s8:/>lane lecs default ethernet default
```

Parameters:

`<type>` The type of ELAN that a LEC or LES asks to join or host.
You can select one of the following types:
“ethernet” - an Ethernet ELAN type.
“unspecified” -to be used when neither an ELAN name nor a specific ELAN type has been specified.

`<ELAN name>` The name of the ELAN to use when a LEC does not specify the ELAN.
If you want to remove a default ELAN name enter `none`.

Viewing ATM Forum compliant statistics for the LECS

If the LECS is local then you can view the ATM Forum compliant statistics that have been gathered for the LECS. These statistics are continuously being monitored and updated.

To view the ATM Forum compliant statistics for the local LECS, use the `lane lecs stats` command:

Command:

```
M15-155s8:/>lane lecs stats
```

Output:

```
control packets in                        14039
successful config requests                12651
malformed config requests                 0
invalid config request parameters         952
rejected due to insufficient resources    0
rejected due to security restrictions     0
rejected because LECID is not zero        0
rejected due to invalid LAN destination   0
rejected due to invalid ATM address       0
rejected because Client is not recognized 0
rejected due to conflicting parameters    0
rejected due to insufficient info         836
```

Chapter 15

Managing the LES/BUS

This chapter describes how to use the command-line interface to manage the LES/BUS in an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface“.

Creating a new LES

Each Avaya M770 module can provide up to 16 combined LES/BUS. If the LECS is hosted in an Avaya M770 then an Avaya LES will use a proprietary “automatic LES address determination method” to register with the LECS. For more information about the proprietary method and different types of LES modes supported, see in Chapter 13, “LANE Services”.

When creating a new LES you should note the following:

- If the LECS is hosted in a non-Avaya device, the LES mode should be set to “manual”.

Note: If the LES mode is set to “manual” and you move the LES then you will need to manually re-configure the LECS to find the LES.

To create a new LES in the switch, use the `lane les create` command. For definitions of the various LES modes, see “changing the LES registration mode” later in this chapter.

Command:

```
M15-155s8:/>lane les create <elan-name> <mode> <type> <les-selector> <bus-selector>
```

Example:

```
M15-155s8:/>lane les create marketing_eth distributed ethernet 82 83
```

Parameters:

`<elan-name>` Enter the name of the ELAN that the new LES will host. The ELAN name should be unique within the ATM network. This parameter is case-sensitive.

`<mode>` Enter the mode type as either “distributed”, “standby”, or “manual”.
See above explanation for correct mode usage.
distributed - automatic registration for distributed LESes.
standby - automatic registration with standby support.
manual - manual registration.

`<type>` Enter the type of LES ELAN as “ethernet”.

`<les-selector>` Enter the 1 or 2 digit hexadecimal ATM selector for the LES.

`<bus-selector>` Enter the 1 or 2 digit hexadecimal ATM selector for the associated BUS functions.

Note: Each selector entered, when creating a LES, must be unique on the switch. You can use the `lane les show` command to view a list of all selectors currently in use. Selectors 7f, 80 and 81 are reserved for special use and cannot be used for the LES or BUS.

Note: The LES name should be the same as the hosted ELAN name.

Note: Avaya *strongly recommends* that you use distributed LES / BUS services instead of resilient.

Deleting a LES

To delete a LES, use the `lane les delete` command.

Command:

```
M15-155s8:/>lane les delete <elan-name>
```

Example:

```
M15-155s8:/>lane les delete marketing_eth
This will force all attached LECs off the ELAN - do you want
to continue (Y/N)?
y
Done!
```

Note: The above command will take immediate effect. The command must be used with care as all LECs will be thrown off the ELAN hosted by the LES.

Viewing all LESes

To list all the LESs currently held in the ATM modules' database use the `lane les show` command.

Command:

```
M15-155s8:/>lane les show
```

Output:

```
                                         Selectors
Name            Type     EnabledLESBUSClients
default         Ethernet Yes    05    06    3

List of all selectors now in use:
(01) (02) (03) (04) (05) (06) (10) (11) (80) (81) (82) (83)
```

If you enter the name of the ELAN that the LES is hosting then more details regarding the specified LES is displayed.

Command:

```
M15-155s8:/>lane les show [<elan-name>]
```

Example:

```
M15-155s8:/>lane les show 'default'
Information for Emulated LAN 'default'
LES address 39.00.00.00.00.00.00.00.00.6F.07.80.E0.00.00.6F.07.80.E0.01
BUS address 39.00.00.00.00.00.00.00.00.6F.07.80.E0.00.00.6F.07.80.E0.02
 Type                       Ethernet
 Maximum frame size         1516 (bytes)
 LES registration mode      Auto, distributed (Num Peer LESs= 3)
The LES is actively running the elan (Num Clients = 3)
```

The `lane les show <elan-name>` command displays the information described in Table 15.1.

Table 15.1 Output from the lane les show command

Field	Description
Information	The name of the ELAN the LES is hosting.
Type	The type of ELAN. This can be either Token-Ring or Ethernet.
Maximum frame size	The maximum frame size the ELAN can support.
LES address	The ATM address of the LES.
BUS address	The ATM address of the BUS.
LES registration mode	The registration mode of the LES.
The LES is actively running the ELAN	Number of clients hosted by this LES.

Viewing LECs using a specific LES

To list all the LECs (clients) currently using a specific LES, use the `lane les clients` command.

Command:

```
M15-155s8:/>lane les clients <elan-name>
```

Example:

```
M15-155s8:/>lane les clients ‘default’
```

Parameter:

`<elan-name>` The name of the ELAN that hosts the LES. This parameter is case-sensitive.

Output:

```
Client ID: 16386
 Address:
39.05.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.61.81
 Registered MAC addresses:
                00.40.0D.87.00.61

Client ID: 16387        Proxy
 Address:
39.05.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.64.02.DE.81
 Registered MAC addresses:
                None

Client ID: 16388
 Address:
39.05.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.77.81
 Registered MAC addresses:
                00.40.0D.87.00.77_
```

The `lane les clients` command displays the information described in Table 15.2.

Table 15.2 Output from the lane les clients command

Field	Description
Client ID	Displays the LEC id for each client that is registered with the LES.
Address	The ATM address of the client.
Registered MAC addresses	The MAC address of the client.
Registered Route Descriptors	If the client is a source-routing bridge then Route Descriptors are also displayed.

Display ATM Forum compliant statistics for a LES

To display the ATM Forum compliant statistics for a LES, use the `lane les stats` command.

Command: `M15-155s8:/>lane les stats <elan-name>`

Parameters: `<elan-name>` The ELAN name that hosts the LES. This parameter is case-sensitive.

Example: `M15-155s8:/>lane les stats default`

Output:

```
Number of successful Join responses 23
Number of version not supported errors 0
Number of invalid request parameters errors 0
Number of duplicate LAN destination errors 0
Number of duplicate ATM address errors 0
Number of insufficient resources to grant errors 0
Number of access denied for security reasons errors 0
Number of invalid LEC ID errors 0
Number of invalid LAN destination errors 0
Number of invalid ATM address errors 0
Number of mal formed request 0
Number of registration failures 0
Number of LE_ARP_REQUEST frames received by the LES 4498
Number of LE_ARP_REQUESTs that the LES forwarded 2
```

Enabling or disabling a LES

To enable or disable a LES, use the `lane les state` command.

Command: `M15-155s8:/>lane les state <elan-name> <param>`

Parameters: `<elan-name>` The name of the ELAN that currently hosts the LES that you wish to change or display. This parameter is case-sensitive.

`<param>` To activate the LES enter either “on” or “enable”.
To deactivate the LES enter “off” or “disable”.

Note: The above command will take immediate effect. The command must be used with care as all LECs will be thrown off the ELAN hosted by the LES.

To display the current status of a LES, specify the name of the ELAN that currently hosts the LES.

Command:

```
M15-155s8:/>lane les state <elan-name>
```

Example:

```
M15-155s8:/>lane les state default
LES ‘default’ is enabled
```

Restarting a local LES and BUS

Certain changes made to the characteristic of a LES are not immediate, for these changes to take effect you must restart the LES.

Note: When restarting a LES, all attached LECs will be thrown off the ELAN hosted by the LES, but they will rejoin the ELAN when the LES restarts, if the LEC criteria is still met. The restart command also affects the BUS functions.

To restart a local LES and BUS, use the `lane les restart` command.

Command:

```
M15-155s8:/>lane les restart <elan-name>
```

Parameters: `<elan-name>` The name of the ELAN that currently hosts the LES that you wish to restart. This parameter is case-sensitive.

Changing the ELAN name that the LES will host

You can change the name of the ELAN that is currently hosted by a LES. The new ELAN must be somewhere on the network and be known to the LECS that your LES is hosting.

To change the ELAN name that the LES will host, use the `lane les elan` command.

Command:
```
M15-155s8:/>lane les elan <old-name> <new-name>
```

Example:
```
M15-155s8:/>lane les elan marketing_eth mrk_eth
```

Parameters:

`<old-name>` The current name of the ELAN that is hosted by the LES that you want to change.
This parameter is case-sensitive.

`<new-name>` The new ELAN that is somewhere on the network and is known to the LECS that the local LES will host. This parameter is case-sensitive.

Note: The above command will take immediate effect. The command must be used with care as all LECs will be thrown off the ELAN hosted by the LES. If a LEC is configured to use the old ELAN name then it must be reconfigured manually to use the new ELAN name.

Changing the LES registration mode

Before you change the registration mode of a LES, you must be aware of the mode of the ELAN that it will be hosting and that the choice of mode is supported by the device containing the LECS.

Refer to Table 15.3 a list of compatible LES and ELAN modes that should be used.

Table 15.3 Compatible LES and ELAN modes

LES mode	LECS ELAN mode
distributed	auto
standby	auto
manual	manual

By default for the pre-defined ELANs, the LES mode is set to register automatically and the LES modes are set to distributed:

To change the registration mode of the LES, enter the `lane les mode` command.

Command:
```
M15-155s8:/>lane les mode <elan-name> {distributed | standby | manual}
```

Example:
```
M15-155s8:/>lane les mode marketing_eth standby
```

Parameters:

`<elan-name>` The name of the ELAN that currently hosts the LES that you wish to change. This parameter is case-sensitive.

`distributed` The LES will register with the LECS using the proprietary “automatic LES address determination method” and will act as a distributed LES.

`standby` The LES will register with the LECS using the proprietary “automatic LES address determination method” and will act as a “single” mode LES but support standby resilient LES.

`manual` The LES will use the ATM Forum-compliant method to manually register the LES with the LECS.

Note: For information about the proprietary “automatic LES address determination method”, see “Creating a new LES” earlier in this chapter.

Note: The above command will take immediate effect. The command must be used with care as all LECs will be thrown off the ELAN hosted by the LES.

Viewing the LES registration mode

To display the registration mode of a LES, use the `lane les mode` command.

Command:

```
M15-155s8:/>lane les mode <elan-name>
```

Example 1:

```
M15-155s8:/>lane les mode M770ElanEth
```

Output:

```
LES ‘M770ElanEth’ registers automatically
The LES can act as a standby LES
```

Example 2:

```
M15-155s8:/>lane les mode M770ElanEth
```

Output:

```
LES ‘M770ElanEth’ registers automatically
The LES can act as a distributed LES
```

Listing the peer LESes in a distributed LANE environment

A peer LES is defined as all distributed LESes hosted by the same ELAN. You can list the ATM address and LEC id range of all peer LESes that a specified distributed LES knows about.

To display a list of the peer LESes in a distributed LANE environment, use the `lane les peers` command.

Command:

```
M15-155s8:/>lane les peers <elan-name>
```

Parameters: `<elan-name>` The name of the ELAN that currently hosts the distributed LES. This parameter is case-sensitive.

Parameters:

```
M15-155s8:/>lane les peer M770ElanEth
 Peer LES ATM address   LEC ID Range
39.84.0F.80.01.BC.61.DF.00.07.80.20.00.00.00.6F.07.80.20.01 1 - 1024
39.84.0F.80.01.BC.61.DF.00.07.80.20.00.00.00.6F.07.80.70.01 1025 - 2048
```

Display ATM Forum compliant statistics for a BUS

To display the ATM Forum compliant statistics for a BUS, use the `lane les busstats` command.

Command:

```
M15-155s8:/>lane les busstats <elan-name>
```

Parameters: `<elan-name>` The ELAN name that hosts the BUS. This parameter is case-sensitive.

Example:

```
M15-155s8:/>lane les busstats default
```

Output:

```
Number of frames discarded due to resource error0
Number of octets that this BUS has received413615667
Number of unicast data frames / control frames 591906
Number of multicast frames this BUS has received 1590697
Number of frames dropped by BUS due to time out 0
Number of unsuccessful multicast send connection attempts0
Number of unsuccessful multicast forward connection attempts 0
```

LANE 2.0 Capability

To display the LANE 2.0 capability of a LES you should type the following:

Command:

```
M15-155s8:/>lane les lane2 <name>  [on|off]
```

Parameters: `<name>` The name of the ELAN which hosts the LES.

Example:

```
M15-155s8:/>lane les lane2 default
```

Output:

```
LES-BUS 'default' has LUNI 2 capability Enabled
```

The on/off parameter shall be used when the LANE 2.0 capability has to be changed.

MAX Frame Size

LANE 2.0 capable servers can work with maximum frame size of 1516 and 1580 bytes. The default configuration is 1516 bytes. Use the following command to display or change the current configuration.

Note: You must not change the maxFrameSize of the ELAN to which the mangement LEC is joined to 1580. If you do so, the LEC will not be able to join the ELAN and switch management will be lost.

Command:

```
M15-155s8:/>lane les maxframesize <elan-name> [1516|1580]
```

Parameters: `<elan-name>` The name of the ELAN hosted by the LES that you want to change.

Example:

```
M15-155s8:/>lane les maxframesize default
```

Output:

```
LES 'default' has max frame size 1516
```

Note: The LES must already be disabled when you use this command. The change only takes effect when the LES is enabled

Chapter 16

Managing an ELAN

This chapter describes how to use the command-line interface to manage an ELAN in an Avaya M770 ATM Switch.
For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

ELAN Database Maintenance

You can create and maintain an ELAN database on any switch that is hosting a resilient LECS. Switches that are hosting resilient LECSes, do not carry out any checking of database consistency. It is up to you to create and maintain the same LANE services information on all switches that could host the “active LECS”. This will ensure that a resilient LECS can smoothly take over the running of the network, should the active elected LECS fail.

Note: Until you have configured a switch hosting a resilient LECS, with the same LANE services information as the active LECS, it may be prudent to set the resilient LECS priority to zero.
This would ensure that the resilient LECS could not be elected as the “active LECS”. For more information about managing the resilient LECS, see Proprietary resilient LECS in Chapter 13, “LANE Services”.

Viewing Default ELANs

When a LEC contacts the LECS, it usually specifies the ELAN name or the ELAN type that it wants to join. The LECS in an M770 ATM Switch will enable you to define up to 64 different ELAN names. You can also define default ELANs that the LEC should join, should it only specify the ELAN type.

However, in some cases the LEC may neither specify an ELAN name nor the ELAN type that it wishes to join. For these cases, you can set a default ELAN that will be used.

The following default ELAN types can be specified in the LECS. The default settings in an M770 ATM Switch are also provided:

- Ethernet type ELAN - A default ELAN name of “default” is specified in an M770 ATM Switch M770 for this ELAN type.
- Unspecified type ELAN - A default ELAN name of “default” will be used when the LEC provides neither an ELAN name nor a specific ELAN type that it wants to join.

To list or change the ELAN names for the default ELAN names, see Specified ELAN Defaults in the LECS in Chapter 14, “Managing the LECS”.

Listing all ELANs known to the local LECS

In an M770 ATM Switch LECS, the LECS will support 64 ELANs including the pre-defined ELAN. The name “default” supports Ethernet ELANs.

If the ELAN mode has been determined by the first LES to register with the ELAN, then an asterisk (*) will be displayed.

An asterisk near the LANE2 capability parameter indicates that it was set to “auto” and the capability has been set by the first LES to register.

An asterisk near the ELAN-ID indicates that it has been calculated by the software.

To display a list of ELANs that are known to the local LECS, enter the `lane elan show` command:

Command:

```
M15-155s8:/>lane elan show
```

Output:

