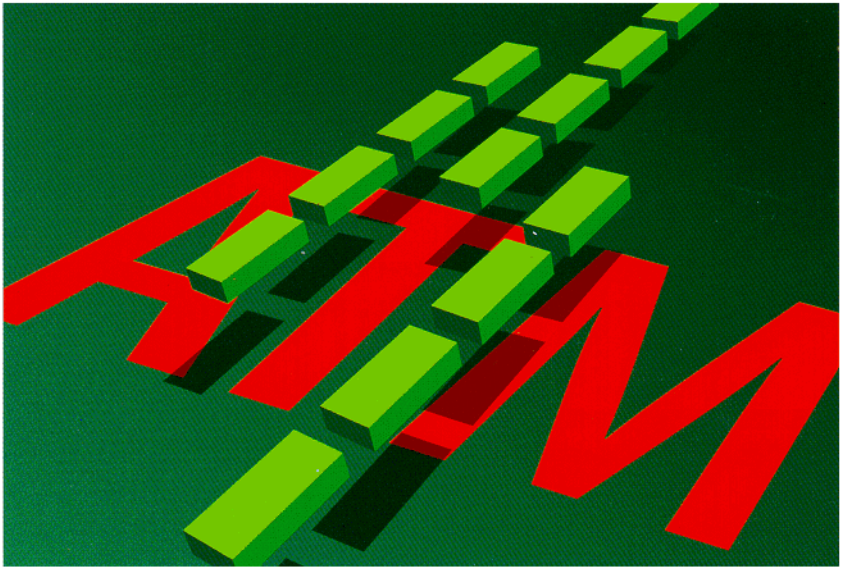
ATM

DOC-6990/5.1.5



CrossFire™ ATM Switch Series

Guide to Operations

olicom
THE NETWORKING COMPANY

CrossFire™ ATM Switch Series

Guide to Operations

Trademarks

GoCard and the Olicom clasped hands logo are registered trademarks of Olicom A/S. CellDriver, ClearServer, ClearSession, ClearSight, CrossFire, LANscout, PowerMACH and RapidFire are trademarks of Olicom A/S. ClearCare, ClearPartner, ClearStep and ExpertWatch are service marks of Olicom A/S. Olicom is a registered trademark. Other brand and product names are trademarks, registered trademarks, service marks or registered service marks of their respective holders.

Copyrights

Olicom A/S reserves the right to modify the information given in this publication without prior notice. The warranty terms and conditions applicable for your purchase of this equipment are given at the time of purchase. Consult your place of purchase for details.

Publication: DOC-6990 v. 5.1.5

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Declaration of Conformity

CLASS 1 LASER PRODUCT

We Olicom A/S
Nybrovej 114
DK-2800 Lyngby
Denmark

declare under our sole responsibility that the products

CrossFire 8008 ATM Switch
CrossFire 9100 ATM Switch
CrossFire 9200 ATM Switch

to which this declaration relates are in conformity with the following standards or other normative documents

EN 50082
EN 55022
EN 60950 including Amendments
EN 60825 including Amendments

following the provisions of 89/336/EEC Directive and 73/23/EEC Directive.

Modifications

If the device is changed or modified without the express approval of Olicom A/S the user may void his or her authority to operate the equipment.

Safety Notices

Danger: To avoid shock hazard, do not connect or disconnect any cables or perform installation, maintenance, or reconfiguring of the CrossFire 8008/9100/9200 ATM Switches during an electrical storm.

Danger: To avoid the possibility of electrical shock, switch power off and unplug the power cord from the outlet before detaching the power cord from the CrossFire 8000 Chassis or the CrossFire 9100/9200 ATM Switch.

Danger: Do not open the CrossFire 8000 Chassis or the CrossFire 9100/9200 ATM Switch. Dangerous voltages inside.

Danger: To avoid shock hazard the power cord must be connected to a properly wired and grounded receptacle. Any equipment to which the CrossFire 8008 or the CrossFire 9100/9200 ATM Switches will be attached must also be connected to properly wired and grounded receptacles.

Caution: Observe the following power cable considerations before you begin installation of the CrossFire 8000 Chassis or the CrossFire 9100/9200 ATM Switches.

1. The socket outlet shall be installed near the equipment and shall be easily accessible.

2. To prevent electrical shock, the power cord set used must comply with national regulations.

2a. The female receptacle of the cord must meet CEE-22 requirements.

2b. The cord must be UL listed, CSA labelled, and consist of three conductors with a maximum of 15 feet in length. Type SVT or SJT cord sets shall be used for units which stand on a desk or table. Type SJT cord sets shall be used for units which stand on floor.

2c. The male plug for units operating at 115 VAC shall consist of a parallel blade, grounding type attachment plug rated 15 A, 125 VAC. The male plug for units operating at 230 VAC shall consist of a tandem blade, grounding type attachment plug rated 15 A, 250 VAC. The male plug for units operating at 230 VAC (outside of the United States and Canada) shall consist of a grounding type attachment plug rated 15 A, 250 VAC and have the appropriate safety approvals for the country in which the equipment will be installed.

Caution: Support the CrossFire 9100/9200 ATM Switch while you are installing the unit to avoid dropping it on the floor or any equipment beneath it in the rack. The CrossFire 9100/9200 ATM Switch unit weighs approximately 22 kg (44 lbs).

Caution: Use care when installing the CrossFire 8000 Chassis. The CrossFire 8000 2-slot Chassis weighs 17 kg (39 lbs). The CrossFire 8000 8-slot Chassis weighs 44 kg (97 lbs).

Caution: To separate the switch from the power, pull out the power cord completely from the socket. The power socket must be easily accessible and located near the unit.

Warning: All RJ-45 connectors must only be connected to safety extra low voltage (SELV) circuits like local area networking (LAN).

Note: RJ-45 plugs (Western Plugs) intended for Token-Ring, Ethernet, or ATM connections are only allowed to be connected with SELV Voltage of EN 60950:1991. (Only for LAN Communications Connections).

Table of Contents

List of Figures

List of Tables

About this Manual

Following is a short description of the content of the chapters and appendixes in this publication:

Chapter 1, "Olicom's ATM Switches", describes Olicom's ClearSession strategy for providing ATM network fault tolerance, the key features provided by the CrossFire switches, and the specific ATM switch features supported by the different models.

Chapter 2, "Installation", explains how to install and set up Olicom's CrossFire 8008, CrossFire 9100, and CrossFire 9200 ATM switches. The CrossFire 9100 and 9200 are a stackable solution, whereas the CrossFire 8008 resides in a chassis.

Chapter 3, "ATM Concepts", provides information about ATM concepts that you should know before you change your ATM switch configuration.

Chapter 4, "Supported ATM Protocols", describes the protocols used to move ATM cells to an end system.

Chapter 5, "Using Console Commands", provides information about using console commands to manage your CrossFire ATM Switch.

Chapter 6, "Configuring LANE and PNNI", describes some configuration information you may need to reference when using the LANE and PNNI protocols on your ATM network.

Chapter 7, "Configuration Backup", describes how to back up and restore switch configuration.

Chapter 8, "Contacting Technical Support", lists Olicom's support services, such as hotline support, fax support and the support web, as well as other services such as bulletin board service, FTP server and e-mail.

Appendix A, "Chassis Maintenance", describes the procedures for inserting a CrossFire 8008 into a CrossFire 8000 chassis, calculating the power supply requirements for the CrossFire 8000 chassis, and general CrossFire 8000 chassis maintenance considerations.

Appendix B, "Error and Status Messages", describes the error and status messages which appear on the alphanumeric display.

❑

1. Olicom's ATM Switches

This chapter describes Olicom's ClearSession™ strategy for providing ATM network fault tolerance, the key features provided by the CrossFire switches, and the specific ATM switch features supported by the different models.

Sections

- The ClearSession Strategy and the ATM Cloud
- Olicom's ATM Switches

Olicom's CrossFire ATM switches provide a cost-effective, high-capacity switching solution for voice, video, and Intranets that require high speed and high bandwidth to operate effectively. The CrossFire ATM switches have a modular design, which makes them a scalable solution that easily accommodates future LAN growth, ensuring its long-term investment value.

The ClearSession Strategy and the ATM Cloud

Olicom has developed ClearSession, which is a combination of software and hardware components embedded in Olicom's Network Interface Cards (NICs), ATM switches, and routers. Enterprises can use devices running the ClearSession strategy to create a fault tolerant network, while maintaining mission-critical performance as they move to ATM high-speed switched networks. Only ClearSession devices residing on your ATM network can deliver complete fault-recovery in just 3 seconds to ensure zero session loss for non-stop networking.

ClearSession Components

The components of ClearSession related to ATM include:

- Fast failure detection and re-routing of ATM links
- Mirror Link Protocol (MLP) to create duplicate ATM links
- ClearServer™ – Olicom's solution to provide ATM server access redundancy
- ATM LAN redundancy – built into Olicom's edge routers, NIC cards, LAN Emulation servers, and switches
- Backup for critical traffic over ATM

Each of these components is available as a stand-alone solution – or for the most comprehensive coverage, you can implement all the ClearSession components.