```
Name                        : default
Type                        : Ethernet
Security                    : Open
Max. Number of LESs         : 5
LES address formula         : Round robin
LANE2 Capable               : yes*
ELAN-ID                     : 4528*
LES Mode and Address(es)    : Distributed*
at 39.03.00.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.B8.05
at 39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.04.05
at 39.04.02.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.00.16.05
at 39.04.01.00.00.00.00.00.00.00.00.00.00.00.40.0D.87.01.23.05
```

Creating a New ELAN

You can define up to 64 ELANs that will be known to the LECS on an M770 ATM Switch.

If the LES is hosted in a device other than the M770 ATM Switch, then you must specify the ATM address where the LES will be located.

If the M770 ATM Switch will host the LES, then you should set the <LES-id> to “auto”. This will enable the LES to automatically register with the ELAN. For information about the automatic LES address determination method, see the Section “The LES and BUS in an Avaya M770 ATM Switch”, in Chapter 13, “LANE Services”.

To create a new ELAN, enter the `lane elan create` command:

Command:	`M15-155s8:/>lane elan create <newname> <les-id> ethernet`		
Example:	`M15-155s8:/>lane elan create elan1 auto ethernet`		
Parameters:	`<newname>`		The name of the new ELAN.
	`<les-id>`	`auto`	If the LES is located in an Avaya M770 then you should use “auto”.
		`ATM address`	If the LES is located in a device other than the M770 then you must specify its ATM address.

Deleting an ELAN

When you delete an ELAN, no new LECs that specify the ELAN name will be able to find it. However, the LECs currently using the deleted ELAN will be not be affected until they lose connection to the LES and try to re-connect.

You must be aware of the following changes that will be required when you delete an ELAN:

- Any LECs that specified the deleted ELAN must now be configured to use a new ELAN.
- If the deleted ELAN was a default ELAN then you should define a new default ELAN to replace the deleted ELAN.
- Any LES or LESes that hosted the deleted ELAN should be deleted, wherever the LES may be located in the network.

To delete an ELAN, enter the `lane elan delete` command:

Command:	`M15-155s8:/>lane elan delete <name>`	
Parameters:	`<name>`	The name of the ELAN to be deleted.

Note: The above change will take effect immediately.

Renaming an ELAN

You can rename an existing ELAN. The `rename` command will change the name known to the LECS. If you are renaming a default ELAN, then the M770 ATM Switch will update the default ELAN name with the new name, therefore no user configuration is required.

You must be aware of the following changes that will be required, when you rename an ELAN:

- Any LECs that specified the old ELAN name, must be configured to use the new ELAN name.

  Otherwise, when the LECs on this ELAN lose their connection with the LES they will not be able to use the renamed ELAN.
- Any LES or LESes that used the old ELAN name should be renamed to use the new ELAN name, wherever the LES may be located in the network.

To rename an ELAN, enter the `lane elan rename` command:

Command:	`M15-155s8:/>lane elan rename <oldname> <newname>`	
Parameters:	`<oldname>`	The current name of the ELAN.
	`<newname>`	The new name of the ELAN

Note: The above change will take effect immediately.

Changing the Operating Mode of an ELAN

You can change the expected operating mode of LESes on a specified ELAN. This is the method that LESes will learn the location of the specified ELAN.

If you are using a M770 LES and wish it to determine the method of registration for the ELAN then you should set the ELAN operating mode to “auto”. For more information about the different automatic LES address determination methods, see Chapter 13, “LANE Services”.

Otherwise you must supply the full ATM address of the LES that will host the specified ELAN.

To change the operating mode of LESes for a specific ELAN, use the `lane elan les` command:

Command: `M15-155s8:/>lane elan les <name> [auto | <atm-addr>]`

Example: `M15-155s8:/>lane elan les elan1 auto`

Parameters:

`<name>`	The name of the ELAN.
`auto`	Select only if an M770 LES will host the ELAN.
`<atm-addr>`	Enter the full ATM address of the LES that will host the ELAN.

Note: You can set a specific automatic registering mode for an ELAN. For more information see Changing the Automatic Registration Mode of an ELAN later in this chapter.

Changing the Automatic Registration Mode of an ELAN

You can set the automatic registration mode for an ELAN. The automatic registering modes are:

- resilient - the ELAN will adopt the resilient automatic registering mode.
- distributed - the ELAN will adopt the mode that supports distributed LANE Services.
- autosense - the ELAN will adopt the mode from the first registering LES.

For more information about the above automatic LES address determination methods, see Chapter 13, “LANE Services”.

To change the automatic registration mode of an ELAN, use the `lane elan autovers` command:

Command: `M15-155s8:/>lane elan autovers <name> <automode>`

Example:

```
M15-155s8:/>lane elan autovers accounts_elan distributed
ELAN autoregistration mode set to distributed
```

Parameters:

`<name>`	The name of the ELAN, this must be 32 characters or less.
`<automode>`	Select one of the following automatic registration modes: resilient, distributed, or autosense. If this last parameter is not entered then the automatic registering mode for the specified ELAN will be displayed.

Note: The above change does not affect the ELAN until the next time it is activated.

Note: You **must** change the ELAN automatic registration mode to distributed before using any of the commands in this Chapter which alter the way distributed ELANs are used.

Changing the Security of an ELAN

You can change the security of an ELAN. By default, all ELANs are open ELANs when they are created. This means that any LEC can request to join the open ELAN.

If an ELAN is closed then only LECs that have client mappings to the ELAN will be able to access the secure ELAN. For more information about setting up client mappings, see Managing ELAN Clients later in this chapter.

To change the security of an ELAN, enter the `lane elan security` command:

Command: `M15-155s8:/>lane elan security <name> {open |closed}`

Parameters:

`<name>`	The name of the ELAN.
`open`	Changes the security of the named ELAN to open. By default all ELANs are set to open security when created.
`closed`	Changes the security of the named ELAN to closed.

Note: The above change will take effect immediately, but will not affect the LECs that are already on the ELAN.

Managing ELAN Clients

A client is a LEC on an ELAN. You can set up ELAN client mappings:

- To enable you to map a LEC from one ELAN to another.
- To allow only the LECs that match the ELAN client mappings to join a specific secure ELAN. For more information about setting up a secure ELAN, see Changing the Security of an ELAN earlier in this chapter.

ELAN client mappings are stored in the local LECS database. These mappings tell the LECS to assign a LEC or group of LECs to a specific ELAN. In total, up to 512 mappings can be stored in the local LECS database.

An ELAN client mapping allows you to map a LEC or group of LECs to a specific secure ELAN based on one of the following:

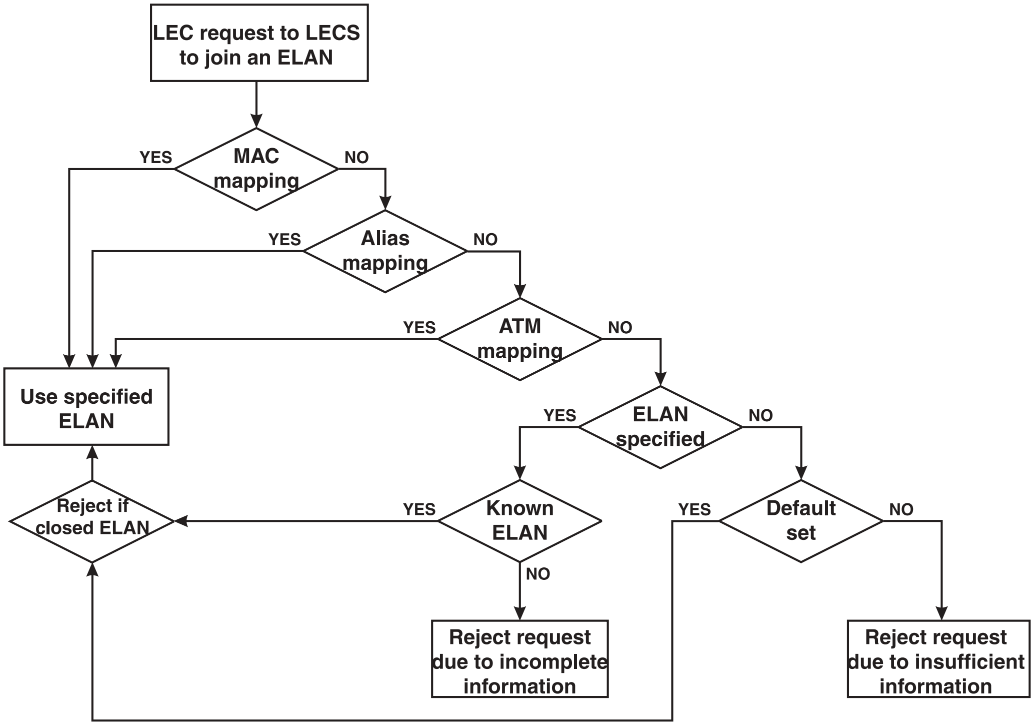
- An ATM address
- A MAC address
- An alias ELAN name. The alias is provided by the LEC in its configuration request to the LECS.

The alias ELAN mapping maps the ELAN name requested by the LEC to another ELAN. This allows the system administrator to change user ELANs at the switch.

An ATM address or an alias ELAN name mapping usually refer to a group of LECs, whereas a MAC address mapping always refers to a specific LEC. In this way you can create generic mappings instead of a separate mapping for each and every LEC.

Figure 16.1 shows how client mappings are used when a LEC sends a request to the LECS to join an ELAN.

Figure 16.1 Flowchart showing how client mapping is used



When a LEC contacts the LECS, the LECS will search its mappings database. If more than one mapping matches the LEC, the first of each mapping type is considered.

If there are still multiple matches, the order of precedence is:

- MAC mapping
- Alias mapping
- ATM mapping

If there are no matches then the ELAN name in the LEC request message is used to match to a known ELAN:

- If a matching ELAN is found and it is an open ELAN then this ELAN is used. If it is a secure (closed) ELAN the LEC request is rejected.
- If the ELAN is not known then the LEC request is rejected due to incomplete information.

Creating an ELAN client mapping

When you create a new ELAN client mapping to a specific ELAN, first you must decide whether it is a single LEC or a group of LECs that is to be mapped.

You must then decide what type of ELAN mapping to use. Possible mapping types are:

- An ATM address: the mappings refer to a specific LEC or a group of LECs.
- An alias ELAN name: the mappings refer to a specific LEC or a group of LECs.
- A MAC address: the mappings always refer to a specific LEC.

To create a new client mapping for a LEC ATM address, use the `lane elan client create atm` command:

Command:

```
M15-155s8:/>lane elan client create atm <address value> <address mask> <ELAN name>
```

Example 1:

The following example shows how to map a specific LEC to the ELAN `accounts_elan`:

```
M15-155s8:/>lane elan client create atm
39.84.0F.80.01.BC.61.DF.00.07.80.20.00.00.00.6F.07.80.20.00
FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF
accounts_elan
```

Example 2:

This example shows how to map all LECs whose addresses begin with a specific prefix to the ELAN `accounts_elan`:

```
M15-155s8:/>lane elan client create atm
39.84.0F.80.01.BC.61.DF.00.07.80.20.00 13 accounts_elan
```

Parameters:

`<address value>`	The full 20-byte ATM address.
`<address mask>`	The portion of the <address value> that needs to match the LEC's ATM address for the mapping to apply. The <address mask> is either entered as a number, (for example, 15 indicates that the first 15 bytes of the <address value> is to be masked), or you can use FF to indicate the byte of the <address value> that is to be masked and 00 to indicate the byte of the <address value> that is not masked. When using the mask as a number, note that the number of bytes entered in the address value should be limited to this number.
`<ELAN name>`	The name of the ELAN known to the LECS.

To create a new client mapping for a LEC MAC address, use the `lane elan client create mac` command:

Command: `M15-155s8:/>lane elan client create mac <MAC address> <ELAN name>`

Example: `M15-155s8:/>lane elan client create mac 00.00.F6.11.2A.3 sales_trn`

Parameters:

`<MAC address>`	The MAC address of the LEC that needs to be mapped to the specified ELAN.
`<ELAN name>`	The name of the ELAN known to the LECS.

To create a new client mapping for a LEC ELAN alias, use the `lane elan client create alias` command:

Command: `M15-155s8:/>lane elan client create alias <alias name> <ELAN name>`

Example: `M15-155s8:/>lane elan client create alias market_UK marketing_eth`

Parameters:

`<alias name>`	The name that the LEC provides in its configuration request to the LECS.
`<ELAN name>`	The name of the ELAN known to the LECS.

In this example, all LECs that request the LES address of the ELAN `market_UK` will receive the LES address of the ELAN `marketing_eth`.

Displaying ELAN Client Mappings

To display all ELAN client mappings, use the `lane elan client show` command:

Command: `M15-155s8:/>lane elan client show [atm | mac | alias]`

Parameters: If no parameter is supplied, all mappings will be listed.

`atm`	Lists only LEC ATM address to ELAN mappings.
`mac`	Lists only LEC MAC address to ELAN mappings.
`alias`	Lists only LEC alias ELAN name to ELAN mappings.

Example: `M15-155s8:/>lane elan client show`

Output:

```
Id                      ATM addressELAN name
                        ATM address mask
---------------------------------------------------------------
1 39.84.0F.80.01.BC.61.DF.00.07.80.20.00.00.00.6F.07.80.20.00

FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.00.00.00.00.00
                        accounts_elan

Id                      MAC address
2                       00.00.F6.11.2A.3

Id                      Alias ELAN name
1                       collage530default
2                       market_UKmarketing_trn
```

Deleting ELAN client mappings

To delete an ELAN client mapping, use the `lane elan client delete` command:

Command:	`M15-155s8:/>lane elan client delete <alias | atm | mac> <id>`	
Example:	`M15-155s8:/>lane elan client delete mac 2`	
Parameters:	`<alias|atm|mac>`	Select which type of client mapping is to be deleted.
	`<id>`	This is the identifier for the mapping you wish to delete. Use the `lane elan client show` command to display the identifiers for the mappings. For more information about this command, see “Displaying ELAN Client Mappings” earlier in this chapter.

Note: The above command does not affect clients that are already registered and joined to the ELAN. If you want to make sure that any deleted clients are no longer using the ELAN then you must restart the LES for the ELAN. If there are distributed LES, you must restart each one that has distributed clients. Use the `lane les restart` command. This will force all clients off the ELAN and all clients will have to re-register.

Changing the Formula for LES address that a LEC will call

This command is only valid if the specified ELAN supports distributed LANE Services. You need to change the ELAN autovers to distributed before you can change the LES address that a LEC will call.

For information about the different LES address formulas that can be selected for a distributed ELAN, see LEC Assigned for a Distributed ELAN in Chapter 13, “LANE Services“.

Note: You must manually change the ELAN autovers to distributed in order to execute the command. If the ELAN is in autosense and has learned that the registration mode is distributed (displayed as “distributed*”), this command will not be executed.

To change the formula for LES address that a LEC will call, enter the `lane elan lesaddress` command:

Command: `M15-155s8:/>lane elan lesaddress <name> <les-address-formula> [<group-address>]`

Example: `M15-155s8:/>lane elan lesaddress accounts_elan longest_match`

Parameters:		
	`<name>`	The name of the ELAN. The name must be 32 characters or less.
	`<les-address-formula>`	Select one of the following formulas that the LEC will used to locate the LES address: "group_address", "round_robin", or "longest_match".
	`<group-address>`	This parameter is only required, if a new group ATM address is being supplied. It must be a 20-byte ATM address.

Note: If only the name of the ELAN is entered then the LES address formula currently in use will be displayed for the specified ELAN.

Changing the Maximum Number of LESes in an ELAN

This command is only valid if the specified ELAN supports distributed LANE Services.

You must be aware of the following, if you change the number of distributed LESes that the ELAN supports:

- If the maximum is increased the change will take effect immediately and additional standby LES(es) will be promoted to active (if there are any).
- If the maximum is decreased the change will not affect the number of LESes currently providing LE Services, but rather will determine whether active LESes which get timed-out, get re-admitted or replaced by a standby LES.

To change the maximum number of LESes in an ELAN, enter the `lane elan maxles` command:

Command: `M15-155s8:/>lane elan maxles <name> <maxles>`

Example: `M15-155s8:/>lane elan maxles accounts_elan 5`

Parameters:

`<name>` The name of the ELAN that supports distributed LANE Services. The name must be 32 characters or less.

`<maxles>` The maximum number of LESes supported in this ELAN. The largest value allowed is 10. The default value is 5.
If this last parameter is omitted then the current maximum number of LESes will be displayed for the selected ELAN.

Note: The above change does not affect the ELAN until the next time it is activated.

LANE 2.0 Capability

The LANE 2.0 capability of an ELAN is, by default, 'auto'. Meaning that the first LES registers to this ELAN determines the capability of the ELAN.

To display and change the LANE 2.0 capability of an ELAN use the `lane elan lane2` command:

Command: `M15-155s8:/>lane elan lane2 <name>  [on|off|auto]`

Parameters: `<name>` The name of the ELAN.

Example: `M15-155s8:/>lane elan lane2 default`

Output

```
Default's LANE 2 capability configured to auto (actual on)
```

Note: If the ELAN capability was changed dramatically (e.g. from 'on' to 'off', or vice versa), the ELAN has to be restarted in order for the change to take effect. The restart of the ELAN may cause temporary disruption.

MAX Frame Size

LANE 2.0 capable servers can work with maximum frame size of 1516 and 1580 bytes. The default configuration is 1516 bytes. Use the `lane elan maxframesize` command to display or change the current configuration.

Command: `M15-155s8:/>lane elan maxframesize <elan-name> [1516|1580]`

Parameters: `<elan-name>` The name of the ELAN. It must be 32 characters or less.

Example: `M15-155s8:/>lane elan maxframesize default`

Output