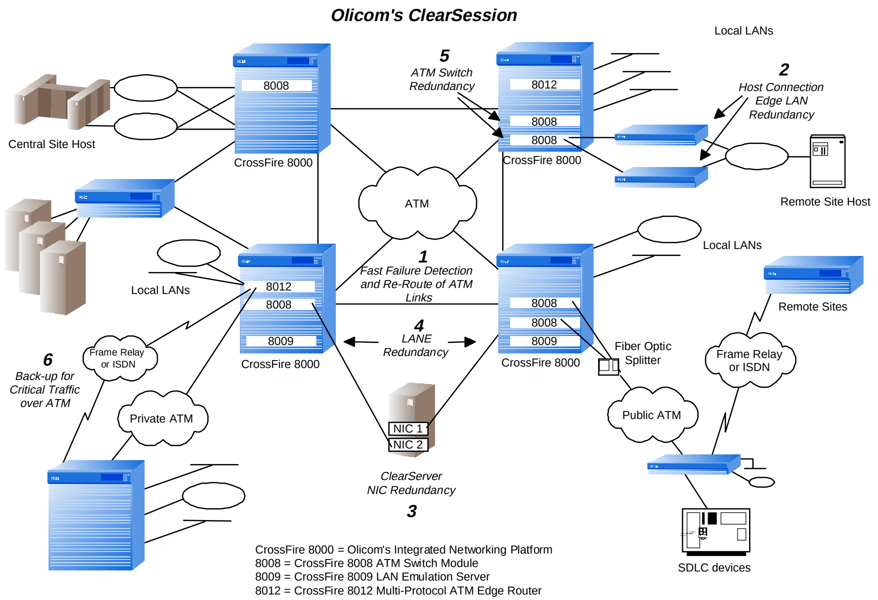


Figure 1. The ClearSession Strategy

The following sections explain each callout in figure 1. The numbers are included in the title to make it easier for you to refer back to the illustration.

1–Fast Failure Detection and Re-routing of ATM Links

With ClearSession implemented, Olicom's products have the capability to detect a failure and recover from it.

2–Host Connection Edge LAN Redundancy

The ClearSession strategy provides edge redundancy for end systems and servers attached to a LAN or connected to an ATM network by connecting multiple ATM edge devices, such as an edge router or an edge switch. The two edge devices communicate with each other using the ClearSession Protocol (CSP). CSP allows the two edge devices to share a common Virtual IP gateway address and a common Virtual MAC address.

Using CSP, one of the devices is nominated to be the active device while the other one becomes the secondary device. When the active device fails, the secondary device immediately becomes active and continues to forward traffic using the same virtual IP and MAC addresses. Without this redundancy, a failed IP gateway results in users being disconnected.

3–ClearServer NIC Redundancy

ClearServer, Olicom’s solution to provide ATM server access redundancy, enables multiple NIC cards in the server to serve as backups for each other. This process is transparent to the server applications and operating system.

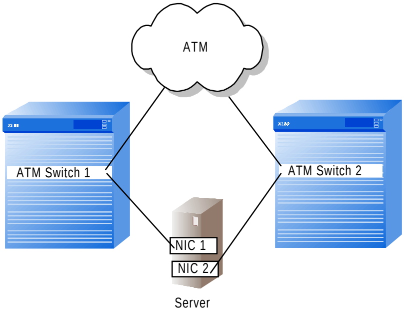


Figure 2. Network Interface Card Redundancy

In case of failure, traffic connected to the first NIC on the server is re-routed to the second NIC to prevent any session loss. The networking and application layers may experience minimal differences during the brief switch over time period.

4–Redundant LAN Emulation (LANE) Servers

You can build redundant LANE services into your ATM network. If you are using a CrossFire 8008 switch, you can have LANE redundancy by adding a CrossFire 8009 card, a redundant LANE server, to your chassis. If you are using a CrossFire 9100 or 9200, you add LANE redundancy by activating the internal LANE servers with redundancy support (see Figure 3). If you have only one LANE server and it fails, LAN Emulation cannot occur.

Olicom's solution is based on a proprietary protocol between a *primary* and a *secondary* LANE server. This protocol is used to update and synchronize the secondary server’s databases, as well as to verify the activity status of the primary server. If the primary server’s hardware or software fails, the secondary server is automatically activated.

Once the secondary server is activated, LANE automatically recreates the SVCs. To reduce the time that ATM edge devices will be disconnected, Olicom provides an option called Persistent Data Direct Connections which delivers the following benefits:

- Maintains data direct SVC sessions during the transition time when one server is down, and the other is coming online. This results in uninterrupted data transfers.

- Eliminates the need for the re-creation of data direct SVCs when the LANE server transitions after failure; this approach eliminates wasting time and resources.

Figure 3 depicts a network employing an ATM LANE backbone with dual LANE servers for redundancy.

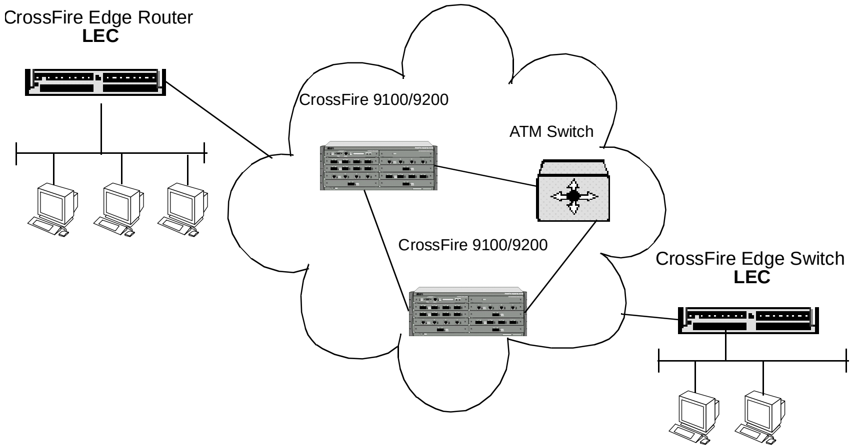


Figure 3. Redundant LANE Servers

5–Redundancy Within the Crossfire 8000 Chassis

Within the CrossFire 8000 chassis you can create redundancy by adding another CrossFire 8008 card. With a redundant CrossFire 8008, the ATM backbone is preserved in the event of failure. In addition, other modules can do load balancing between switches. If you add a redundant switch module to your chassis and the primary switch fails, all modules within the chassis will automatically reconnect to the secondary switch while preserving all active sessions.

6–Backup for Critical Traffic over ATM

With the ClearSession strategy, you can use an ATM edge router as a back-up system for critical traffic over ATM. This edge router provides an alternate communication link if an ATM link fails.

Olicom’s ATM Switches

You can use the CrossFire ATM switches either as a stand-alone solution, or integrated with other modular equipment to build high-performance ATM-to-LAN infrastructures. The CrossFire ATM switches support both Permanent Virtual Connections (PVCs) and Switched Virtual Connections (SVCs), and have *high-availability* features that provide link redundancy–enabling the ATM switches to recover quickly from a network failure.

Olicom has two types of ATM switches; the CrossFire 8008 *chassis-based* switch and the CrossFire 9100 and 9200 *stand-alone* switches. The CrossFire 8008, which is an integral part of Olicom’s chassis-based network architecture, supports the CrossFire 8000 line of modular products, provides ATM connectivity between Olicom and other vendor’s ATM switches and products, and provides connectivity to high-performance ATM attached servers.

The CrossFire 9100 and 9200 models are stand-alone, high performance, ATM switches. You can use these switches to build ATM backbones and provide connectivity to attached ATM server farms.

You can use the CrossFire ATM switches either as a stand-alone solution, or integrated with other Olicom and other vendor’s ATM equipment to build ATM infrastructures.

Key Features of the CrossFire ATM Switches

Olicom ATM switches provide the following key features.

Permanent Virtual Path Tunnels

Olicom’s Permanent Virtual Path Tunneling capability creates tunnels across *foreign* ATM networks; foreign meaning ATM networks made up of other vendor’s ATM devices. Using this feature allows *all* the ATM switches to take advantage of Olicom’s dynamic features.

Proxy User

Proxy user increases the interoperability of CrossFire ATM switches with other vendors’ ATM switches. Using this feature, the CrossFire ATM switches communicate with other switches using the User to Network (UNI) interface, which is a well established and simple interface. Devices connected to the CrossFire ATM switches appear as if they are directly connected to another vendor’s switch.

SNMP over MAC

You can use the Simple Network Management Protocol (SNMP) to access remote devices, usually to configure them. Since the SNMP stack consists of IP, normally someone would have to configure an IP address on the remote device before you use SNMP to access it.

Olicom has developed a proprietary method to run SNMP over MAC, thus enabling you to use SNMP to access a remote device that has not been configured with an IP address. SNMP communicates over the MAC layer instead of the IP layer.

High-Speed Campus Network Solution

For organizations spread over a large area, such as a university or business campus, it is normally important that the high-speed network be capable of extending over a relatively long distance. The CrossFire 9232 single-mode fiber module provides a 622 Mbps ATM connection that can extend up to 15 km, so servers located on the other side of the campus can be accessed just as quickly as a server in the next room.

To connect two buildings that have ATM networks, add a CrossFire 9232 module to a CrossFire ATM switch chassis in each network and extend a single-mode fiber between them, as shown in Figure 4.

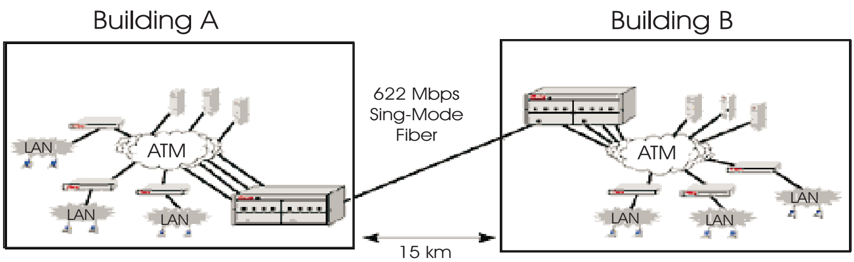


Figure 4. Extending the ATM Network Across a Campus

ATM Service Solution

All of the CrossFire chassis accept a wide range of modules, including ATM, Token-Ring, and Ethernet switches–plus a router module to enable communication to a WAN and between Ethernet and Token-Ring. It can support leased line connections to public ATM systems, and 45 Mbps DS3 connections. This allows users on both Ethernet and Token-Ring LANs access to the high-speed ATM network and will even be able to communicate directly with one another and out into the wide area.

The scenario illustrated in Figure 5 shows a configuration using three CrossFire 9100s, one CrossFire 8000 chassis, and several LAN switches. The CrossFire 8000 chassis contains a CrossFire 8011 or 8012 Multi-protocol Router for communicating the WAN and translating between Ethernet and Token-Ring, an AES Ethernet Switch and a CrossFire 8000 ATM switch for connecting to the local ATM network and to a public ATM service.

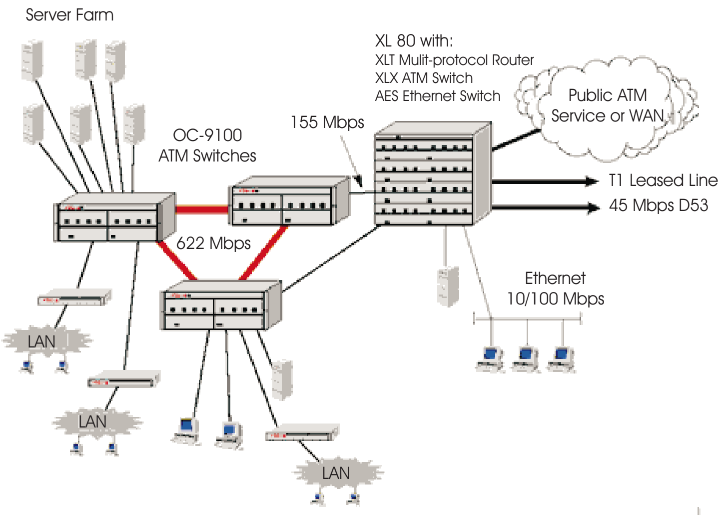


Figure 5. ATM Network Using CrossFire 8000 Chassis for Switch, Router and WAN Services

CrossFire Switch Overview

Olicom's CrossFire ATM switches offer a high-availability, fault-tolerant system with multiple power supplies, fan-packs, and non-disruptive software upgrades. They support multiple routing, LAN switching, and ATM switching modules – all of which are completely hot swappable (meaning the component can be serviced online without affecting other components).

The CrossFire ATM switches support all methods of connection set up, including signaled connections and management-defined connections (PVCs and PVPs), tunnels across *foreign* ATM networks, soft PVCs and PVPs, and point-to-multipoint and point-to-point connections. The CrossFire ATM switches also provide proactive error detection and monitoring, automatic termination of "broken" virtual circuits, and scale to thousands of switches (with no theoretical limit) while still delivering interoperable, QoS-based routing.

Some of the common features for the CrossFire ATM switches include:

- Support for up to 14,480 Virtual Channels and 255 Virtual Paths
- Supports the following interface connections:
  - OC-3 SONET Multi-mode, Single Mode, and UTP interface
  - OC-12 SONET Multi-mode and Single Mode
  - Digital Signal Level 3 (DS3) – dual coaxial BNC connector (CrossFire 8008 only)
  - Eight internal interfaces (CrossFire 8008 only)
- Out-of-band management over Ethernet using ClearSight or SNMP. If ClearSight is not available, you can use the command line user interfaces. Command line user interfaces can be:
  - serial console
  - virtual console (across the CrossFire 8000 chassis only)
  - modem
  - Telnet over Ethernet (out-of-band)
  - Telnet using CLIP (Classical IP over ATM)
  - LAN Emulation (LANE) In-band (CrossFire 9100 and 9200 only)
- In-band management via CLIP or LAN Emulation (CrossFire 9100 and 9200 only)
- Dedicated Diagnostic Processor which monitors chassis and power supplies.

About the CrossFire 8008

You can order the CrossFire 8008 in a variety of configurations with several types of ATM interfaces. You can configure the CrossFire 8008 with:

- four, eight, or twelve outward-facing (external) interfaces (with no internal interfaces)
- eight internal interfaces (CrossPoint Matrix interfaces) with four and eight external interfaces.

The cross-connect CrossFire 8008 is unique in that the switching fabric and I/O modules are resident on the same pre-configured module. This provides for high reliability and low cost.

CrossFire 8008 Features

The CrossFire 8008 ATM switch supports the following features:

Feature	Description
Processor	33 MHz Intel 960CF
System Memory	32 MB
Flash Memory	4 MB
Cell Buffering	Centralized cell buffering with a capacity of 16,384 cells

Table 1. ATM Switch Features

The CrossFire 8008 provides external ATM interfaces to connect to other ATM devices including:

- The CrossFire 8011/F ATM Edge Bridge/Router
- ATM attached workstations, file servers, and other hosts
- LAN Emulation Service (CrossFire 8009 LANE Servers or other vendor's)
- Other ATM switches

The ClearSession CrossFire modules, such as the ATM Edge Switch, CrossFire 8011 ATM Edge Bridge/Router, and the CrossFire 8011/F ATM Edge Router provide legacy LAN to ATM conversion. Figure 6 illustrates the ATM cloud as a network backbone.

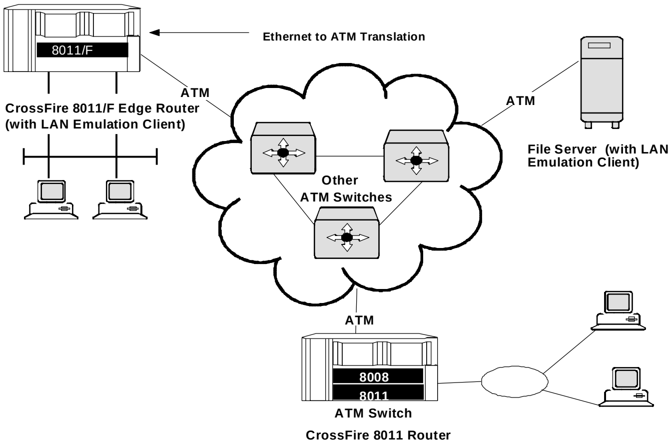


Figure 6. ATM Network Backbone

The key element of the ClearSession strategy is that the ATM cloud provides both WAN and LAN-backbone connectivity, while "collapsing" the backbone internally within the Olicom CrossFire 8000 platform.

Figure 7 shows how the CrossFire 8008 works with the CrossFire 8011/F ATM Edge Router to improve data flow from remote LANs to the corporate backbone.

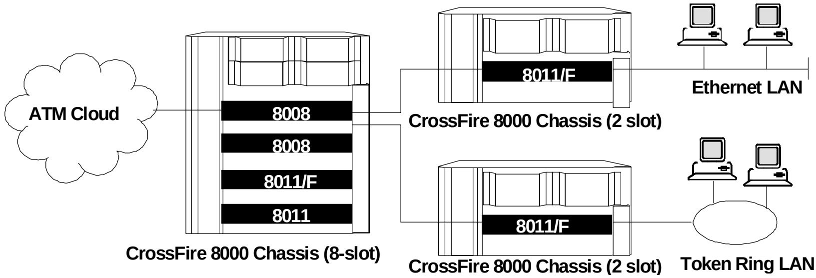


Figure 7. CrossFire 8008 and CrossFire 8011/F Router

As a component of Olicom's chassis based strategy, you can install the CrossFire 8008 in both the 2-slot and 8-slot CrossFire 8000 Chassis. When installed in a CrossFire 8000 Chassis, the built-in CrossPoint Matrix (CPM) backplane enables a CrossFire 8008 equipped with a rear-facing PHY Module to switch ATM cells internally between multiple CrossFire 8008s and other CrossFire 80xx-series modules, including:

- The CrossFire 8011 ATM Edge Bridge/Router with an internal ATM interface
- The CrossFire 8009 LAN Emulation Service with internal ATM interface

Note: Any references to the CrossFire 8011 ATM Edge Router also apply to the CrossFire 8012 ATM Edge Router.

Figure 8 shows a common CrossFire 8008 configuration with eight outward OC-3 MM interfaces and eight internal interfaces.

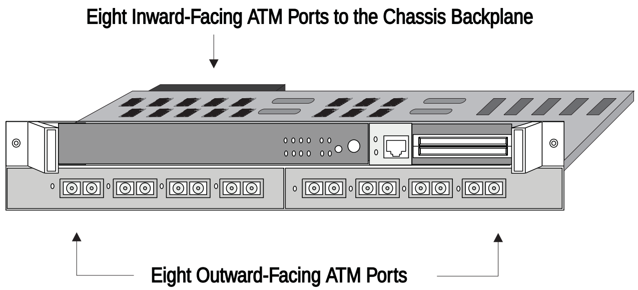


Figure 8.   CrossFire 8008 Card with Inward-Facing Interfaces

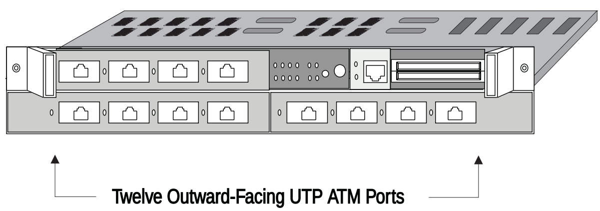


Figure 9.   Front View of the CrossFire 8008 with UTP Ports

About the CrossFire 9100 and 9200

The CrossFire 9100 and CrossFire 9200 are functionally the same product with a few differences. While the chassis for both models is the same, they support a different number of expansion slots and processing power.