```
Maximum Frame Size is 1516
```

Note: The change of the max frame size of an ELAN, does not affect the ELAN until the next time it is activated.

Chapter 17

Managing System Commands

This chapter describes how to use the command-line interface to manage the system, and terminal commands. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Using System Commands

This section describes system commands that are used to monitor or perform operations on the Avaya M770 ATM Switch.

You can carry out the following system operations:

- Download and upload microcode
- View system exceptions
- Controlled shutdown of the switch
- Take a snapshot of the current system configuration
- Reboot the switch
- View memory allocations
- View time received from time server
- Set the module to its factory defaults

Downloading over TFTP

In order to download over TFTP (Trivial File Transfer Protocol), the remote file server must be accessible from the ELAN to which the management LEC belongs or from the MSPV Ethernet Sideband port. To verify this connectivity you should ping from the file server to the IP of the LEC or to the IP of the M-SPV/M-SPX/M-SPS.

To download a software image over TFTP, use the `system download tftp` command.

Command:	`M15-155s8:/>system download tftp <ip_address> <filename> [<gateway>]`	
Example:	`M15-155s8:/>system download tftp 194.31.222.23 m770ATM`	
Parameters:	`<ip_address>`	The IP address of the remote TFTP server.
	`<filename>`	The full name of the file on the TFTP server. If the file is contained in a sub-directory, the complete path and filename must be supplied.
	`<gateway>`	The gateway through which you should perform the download: lec - through the LANE Client mspv - through the M-SPV/M-SPX/M-SPS (optional, default value: lec)

Uploading over TFTP

In order to upload over TFTP (Trivial File Transfer Protocol), the remote file server must be accessible from the ELAN to which the management LEC belongs or from the MSPV Ethernet Sideband port. To verify this connectivity you should ping from the file server to the IP of the LEC or to the IP of the MSPV.

To upload a file over TFTP, use the `system upload tftp` command.

Command:	`M15-155s8:/>system upload tftp <ip_address> <flashfile> <destination_filename> [<gateway>]`	
Example:	`M15-155s8:/>system upload tftp 194.31.222.23 m770ATM m770ATM_new`	
Parameters:	`<ip_address>`	The IP address of the remote TFTP server.
	`<flashfile>`	The full name of the file in flash memory.
	`<destination_filename>`	The full destination file name on the remote TFTP server. If the file is contained in a sub-directory, the complete path and filename must be supplied.
	`<gateway>`	The gateway through which you should perform the upload: • lec - through the LANE Client • mspv - through the M-SPV/M-SPX/M-SPS (optional, default value: lec)

Note: The main purpose of upload command is to save configuration files on a source other than the M770 ATM Switch.

Viewing a list of fatal system exceptions

A fatal system exception occurs when the CPU detects an error such as a division by zero, or accesses to non-existent memory. A fatal exception causes the M770 ATM Switch to reboot. A breakpoint is a special type of exception which is invoked by the M770 ATM Switch software when it detects an internal inconsistency.

To dump a list of fatal system exceptions, use the `system breaklog` command.

Command:

```
M15-155s8:/>system breaklog
```

Output:

```
Filename:                lmaux.c
Line No:                 553
pml_time:                1234
Abs_time:                Unknown
Stablised Count:         0
Reason:                  0000b024
epc:                     c005dce4
badva:                   c8681734
```

Note: The breaklog provides vital information for diagnosing why the M770 ATM Switch has crashed. This information needs to be reported to Avaya Technical Support.

Clearing the list of fatal system exceptions

To clear the list of fatal system exceptions, use the `system breaklog clear` command.

Command:

```
M15-155s8:/>system breaklog clear
```

Controlled shutdown of the module

This command is used for a controlled shutdown of a module, any connections that still remain on the module will be lost. A warning to this effect is displayed and confirmation is requested before the module is powered down.

To carry out a controlled shutdown of the module in preparation for a power down, use the `system halt` command.

Command:

```
M15-155s8:/>system halt
```

Output:

```
This will stop the module, losing all connections - do
you want to continue (y/n)?
```

Taking a snapshot of the current system configuration

You can take a snapshot of the current system configuration of your module to produce a backup configuration file or before you carry out a system upgrade. This file is saved into the flash directory of the switch.

To take a snapshot of the current system configuration of the switch, use the `system snapshot` command.

To re-activate the configuration file later, use the `flash config` command.

Command:

```
M15-155s8:/>system snapshot <filename>
```

Output:

```
M15-155s8:/>system snapshot snap1408.txt
Flash and NVwrites stopped...
Snapshot saved to Configuration file 'snap1408.txt'
```

Note: The snapshot command saves all the module's parameters in the same file (system wide, module specific, LANE etc).

LANE parameters only, are automatically saved in the text file *config.data*. This file may also be uploaded and downloaded and can be used to copy a LANE configuration from one module to another (in the same or another switch). After you have downloaded a new *config.data* file you need to reset the module manually using the <- -> reset pushbuttons on the module front panel in order for the information in the new *config.data* file to take effect (do not use the CLI `reboot` command because this will change the *config.data* file with its current RAM data). During the power-up process the module will use the information stored in the new *config.data* file.

Resetting the module to its factory defaults

You can return a module to its factory default by the `system default` command. This command returns all parameters to its factory defaults.

Command:

```
M15-155s8:/>system default
```

Example:

```
M15-155s8:/>system default
```

Output:

```
WARNING: This command will erase the entire module
configuration. All current parameters will be lost and
replaced by the factory defaults

NOTE: Changes will take effect only after a module reset.
Do you want to continue (Y/N)?y
```

Note: To return the entire switch to its factory defaults, type `system default` on each of the modules and afterwards perform a reset to the entire switch.

Rebooting the module or switch

It is highly recommended that you use the `system reboot` command to reboot a module in the M770 ATM Switch or the entire switch, instead of using the reset button. This is because the `system reboot` command first flushes any outstanding configuration updates to the non-volatile memory, whereas pressing the reset button may cause configuration information to be lost.

To reboot the module or switch, use the `system reboot [module|switch]` command. You will be prompted to confirm the operation.

Command:

```
M15-155s8:/>system reboot [module|switch]
```

Parameters:

`module` The module will be restarted, losing all connections to the module.

`switch` The switch will be restarted, losing all connections to the switch.

Example:

```
M15-155s8:/>system reboot module
```

Output:

```
This will restart the module, losing all connections -
do you want to continue (y/n)?
```

Note: When the M770 ATM Switch is rebooted, all connections will be lost.

Viewing the current switch memory allocation

You can view the current breakdown of memory allocation on the modules. The total amount of memory is equal to the amount of RAM memory you have in the module.

To display the current M770 ATM Switch memory allocation, use the `system memory` command.

Command:

```
M15-155s8:/>system memory
```

Output:

```
Free memory:            22000 kbytes
Total memory:           32768 kbytes
```

Viewing time received from the time server

A time server is a server that provides the date and time, (as specified by RFC 868), such as a UNIX machine running ‘timed’ to the M770 ATM Switch. For information about setting up a time server, see Viewing or Changing the IP Time Server Address in Chapter 4, “Managing Miscellaneous Commands”.

To view the current time received from the time server, use the `system time` command.

Command:

```
M15-155s8:/>system time
```

Output:

```
The time is 14:28:04 14 Aug 1998 GMT
```

Manually changing the date or time on an Avaya M770 ATM Switch

You can manually change the date or time on the switch. You do not have to enter both the date and time, only the parameter that you wish to change. Note that the date and time will be reset, when you reboot the switch.

To change the date or time on a switch, use the `system time set` command.

Command: `M15-155s8:/>system time set <date> <time>`

Example: `M15-155s8:/>system time set 08/25/98 15:22`

Parameters: `<date>` Enter the date in the form MM/DD/YY or DD MMM YYYY. Where D is the day, M is the month, and Y is the year.

`<time>` Enter the time in the form HH:MM or HH:MM:SS. Where H is the hour, M is the minute, and S the seconds.

Viewing the current time zone

A time zone is defined by the name of the time zone and the difference in hours from Greenwich Mean Time (G.M.T.).

To view the current time zone, use the `system time zone` command.

Command: `M15-155s8:/>system time zone`

Example: `Current Time Zone is EST -5`

Manually changing the time zone

You can manually change the time zone using the `system time zone` command.

Command: `M15-155s8:/>system time zone [<name> <+/- GMT>]`

Example: `M15-155s8:/>system time zone EST - 5`

Parameters: `<name>` This is the name of the time zone. You can enter up to ten characters

`<+/-GMT>` This is the time difference in hours from G.M.T.

To set the time zone back to G.M.T. use the following command:

Command: `M15-155s8:/>system time zone GMT 0`

Using Terminal Commands

These commands allow you to configure how the Avaya M770 ATM Switch displays output on the terminal.

Viewing the pager status

The pager is a facility that enables you to view the information that the M770 ATM Switch outputs to the screen, a number of lines at a time. By default, the pager is enabled.

To display the pager status, use the `terminal pager` command.

```
Command:   M15-155s8:/>terminal pager
Output:    pager is enabled
```

Enabling the pager

If the pager is enabled, the M770 ATM Switch displays output on the terminal screen, a number of lines at a time. To enable the pager, use the `terminal pager enable` command.

```
Command:   M15-155s8:/>terminal pager enable
Output:    pager enabled
```

Disabling the pager

If the pager is disabled, the M770 ATM Switch displays output on the terminal screen continuously. To disable the pager, use the `terminal pager disable` command.

```
Command:   M15-155s8:/>terminal pager disable
Output:    pager disabled
```

Viewing the number of lines

If the pager is enabled, this is the number of lines that the M770 ATM Switch will output before pausing. For more information about the pager, see Viewing the prompt later in this chapter.
By default, the number of terminal lines is set to 24.

To display the current number of lines, use the `terminal lines` command.

```
Command:   M15-155s8:/>terminal lines
Output:    terminal ines: 24 (auto-detected) or
                             (user-configured)
```

Setting the number of lines

To set the number of lines, use the `terminal lines` command.

Command: `M15-155s8:/>terminal lines <rows>`

Example: `M15-155s8:/>terminal lines 48`

Parameter: `<rows>` The number of lines to be displayed on the terminal.

Viewing the terminal width

By default, the terminal width is set to 79.

To display the current terminal width, use the `terminal width` command.

Command: `M15-155s8:/>terminal width`

Output:

```
terminal width 79 (auto-detected) or
                  (user-configured)
```

Setting the terminal width

To set the terminal width, use the `terminal width` command.

Command: `M15-155s8:/>terminal width <columns>`

Example: `M15-155s8:/>terminal width 90`

Parameter: `<columns>` The number of columns to be displayed on the terminal.

Viewing the wordwrap status

To display the wordwrap status, use the `terminal wordwrap` command.

Command: `M15-155s8:/>terminal wordwrap`

Output:

```
wordwrapping enabled or
wordwrapping disabled
```

Setting the wordwrap

To set the wordwrap, use the `wordwrap` command.

Command:

```
M15-155s8:/>terminal wordwrap [on | enable | off |
disable]
```

Example: `M15-155s8:/>terminal wordwrap enable`

Viewing the linewrap status

To display the linewrap status, use the `terminal linewrap` command.

Command: `M15-155s8:/>terminal linewrap`

Output:

```
no linewrapping
```

Setting the linewrap

To set the linewrap, use the `terminal linewrap` command.

Command: `M15-155s8:/>terminal linewrap {none | pager | terminal}`

Example: `M15-155s8:/>terminal linewrap pager`

Parameter:

- `none` The line wrapping is carried out by the terminal. The M770 ATM Switch will not try to calculate how many lines have actually been used on the terminal. In fact, it will assume that no wrapping has occurred when performing pager functions.
- `pager` When the line output by the M770 ATM Switch reaches the defined terminal length, the M770 ATM Switch will insert a line break and assume that no line wrapping is carried out by the terminal.
- `terminal` The line wrapping is carried out by the terminal. The M770 ATM Switch will keep a record of the number of lines (using the terminal width).

Viewing the prompt

To display the current system prompt, use the `terminal prompt` command.

Command: `M15-155s8:/>terminal prompt`

Output: `prompt is “M15-155s8”`

Changing the prompt

To change the system prompt, use the `terminal prompt` command.

Example: `M15-155s8:/>terminal prompt Caj770`

Output: `Caj770s8:/>`

Note: The only value that should be changed is the prefix (e.g. M770). The sX (X=current slot number) should not be written as a system prompt.

Managing Events

This chapter describes how to use the command-line interface to set and display event priority levels that occur on an Avaya M770 ATM Switch. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Assigning an Event Priority Level

All events in the Avaya M770 ATM Switch are assigned a priority level between 1 and 16, in order of severity. Examples of priority levels:

- Priority 1 is assigned to low priority events, such as setting up a Telnet connection.
- Priority 8 is assigned to informational events such as LANE services.
- Priority 15 is assigned to fatal events that do not cause the M770 ATM Switch to reboot.
- Priority 16 is assigned to fatal events that cause the M770 ATM Switch to reboot.

Note: The event log is a temporary file, and will not be saved when the M770 ATM Switch is restarted.

Displaying or setting the event logging priority level

All events in the M770 ATM Switch are assigned a priority level between 1 and 16, in order of severity. For examples of priority levels, see Assigning an Event Priority Level earlier in this chapter.

You can specify a priority level for events that will be logged. Once you have assigned a priority level, all events assigned with this priority or higher that occur will be logged in the event log file.
By default all events on the M770 ATM Switch are logged.

To display the event logging priority level, use the `event log` command.

```
Command:   M15-155s8:/>event log
Output:    All events are being logged.
```

If you change the event priority, this will not affect the existing contents of the event log.

To set the event logging priority level, use the `event log` command.

Command:	`M15-155s8:/>event log [ <number> | all | none ]`	
Parameters:	`<number>`	An event priority level is assigned, where events with the same priority or higher will be logged.
	`all`	All events will be logged. This can cause the event log to fill up quickly.
	`none`	No events will be logged.

Displaying or setting the event trap priority level

When an event occurs the switch will dispatch a trap, via SNMP, to all attached SNMP network management stations. All events in the M770 ATM Switch are assigned a priority level between 1 and 16, in order of severity. For examples of priority levels, see Assigning an Event Priority Levelearlier in this chapter.

You can specify a priority level for event traps that will be dispatched. Once you have assigned a priority level, all event traps assigned with this priority, or higher, that occur on the switch will be reported. By default, all events on the M770 ATM Switch are dispatched as traps.

To display the event trap priority level, use the `event trap` command.

Command:
```
M15-155s8:/>event trap
```
Output:
```
All events are being dispatched as traps.
```

To set the event trap priority level, use the `event trap` command.

Command:	`M15-155s8:/>event trap [ <number> | all | none ]`	
Parameters:	`<number>`	An event priority level is assigned, where events with the same priority or higher will be dispatched via SNMP traps.
	`all`	All events will be dispatched via SNMP traps.
	`none`	No events will be dispatched via SNMP traps.

Displaying logged events

You can list the 100 most recent event messages that have been logged on the Avaya M770. The most recent event is displayed first.

Note: This event log will not be saved when the M770 ATM Switch is restarted.

To display any logged events, use the `event show` command.

Command:

```
M15-155s8:/>event show
```

Output:

```
09:13:53 04 Jun 1996 GMT TELNET:console Connection accepted
09:13:53 04 Jun 1996 GMT TELNET:console Connection opened from
194.32.220.154
17:16:03 03 Jun 1996 GMT TELNET:console Connection from 194.32.220.154
closed
09:09:25 03 Jun 1996 GMT TELNET:console Connection accepted
09:09:25 03 Jun 1996 GMT TELNET:console Connection opened from
194.32.220.154
17:07:18 31 May 1996 GMT TELNET:console Connection from 194.32.220.154
closed
16:35:21 31 May 1996 GMT LES:suraya ELAN activated
11:52:10 31 May 1996 GMT TELNET:console Connection accepted
11:52:10 31 May 1996 GMT TELNET:console Connection opened from
194.32.220.154
00:00:14 01 Jan 1970 GMT LEC:joined ELAN successfully
00:00:11 01 Jan 1970 GMT LEC:failed to connect to LECS
00:00:00 01 Jan 1970 GMT LECS activated
```

Resetting logged events

You can remove all entries from the events log.

To clear logged events, use the `event clear` command.

Command:

```
M15-155s8:/>event clear
```

Chapter 19

Upgrading Avaya M770 ATM Switch Software

This chapter describes how to use the command-line interface to upgrade the software on a module. For information about how to access and use the Avaya M770 ATM Switch command-line interface, see Chapter 3, “How to Use the Command-line Interface”.

Managing Switch Software

The M770 ATM Switch is designed as a software-upgradable product. Therefore, you can expand the functionality of the switch by downloading new microcode.

The M770 ATM Switch has flash memory that contains the run-time software. To find out whether you are running the latest software release, you can view the release of the software in the flash memory. This chapter explains how to manage the run-time software that is held in flash memory, and how to upgrade/ downgrade via TFTP from the CLI. For more information on how to download or upload microcode to the M770 ATM Switch, see Chapter 17 Managing System Commands.

Viewing Software Version Information

To obtain software version information, use the `version` command.

Command:

```
M15-155s8:/>version
```

Output:

```
MAC Address                  : 00.00.F6.65.00.66
Boot ROM Version             : 1.0.0
Build Version                : 1.0.20
Build Time                   : Tue Jan 31 13:06:29 GMT 1999
Built By                     : release
Build Directory              : /release/avayaM770
Build Host                   : builder
```

Upgrading Software via TFTP from the Command Line Interface (CLI)

To download files to the ATM Module via TFTP use the procedure outlined below.

This example explains how to download version 2.0 software.

1 Before downloading a new software version, it is recommended to take a snapshot of your current module configuration. If it is needed to revert to a previous version, it is best to use the configuration that was used with that version. To take a snapshot use the `system snapshot` command.

Command:

```
M15-155s8:/>system snapshot <filename>
```

Output:

```
M15-155s8:/>system snapshot snap1408.txt
Flash and NVwrites stopped...
Snapshot saved to Configuration file 'snap1408.txt'
```

2 Before you can download software updates via TFTP from the CLI determine how many S/W Main images and Boot Loader versions are in flash memory.

To display a listing of the flash memory, use the `flash directory` command:

Command:

```
M770s8:/>flash directory
```

Output:

```
Flash Filing System contains 5 files
BOOT+       423865      m770ATMbl.2.0.3
TEXT        8611        config.data - do not delete
MAIN (C)    1005795     m770ATM.1.1.7
MAIN* (C)   1012725     m770ATM.1.2.14
CONFIG      1024        snapshot_1.1
```

The Main S/W image is of the type “MAIN,” and the * means that this image will be used on the next reboot (to see the current Main S/W version, type the command `/version`). The Boot loader image is of the type “BOOT,” and the + next to it means that this Boot loader will be used on the next reboot.

The M770 ATM module flash memory can hold a maximum of two Main S/W versions and two Boot loader versions. This means that before you can TFTP a new Main or Boot loader software version, there can only be one of that type in flash memory. To delete a file from flash memory, use the `flash delete` command and confirm the deletion.

Command:

```
M15-155s8:/>M770s8:/>flash delete <filename>
```

Example

```
M15-155s8:/>M770s8:/>flash delete m770ATM.1.2.14
```

Parameter: `<filename>` The name of the file you wish to delete from the flash directory.

3 In order to download via TFTP, the remote file server must be accessible from the ELAN to which the management LEC belongs or from the M-SPV/ M-SPX/ M-SPS Ethernet Sideband port. To verify this connectivity you should ping from the file server to the IP of the LEC or to the IP of the M-SPV/ M-SPX/ M-SPS. To download a software image over TFTP, use the `system download tftp` command.

Command:

```
M15-155s8:/>M770s8:/>system download tftp <ip_address>
<filename> [<gateway>]
```

Example:

```
M15-155s8:/>M770s8:/>system download tftp 194.31.222.23
m770ATM.2.0.16
```

Parameters:

`<ip_address>` The IP address of the remote TFTP server.

`<filename>` The full name of the file on the TFTP server.
If the file is contained in a sub-directory, the complete path and filename must be supplied.

`<gateway>` The gateway through which you should perform the download:

- lec - through the LANE Client
- mspv - through the M-SPV/ M-SPX/ M-SPS (optional, default value: lec)

4 After downloading the new software version to all ATM modules in the M770 ATM switch, reboot the switch using the `system reboot switch` command to run the new version.

Note: It is recommended that **all** modules in the M770 ATM switch use the same software version. To check which software is currently running on the ATM module, use the command version.

Downgrading the Main Software Version via TFTP from the CLI

When returning to a previous Main S/W version, it is recommended to use the configuration file that was created using the previous version. If a snapshot was not taken with the previous version, a configuration file was automatically taken for you and stored in flash after downloading and rebooting the module with the latest Main S/W version. This file is called "oldconfiguration.X.Y.Z where X.Y.Z is the Main Software version.

To return to a previous version you need to perform the following:

1 Change the main image that will be run on the next reboot by using the `flash default` command:

Command:	`M15-155s8:/>flash default <filename>`	
Example	`M15-155s8:/>flash default m770ATM.2.0.16`	
Parameter:	`<filename>`	The name of the image that the M770 ATM Switch will next run.

2 Restore the appropriate configuration file (the one that was used with the version changed in step 1 above), by typing the following:

Command:	`M15-155s8:/>/>flash config <filename>`	
Example	`M15-155s8:/>flash config oldconfiguration.1.2.14`	
Parameters:	`<filename>`	The name of the configuration file that you wish to activate

3 After changing the configuration file and main image on each of the modules in the M770 ATM switch, reboot the switch using the system reboot switch command to run the previous version.

Note: It is recommended that **all** modules in the M770 ATM switch use the same software version. To check which software is currently running on the ATM module, use the command version**.**

Note: If a new configurarion file and S/W Main Image is changed at the same time, a file called oldconfiguration.unknown will be saved in Flash memory on reboot of this module.

Managing the Flash Filing system

The following commands enable you to manage the flash memory.

Viewing the contents of the flash memory

You can view all files that are held in flash memory. A maximum of 15 files can be saved in flash memory. For each file in the directory the following information is displayed:

- The type of file.
- The size of each file in bytes.
- The name of the file.
- The default configuration file is distinguished with a “+” (plus) sign, next to the file type.
- The default boot loader image file is distinguished with a “+” (plus) sign, next to the file type.
- The default main image is distinguished with an “*” (asterisk), next to the file type.
- Any main image file that is compressed, is indicated with the letter “C”.
- Any main image file that is uncompressed, is indicated with the letter “U”.
- Also displayed are comments attached to files.

To display a listing of the flash memory bank, use the `flash directory` command.

Command:

```
M15-155s8:/>flash directory
```

Output:

```
Flash Filing System contains 6 files
BOOT+       343557       boot_loader.1.2.7
BOOT        376442       boot_loader.1.2.0
TEXT        5516         snapshot_config.1.2 - do not delete
MAIN U)     1598440      m770ATM.1.1.7
MAIN* C)    494710       m770ATM.1.2.0
CONFIG+     1024         snapshot_1.2.0
```

Note: A maximum of two main image files and two boot loader files are allowed in flash memory. A total of 15 files are allowed (including snapshot files).

Viewing the default image

The default image is the software image that will be run when the Avaya M770 boots up.

To display the default image, use the `flash default` command.

Command:

```
M15-155s8:/>flash default
```

Output:

```
The current default boot image is "m770ATM".
```

Changing the main image

To change the main image that the M770 ATM Switch will next run, use the `flash default` command.

Command:	`M15-155s8:/>flash default <filename>`	
Example	`M15-155s8:/>flash default m770ATM.1.2.0`	
Parameter:	`<filename>`	The name of the image that the M770 ATM Switch will next run.

Note: This command checks the integrity of the selected image therefore it may take a few seconds for the cursor to return.

Viewing the default boot loader image

To view the default boot loader image that the M770 ATM Switch will load, use the `flash loader` command.

Command:	`M15-155s8:/>flash loader`
Output:	`The current flash loader boot loader is “boot_loader.1.2.5”`

Changing the default boot loader image

To change the default boot loader image that the M770 ATM Switch will load, use the `flash loader` command.

Command:	`M15-155s8:/>flash loader <filename>`	
Example:	`M15-155s8:/>flash loader boot_loader.1.2.7`	
Parameter:	`<filename>`	The name of the default boot loader image that the M770 ATM Switch loads.

Note: This command checks the integrity of the selected image therefore it may take a few seconds for the cursor to return.

Activating a configuration file

You can restore an old configuration file stored in the flash directory that was generated with the `system snapshot` command.

To activate a configuration file, use the `flash config` command.

Command:	`M15-155s8:/>flash config <filename>`	
Example	`M15-155s8:/>flash config new_cfile`	
Parameters:	`<filename>`	The name of the configuration file that you wish to activate

Note: The restored configuration file will only be activated when the switch is next rebooted.

Note: After activating a new configuration file and performing a reset to the module, the module takes longer than usual to boot because it is using the new values. Because of this, when activating a configuration file that has switch-wide parameters (such as the ATM prefix or IP address) different from the current RAM settings, the module needs to be alone in the switch. If there are other modules in the switch, the module using the new config file will take longer to boot up, and another module in the switch will become the Master Agent and use the old switch-wide settings.

When the module reboots using the new configuration file, the current LANE configuration is saved in the file config.bak. If you need to restore the previous LANE configuration, you need to perform the following steps.

1. Delete the file config.data using the `flash delete` command.
2. Rename the file config.bak to config.data using the `flash rename` command.
3. Reset the module using the <- -> reset pushbuttons on the module front panel.

Deactivating an active configuration file

To deactivate an active configuration file, use the `flash config disable` command.

Command:

```
M15-155s8:/>flash config disable
```

Output:

```
No configuration file is currently active.
```

Deleting a file from the flash memory bank

To delete a file from the flash memory bank, use the `flash delete` command. You will be asked to confirm the deletion.

Command:	`M15-155s8:/>flash delete <filename>`	
Example	`M15-155s8:/>flash delete m770ATM`	
Parameter:	`<filename>`	The name of the file you wish to delete from the flash directory.

Note: Once a file is deleted it cannot be recovered. The file must be downloaded again. You must not delete the *config.data* file during normal operation, as this will reset all the LANE configuration on the module.
If you want to reset the module's LANE parameters to the factory defaults, delete or rename the *config.data* file. The module will create a new *config.data* file based on LANE factory defaults.

Renaming a file in the flash memory bank

To rename a file in the flash memory bank, use the `flash rename` command.

Command:	`M15-155s8:/>flash rename <old_name> <new_name>`	
Example	`M15-155s8:/>flash rename m770ATM fieldrelease`	
Parameters:	`<old_name>`	The current name of the flash file.
	`<new_name>`	The new name you wish to assign to the file.

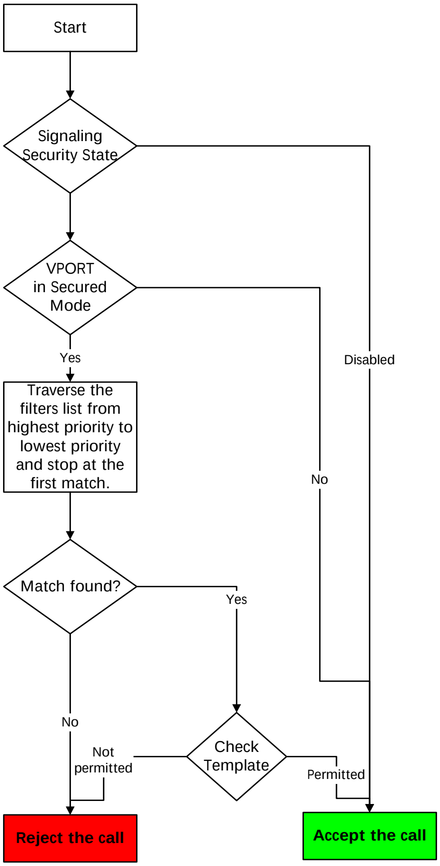
Chapter 20

Signaling Security (Access Control) Commands

This part lists and describes the CLI commands of the Avaya M770 ATM switch's Signaling Security (Access Control) feature. The purpose of the Signaling Security feature is to filter out calls during the setup phase at the signaling level. The filtering is based on the source / destination ATM addresses present in the call setup. The rules by which calls are screened are based on creating a Template that defines the addresses mask and the rule (permit / deny) and creating filters that assign templates to vports.

The calls screening procedure is as follows:

Figure 20.1 Call Screening Procedure



Note: Once signaling security is enabled, the default behavior is to reject calls.

Note: Any Signaling Security configuration also has an effect on existing calls, i.e. when setting up a security configuration, you should be aware that any existing call that would not have been accepted once the configuration is set up will be torn down.

All Signaling Security related commands are located under /vport/sig/ sigsecurity> CLI directory.

Signaling Security State

Managing Signaling Security State

The entire switch's signaling security can be set to Enabled or Disabled mode. When the switch is in the Disabled mode all configured security parameters have no effect and calls are never rejected by the Signaling Security application. The commands for managing the switch's security state are available only in the Master Agent (MA) module.

Command:
```
M15-155s8:/> vport sig sigsecurity disable
```
Command:
```
M15-155s8:/> vport sig sigsecurity enable
```

Displaying Signaling Security State

Command:
```
M15-155s8:/> vport sig sigsecurity show
```
Output:
```
Current overall signaling-security configuration
================================================

The switch security access control is Enabled.
Configured templates:
---------------------
Template name:         accept-all
Action:                permit
Source NSAP/MASK:      *
Destination NSAP/MASK: *

Template name:         reject-1
Action:                deny
Source NSAP/MASK:      39.30.20*
Destination NSAP/MASK: *

Total number of templates: 2
Configured filters:
--type q to quit or any other key to continue--
-------------------

PRIORITY | VPORT   | STATE | INCOMING TEMPLATE   | OUTGOING
TEMPLATE
==========================================================
==========
16       | 9.1.0   | ON    | accept-all          | *
16      | 9.1.0   | ON    | *                  | accept-all

Total number of filters: 2

Secured vports list:
--------------------
9.1.0
```

Signaling Security Templates

Creating a template

Signaling Security templates define rules for calls screening based on the call's source/destination addresses.

A template holds the following information:

1 Name of template - up to 20 characters template name.

2 Source NSAP/Mask - A specific NSAP address or an address mask.

3 Destination NSAP/Mask - A specific NSAP address or an address mask.

4 The rule - deny or permit.

An address mask is an expression designed to define a set of addresses. A mask expression may include two wildcards characters '*' and '?' where '*' represents any address portion (i.e. any number of nibbles) and '?' represents a single nibble (half a byte).

Example: an address mask that is designed to match an ATM host having a MAC address of 11.22.33.44.55.66 (i.e. bytes 14-19are the MAC) would have the form of: *.11.22.33.44.55.66.??, where the '*' represents the ATM prefix, and the '??' represents the Selector.

Example: an address mask that is designed to match all the hosts having an address prefix 39.03.00.00.00.00.00.00.00.00.00.00.00 would have the form of 39.03.00.00.00.00.00.00.00.00.00.00.00.*

Where the '*' represents all possible combinations for ESI + Selector.

Creating a template:

Command:

```
M15-155s8:/> vport sig sigsecurity template create <name>
[srcnsap <mask>] [dstnsap <mask>] <action>
```

Example:

```
M15-155s8:/>vport sig sigsecurity template create block-
r&d srcnsap 39.03.00.00.00.* dstnsap * deny
```

Parameters

`<name>`	name of the template
`<mask>`	source/destination address masks
`<action>`	“deny” - to reject the call “accept” - to accept the call

Displaying configured templates

Command:

```
M15-155s8:/>vport sig sigsecurity template show
```

Output:

```
Template name:         accept-all
Action:                permit
Source NSAP/MASK:      *
Destination NSAP/MASK: *


-----------------------------

Template name:         block-r&d
Action:                deny
Source NSAP/MASK:      39.03.00.00.00/*
Destination NSAP/MASK: *


-----------------------------

Template name:         reject-1
Action:                deny
Source NSAP/MASK:      39.30.20*
Destination NSAP/MASK: *
```

Displaying a specific template's information:

Command:

```
M15-155s8:/>vport sig sigsecurity template show <name>
```

Example:

```
M15-155s8:/>vport sig sigsecurity template show accept-all
```

Output:

```
Template name:         accept-all
Action:                permit
Source NSAP/MASK:      *
Destination NSAP/MASK: *

Associated filters:
-------------------
VPORT   | PRIORITY | DIRECTION | STATE
========================================
9.1.0   | 16       | Incoming  | On
9.1.0   | 16       | Outgoing  | On
```

Deleting a template

Command:

```
M15-155s8:/> vport sig sigsecurity template remove <name>
```

Example:

```
M15-155s8:/> vport sig sigsecurity template remove block-r&d
```

Signaling Security Filters

A signaling security filter is the assignment of a template to a vport for specific direction (incoming/outgoing) with a specific priority. Up to 16 filters can be created for a vport-direction coupling.

Filter priority – a number in the range 1..16 where 1 represents the highest priority and 16 the lowest.

The filters priority defines the order of the filters, i.e. if filter A has a higher priority then B, filter A will be checked prior to filter B when testing a call setup.

Direction – the direction specifies if the filter is assigned to calls incoming to the vport or outgoing from the vport.

Filter's state – A filter may be in one of two states: ON or OFF. When a filter is in the OFF state it is ignored when testing a call setup and has no effect.

Creating a filter:

Command:

```
M15-155s8:/>vport sig sigsecurity filter create <vport>
<priority> <template name> <incoming|outgoing>
```

Example:

```
M15-155s8:/>vport sig sigsecurity filter create 1.1.0 10
block-r&d incoming
```

Parameters

`<vport>`	The filter's vport
`<priority>`	The filter's priority - (1..16)
`<template name>`	The name of a configured template
`<incoming|outgoing>`	The filter's direction (applicable to incoming or outgoing calls)

Displaying configured filters

Command:

```
M15-155s8:/> vport sig sigsecurity filter show <vport>
```

Example:

```
M15-155s8:/> vport sig sigsecurity filter show 9.1.0
```

Output:

```
VPORT   | PRIORITY | STATE | INCOMING TEMPLATE   | OUTGOING
TEMPLATE
==========================================================
==========
9.1.0   | 10       | ON    | block-r&d           | *
9.1.0   | 16       | ON    | accept-all          | *
9.1.0   | 16      | ON    | *                 | accept-all
```

Filter’s state

A filter may be in one of two states: ON or OFF. When a filter is in the OFF state it is ignored when testing a call setup and has no effect.:

Command:

```
M15-155s8:/> vport sig sigsecurity filter disable <vport>
<priority> <incoming|outgoing>
or:
M15-155s8:/> vport sig sigsecurity filter enable <vport>
<priority> <incoming|outgoing>
```

Example:

```
M15-155s8:/> vport sig sigsecurity filter disable 9.1.0 10
incoming
```

Parameters

`<vport>`	The filter’s vport
`<priority>`	The filter’s priority - (1..16)
`<incoming|outgoing>`	The filter’s direction (applicable to incoming or outgoing calls)

Deleting a template

Command:

```
M15-155s8:/> vport sig sigsecurity filter remove <vport>
<priority> <incoming|outgoing>
```

Example:

```
M15-155s8:/> vport sig sigsecurity filter remove 9.1.0 10
incoming
```

Parameters

`<vport>`	The filter’s vport
`<priority>`	The filter’s priority - (1..16)
`<incoming|outgoing>`	The filter’s direction (applicable to incoming or outgoing calls)

Virtual Port's Security Mode

Virtual port's security mode

A vport can be either in a secured mode or unsecured mode. When a vport is in an unsecured mode no access control is applied to call setups passing through it. When a vport is secured every call setup passing through it is tested in terms of access control.

Setting a vport to secured mode:

Command: `M15-155s8:/> vport sig sigsecurity filter enable vport <vport>`

Example: `M15-155s8:/> vport sig sigsecurity filter enable vport 9.1.0`

Parameters `<vport>` The filter's vport

Setting a vport to unsecured mode:

Command: `M15-155s8:/> vport sig sigsecurity filter disable vport <vport>`

Example: `M15-155s8:/> vport sig sigsecurity filter disable vport 9.1.0`

Parameters `<vport>` The filter's vport

Testing vport's Security configuration by simulation

The Signaling Security feature provides a handy utility for checking the vport's security configuration by simulating call setups.

Command:

```
M15-155s8:/> :/> vport sig sigsecurity filter simulate <vport>
<incoming|outgoing> <srcnsap> <dstnsap>
```

Example:

```
M15-155s8:/> M15-155Fs9:/> vport sig sigsecurity filter
simulate 9.1.0 incoming
39.03.00.00.00.11.22.33.44.55.66.77.88.AA.BB.CC.DD.EE.FF.00
39.11.22.33.44.55.66.77.88.99.00.11.22.33.AA.AA.AA.AA.AA.00
```

Parameters

<vport>	The filter's vport
<incoming| outgoing>	The filter's direction (applicable to incoming or outgoing calls)
<srcnsap>	the simulated call setup source ATM address
<dstnsap>	the simulated call setup destination ATM address

Output:

```
Simulated call setup rejected.

Matching filter info summary:
Filter's priority:          6
Filter's template name:     block-r&d
Filter's template src mask: 39.03.00.00.00.*
Filter's template dst mask: *
Filter's template action:   deny
```

Signaling Security Event Log and Traps

The Signaling Security feature keeps track of access control violation attempts. Every time a call setup is being rejected due to access control violation an event is logged. Up to 100 most recent events are logged (i.e. if the log is full and a call is being rejected an event will be logged and the oldest event will be removed).

Note: Access control violation events are **not** saved in a non-volatile memory.

Signaling Security Traps Management

The switch can either send or not send SNMP traps to the NMS in case access control violation attempt occurs. The SNMP trap contains information about the violation attempt.

Enabling/Disabling Signaling Security related SNMP traps:

Command:

```
M15-155s8:/> vport sig sigsecurity traps enable
```

Command:

```
M15-155s8:/> vport sig sigsecurity traps disable
```

Displaying event logs

Command:

```
M15-155s8:/> vport sig sigsecurity event show
```

Output

```
vport:           9.13.0
direction:       outgoing
srcnsap:
39.02.02.00.00.00.00.00.00.00.00.00.00.00.f6.00.01.3c.82
dstnsap:
39.00.00.00.00.00.00.00.40.0d.87.00.2c.00.40.0d.87.00.2c.82
filter priority:255
template:        Base
ruletime:        08:42:02 01 Jun 2000 GMT
-------------------

vport:           9.1.0
direction:       incoming
srcnsap:
39.00.00.00.00.00.00.00.40.0d.87.00.2c.00.40.0d.64.03.ea.81
dstnsap:
39.01.01.00.00.00.00.00.00.00.00.00.00.00.40.0d.87.00.4e.86
filter priority:10
template:        block-1
time:            00:00:49 01 Jan 1970 GMT
```

Clearing the event log

Command:

```
M15-155s8:/> vport sig sigsecurity event clear
```

Chapter 21

Command Line Interface Scripts

This chapter describes how to create and to run Command Line Interface (CLI) scripts. For common information related to the CLI see Chapter 3, “How to Use the Command-line Interface”.

What CLI Scripts Are

Until version 2.1 of the Avaya M770 ATM Switch, there were several ways to access the Command-line interface of the M770 ATM Switch. These methods include:

- Direct connection via serial port of the module
- Telnet connection combined with the `access` command
- The MSP-X menu.

CLI scripts now allow yet another way to access CLI commands. A CLI script is a plain ASCII file, which contains set of almost any usual CLI commands, and may be prepared using any text editor that is capable to store its output files in ASCII-only format - Windows' Word, Notepad or WordPad, or UNIX's vi or emacs are examples of such editors. The scripts are downloaded to the M770 ATM switch using usual tftp download procedure, and run using special command (see below). During the script running, the switch executes commands consecutively as they appear in the script. Output of the commands is stored in temporary log, or, alternatively, displayed on the console terminal. The script may be run on a single module, or on multiple modules simultaneously, if started from the Master Agent module.

Structure of the CLI Script File

A CLI script consists of two parts: the Script File Header and the Command List.

The Script File Header must be located at the beginning of the file. It consists of a set of strings of pre-defined format and contents. The purpose of the Script File Header is to identify the file as a CLI Script file and to specify the Script File name in the Flash File System at the file download.

The Script File Header

The Script File Header looks like the following:

```
TYPE @M770-ASCII-FILE
NAME <file-name>
END
```

- The first string, TYPE, notifies the switch that the file is a CLI script. This string has to be the very first string in the script file.
- The second string, NAME, specifies name, which will appear as the script file's name in the M770 ATM Flash File System. The <file-name> is be a set of up to 32 printable ASCII characters, which doesn't contain white spaces. The name is case-sensitive.
- The third string, END, simply closes the Script File Header.

Any number, zero or more, of comment strings that begin with '#' in the first column of the string may be included in any place of the script file below the TYPE string. The comment strings are ignored when the script is executed.

The Script File Command List

The Script File Command List is simply a list of usual CLI commands, where each command is terminated by Carriage Return (<Enter>).

Comment strings (lines that start with the “#” character) may be inserted in any place of the Command List. They are ignored when the script is running.

Empty strings are interpreted as pressing on <Enter> key on usual CLI, i.e. moving one step towards root of the CLI tree.

Almost any command may be part of the Command List. See “CLI Scripts Restrictions” on page 265 for the list of commands not allowed in the scripts.

CLI Script File Downloading and Maintenance.

A CLI Script File may be downloaded in the same manner as any other type of file, like executable or configuration file, using system download tftp command (please refer to “Downloading over TFTP” on page 227). Note that during download the Script File Header is converted into internal representation.

After being downloaded, the Script File may be manipulated as a file of any other kind - it may be copied, deleted or uploaded.

Running a CLI Script

Running a CLI script on a single module

To run a CLI script on a single module, perform the following steps:

1 Download the script file to the file system of this module, as described above. Make sure that the download succeeded.

Note: A file download may fail due to the lack of contiguous memory in the Avaya M770 ATM switch file system or due to there being more than 15 files (the maximum allowed) in the flash memory file system.

2 You may examine contents of the script file using the `script dump` command (not mandatory but recommended). This command will just dump the script file to the console / Telnet window.

Command: `M15-155s8:/> script dump <script-file-name>`

Parameters: `<script file name>` The name of the script file in the Flash File System as it appears in the output of the `/flash dir` command.

Example: `M15-155s8:/>script dump script.txt`

3 Then actually run the script using the `script run` command

Command: `M15-155s8:/> script run <script-file-name> [log|console] [delay=<delay-value>]`

Parameters: `<script file name>` The name of the script file in the Flash File System as it appears in the output of the `/flash dir` command.

`[log|console]`	The destination of the output of the executed commands contained in the script file. If “log” specified, the output will be stored in the script log. The script log may be viewed later using “script log show” command (see below). Otherwise, if “console” specified, the script output will be redirected to that terminal, from which the script was started, i.e. serial terminal or Telnet window. If neither specified, “log” is used by default.
`[delay=<delay-value>]`	Insert delay between running of consequent commands of the script, measured in milliseconds. The <delay-value> may vary between 0-5000 ms. If is not specified, zero is used.

Example:

```
M15-155s8:/>script run script.txt console delay=100
```

Monitoring CLI Script Execution

You can monitor the progress of the script execution using the `script showprogress` command.

Command:

```
M15-155s8:/> script showprogress
```

Output:	`Script file execution progress: 11%`	If the script is still running
	`No script file execution in progress`	If the script file hasn't been run or has already finished running.

Stopping a CLI Script

You can abort a running script execution using the `script stop` command.

Note: The script will stop only when currently executed script command is finished.

Script Execution Log

When script output was directed into a log, use the `script log show` command to observe results of the script's commands running.

Command: `M15-155s8:/> script log show`

Output: If the script file execution finished, this command will print results of each command executed

If no output was produced or the log was cleared (see below), the following message will appear: `Log is empty`.

If the script execution is currently in progress, the following message will appear:

```
This command can not be accessed for the moment,
because a script file is currently running. You
can use script stop command to abort the
execution.
Execution progress: 57%
```

Note: The script execution log will be destroyed automatically if isn't accessed during 30 minutes, in order to release memory allocated for the log.

The log may also be cleared on demand. To clear the log, use the `script log clear` command.

Command: `M15-155s8:/> script log clear`

Output: `Done`

Running a CLI script on a multiple modules

It is possible to run the same command script on several or all modules of the M770 ATM switch simultaneously. Simultaneous execution of a script can significantly minimize effort needed for initial configuration of switch containing many modules.

In order to run a script on multiple modules, connect to Master Agent module via a serial terminal, Telnet or MSP-X connection:

Note: You should ensure that there is enough space in all of the modules' flash file system (see Chapter 19) **before** you download and run the script.

1 Download the script file to the Master Agent module `system download`

2 Perform the `script run` command.

On the Master Agent module the `script run` command has an additional optional parameter, which specifies the set of modules that are required to run the same script.

Command:

```
M15-155s8:/> script run <script-file-name> [log|console]
[delay=<delay-value>] [<slot-list>|all]
```

Parameters:

`<script file name>` The name of the script file in the Flash File System as it appears in the output of the `/flash dir` command.

`[log|console]` The destination of the output of the executed commands contained in the script file. If “log” specified, the output will be stored in the script log. The script log may be viewed later using “script log show” command (see below). Otherwise, if “console” specified, the script output will be redirected to that terminal, from which the script was started, i.e. serial terminal or Telnet window. If neither specified, “log” is used by default.
Note that [log|console] parameter has only local significance. On remote modules an output will always be redirected to the log.

`[delay=<delay-value>]` Insert delay between running of consequent commands of the script, measured in milliseconds. The <delay-value> may vary between 0-5000 ms. If is not specified, zero is used.

`<slot-list>` A simple list of slot numbers of modules, which are required to run the script. In case of split backplane, all the modules in the list must belong to the same switch as the Master Agent module. If “all” specified in the list of modules, all the modules of the switch are required to run the script. If nothing specified in the slot list, only local (Master Agent) module will be required to run the script.

Example:

```
M15-155s8:/>script run script.txt log delay=100 1 2 3
```

Upon receiving the `script run` command, the Master Agent validates the slots specified in the `<slot-list>` parameter. If one or more elements is invalid (for example, slot number is wrong, or specified slot is empty, or belongs to another switch, or its software version doesn't support scripts), or one or more of the specified modules are currently running another script, entire command will fail and no modules will run the script. In this case, appropriate message will be highlighted.

Remote Script Execution Status

At any time, it is possible to monitor status of the remote script execution using the `script status` command.

Command:
```
M15-155s8:/> script status
```

This command represents current status of the script execution on all the modules that are capable to run the script. Possible script running states are as follows:

Message	Meaning
`Invalid status`	The module does not support scripts
`Idle`	The module has not run the script since the last reset
`Loading script`	The module is downloading the script file from the Master Agent
`Running script`	The module is running the script
`Script running finished`	The module has successfully finished running the script
`Script running failure`	The module failed to run the script

Note: All commands in the “script” sub-menu except “run” and “status” have local significance only.

CLI Scripts Restrictions

There are a few CLI commands, which can't be run in context of script. A result of running of such commands will usually be the command failure. These commands are:

- All types of “system download” and “system upload” when the `script run` command is invoked on multiple modules
- Recursive running of the same script will most probably cause crash of the modules' software.

AppendixA

Default Settings on a New Avaya M770 ATM Switch

The factory-configured default settings for an Avaya M770 ATM Switch are shown in Table 1.

Table A.1 Default settings for an Avaya M770 ATM Switch

System default parameters	
Community password	PUBLIC
Serial/Telnet password	No password
Date	01-JAN-1970
Time	00:00:00
IP address	Will use BOOTP to obtain an IP address.
SNMP Secure mode	Disabled
IP for the management LEC	Enabled

LANE Services default parameters	
LECS location	Remote at WKA
Internal LES	Enabled
Default Ethernet ELAN	default
Default Unspecified ELAN	default The above ELAN is used when the name and type of ELAN is not given.
Ethernet LES name	default
Management LEC status	Enabled
Management LEC ELAN	Will join the “default” ELAN.
Management LEC type	Ethernet

Table A.1 Default settings for an Avaya M770 ATM Switch (Continued)

Default port configurations parameters (per port configurations)	
ILMI	Inactive
Signalling stacktype	PNNI 1.0
Signalling profile	Net
M15-155 VPI range	[0..7]
M15-155 VCI range	[32..4095]
M15-155 Signalling VPCI range	[0..7]
M3-622 VPI range	[0..15]
M3-622 VCI range	[32..4095]
M3-622 Signalling VPCI range	[0..15]

Default port configurations parameters (per module configurations)	
M15-155 VPI bits	3
M15-155 VCI bits	12
M3-622 VPI bits	4
M3-622 VCI bits	12

Default PNNI parameters	
Level	56
Node ID	Derived from ATM address
Peer Group ID	Derived from ATM address
Summary	Derived from ATM address
Admin weight	5040

Using BOOT Loader

This appendix describes the commands that are available in the BOOT Loader interface.

Start-up Process

During the normal boot-up process, the Avaya M770 ATM Switch monitors the hardware for non-critical faults. If no problems are detected then the BOOT Loader will not be activated. If a fault is detected then the BOOT Loader is enabled.

Note: The status indicators on the front panel of the Avaya M770 ATM Switch will indicate any fault that has occurred during the start-up process. For more information about the start-up test, refer to the Modules' Installation Guides.

Getting connected to the BOOT Loader

The BOOT Loader program will only be executed by the Avaya M770 ATM Switch, if one of the following occurs:

- a fault is detected during hardware self test.
- by pressing, continuously, the <– and –> buttons on the module front panel at the start of the boot-up process until the OPR LED turns OFF.

You can access the Avaya M770 BOOT Loader by direct connection on the serial interface, using a VT100 terminal or a PC running a terminal emulation program. For information about the default settings and pin-out of the serial port, see the Module Installation Guides.

When you have connected a VT100 terminal and the BOOT PROM software has been executed, the terminal screen will display the BOOT MENU.