Model	Expansion Slots	Processing Power
CrossFire 9100	4	80 MHz
CrossFire 9200	8	120 MHz

Table 2. Expansion Slots and Processing Power

You can use the CrossFire 9100's four expansion slots for the following:

- Sixteen OC-3 ports
- Three OC-12 ports and four OC-3 ports
- Any other combination where one OC-12 port can be replaced by four OC-3 ports

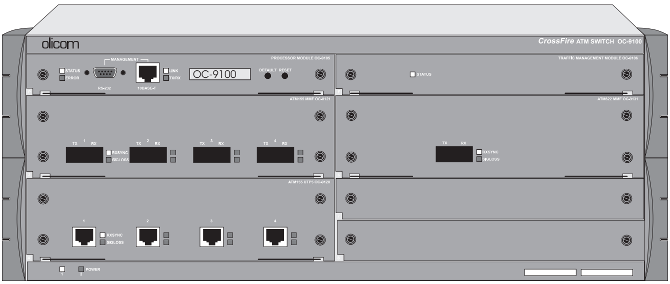


Figure 10. Front View of the CrossFire 9100 ATM Switch

You can use the CrossFire 9200's eight expansion slots for the following:

- Thirty-two OC-3 ports
- Seven OC-12 ports and four OC-3 ports

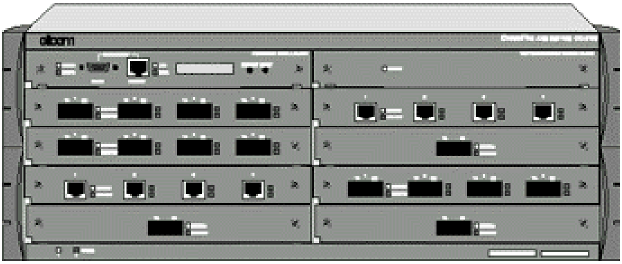


Figure 11. Front View of the CrossFire 9200 ATM Switch

CrossFire 9100/9200 Features

The CrossFire 9100 and 9200 ATM switches support the following features:

Feature	Description
Processor	80 MHz IDT R4650 133 MHz IDT R4650
System Memory	80 MB
Flash Memory	4 MB
Cell Buffering	Centralized cell buffering with a capacity of: • 16,384 cells (CrossFire 9100) • 32,768 (CrossFire 9200)
Redundant Power Supply	Each 9100/9200 comes with a redundant power supply module. This module provides fault tolerance redundancy and can be used if extra power consumption is required.
Redundant LANE Server	Internal LANE server is built into every CrossFire 9100/9200. To use this redundancy feature, you must activate it through LANE configuration.

Table 3. ATM Switch Features

With a 2.5 Gbps (CF-9100) and 5 Gbps (CF-9200) shared memory, fully non-blocking switch fabric, Olicom's new CrossFire 9100 and 9200 switches are designed to respond to the performance challenges network managers face in their existing LAN servers, server farms, and backbones.

Supported Modules

You can install any of the following "easy-to-install" modules in the CrossFire 9100/9200 chassis:

- CrossFire 9205 Processor Module (comes with chassis)
- CrossFire 9206 Traffic Management Module
- CrossFire 9220 - 155 Mbps UTP-5 Expansion Module (4-port)
- CrossFire 9221 - 155 Mbps MMF Expansion Module (4-port)
- CrossFire 9223 - 155 Mbps SMF Expansion Module (4-port)
- CrossFire 9231 - 622 Mbps MMF Expansion Module (1-port)
- CrossFire 9232 - 622 Mbps SMF Expansion Module (1-port)

Note: See "Physical Layer" on page 49 for a description of the supported interface types.

❑

2. Installation

This chapter describes the installation and setup of Olicom's ATM switches.

Sections

- Installing a CrossFire 8008 ATM Switch
- Installing a CrossFire 9100/9200 ATM Switch
- Making Connections for CrossFire ATM Switches
- Connecting a Console to Your Switch
- Troubleshooting a CrossFire ATM Switch

Installing a CrossFire 8008 ATM Switch

This section explains how to setup a CrossFire 8008 prior to operation, install a card in either the 2-slot or 4-slot CrossFire 8000 chassis, and power on your CrossFire 8000 chassis. For information about installing a CrossFire 9100 or 9200 switch, refer to page 25.

CrossFire 8008 Setup

The following procedure describes how to set up a CrossFire 8008 prior to operation.

1. Upon receipt of your CrossFire 8008, inspect the shipping carton for any damage that may have occurred during shipping. If the shipping carton shows any signs of external damage, notify your Olicom representative.
2. Unpack the shipping carton and make sure you have received the following items:
   — The correct CrossFire 8000 communication platform, either a CrossFire 8000 Chassis (2-slot) or CrossFire 8000 Chassis (8-slot)
   — The CrossFire 8008 module with the correct interface configurations
   — CrossFire ATM Switch Series–Guide to Operations (DOC-6990)
   — CrossFire 8008 Assembly Configuration and Test Sheet
   — CrossFire 9177 Release Notes

— Power cable (U.S.)

— Terminal cable

— ESD wrist strap

Note: When unpacking the CrossFire 9100/9200, be sure to keep all original packing materials. You may need them for storing and transporting. All components returned under warranty should be shipped in their original packing materials.

3. Verify that you have received all the optional items ordered, for example an external modem or Richmond kit.
4. Read the *CrossFire 9177 Release Notes* for important information that could affect the installation and operation of the CrossFire 8008.

CrossFire 8008 Components

Figure 12 shows the CrossFire 8008 outward-facing panel components.

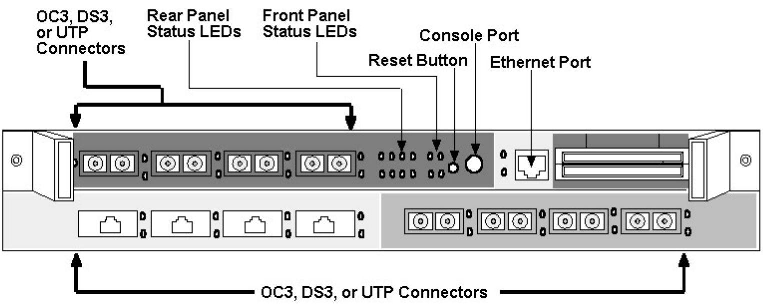


Figure 12. CrossFire 8008 Components

Status LEDs

Each OC-3 port on the CrossFire 8008 outward-facing panel is associated with a single LED (Figure 13).There are four OC-3 ports per OC-3 module. The CrossFire 8008 can be configured with up to three OC-3 modules for a total of 12 OC-3 ports.

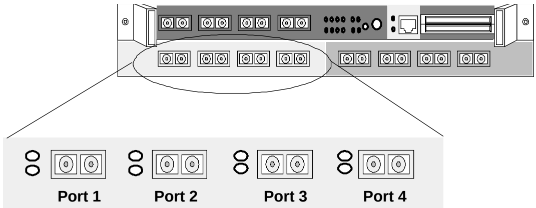


Figure 13. Port LEDs

LED	Function
Top LED 1 through 4 (Green)	Indicates that SONET framing is correct and operating normally.
Bottom LED 1 through 4 (Green)	Indicates the interface is active.

Table 4. Functions of Port LEDs

Figure 14 shows the standard CrossFire 8008 outward-facing panel LEDs.

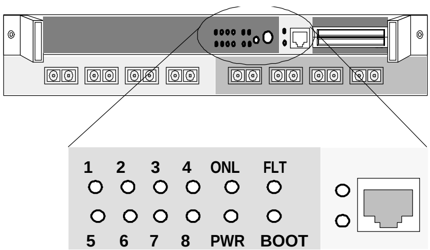


Figure 14. CrossFire 8008 Outward-Facing Panel LEDs

LED	Indicates
1 through 8 (Green)	The status of each internal port on the CrossFire 8008's inward facing panel.
ONL-online (Flashing Green)	The CrossFire 8008 is online and operational.
FLT-fault (Red)	There is a serious problem with the CrossFire 8008.
PWR-power (Green)	The CrossFire 8008 is powered on.
BOOT (Yellow)	When the CrossFire 8008 initializes, and when a download to the internal FLASH is in progress.
Ethernet Port-top (Green)	The link status.
Ethernet Port-bottom (Yellow)	Ethernet activity.

Table 5. CrossFire 8008 LEDs

CrossFire 8000 Communication Platforms

The Olicom CrossFire 8000 communication platforms are optimized for fail-safe networking, and offer your network growth and flexibility. Using a modular architecture, these products allow you to combine a variety of networking options to accommodate your specific communications needs.

The CrossFire 8008 can be installed into the following CrossFire 8000 communication platforms:

- CrossFire 8000 Chassis (2-slot)
- CrossFire 8000 Chassis (8-slot)

CrossFire 8000 Chassis (2-slot)

The CrossFire 8000 Chassis (2-slot) (Figure 15) is a two-slot or four-slot chassis that is well suited for a regional office. Modules, such as the CrossFire 8008, that occupy two slots must be installed in slots 1 and 2 or 3 and 4. The slot numbers are shown at the right.

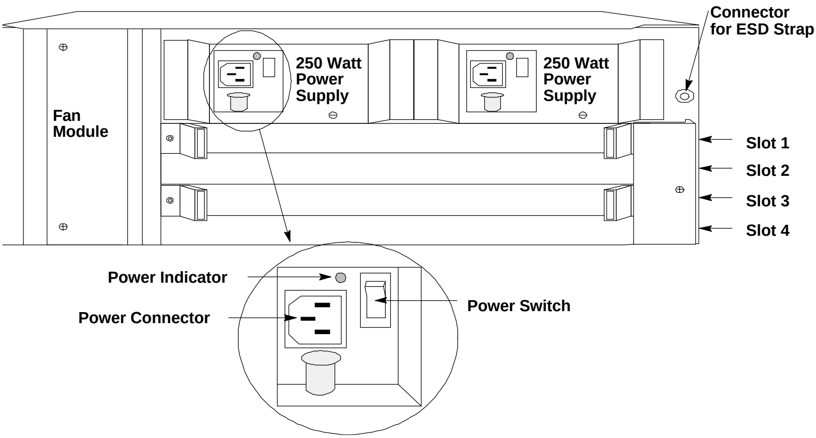


Figure 15. CrossFire 8000 Chassis (2-slot)

The location you select for the CrossFire 8000 Chassis (2-slot) must meet the physical and environmental specifications shown in the following table.

Specification	Value
Height	18.4 cm. (7.25 in.)
Width	44.7 cm. (17.6 in.)
Depth	30.5 cm. (12.0 in.)
Maximum Weight	19.1 kg. (42.5 lb.)
Power Cord Length	1.8 m. (6 ft.)
Clearance Required	10 cm. (4 in.)
Temperature	0° C to 40° C 32° F to 104° F
Relative Humidity	10% to 90% Non-condensing

Table 6. CrossFire 8000 Chassis (2-slot) Physical and Environmental Specifications

CrossFire 8000 Chassis (8-slot)

The CrossFire 8000 Chassis (8-slot) (Figure 16) can be used as either a half-height 8-slot or 16-slot chassis that provides the processing power and performance necessary for a corporate backbone. Modules that occupy two slots must be installed in slots 1 and 2, 3 and 4, 5 and 6, and so on. The slot numbers are shown at the right.

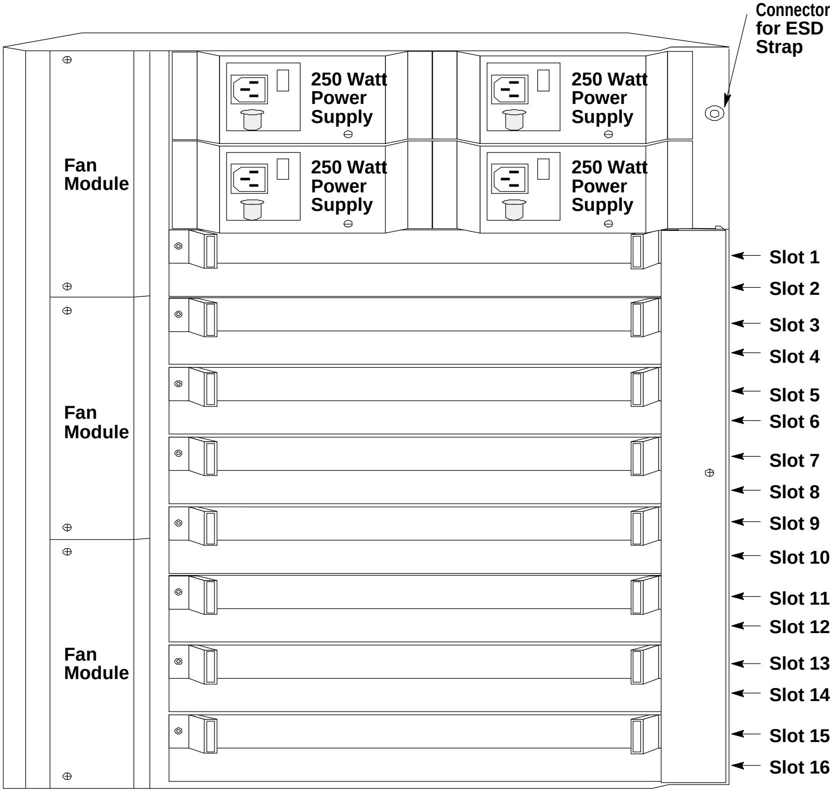


Figure 16. CrossFire 8000 Chassis (8-slot)

The location you select for the CrossFire 8000 Chassis (8-slot) must meet the physical and environmental specifications shown in the following table.

Note: You should not install two CrossFire 8000 chassis next to one another in adjacent corners.

Height	54.6 cm. (21.5 in.)
Width	44.7 cm. (17.6 in.)
Depth	31.8 cm. (12.5 in.)
Maximum Weight	58.2 kg. (107 lb.)
Power Cord Length	1.8 m. (6 ft.)
Clearance Required	10 cm. (4 in.)
Temperature	0° C to 40° C 32° F to 104° F
Relative Humidity	10% to 90% Non-condensing

Table 7. CrossFire 8000 Chassis (8-slot) Physical and Environmental Specifications

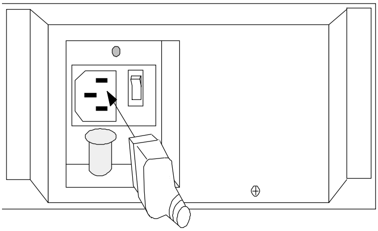
Powering on the CrossFire 8008

To power on your CrossFire 8000 chassis, do the following:

1. Verify that you have the appropriate number of power supplies installed. See “CrossFire 8000 Chassis (2-slot)” on page 19 for information on power supply requirements.

Note: All power supplies must be of the same type: 175 Watt or 250 Watt. Keep in mind that each 175 Watt power supply provides a maximum of 150 Watts at 5 Volts.

2. Verify that the power switch is set to **off**.
3. Connect the power cord to the chassis.



4. Connect the other end of the power cord into a three-prong grounded power receptacle or uninterruptible power supply (UPS). Make sure the power meets the following electrical requirements:
   - Voltage: 100–240 Volts
   - Frequency: 50–60 Hz

Warnings

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system and other connected devices. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

It is the customer's responsibility to select and install lightning protection appropriate to the use and location of the equipment. Lightning protection should be seriously considered in areas that are subject to electrical storms or equivalent power surges, especially if wide-area communications interfaces are used.

For safe operation, it is recommended that a 15-ampere branch circuit be used to supply power to the chassis. This circuit must be grounded to a safety ground, not to a neutral ground that returns current to the transformer.

5. Simultaneously set all the power switches to on. It is important that the required power be supplied to the modules when they are being powered on.
6. Verify that the power supply indicator is lit for each of the power supplies. If the indicator is not lit, refer to"Troubleshooting a CrossFire ATM Switch" on page 44.

CrossFire 8008 Power-On Sequence

The CrossFire 8008 power-on sequence takes approximately one minute. We recommend that you monitor the sequence on your console. When power is supplied to a CrossFire 8008, the following occurs:

- The *PWR* indicator lights.
- The *BOOT* indicator light flashes during system initialization, then goes off when initialization is complete.
- The *ONL* indicator remains off during diagnostics. When the CrossFire 8008 passes diagnostics, the indicator blinks while the CrossFire 8008 is on-line.

If your CrossFire 8008 is not operating properly, refer to See “Troubleshooting a CrossFire ATM Switch” on page 44.

What’s Next

Now that you have set up and powered-on your CrossFire 8008 switch, continue to the “Making Connections for CrossFire ATM Switches” on page 33. This section explains how to connect the appropriate network interface cable and a console to your switch.

Installing a CrossFire 9100/9200 ATM Switch

This section explains how to mount a CrossFire 9100/9200, interpret the visual indicators on the CrossFire 9205 Processor Module front panel, and how to power on your CrossFire 9100/9200.

CrossFire 9100/9200 Setup

The installation instructions for the CrossFire 9100 and CrossFire 9200 are identical. References to the CrossFire 9100 and 9200 are used interchangeably throughout these instructions.

The following procedure describes how to set up a CrossFire 9100/9200 prior to operation.

1. Upon receipt of your CrossFire 9100/9200, inspect the shipping carton for any damage that may have occurred during shipping. If the shipping carton shows any signs of external damage, notify your Olicom representative.

   If you have received your equipment before your site is fully prepared, after inspection, you should keep all of the components in the original shipping containers and store them in a physically and environmentally safe place.

2. Unpack the shipping carton and make sure you have received the following items:

   — One CrossFire 9100 or CrossFire 9200 ATM Switch

   — CrossFire 9177 ATM Switch Program Disks

   — Rack mounting bracket kit

   — A warranty card

   — CrossFire ATM Switch Series–Guide to Operations (DOC-6990)

   — CrossFire 9100/9200 Assembly Configuration and Test Sheet

   — CrossFire 9177 Release Notes

   — Power cable (U.S.)

   — Terminal cable

   — ESD wrist strap

Note: When unpacking the CrossFire 9100/9200, be sure to keep all original packing materials. You may need them for storing and transporting. All components returned under warranty should be shipped in their original packing materials.

3. Verify that you have received all the optional items ordered.
4. Read the *CrossFire 9177 Release Notes* for important information that could affect the installation and operation of the CrossFire 9100/9200.

Mounting Instructions

The CrossFire 9100/9200 ATM Switch can be mounted in a standard 19-inch rack or cabinet, or on any flat surface such as a tabletop. The installation area should be near a power source and should have enough room around the front and rear panels for cabling and access to controls. Use the following procedures to install the CrossFire 9200 ATM Switch.

Warning: Only trained and qualified personnel should be allowed to install or replace this equipment.

Warning: A fully configured switch weighs 20 kg (44 lbs.). To avoid injury or damage to the equipment, exercise caution when mounting the chassis.

Rack or Cabinet Mounting

If you install the equipment in a closed or multi-unit rack, observe the environmental guidelines described earlier.

Caution: The following rack mounting instructions need to be observed to ensure that the CrossFire 9100/9200 ATM Switch and any other equipment are mechanically stable.

The following procedure describes how to mount the switch in a rack or cabinet:

1. Remove the bracket covers on each side of the CrossFire 9100/9200 ATM Switch to expose the rack mounting brackets. Access to the retaining screws is obtained by opening the cap on the front of each bracket cover. See figure 17. Use the Allen key supplied with the switch to remove the two 6 mm Allen screws. When you have removed the screws, push the bracket cover towards the back of the switch and lift the cover off. Keep the screws for later use.

Note: Before starting the next step, be sure you have the proper hardware for mounting the chassis with the exposed brackets to your cabinet or rack.

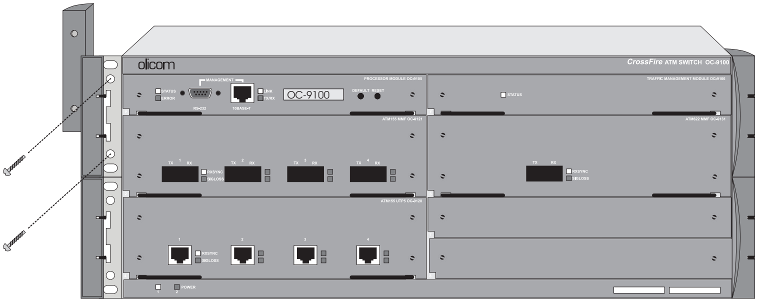


Figure 17. Removing the Bracket Covers to Expose the Rack Mounting Bracket

2. Position the switch, with the exposed mounting brackets, in the rack or cabinet and slide it up or down until the bracket holes line up with the rack holes. See Figure 17. Attach the chassis brackets to the rack using the Allen screws you removed in step 1 and the nuts supplied with the switch. Close the cap again to conceal the screws.