```
Welcome to M770 - PROM 1.2.0
1 Run boot loader image 1
2 Run boot loader image 2 - current default
3 Download boot loader image (9600 baud)
4 Download boot loader image (38400 baud)

Select a menu item (1-4):
```

From the BOOT MENU, you can view the current default BOOT Loader image that is stored in flash memory. You can execute this image file or select the secondary BOOT Loader image. If the secondary image is selected then this will become the new default BOOT Loader image when the switch is next booted.

The last two options on the BOOT MENU, enable you to download a BOOT Loader image on to the M770 ATM Switch via XMODEM at either 9600 Baud or 38400 Baud.

Note: The download options should only be used in an emergency since all files and configuration on the M770 ATM Switch will be wiped.

How the BOOT Loader Command-line Interface Works

The command-line interface provides a set of commands that you can use to configure the BOOT Loader in a M770 ATM Switch. These commands are arranged in a hierarchy such that related commands are grouped together in a single functional group. A functional group can also contain one or more functional groups, and so forth. When you login to the BOOT Loader command-line interface you will be placed at the root of the hierarchy. To perform an operation using a command you will need to specify the full hierarchical path followed by the command. For example:

```
M15-155s8:/>hardware wipe
```

This command shows `hardware wipe` commands that are contained in the `hardware` functional group. Alternatively, you can descend the hierarchy by typing:

```
M15-155s8:/>hardware
```

This will cause the prompt to change, displaying the position in the hierarchy:

```
Monitor:hardware>
```

You can now perform the command simply by typing `wipe` :

```
Monitor:hardware>wipe
```

The advantage of descending the hierarchy is that you can perform multiple related commands without having to type them out in full (that is, specifying their full hierarchical path).

Table B.1 lists the commands that are used to navigate the hierarchy.

Table B.1 Navigational commands

Command	Description
top	Returns you to the root of the hierarchy.
up	Returns you to the previous level in the hierarchy.

Note: If you press the RETURN key immediately after the prompt, it has the same effect as entering the `up` command.

If you are at a particular point in the hierarchy and you need to perform a command elsewhere in the hierarchy, you must enter the slash symbol (/) followed by the full hierarchical path followed by the command. For example:

```
Monitor:hardware>/flash directory
```

This command will list all files in the flash directory while you are in the `hardware` functional group. After the command has been executed you will still be in the `hardware` functional group.

Command hierarchy

The hierarchy of the commands in the BOOT Loader command-line interface can be obtained at any time by typing `tree`

Note: Certain functional groups in the hierarchy are also commands on their own.

Conventions used to describe commands

Throughout this chapter the following conventions are used:

- All command examples are given in relation to the root of the hierarchy. That is, this is how you would enter the command if you were at the root of the hierarchy.
- The syntax of commands are described using the symbols displayed in Table 3.2, on page 24.

Using the on-line help

On-line help is always available and can be obtained at any time by typing `help` . The following information will be displayed:

- All commands and functional groups available at the current position in the hierarchy, in alphabetical order.
- The universal commands. These are commands that are independent of the hierarchy. They can be executed irrespective of where you are in the hierarchy.

The help output from the root is shown below.

Command:

```
M15-155s8:/>help
```

Output:

```
Commands:-
flash                   --- Flash management
commands
hardware                --- Hardware commands
system                  --- System wide commands
terminal                --- Terminal settings
version                 --- Display build version
number

Universal commands:-
exit, help, retstatus, top, up
```

Help is also available for individual commands. To obtain help on a command, type `help` followed immediately by the full command. As an example, the help output for the `system download xmodem` command is:

Command:

```
M15-155s8:/>help system download xmodem
```

Output:

```
Syntax:   download xmodem <baud_rate>
          valid baud rates are [4800|9600|19200|38400]
          baud rate defaults to 9600
```

Note: If there is a discrepancy between the information in the on-line help and the information in this manual, always follow the advice in the on-line help, as it is the most current information available.

Managing the Flash Filing system

The following commands enable you to manage the flash memory bank.

Contents of the flash memory

You can view all files that are held in flash memory. For each file in the directory the following information is displayed:

- The type of file.
- The size of each file in bytes.
- The name of the file.
- The default configuration file is distinguished with a “+” (plus) sign, next to the file type.
- The default boot loader image file is distinguished with a “+” (plus) sign, next to the file type.
- The default main image is distinguished with an “*” (asterisk), next to the file type.
- Any main image file that is compressed, is indicated with the letter “C”.
- Any main image file that is uncompressed, is indicated with the letter “U”.
- Also displayed are comments attached to files.

To display a listing of the flash memory bank, use the `flash directory` command.

Command:

```
M15-155s8:/>flash directory
```

Output:

```
Flash Filing System contains 6 files
BOOT+     343557    boot_loader.1.2.7
BOOT      376442    boot_loader.1.2.0
TEXT      5516      snapshot_config.1.2 - do not delete
MAIN(U)   1598440   m770ATM
MAIN*(C)  494710    m770ATM_new
CONFIG+   1024      snapshot_1.2.0
```

Viewing the default image

The default image is the software image that will be run when the M770 ATM Switch boots up. To display the default image, use the `flash default` command.

Command:

```
M15-155s8:/>flash default
```

Output:

```
The current default boot image is "m770ATM_new".
```

Changing the main image

To change the main image that the M770 ATM Switch will next run, use the `flash default` command.

Command:	`M15-155s8:/>flash default <filename>`	
Example	`M15-155s8:/>flash default m770ATM_new`	
Parameter:	`<filename>`	The name of the image that the M770 ATM Switch will next run.

Note: This command checks the integrity of the selected image therefore it may take a few seconds for the cursor to return.

Viewing the default boot loader image

To view the default boot loader image that the M770 ATM Switch will load, use the `flash loader` command.

Command:

```
M15-155s8:/>flash loader
```

Output:

```
The current flash loader boot loader is
“boot_loader.1.2.5”
```

Changing the default boot loader image

To change the default boot loader image that the M770 ATM Switch will load, use the `flash loader` command.

Command:	`M15-155s8:/>flash loader <filename>`	
Example:	`M15-155s8:/>flash loader boot_loader.1.2.7`	
Parameter:	`<filename>`	The name of the default boot loader image that the M770 ATM Switch load.

Note: This command checks the integrity of the selected image therefore it may take a few seconds for the cursor to return.

Activating a configuration file

You can restore an old configuration file stored in the flash directory that was generated with the `system snapshot` command.

To activate a configuration file, use the `flash config` command.

Command:	`M15-155s8:/>flash config <filename>`	
Example	`M15-155s8:/>flash config new_cfile`	
Parameters:	`<filename>`	The name of the configuration file that you wish to activate

Note: The restored configuration file will only be activated when the switch is next rebooted.

Deactivating an active configuration file

To deactivate an active configuration file, use the `flash config disable` command.

Command:	`M15-155s8:/>flash config disable`
Output:	`Active configuration file has been disabled.`

Deleting a file from the flash memory bank

To delete a file from the flash memory bank, use the `flash delete` command. You will be asked to confirm the deletion.

Command:	`M15-155s8:/>flash delete <filename>`	
Example	`M15-155s8:/>flash delete m770ATM`	
Parameter:	`<filename>`	The name of the file you wish to delete from the flash directory.

Note: Once a file is deleted it cannot be recovered. The file must be downloaded again.
You must not delete the *config.data* file without consulting Avaya Technical Support.

Renaming a file in the flash memory bank

To rename a file in the flash memory bank, use the `flash rename` command.

Command: `M15-155s8:/>flash rename <old_name> <new_name>`

Example `M15-155s8:/>flash rename Avaya M770.1.2.0 fieldrelease`

Parameters:

`<old_name>`	The current name of the flash file.
`<new_name>`	The new name you wish to assign to the file.

Hardware Commands

This section describes hardware commands that are available in the BOOT Loader.

Wiping flash and eerom memory in an Avaya M770 ATM Switch

To wipe non-volatile memory in an Avaya M770, use the `hardware wipe` command.

Command:

```
M15-155s8:/>hardware wipe [eerom | flash | all]
```

Parameters

`eerom`	Wipes the eerom memory. This will clear all configuration information that has been setup in the switch.
`flash`	Wipes the flash memory. This will erase all the image files from flash memory.
`all`	Wipes both the eerom and flash memory.

Note: Use this command with care, you cannot reverse the operation and the effect is immediate.

Note: You must download a boot loader and main image if you wipe flash memory before you reset the switch.

Setting/Displaying the speed for the serial port

To display the current speed for the serial interface port, use the `hardware serial speed` command.

Command:

```
M15-155s8:/>hardware serial speed
```

Output:

```
M15-155s8:/>9600
```

To set up the speed for the serial interface port, use the `hardware serial speed` command and type the desired speed after the command as shown:

Command:

```
M15-155s8:/>hardware serial
speed [4800|9600|19200|38400]
```

Example:

```
M15-155s8:/>hardware serial speed  9600
```

Parameters:

`[4800	38400]`	Select the speed at which the serial interface port will communicate.

System-wide Commands

This section describes system commands that are available in the BOOT Loader.

Viewing the invariant information in BOOT Loader

Invariant information is shared between the BOOT PROM image, the BOOT Loader image and the main image. This is common information in all the image files.

To view invariant information, use the `system invariant` command.

Command:

```
M15-155s8:/>system invariant
```

Output:

```
Software is running in 1.1+ mode
Serial Number is set to:....
BIA is set to :0000f6123456
Loader 1 : start OX12345678, length 345841
Loader 2 : start OXb2615678, length 345841
Selected boot image: 2
Done!
```

`Software is running`	Indicates the software image that is currently running on the switch.
`BIA is set to`	The BIA of the switch.
`Loader is started`	The BOOT Loader start address (in hexadecimals) and the length of the BOOT Loader file.
`Selected boot image`	The BOOT Loader image that has been selected.

Viewing a list of fatal system exceptions

A fatal system exception occurs when the Central Processing Unit (CPU) detects an error such as a division by zero, or accesses to non-existent memory. A fatal exception causes the M770 ATM Switch to reboot. A breakpoint is a special type of exception which is invoked by the M770 ATM Switch software when it detects an internal inconsistency.

To dump a list of fatal system exceptions, use the `system breaklog` command.

Command:

```
M15-155s8:/>system breaklog
```

Output:

```
Filename:                lmaux.c
Line No:                 553
pml_time:                1234
Abs_time:                Unknown
Stablised Count:         0
Reason:                  0000b024
epc:                     c005dce4
badva:                   c8681734
```

Note: The breaklog provides vital information for diagnosing why the M770 ATM Switch has crashed. This information needs to be reported to Avaya Technical Support.

Clearing the list of fatal system exceptions

To clear the list of fatal system exceptions, use the `system breaklog clear` command.

Command:

```
M15-155s8:/>system breaklog clear
```

Running all the hardware tests

You can run all the non-critical hardware tests on a M770 ATM Switch. If all the tests pass the M770 ATM Switch will respond with DONE!

If a test fails, then the BOOT Loader will display the test that has the failed and the M770 ATM Switch LEDs will display the sequence that represents the error. For more information about the LED status sequence, see the Module Installation Guides.

To run all hardware tests, use the `system test` command.

Command:

```
M15-155s8:/>system test
```

Output example when all tests pass:

```
Done!
```

Output example when there is a failure:

```
The boot loader SELF-TEST failed
```

Downloading over XMODEM

Download from XMODEM will provide some protocol checks during transfer, whereas the serial download provides no check on the data transfer.

The following sequence shows you how to download a software image over XMODEM.

1 Connect the serial cable to the serial interface port. For more information about the default settings and pin-out of the serial port, see the Modules' Installation Guides.

2 Enter the `system download xmodem` command:

Command:	`M15-155s8:/>system download xmodem`
Example:	`M15-155s8:/>system download xmodem`

After you press ENTER, the M770 ATM Switch will wait for data on the selected serial interface port and transmission baud rate will default to 9600.

3 Start the transmission on the serial link.

Note: Set up of new calls has priority over the XMODEM download, so on a busy network it may be necessary to disconnect the M770 ATM Switch from the network in order to achieve a successful download via the bootloader.

Downloading over serial interface

You can only download a software image over the serial interface.

To download over serial interface, use the following steps:

1 Connect the cable to the serial interface port to download the software image.

2 Enter the `system download serial` command:

Command:	`M15-155s8:/>system download serial <baud_rate>`	
Example:	`M15-155s8:/>system download serial 9600`	
Parameter:	`<baud_rate>`	The default baud rate is 9600. The highest baud rate that is supported is 38400.

After you press ENTER, the M770 ATM Switch will wait for data on the serial interface.

3 Start the transmission on the serial link.

Downloading over tftp

In order to download over TFTP (Trivial File Transfer Protocol), the remote file server must be accessible from the MSPV Ethernet Sideband port. To verify this connectivity you should ping from the file server to the IP of the MSPV.

To download a software image over TFTP, use the `system download tftp` command.

Command:	`M15-155s8:/>system download tftp <ip_address> <filename> [<gateway>]`	
Example:	`M15-155s8:/>system download tftp 194.31.222.23 m770ATM`	
Parameters:	`<ip_address>`	The IP address of the remote TFTP server.
	`<filename>`	The full name of the file on the TFTP server. If the file is contained in a sub-directory, the complete path and filename must be supplied.
	`<gateway>`	You should perform the download using the MSPV/MSPX gateway (optional field).

Uploading over XMODEM

The following sequence shows you how to upload a file over XMODEM.

1 Connect the serial cable to the serial interface port. For more information about the default settings and pin-out of the serial port, refer to the Module Installation Guides.

2 Enter the `system upload xmodem` command:

Command:	`M15-155s8:/>system upload xmodem <file> <baud_rate>`	
Example:	`M15-155s8:/>system upload xmodem test 9600`	
Parameters:	`<file>`	Enter the name of the file in flash memory that is to be uploaded.
	`<baud_rate>`	The default baud rate is 9600. The higher rate is not recommended but can be set to 38400.

3 Start the receiver on the serial link.

4 Press ENTER, the M770 ATM Switch will send data on the selected serial interface port.

Note: Set up of new calls has priority over the XMODEM upload, so on a busy network it may be necessary to disconnect the M770 ATM Switch from the network in order to achieve a successful upload via the bootloader.

Uploading over tftp

In order to upload over TFTP (Trivial File Transfer Protocol), the remote file server must be accessible from the MSPV / MSPX Ethernet Sideband port. To verify this connectivity you should ping from the file server to the IP of the MSPV / MSPX.

To upload a file over TFTP, use the `system upload tftp` command.

Command:

```
M15-155s8:/>system upload tftp <ip_address> <flashfile>
<destination_filename> [<gateway>]
```

Example:

```
M15-155s8:/>system upload tftp 194.31.222.23 m770ATM m770ATM_new
```

Parameters:

`<ip_address>`	The IP address of the remote TFTP server.
`<flashfile>`	The full name of the file in flash memory.
`<destination_filename>`	The full destination file name on the remote TFTP server. If the file is contained in a sub-directory, the complete path and filename must be supplied.

Note: The main purpose of upload command is to save configuration files on a source other than the M770 ATM Switch.

Rebooting the switch

It is highly recommended that you use the `system reboot` command to reboot the Avaya M770 instead of using the reset button. This is because the `system reboot` command first flushes any outstanding configuration updates to the non-volatile memory, whereas pressing the reset button may cause configuration information to be lost.

To reboot the switch, use the `system reboot` command. You will be prompted to confirm the operation.

Command:

```
M15-155s8:/>system reboot
```

Note: When the M770 ATM Switch is rebooted, all connections to the switch will be lost.

Controlled shutdown of the switch

This command is used for a controlled shutdown of a module, any connections that still remain on that module will be lost. A warning to this effect is displayed and confirmation is requested before the module is powered down.

To carry out a controlled shutdown of the switch in preparation for a power down, use the `system halt` command.

Command:

```
M15-155s8:/>system halt
```

Output:

```
This will stop the module, losing all
connections - do you want to continue (y/n)?
```

Note: This command should be carried out before the M770 ATM Switch has its power disconnected.

Terminal Commands

These commands allow you to configure how the BOOT Loader in a M770 ATM Switch displays output on the terminal.

Viewing the number of lines

If the pager is enabled, this is the number of lines that a M770 ATM Switch will output before pausing. For more information about the pager, see Viewing the pager status later in this chapter.

To display the current number of lines, use the `terminal lines` command.

Command:	`M15-155s8:/>terminal lines`
Output:	`lines: 24`

Setting the number of lines

To set the number of lines, use the `terminal lines` command.

Command:	`M15-155s8:/>terminal lines <rows>`	
Example:	`M15-155s8:/>terminal lines 48`	
Parameter:	`<rows>`	The number of lines to be displayed on the terminal.

Viewing the terminal width

To display the current terminal width, use the `terminal width` command.

Command:	`M15-155s8:/>terminal width`
Output:	`terminal width 79`

Setting the terminal width

To set the terminal width, use the `terminal width` command.

Command:	`M15-155s8:/>terminal width <columns>`	
Example:	`M15-155s8:/>terminal width 90`	
Parameter:	`<columns>`	The number of columns to be displayed on the terminal.

Viewing the wordwrap status

To display the wordwrap status, use the `terminal wordwrap` command.

Command:	`M15-155s8:/>terminal wordwrap`
Output:	`no wordwrapping`

Setting the wordwrap

To set the wordwrap, use the `wordwrap` command.

Command: `M15-155s8:/>terminal wordwrap [on | enable | off | disable]`

Example: `M15-155s8:/>terminal wordwrap enable`

Viewing the linewrap status

For more information about the different linewrap settings, see Setting the linewrap later in this chapter.

To display the linewrap status, use the `terminal linewrap` command.

Command: `M15-155s8:/>terminal linewrap`

Output: `no linewrapping`

Setting the linewrap

To set the linewrap, use the `terminal linewrap` command.

Command: `M15-155s8:/>terminal linewrap {none | pager | terminal}`

Example: `M15-155s8:/>terminal linewrap pager`

Parameters:

`none` Line wrapping is carried out by the terminal.
The M770 ATM Switch will not try to calculate how many lines have actually been used on the terminal. In fact, it will assume that no wrapping has occurred when performing pager functions.

`pager` When the line output by the M770 ATM Switch reaches the defined terminal length, the M770 ATM Switch will insert a line break and assume that no line wrapping is carried out by the terminal.

`terminal` Line wrapping is carried out by the terminal.
The M770 ATM Switch will keep a record of the number of lines (using the terminal width).

Viewing the pager status

To display the pager status, use the `terminal pager` command.

Command: `M15-155s8:/>terminal pager`

Output: `pager is enabled`

Enabling the pager

To enable the pager, use the `terminal pager enable` command.

Command: `M15-155s8:/>terminal pager enable`

Output: `pager enabled`

Disabling the pager

To disable the pager, use the `terminal pager disable` command.

Command: `M15-155s8:/>terminal pager disable`

Output: `pager disabled`

Viewing the prompt

To display the current system prompt, use the `terminal prompt` command.

Command: `M15-155s8:/>terminal prompt`

Output: `prompt is “Monitor”`

Changing the prompt

To change the system prompt, use the `terminal prompt` command.

Command: `M15-155s8:/>terminal prompt Monitor_M770`

Output: `Monitor_M770:/>`

Note: The Boot Loader prompt is not saved when changed. The next time the loader is run the prompt will revert to the default setting of “Monitor”.

Viewing Software Version Information

You can list information about the BOOT PROM and the BOOT Loader images that have been loaded on the M770 ATM Switch.

To view the software version information, use the `version` command.

Command:

```
M15-155s8:/>version
```

Output:

```
Avaya M770 ATM Switch Version Information

MAC Address       :      00.40.0C.87.00.0E
Boot ROM Version  :      1.1.2
Software Version  :      2.0.18
Build Time        :      Sun Dec 26 21:13:21 IST 1999
Built By          :      release
Build Directory   :      /home0/users/release/
Build Host        :      linalpha1
```

Creating PVCs

This appendix describes the procedure for creating PVCs on Avaya M770 ATM Modules.

Creating P2P

PVCs are virtual circuits that are set up through manual configuration rather than through UNI signaling between the ATM endpoints as is done for the switched virtual circuits (SVCs).

There are three steps in creating a P2P PVC on the M770 ATM switch:

1 Create the Traffic Descriptor (TD) that will be used for the PVC

2 Limit the Signaling SVC range on the vport

3 Create the P2P PVC.

The next three subsections explain how to setup a PVC on the M770 ATM switch. In this example, a P2P PVC will be setup on the M770 between ports 1.1 and 1.2 using VPI 0/ VCI 115.

The M770 ATM switch uses the following system to describe a VC. The number, “1.2.0.115:” indicates that there is a VC on slot 1, port 2 using VPI 0 and VCI 115.

Creating a Traffic Descriptor

A Traffic Descriptor must be defined with the service class that will be used to transport the traffic and the bandwidth that is required. The example below shows a cell rate of 4152 cells per second, appropriate for a DS1 (24 DS0s times 173 cps)

Command:M770s1:/>td setup CBR <td_id> pcr0+1=<pcr0+1> [pcr0=<pcr0>]

Example:M770s1:/> td setup CBR 5 pcr0+1=4152

To determine which td_id is available, type `td` show to display all defined Traffic Descriptors.

Limiting the Signaling SVC range for the virtual port

Before a VCI may be used for a PVC, the signaling SVC range on that vport must be limited to prevent this VCI from being used by an SVC. In this example, we are using the VCIs 114 and 115, so we will limit the signaling SVC range to VCI 100.

Command:

```
M15-155s8:/>vport set vcirange <vport id> <range>
```

Example:

```
M15-155s8:/>vport disable 1.1.0
M15-155s8:/>>vport disable 1.2.0
M15-155s8:/>>vport set vcirange 1.1.0 [32..100]
M15-155s8:/>vport set vcirange 1.2.0 [32..100]
M15-155s8:/>vport enable 1.1.0
M15-155s8:/>vport enable 1.2.0
```

Before the vport parameter may be set, it must be disabled as shown in the example.

Creating the P2P PVC

In this example, we are using td (traffic descriptor) 5 which was defined in the steps above..

Command:

```
M15-155s8:/>pvc setup pp <vci1index> <vci2index> [<td1> [
<td2>]]
```

Example:

```
M15-155s8:/>pvc setup pp 1.1.0.114 1.2.0.115 5 5
```

Parameters

`<vci1index>` The first VCL for the PVC connection in the format <slot.port number.vpi.vci

`<vci2index>` The second VCL for the PVC connection in the format <slot.port number.vpi.vci>

`<td1>` This refers to the transmit traffic descriptor of the first VCL and the receive traffic descriptor of the second VCL on the PVC connection.

`<td2>` This refers to the receive traffic descriptor of the first VCL and the transmit descriptor of the second VCL on the PVC connection.
Note:if td2 is omitted then it defaults to the same as td1

If the PVC is from one module to another, the PVC setup must be performed on both modules.

Creating P2MP PVCs

There are four steps in creating a P2MP PVC on the M770 ATM switch:

1 Create the Traffic Descriptor (TD) that will be used for the PVC

2 Set the Trunk ID range for the module

3 Limit the Signaling SVC range on the vport(s)

4 Create the P2MP PVC.

The next four subsections explain how to setup a P2MP PVC on the M770 ATM switch. In this example, a P2MP PVC will be setup on the M770 between ports 1.1, 2.1 and 3.1 using trunk ID 150 and VPI 0/ VCI 115.

The M770 ATM switch uses the following system to describe a VC. The number, "1.2.0.115:" indicates that there is a VC on slot 1, port 2 using VPI 0 and VCI 115.

Creating a Traffic Descriptor

A Traffic Descriptor must be defined with the service class that will be used to transport the traffic and the bandwidth that is required. The example below shows a cell rate of 4152 cells per second, appropriate for a DS1 (24 DS0s times 173 cps)

Command:	`M15-155s8:/>td setup CBR <td_id> pcr0+1=<pcr0+1> [pcr0=<pcr0>]`
Example:	`M15-155s8:/>td setup CBR 5 pcr0+1=4152`

To determine which td_id is available, type `td` show to display all defined Traffic Descriptors.

Setting the Trunk ID range for the module

Each P2MP PVC has a manually-assigned Trunk ID. The Trunk ID is used as a unique identifier for the P2MP call on both the ingress module (on which the root of the call is connected), and on the egress modules (on which the leaves of the call are connected). The Trunk ID values that are allowed for use by the P2MP call must be defined on the module. The following example configures the Trunk ID Range for the module from 0 to 200.

Command:	`M15-155s8:/>hardware trunkidrange <maxTrunkId> | disable`	
Example:	`M15-155s8:/>hardware trunkidrange 200`	
Parameters	`<maxTrunkId>`	Maximum trunk ID for P2MP PVCs on all ports of the module

Limiting the Signaling SVC range for the virtual port

Before a VCI may be used for a PVC, the signaling SVC range on that vport must be limited to prevent this VCI from being used by an SVC. In this example, we are using the VCIs 114 and 115, so we will limit the signaling SVC range to VCI 100

Command:	`M15-155s8:/>vport set vcirange <vport id> <range>`
Example:	

Module 1

```
M15-155s8:/>vport disable 1.1.0
M15-155s8:/>vport set vcirange 1.1.0 [32..100
M15-155s8:/>vport enable 1.1.0
```

Module 2

```
M770s2:/>vport disable 2.1.0
M770s2:/>vport set vcirange 2.1.0 [32..100]
M770s2:/>vport enable 2.1.0
```

Module 3

```
M770s3:/>vport disable 3.1.0
M770s3:/>vport set vcirange 3.1.0 [32..100]
M770s3:/>vport enable 3.1.0
```

Before the vport parameter may be set, it must be disabled as shown in the example.

Creating the P2MP PVC

In this example, we are using td (traffic descriptor) 5 and Trunk ID 150 which was defined in the steps above. We are setting up a P2MP PVC from 1.1.0.114 to 2.1.0.115 and 3.1.0.115

Command:

```
M15-155s8:/>pvc setup pmp <vci1index> <vci2index>...<vciNindex>…
<trunkId> [<fwd td>]
```

Example:

```
M15-155s8:/>hardware trunkidrange 200
```

Module 1

```
M15-155s1:/>pvc setup pmp 1.1.0.114
2.1.0.115  3.1.0.115  1.150  5
```

Module 2