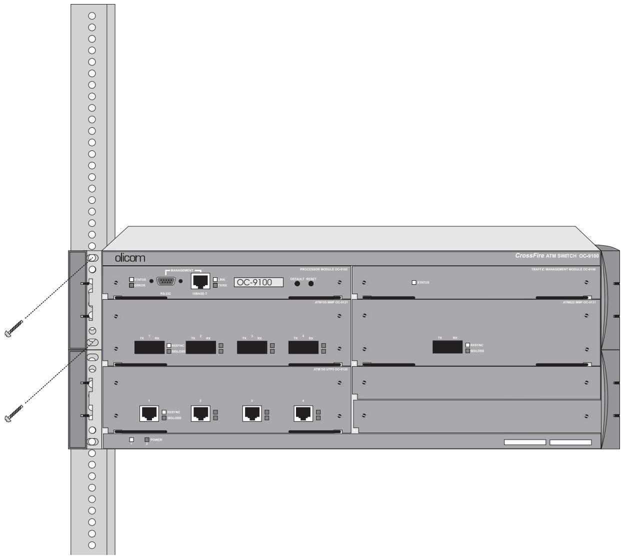


Figure 18. Mounting the CrossFire 9100/9200 ATM Switch in a Rack or Cabinet

Note: Only fixed brackets are supplied with the CrossFire 9100/9200 ATM Switch. If you want to install a sliding pull-out mount, you will need to provide the extra mounting hardware.

Table-Mounting

The CrossFire 9100/9200 ATM Switch operates at a low noise level, which makes it suitable for a work area or almost anywhere with a large enough flat surface such as a table, desktop, or similar area.

Four self adhesive pads are supplied with the switch. The pads must be mounted in the four recesses on the bottom of the switch. When the pads are mounted, simply place the switch on a clear, level location. Leave enough room around the switch for ventilation and access to the controls and cable connectors.

Caution: Due to weight constraints, place no more than two units (or the equivalent weight of other equipment) directly on top of another chassis. More than three units on top of another unit may cause damage to the lower unit.

CrossFire 9100/9200 Components

Power LEDs

The power LEDs are located on the lower left of the switch front panel. The LEDs indicate that the corresponding power supply unit is connected to a power outlet and that the power supply unit is functioning correctly.

MAC Address Label and Custom Label

The MAC address label is located on the lower right of the switch front panel, and contains the default MAC address of the switch. This address is used on the Ethernet port and in constructing the ATM address of the switch.

The custom label, also on the lower right of the switch front panel, can be used for any user defined purpose. Suggested uses are the switch IP address or a name you have assigned to the switch.

CrossFire 9205 Processor Module Front Panel

Most of the visual indicators are found on the Processor Module (see Figure 19). The objects on this module are, from left to right:

- Status and Error LEDs
- RS-232 connector for serial line management
- 10 Base-T connector for Ethernet management
- Link and Tx/Rx LEDs indicating the status of the Ethernet connection
- Alphanumeric display
- Default push button
- Reset push button

Each of these objects is described in greater detail below.

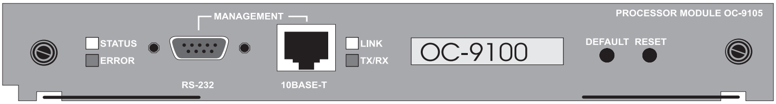


Figure 19. CrossFire 9205 Processor Module Front Panel

Status and Error LEDs

The Status and Error LEDs provide general information about the operation of the switch. The following table illustrates the meaning of the LEDs:

Status LED	Error LED	Meaning
Flashing	Flashing	Execution of internal bootstrap ROM
Flashing	Off	The switch is being initialized
On	Off	Normal operation
Off	On	Alphanumeric display does not work properly
On	On	An error is indicated in the alphanumeric display

Table 8. Status and Error LEDs

Management Connectors

The two connectors on the processor module provide access to the serial line and/or Ethernet based management functions.

Link and Tx/Rx LEDs

The Link and Tx/Rx (Transmit/Receive) LEDs provide information about the operation of the Ethernet connection. The Link LED is on when the switch is connected to an Ethernet; the Tx/Rx LED is on when there is activity on the Ethernet.

Alphanumeric Display

During normal operation, the alphanumeric display shows the system name that has been set by the management applications.

If an error occurs, the display switches between an alphabetic and a numeric error code. The details are given in Appendix B, "Errors and Status Messages".

Default and Reset Push Buttons

The push buttons can be operated using a thin pen or pencil.

Pressing the "Reset" push button resets the switch and forces it to restart its operation.

Pressing the "Default" push button resets the switch and forces it to restart with the default configuration. This button provides a fall-back capability in cases where the operator has lost the password or other communication parameters giving him or her access to control the switch, or the switch has been moved to another part of the network. Pressing "Default" will cause all the switch's configuration and status information stored in non-volatile memory to be set to default values. Therefore, the "Default" button should be used only as a last resort.

Pressing "Reset" and "Default" simultaneously resets the switch, reverts to the default configuration, and forces the switch to download its software from a BOOTP server. This function is intended as a last resort if faulty software has been loaded into the switch.

Powering On the CrossFire 9100/9200

The CrossFire 9100 and 9200 ATM Switch chassis do not have an on/off switch. Power is on when the unit is plugged into a power source.

There are no user serviceable parts inside the switch. Any internal upgrades or service should be performed by qualified personnel only.

Warning: When installing the unit, the ground connection must always be made first and disconnected last.

Warning: Do not touch the power supply when the power cord is connected. Line voltages are present within the power supply when the power cord is connected.

Use the following steps to power on your equipment:

1. Ensure that you are using the correct power source.
2. Using a power cable that complies with national regulations, plug the female end of the cable into the AC receptacle on the switch back panel.

   For North America the power cable must be UL listed, CSA labeled and consist of three AWG18 conductors with a maximum of 15 feet in length. Cable type must be SJT or SVT. The female receptacle of the cable must meet IEC320 requirements.
3. Plug the male end of the power cord(s) into a properly grounded electrical outlet.

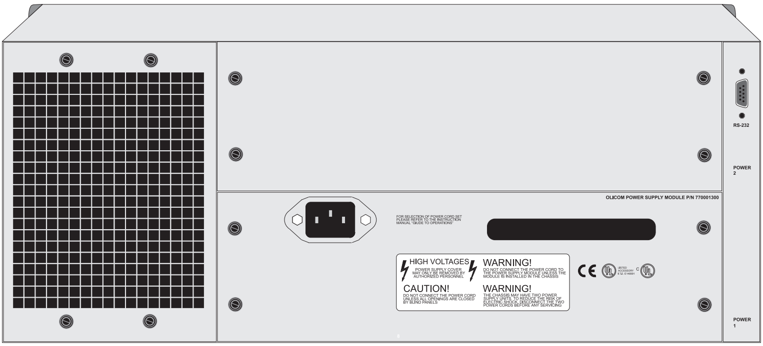


Figure 20. The AC Connector on the Power Supply Module

4. If your switch has two power supplies installed, verify that both power LEDs on the front panel are on. If your switch has only one power supply installed, verify that one of the power LEDs is on. If this is not the case, make sure the outlet is working properly.

5. When the CrossFire 9100/9200 ATM Switch powers on, the progress of the bootstrapping process is shown in the alphanumeric display. The Status LED also blinks to indicate software initialization. The initialization process takes about two minutes, after which the system name of the switch is displayed. The factory setting of this name can be “OC-9100”.

Note: If the switch is configured to the default configuration, which is the case with a new switch or after the Default button has been depressed, the alphanumeric display will alternate between “M03” and “DEFCONFI”.

Note: If the CrossFire 9100/9200 ATM Switch encounters an error during the start-up process, the alphanumeric display will show an error code.
See Appendix B for a listing of error codes and their meanings.

What’s Next

Now that you have mounted and powered-on your CrossFire 9100/9200 switch, continue to “Making Connections for CrossFire ATM Switches” on page 33. This section explains how to connect the appropriate network interface cable and a console to your switch.

Making Connections for CrossFire ATM Switches

After you set up your CrossFire ATM switch and go through the power on sequence, you must connect the proper interface cable and a console to your switch. This section explains how to connect both. Use the following table to go to the desired procedure.

To connect the...	Go to page...
OC-3 Interface	33
DS3 Interface	36
UTP Interface	37
Ethernet Interface	39
Console to a CrossFire 8008	41
Console to a CrossFire 9100/9200	42

Table 9. Connections for CrossFire ATM Switches

Throughout this section, when the connection interface is identical between the CrossFire 8008, 9100 and 9200, the front panel of the CrossFire 8008 is used as an example.

Connecting the OC-3 Interface

You can connect an OC-3 fiber optic cable to a CrossFire switch as follows:

Note: This section assumes you are using a square SC type connector. If you are using a round ST type connector, the Tx and Rx connections are not automatically aligned.

1. Remove the protective plugs from both the front of the OC-3 module and cable ends. Be sure to keep the plugs in case the equipment requires shipment.
2. Plug one end of the Duplex SC fiber optic cable into an OC-3 ATM interface on the CrossFire switch.

3. Plug the other end of the Duplex SC fiber optic cable into another ATM device. Cable ends are often clipped together to automatically align Tx and Rx fiber links properly.

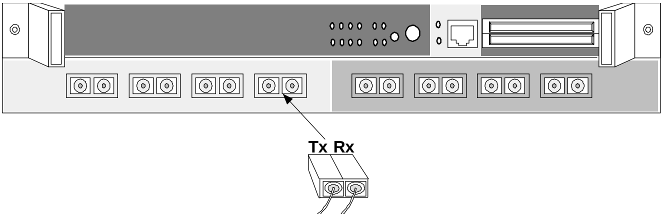


Figure 21. Connecting the OC-3 Interface Cable

Multi-mode OC-3 Cable Specifications	
Connector	Duplex SC
Type	62.5/125 micron (2 fibers)
Data Rate	155 Mbps

Table 10. Multi-mode OC-3 Cable Specifications

Single Mode OC-3 Cable Specifications	
Connector	Duplex ST
Type	8.3/125 micron (2 fibers)
Data Rate	155 Mbps

Table 11. Single Mode OC-3 Cable Specifications

Fiber Optic Cabling Specifications

A detector receiving power below or above its minimum or maximum sensitivities will cause transmission errors, or complete failure of the link.

Fiber Optic Connectors	Power Range
Multi-mode LED TX Power (both SC and ST connectors)	Min: -18.5 dBm Max: -14 dBm
Multi-mode Detector (RX) Sensitivity (both SC and ST connectors)	Min: -31 dBm Max: -14 dBm
Single-mode Intermediate Range TX Power (both SC and ST connectors)	Min: -15.2 dBm Max: -8 dBm Typical: -13 dBm
Single-mode Long Range TX Power (both SC and ST)	Min: -5.2 dBm Max: 0 dBm Typical: -3 dBm
Single-mode Detectors (RX) Sensitivity, all models	Min: -31 dBm Max: -5 dBm
Multi-mode RX	-14/-31
Single-mode TX	-8/-13/-15.2
Single-mode RX	-5/-31
Single-mode Long Range TX	0/-3/-5.2

Table 12. Fiber Optic Cable Specifications

Connecting the DS3 Interface

You can connect a DS3 interface to a CrossFire 8008 only. To connect the cable, complete these steps:

Note: You need two coax cables: one for Transmit (Tx) and one for Receive (Rx).

1. Connect the first coax cable BNC connector to the left BNC connector on the CrossFire 8008.
2. Connect the other end of the first coax cable to the Tx connector on another ATM device.
3. Connect the second coax cable BNC connector to the right BNC connector on the CrossFire 8008.
4. Connect the other end of the second coax cable to the Rx connector on the other ATM device.

Note: If you need to connect two CrossFire 8008s back-to-back, you must "Crossover" the Tx and Rx connections. Be sure to set one of the CrossFire 8008s to generate "Clock" and the other to "Loop Timed".

Note: Be sure to set the parameter for long or short coax cables using ClearSight or the `atm set ds3 <interface> cable long|short` console command.

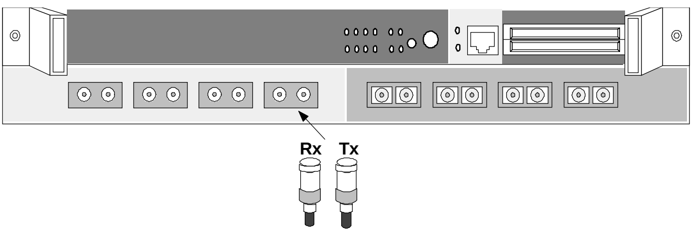


Figure 22. Connecting the DS3 Interface Cable

DS3 Cable Specifications

DS3 Cable Specifications	
Connector	BNC
Type	RG59u
Data Rate	44.736 Mbps
Max Length Min Length	500 m (approx.1640 feet) 6 m (approx. 20 feet)

Table 13. DS3 Cable Specifications

Connecting the UTP Interface

You can connect a UTP interface to either a CrossFire 8008 or a CrossFire 9100/9200. To do so, plug your UTP cable into any one of the UTP connectors on switch as shown in the illustration below.

Note: If you need to connect two CrossFire switches back-to-back, you must "Crossover" the Tx and Rx connections.

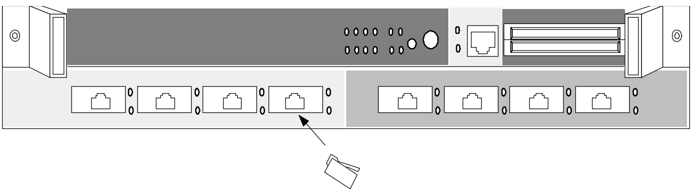


Figure 23. Connecting the UTP Interface Cable

UTP Cable Specifications

UTP Cable Specifications	
Connector	RJ-45
Type	CAT 5
Data Rate	155 Mbps
Max Length	150 m

Table 14. UTP Cable Specifications

UTP Cable Pinout

The “not used” pairs may transport non-interfering signals, providing the bit error rate of the pair in use is low.

Contact	Signal at the User Device MIC	Signal at the Network Equipment NIC
1	Transmit+	Receive+
2	Transmit-	Receive-
3	not used	not used
4	not used	not used
5	not used	not used
6	not used	not used
7	Receive+	Transmit+
8	Receive-	Transmit-

Table 15. UTP Contact Assignments

Connecting the Ethernet Interface

You can connect an Ethernet cable to a CrossFire switch as follows:

- If you are connecting directly to a 10 Base-T network, use a 10 Base-T straight-through cable. Connect one end to the CrossFire switch and the other end to the hub, repeater, or transceiver.
- If you are connecting to a media converter, or directly to an Ethernet station, use the 10 Base-T crossover cable shipped with the media converter. Connect one end to the CrossFire switch and the other end to the media converter. Follow the directions that came with the media converter for cabling from the converter to the network.

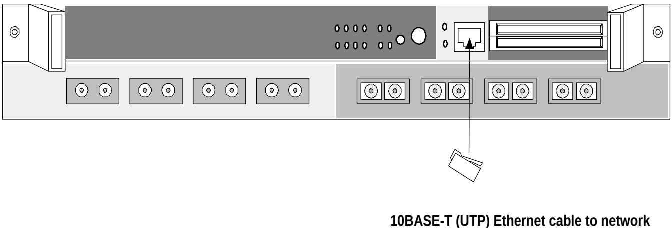


Figure 24. Connecting the Ethernet Interface Cable

Ethernet Cable Specifications	
Connector	RJ-45
Type	UTP (category 3, 4, & 5)
Data Rate	10Mbps
Max Length	100 meters
Maximum Network	4 repeaters

Table 16. Ethernet Cable Specifications

Connecting a Console to Your Switch

You can connect a console to your switch to use Olicom's ClearSight to configure and manage a CrossFire ATM switch. However, if ClearSight is not available you can use Olicom's Virtual Console feature.

A physical connection to the console port, on any installed module that supports a console, provides a logical connection to all other modules operating in the chassis. This enables you to use console commands through one physical console connection to configure some of the ATM parameters.

You can access a console using one of the following methods:

- Local console cable
- External modem
- Telnet session

Console Terminal Requirements	
Terminal type	ASCII, VT100 compatible
Baud rate	9600
Data bits	8
Stop bits	1
Parity	none

Table 17. Console Terminal Requirements

Connecting a Console to a CrossFire 8008

To connect a console to a CrossFire 8008 to use ClearSight or Virtual Console to configure and maintain an ATM switch, follow these steps:

1. Connect the console cable to the CrossFire 8008.
2. Connect the other end of the console cable to a console terminal.

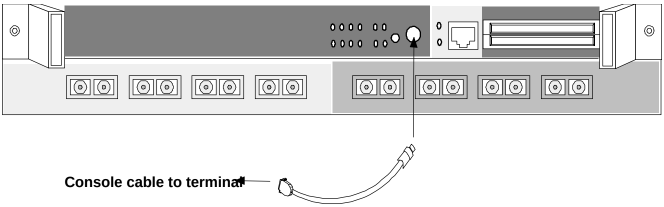


Figure 25. Attaching a Console to Your Switch

Console Cable Requirements	
Connector	DB-9 (female) to Phono Plug
Required Signals (DB-9)	Pin 1 - Gnd Pin 2 - Tx Pin 3 - Rx
Max Length	15 Meters

Table 18. Console Cable Requirements

Connecting a Console to a CrossFire 9100/9200

All cables connecting a Terminal/PC or a modem to the CrossFire 9100/9200 must at least connect the following RS-232 signals: RD (receive data), TD (transmit data), DCD (data carrier detect), DTR (data terminal ready), DSR (data set ready), RTS (request to send), CTS (clear to send) and SG (signal ground).

A modem can be connected to the CrossFire 9100/9200 using a standard serial cable as shown in Figure 26.

1: 9/25 pin male sub-D connector
2: 9 pin female sub-D connector

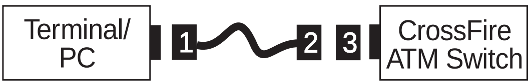
Figure 26. Modem to CrossFire 9100/9200 Connection

The CrossFire 9100/9200 is equipped with a 9 pin male Sub-D DTE connector. To connect a terminal - or a PC which is also equipped with male Sub-D DTE connectors - a special cable with connections similar to a null modem cable (Figure 25) or a standard cable and a null-modem adapter (Figure 22) is necessary.

.

1: 9 pin female sub-D connector
2: 9 pin female sub-D connector

Figure 27. Terminal/PC to CrossFire 9100/9200 Connection - 1



1: 9 pin female sub-D connector
2: 9 pin female sub-D connector
3: Null modem

Figure 28. Terminal/PC to CrossFire 9100/9200 Connection - 2

The null modem cable connections can be seen in Figure 29.

You can use a special cable with female Sub-D connectors at each end instead of a null-modem cable.

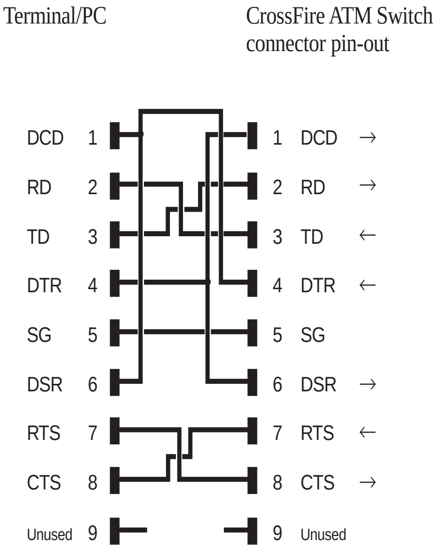


Figure 29. Null Modem Pin Connection

Note: The serial port on the CrossFire 9100/9200 may also be used for running the IP protocol. In this case, the text-based management application cannot be run directly through the serial port. However, when the switch is shipped, the serial line is by default set to be used by the text-based management application.