```
M15-155s2:/>pvc setup pmp 1.1.0.114
2.1.0.115  1.150  5
```

Module 3

```
M15-155s3s1:/>pvc setup pmp 1.1.0.114
3.1.0.115  1.150  5
```

Parameters

`<vci1index>`	The first VCL for the PVC connection in the format <slot.port number.vpi.vci>.
`<vci2index>...<vciNindex>`	The branch VCLs (until the Nth branch) for the PMP PVC connection in the format <slot.port.vpi.vci>
`<trunkId>`	The identifier of the P2MP call. It must be the same on both the root module and the branch module. The format is <slot>.<index> where the slot is the slot of the root port and the range of trunk IDs are determined by the module that holds the root.
`<fwd td.`	Index of the traffic descriptor for the forwarding direction (rx for the root VCL, and tx for the branch VCLs).

If the P2MP PVC is from one module to another, the PVC setup must be performed on both modules. The order of the VCLs should NOT switch places. The root VCL comes first, and the branch VCLs come second.

AppendixD

Creating PVPs

This appendix describes the procedure for creating PVPs on Avaya M770 ATM Modules.

Creating PVPs

What do you do when you want all VCs from a particular VPI to be switched from one endpoint to another? You would define a Permanent Virtual Path (PVP). When a PVP is configured, the cell is switched using only its VPI - the VCI is ignored. The VPI on the ingress port can be the same or different than the VPI on the egress port. This section contains examples on defining PVPs. The following 2 examples show in detail how to define PVPs between ports on the same module and between ports on different modules in the ATM switch.

Example 1

Define a PVP that takes all VCs coming in on slot 1 port 1 for VPI 6 and switch them to slot 1 port 2 VPI 7.

Example 2

Define a PVP that takes all VCs coming in on slot 1 port 1 for VPI 6 and switch them to slot 3 port 2 VPI 7.

There are four steps in creating a PVP on the M770 ATM switch:

1 Define the VPI range that is used for VP switching

2 Define the VPI range to be used for Signalled VPs. The rest are used for Permanent VPs

3 Create the Traffic Descriptor (TD) that will be used for the PVP

4 Create the PVP.

Before you get started, there is an additional command/feature in the M770 ATM switch to help you configure PVPs. This is the ability to change the maximum number of VPIs on the module. For example, the default configuration for the M15-155 is 3 bits for the VPI range and 12 bits for the VCI range. This gives you a total of 8 VPIs (23) to play with. If more VPIs are needed, you can “steal” them from the VCI range. By using the command hardware vpivcirange, you can allocate up to 6 bits for the VPI range (26 or 64 VPIs). For more information on changing the VPI and VCI bit range, please see section "“Managing the number of VPI and VCI bits” on page 98.

For our examples, it is assumed that the module is an M15-155 and its VPI and VCI bits are set to 3 and 12 accordingly.

The next three subsections explain how to setup a PVP on the M770 ATM switch.

Define a VPI range for VP switching

By default, all VPIs on a module are used for VC switching and VP switching is disabled. The following command defines the range of VPIs that will be used for Virtual Path (VP) switching for all ports on the module. The command must be executed on all modules that will perform VP switching. For our examples, we need to configure the VPI range 5 - 7 for VP switching .

Command:	`M15-155s1:/>hardware vpcvpirange <minVpcVpi>`	
Example 1:	*Module 1*	`M15-155s1:/>hardware vpcvpirange 5`
Example 2	*Module 1*	`M15-155s1:/>hardware vpcvpirange 5`
	Module 2	`M15-155s2:/>hardware vpcvpirange 5`
Parameters	`<minVpcVpi>`	Minimum number for Vpc Vpi for all ports on the module. Maximum Vpc Vpi is set to maximum Vpi according to vpivcibits set in the command "hardware vpivcibits"

Note: You must reset each module in order for the change to take place.

After resetting the module, you can verify that the VPIs have been reserved for VP switching by typing in the command, `vport show vpivciranges`.

Define the VPI range to be used for Signaled VPs

In step 1, all of the VPIs reserved for VPs are automatically reserved for Signaled VPs. Before a VPI may be used for a PVP, the signaling VP range on that vport must be limited to prevent this VPI from being used by a Signaled VP.

There are some rules to remember in defining the range for Signaled VPs:

1 At least one of the VPIs defined in Step 1 MUST be reserved for Signaling VPs.

2 In defining the range for Signaled VPs, the lower bound MUST be the minimum VPI defined in the Step 1.

In this example, we are using VPIs 6 and 7, so we will limit the signaling VPIs to just VPI 5. This meets the criteria defined above.

Command:	`M15-155s1:/>vp set sigvpcvpirange <root vport id> [<range>]`	

Example 1:	*Module 1*	`M15-155s1:/>vport disable 1.1.0`
		`M15-155s1:/>vport disable 1.2.0`
		`M15-155s1:/>vport set sigvpcvpirange 1.1.0 [5..5]`
		`M15-155s1:/>vport set sigvpcvpirange 1.2.0 [5..5]`
		`M15-155s1:/>vport enable 1.1.0`
		`M15-155s1:/>vport enable 1.2.0`

Example 2	*Module 1*	`M15-155s1:/>vport disable 1.1.0`
		`M15-155s1:/>vp set sigvpcvpirange 1.1.0   [5..5]`
		`M15-155s1:/>vport enable 1.1.0`

	Module 3	`M15-155s3:/>vport disable 3.2.0`
		`M15-155s3:/>vp set sigvpcvpirange 3.2.0   [5..5]`
		`M15-155s3:/>vport enable 3.2.0`

Parameters	`<root vport id>`	Virtual port identifier in the form<slot>.<port>.0
	`<range>`	in the form: [<lower bound>..<upper bound>] <lower bound> must be the minimum VPI number for VP switching as defined by "hardware vpcvpirange"

Note: A previously defined PVP on a vport will be disabled if you type in the command `vport set sigvpcvpirange`. In order to re-enable the PVPs, use the `pvp enable command`.

Note: Before the vport parameter may be set, it must be disabled as shown in the above examples.

Creating a Traffic Descriptor

A Traffic Descriptor must be defined with the service class that will be used to transport the traffic and the bandwidth that is required. The example below defines a traffic descriptor where its td_id = 5 and a cell rate of 4152 cells per second.

Command:	`M15-155s1:/>M15-155s1:/>td setup CBR <td_id> pcr0+1=<pcr0+1> [pcr0=<pcr0>]`	
Example 1:	*Module 1*	`M15-155s1:/>td setup CBR 5 pcr0+1=4152`
Example 2	*Module 1*	`M15-155s1:/>td setup CBR 5 pcr0+1=4152`
	Module 3	`M15-155s3:/>td setup CBR 5 pcr0+1=4152`

To determine which td_id is available, type `td show` to display all defined Traffic Descriptors.

Components in LANE Services

This chapter gives a basic overview on the components of LANE Services.

LAN Emulation

The principles of LAN Emulation

LAN Emulation (LANE) enables legacy LAN applications to use an ATM transport medium transparently. Therefore, end-stations on existing Token Ring and Ethernet LANs can communicate with ATM end-stations.

Components of LAN Emulation

- LAN Emulation Client (LEC)

  Every device on an ELAN has one or more LECs. This interfaces with the ATM network and performs most of the work of LAN emulation.
- LAN Emulation Server (LES)

  There is at least one active LES (which may be a part of a distributed LES) allocated to each Emulated LAN (ELAN). The LES maintains a list containing both the LAN address (MAC address) and / or the route descriptor, and the ATM address for every LEC that is active on the ELAN.
- Broadcast Unknown Server (BUS)

  There is only one active BUS (which may be a part of a distributed BUS) on an ELAN. The BUS is normally part of the same software module as the LES and provides the ELAN with broadcast and multicast facilities. It has direct connections to every LEC on the ELAN.
- LAN Emulation Configuration Server (LECS)

  There is only one active LECS (however, you may have a number of standby LECS) on the network. The LECS maintains a list of all LESes. The LECS provides each LEC that contacts it with the ATM address of the LES hosting the ELAN that it should join. The LECS is usually located locally or remotely at the following ATM Forum Well-Known Address (WKA) 47.00.79.00.00.00.00.00.00.00.00.00.00.a0.3e.00.00.01.

Communication on an Emulated LAN

It is the LEC in an ATM device that will perform most of the work of LAN emulation. To do this it must join an ELAN.

Discovering the ATM address of the LES

Before a LEC can join an ELAN, it typically gets the ATM address of the LES from the LECS. The LECS decides which LES to direct a LEC to, on the basis of the information that the LEC gives it. For example, the LEC may provide the name of the ELAN it expects to join. Alternatively, the LECS may be configured to associate a particular LEC with a specific ELAN.

Discovering the ATM address of another LEC

Every LEC has one or more LAN addresses (for example, MAC address) and an ATM address associated with it. When the network operating system passes a frame to a LEC to transmit, the LEC checks whether it already has a connection set up to that frame's LAN destination address. If there is no existing connection, the LEC must discover the ATM address for that destination end-station, signal to the network for a connection, and then transmit the data.

To discover an ATM address, the LEC consults its list of ATM stations that it has communicated with. If the LEC cannot find the address it requires from its own list, it will communicate with the LES for the required address.

When a LEC needs an ATM address, it sends a LANE ARP (Address Resolution Protocol) request to the LES. If the LES knows the ATM address, it sends it to the LEC. If it does not know the ATM address, the LES may forward the address request to any LECs that are registered with it so that they can respond directly to the LES. The LES will then forward the response to the LEC.

Setting up the connection

When the LEC has discovered the ATM address of the required LEC, it signals to the ATM network for a Virtual Circuit Connection (VCC) to that LEC.

Transmitting the data

When the VCC is set up, the LEC transmits its data through the ATM network to the destination LEC.

Locating the LECS, LES, and BUS services

An ATM network may contain several ELANs. The network must only have one LECS, and each ELAN must have one active LES and one BUS (which may be part of a distributed LES/BUS).

The LECS, LES, and BUS constitute the LANE Services. These elements must reside on hosts that all the LECs on a network can access. They can be located on the same host or on different hosts, which may be one of the following:

- An ATM switch
- A dedicated workstation
- An existing or dedicated server. For example, the services could be implemented as NetWare Loadable Modules (NLMs) on a NetWare server.

Appendix F

Routing and Signalling Concepts

This chapter describes how the Avaya M770 ATM Switch switches ATM cells through an ATM network, and provides background information about the concepts of routing and signalling.

Switching ATM cells through the ATM network

There are two types of connection that can be used to switch ATM cells through an ATM network.

- Permanent Virtual Circuits (PVCs), which are created manually by the network administrator. Every switch through which the connection will pass will need to be configured separately. PVCs are used for communication between two endpoints, through a pre-configured circuit, until the administrator disables the PVC and frees the connection.
- Switched Virtual Circuits (SVCs), which are established on demand by UNI (User-to-Network Interface) / NNI (Network-to-Network Interface) signalling protocols. SVCs are used for communication between two endpoints until one endpoint clears the connection. There are two types of SVCs:
  - Point-to-point virtual circuits
  - Point-to-multipoint virtual circuits.

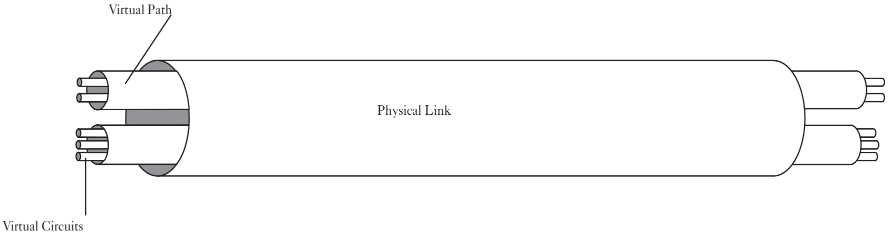
In an ATM network, an end-station can establish a SVC to another end-station by transmitting a signalling call setup request across the network. This request is routed across the ATM network to the destination end-station. If the destination agrees to accept the connection, a SVC is set up across the ATM network, between the two end-stations.

Virtual Circuits and Virtual Paths

In ATM networks data is multiplexed on physical links using virtual circuits and virtual paths. A virtual circuit is a channel of communication that allows data transfer between two ATM devices. A virtual path is used to group virtual circuits within the same transmission medium so that they can be switched together. Virtual circuits are identified by an unique Virtual Circuit Identifier (VCI). Virtual paths are identified by an unique Virtual Path Identifier (VPI).

Figure C.1 shows how virtual circuits are bundled together within a virtual path.

Figure F.1 Virtual circuits in a virtual path



Virtual Ports

To support terminating virtual paths, the M770 ATM Switch uses virtual ports. Virtual ports are typically used for Virtual Port Muxing, or tunnelling, through public networks.

A physical port contains several virtual ports and each virtual port can be considered a port in its own right. When a physical port initializes, a default root virtual port is created. Further virtual ports can be created when you need them. Connections are set up between virtual ports, and you can perform operations on virtual ports, such as enabling and disabling them.

The maximum number of non-root vports that can be defined in the system is 32. The maximum number of vports (root vports plus non-root vports) that can be defined on a physical port depends on the number of vpi bits configured for the module.

For example, if the number of VPI bits is 3, then the maximum number of vports that can be defined on a physical port is 8. That is, 1 root vport (0) and 7 non-root vports (1-7).

A virtual port will use a single VPI or a range of VPIs for all calls set up through that virtual port.

Note: Only the root virtual port can have a range of VPIs. Subsequent virtual ports can only be assigned a single VPI.

A virtual port has a range of VPIs so that:

- It can support a larger number of circuits than it could on the basis of its VCI range alone.
- It can contain several virtual paths that are to be tunnelled up to a certain point in the network after which they will diverge.

A virtual port in the M770 ATM Switch is represented by:

<slot number>.<port number>.<virtual port number>.

For example, 2.1.1 represents a virtual port number of 1, on physical port number 1 on module number 2. Root virtual ports are all assigned with an identifier of 0.

For more information about managing virtual ports, see Managing Virtual Ports in Chapter 6.

ILMI

The M770 ATM Switch supports ILMI and several signalling protocols.

ILMI is used between an end-station and a switch for the following:

- Automatic configuration of signalling and port parameters
- Address registration.

Setting up SVCs

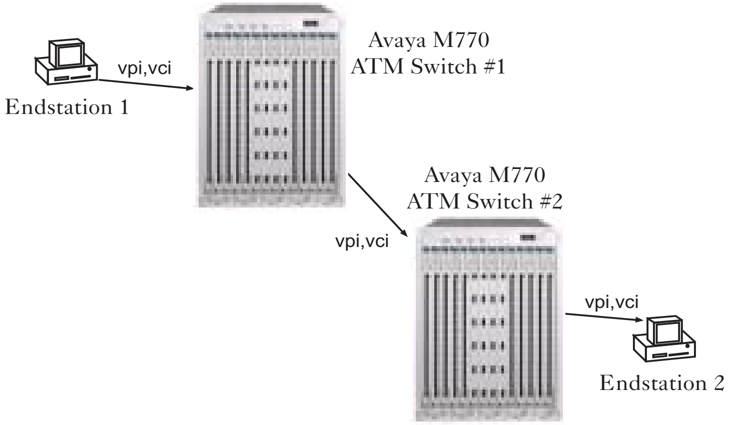
The M770 ATM Switch supports UNI 3.0, 3.1 and 4.0 signalling for connection setup between an end-station and a switch. IISP and PNNI 1.0 signalling are used for inter-switch connection.

When a connection setup request is transmitted by an end-station using the UNI signalling protocol, the M770 ATM Switch will use the ATM address of the called party and look up the longest matching addresses in its internal routing table.

If there is more than one longest matching address, it selects the appropriate port to route in terms of meeting the CoS and QoS requirements, and the minimum cumulative Administrative Weight of the links on the path to the destination.

Once the preferred output port has been determined, the setup request is forwarded to that port. Each switch forwards the connection setup request in the same manner, until the destination end-station is reached. If the destination end-station agrees to accept the connection, a SVC is set up.

Figure F.2 Signalling through the switches



All setup requests, travel on reserved channel 0/5 (VPI=0, VCI=5 on root virtual port 0), but the ATM switch will assign an incoming and outgoing VPI and VCI on a particular port, for the connection through the switch. Therefore, an ATM virtual circuit is a sequence of switch VPI/VCI translations.

The value of the VPI and VCI within a particular ATM cell header will change as the ATM cell is switched through the ATM network. In a single switch configuration a cell's VPI and VCI are translated only once, but in a multiple switch environment a cell's VPI and VCI may be translated many times. VPI and VCI values are assigned symmetrically, that is, the same values are reserved in both directions across a link. This means that all virtual circuits are inherently bi-directional. This does not imply that SVC traffic must be sent in both directions; it can be either bi-directional or uni-directional. With point-to-multipoint virtual circuits, data is only sent from the root (source) to the leaves (destination parties).

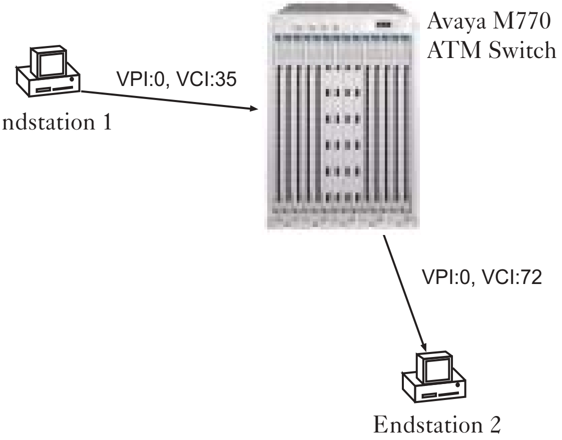
Note: On a given link, VPI/VCI identifiers are assigned in both directions of a circuit. However if a circuit is uni-directional, one of these will not be used.

Note: A cell's VPI and VCI are of local significance only. They identify the cell as being associated with a particular virtual circuit through a single link.

When the M770 ATM Switch receives a cell, it examines the ATM cell header to determine the VPI/VCI on which the cell was transmitted. Using this information, the M770 ATM Switch determines the destination port and appropriate VPI/VCI for the transmission of the ATM cell.

For example, in a single switch environment the switch can be configured such that a cell received on port A with VPI.VCI=0.35 is switched to port B with VPI.VCI=0.72. The translation from input port VPI and VCI to output port VPI and VCI is carried out by the switch hardware.

Figure F.3 Cell switching through a M770 ATM Switch from end-station one to end-station two



Setting Address Prefixes to Match Hierarchical PNNI

Algorithm for Automatic Setting of ATM Prefixes

1 Identify a pre-assigned prefix, possibly given by an ATM Service Provider. If none, use our factory prefix 39.00.00.00.00.00.00.00.00.00.00.00.00

2 List switches that exist in the network.

3 The user identifies the highest level (L) for the hierarchy.

— The level range is 1-104. It is recommended to use the range 8-96

— The recommended value should be a multiple of eight.

4 For all switches set the L/8 left-most bytes to be the same as those bytes in the pre-assigned prefix.

5 Select a group of switches that will be in the same level peer group, start from the higher level peer group (lower number), and go down the hierarchy (higher numbers).

6 Determine at which level this peer group should reside and make this level L1.

— Never select a level that is higher (lower in number) than a level that was previously selected.

7 For all the switches in a peer group (L1), set an unused level-index (1-255) to the (L1)/8 byte and mark this index “used”.

8 Determine whether this is the lowest level. If so, set to each one of the switches in the peer group an unused index for the next byte and mark this index ‘used”.

9 Repeat steps 5-8 until the user decides that the process ends.

10 At this point, all bytes up to the 13th are set to 0.

Example:

1 The pre-assigned prefix is 39.00.00.00.00.00.00.00.00.00.00.00.00

2 Here is the list of switches:
A, B, C, D, E, F, G

3 The highest level of the hierarchy (user input): 40

4 The first five (40/8) bytes of all prefixes will be: 39.00.00.00.00

5 The user selects switches: A,B,C,D to be together at level 48.

6 Assign the sixth (48/8=6) byte to be 1, mark the index 1 for byte six “used”.

— The prefix for switches A,B,C,D so far is: 39.00.00.00.00.01

7 The user selects switches A,B to be together at level 56

8 Assign the 7 byte to be 1, mark the index 1 for byte seven “used”.
The prefix for switches A,B is: 39.00.00.00.00.01.01

9 The user says it is the lowest level for switch A,B

— Assign the next byte (8) to the switches in the peer group.

- The prefix of switch A: 39.00.00.00.00.01.01.01
- The prefix of switch B: 39.00.00.00.00.01.01.02

10 The user selects switches C,D to be together at level 56

11 Assign the seventh byte to be 2 (1 is already used for byte 7), mark the index 2 for byte seven - “used”.

- The prefix for switches C,D is: 39.00.00.00.00.01.02

12 The user says it is the lowest level for switch C,D

13 Assign the next byte (8) to the switches in the peer group.

- The prefix of switch C: 39.00.00.00.00.01.02.01
- The prefix of switch D: 39.00.00.00.00.01.02.02

14 The user selects switches E,F,G to be together at level 56

15 Assign the seventh byte to be 3 (1 and 2 are already used for byte 7), mark the index 3 for byte seven “used”.

- The prefix for switches E,F,G is: 39.00.00.00.00.00.03

16 The user says it is the lowest level for switch E,F,G

17 Assign the next byte (8) to the switches in the peer group.

- The prefix of switch E: 39.00.00.00.00.00.03.01
- The prefix of switch F: 39.00.00.00.00.00.03.02
- The prefix of switch G: 39.00.00.00.00.00.03.03

18 The user decides that this is it. For all switches, set all the remaining bytes up to the 13th byte, to 0.

- The prefix of switch A: 39.00.00.00.00.01.01.01.00.00.00.00.00
- The prefix of switch B: 39.00.00.00.00.01.01.02.00.00.00.00.00
- The prefix of switch C: 39.00.00.00.00.01.02.01.00.00.00.00.00
- The prefix of switch D: 39.00.00.00.00.01.02.02.00.00.00.00.00
- The prefix of switch E: 39.00.00.00.00.00.03.01.00.00.00.00.00
- The prefix of switch F: 39.00.00.00.00.00.03.02.00.00.00.00.00
- The prefix of switch G: 39.00.00.00.00.00.03.03.00.00.00.00.00

Index

How to Contact Us

To contact Avaya's technical support, please call:

In the United States

Dial 1-800-237-0016, press 0, then press 73300.

In the EMEA (Europe, Middle East and Africa) Region

Country	Local Dial-In Number
Albania	+31 70 414 8001
Austria	+43 1 36 0277 1000
Azerbadjan	+31 70 414 8047
Bahrain	+800 610
Belgium	+32 2 626 8420
Belorussia	+31 70 414 8047
Bosnia Herzegovina	+31 70 414 8042
Bulgaria	+31 70 414 8004
Croatia	+31 70 414 8039
Cyprus	+31 70 414 8005
Czech Rep.	+31 70 414 8006
Denmark	+45 8233 2807
Egypt	+31 70 414 8008
Estonia	+372 6604736
Estonia	+372 6604736

Country	Local Dial-In Number
Finland	+358 981 710 081
France	+33 1 4993 9009
Germany	+49 69 95307 680
Ghana	+31 70 414 8044
Gibraltar	+31 70 414 8013
Greece	+00800 3122 1288
Hungary	+06800 13839
Iceland	+0800 8125
Ireland	+353 160 58 479
Israel	+1 800 93 00 900
Italy	+39 02 7541 9636
Jordan	+31 70 414 8045
Kazakhstan	+31 70 414 8020
Kenya	+31 70 414 8049
Kuwait	+31 70 414 8052

Country	Local Dial-In Number
Latvia	+371 721 4368
Lebanon	+31 70 414 8053
Lithuania	+370 2 756 800
Luxemburg	+352 29 6969 5624
Macedonia	+31 70 414 8041
Malta	+31 70 414 8022
Mauritius	+31 70 414 8054
Morocco	+31 70 414 8055
Netherlands	+31 70 414 8023
Nigeria	+31 70 414 8056
Norway	+47 235 001 00
Oman	+31 70 414 8057
Pakistan	+31 70 414 8058
Poland	+0800 311 1273
Portugal	+351 21 318 0047
Qatar	+31 70 414 8059
Romania	+31 70 414 8027
Russia	+7 095 733 9055

Country	Local Dial-In Number
Saudi Arabia	+31 70 414 8022
Slovakia	+31 70 414 8066
Slovania	+31 70 414 8040
South Africa	+0800 995 059
Spain	+34 91 375 3023
Sweden	+46 851 992 080
Switzerland	+41 22 827 8741
Tanzania	+31 70 414 8060
Tunisia	+31 70 414 8069
Turkey	+800 4491 3919
UAE	+31 70 414 8036
Uganda	+31 70 414 8061
UK	+44 0207 5195000
Ukraine	+31 70 414 8035
Uzbekistan	+31 70 414 8046
Yemen	+31 70 414 8062
Yugoslavia	+31 70 414 8038
Zimbabwe	+31 70 414 8063

Email: csctechnical@avaya.com

In the AP (Asia Pacific) Region

Country	Local Dial-In Number
Australia	+1800 255 233
Hong Kong	+2506 5451
Indonesia	+800 1 255 227
Japan	+0 120 766 227
Korea	+0 80 766 2580

Country	Local Dial-In Number
Malaysia	+1800 880 227
New Zealand	+00 800 9828 9828
Philippines	+1800 1888 7798
Singapore	+1800 872 8717
Taiwan	+0 80 025 227

Email: sgcoe@avaya.com

In the CALA (Caribbean and Latin America) Region

Email: caladatasupp@avaya.com

Hot Line:+1 720 4449 998

Fax:+1 720 444 9103

For updated information, visit www.avayanetwork.com, and click “Global Support Organization (GSO)”.