Accessing Other Modules in 8000 Chassis

1. To access a module other than the one you are physically connected to, type: **`ATTACH n`** where ***n*** is the slot number of the router module you want to access. The command returns a prompt indicating (in parentheses) the slot to which you are logically connected.
2. To return access to the module you are physically connected to, type: **`DETACH`** The command returns a prompt indicating (in parentheses) the slot to which you were physically connected to.

Troubleshooting a CrossFire ATM Switch

Once the Olicom ATM switch is powered on, most troubleshooting can be done by the network manager using ClearSight. This section describes the steps you can take at the local site to solve a problem or to assist the network manager in troubleshooting. It addresses how to identify and solve problems specific to an Olicom ATM Switch.

- For information about troubleshooting a problem with the CrossFire 8000 Chassis, refer to *Appendix A, CrossFire 8000 Chassis Maintenance*.
- For additional information about CrossFire 9100/9200 troubleshooting, please reference *Appendix B Error and Status Messages.*

To find out how to contact Technical Support, refer to: Contacting Technical Support in this manual.

The CrossFire 8008 Does Not Power-On

If the *PWR* indicator is not lit:

1. Verify there is power to the CrossFire 8000 Chassis.
2. Make sure the CrossFire 8008 is correctly inserted in the CrossFire 8000 Chassis.
3. Contact Olicom Technical Support if the problem persists. Refer to Chapter 8 for information about contacting Technical Support.

The Olicom ATM Switch Is Not Forwarding Cells

If the *ONL* indicator is flashing, but the LEDs associated with the connected interfaces are off:

1. Make sure you are using the proper cables. For cable information, refer to the configuration sheet and *Olicom Cable Specifications*.
2. Make sure the cables are properly connected.
3. Refer to one of the following sections for more detailed information:
   - No activity on the ATM Interface
   - No activity on an Ethernet Interface
4. Contact Olicom Network Services if the problem persists.

No Activity on the ATM Interface

For an OC-3 fiber connection:

1. Make sure the Duplex SC connectors are seated properly.
2. Make sure the fiber connectors are properly maintained with dust boots and are free from dirt.
3. Contact Olicom Network Services if the problem persists.

No Activity on the Ethernet Interface

If the activity indicator for an Ethernet interface is not blinking, or is blinking but packets are not being forwarded:

1. Check the Interface Status indicator associated with the Ethernet interface.

- If the indicator is not steadily lit, there is most likely a problem with a cable connection. Check all connections.
- If the indicator is steadily lit, and packets are not being forwarded, there is most likely a problem with another station on the Ethernet.

2. Contact Olicom Network Services if the problem persists.

Unexpected Line, Section, or Path Errors

If statistics indicate an abnormal or unexpected number of errors on a particular interface, for example Header Checksum Errors, Line Errors, or Path Errors, check the following:

1. For OC-3 single or multi mode fiber cables, be sure the “fiber plant loss budget” is figured into the receive sensitivity of the interface. Too much or too little optical power can cause cell loss and other errors. Be especially aware of OC-3 single-mode connections, as an alternator may be required.
2. For DS3 cables, be sure to set the cable length parameter correctly. For DS3 cables less than 20 meters long, use **SHORT-CABLE**. For DS3 cables longer than 20 meters, use **LONG-CABLE**.
3. For all fiber cables, be sure the optics are clean and the connectors are properly installed.

❑

3. ATM Concepts

This is a reference chapter you can use to learn about ATM. Use this chapter to become more familiar with ATM concepts, or to learn about a specific topics before you change your ATM switch configuration.

Sections

- ATM Architecture
- Virtual Connections
- ATM Switching Concepts
- ATM Traffic
- Available Bit Rate (ABR)

ATM Architecture

ATM functionality corresponds to the Physical Layer and a portion of the Data Link Layer of the Open Systems Interconnection (OSI) Reference Model (Figure 30). However, it should be noted that the suite of protocols used to create ATM based networks are often referred to as “ATM”. In this case, ATM can have components that may be considered part of other layers in the OSI Reference Model. For instance, “signaling” functions may be part of the network layer.

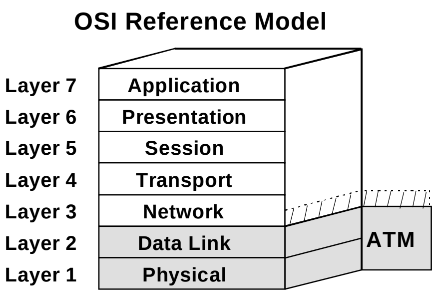


Figure 30. ATM and the OSI Reference Model

The ATM protocol functionality must be implemented in both user equipment, like end systems, and network elements, such as ATM switches. The network does not know anything about the end-to-end application that is running over an ATM connection after the connection has been setup.

The basic service of an ATM network is the transport and switching of ATM *cells* (Figure 31). An ATM cell has 48 bytes, or octets, of payload called the *Information Field*, and a five octet header. While the information field is available to the user, the header contains information to forward the cell to its destination.

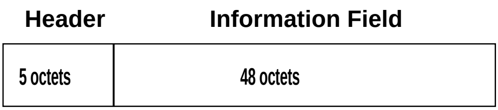


Figure 31. ATM Cell

All ATM cells are the same size, unlike Frame Relay and LAN systems in which data packets can vary in size.

The ATM cell header contains VPI/VCI information that is used in switching decisions at each node. This header information determines which physical interface the cell is output to. All possible connection topologies can be implemented within this switching architecture, including:

- Point–to–Point
- Point–to–Multipoint

ATM Protocols

In today's communication systems, a layered approach is used for the organization of communication functions. The functions of the layers, and the relationship of each layer to the other layers, are shown in the ATM Protocol Reference Model as shown below.

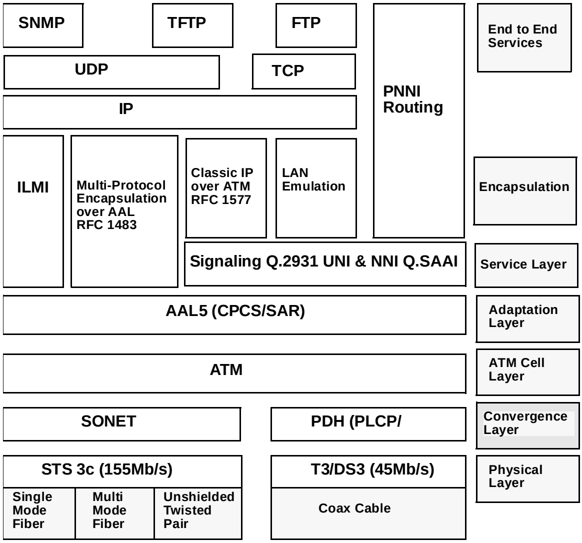


Figure 32. ATM Protocol Reference Model

Physical Layer

The Physical Layer defines the electrical, mechanical, procedural and functional specifications for activating, maintaining, and deactivating the physical link between end-systems. This layer is further divided in two sublayers: the transmission convergence sublayer and the physical medium dependent sublayer.

The transmission convergence sublayer performs the following functions:

- Generation and recovery of the transmission frame
- Cell framing and recovery
- Bit timing
- Header error control sequence generation

The physical medium dependent sublayer provides the bit transmission capability, including bit alignment, line coding, and electrical/optical conversion. Media that currently supports ATM includes:

- OC-3 – A Synchronous Optical Network (SONET) based fiber-optic User Network Interface operating at 155.52 Mbits/sec on either of the following cable types:
  - — Single Mode Fiber
  - — Multi-Mode Fiber
- OC-12 – A Synchronous Optical Network (SONET) based fiber-optic User Network Interface operating at 622 Mbits/sec on either of the following cable types:
  - — Single Mode Fiber
  - — Multi-Mode Fiber
- DS3 – A Digital Signal Level 3 based coaxial cable User Network Interface operating at 44 Mbits/sec.
- UTP – Unshielded Twisted Pair a cable based User Network Interface operating at either of the following rates:
  - — 155 Mbit Sonet

ATM Layer

The ATM Layer provides for the transport of fixed-size cells between the end-points of a virtual connection. The ATM Layer also provides multiplexing functions to allow the establishment of multiple connections across a single user network interface.

The ATM Layer performs the following functions:

- In the transmit direction, ATM cells from individual virtual channels are multiplexed across one interface.
- At the receiving end, the cell demultiplexing function splits the arriving cell streams into individual cell flows appropriate to the virtual channel.

ATM cells are identified and switched by means of the label in the ATM cell header. The header of a UNI cell is shown in Figure 33. The header of an NNI cell is shown in Figure 34. The table following Figure 34 explains each header component. The principle difference between a UNI and an NNI header is the presence of a 4-bit Generic Flow Control (GFC) field in the UNI header. The NNI header replaces the GFC fields with 4 additional VPI bits.

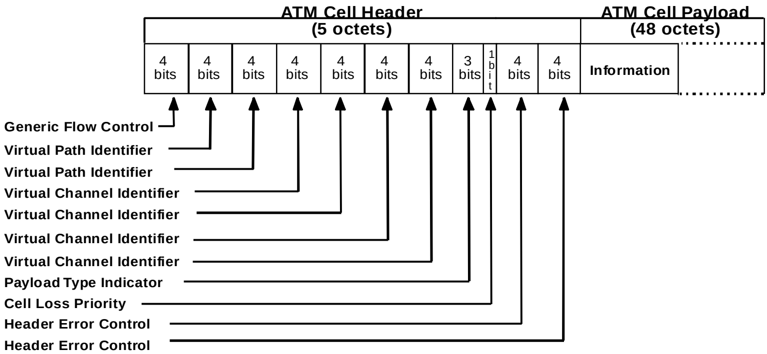


Figure 33. UNI ATM Cell Header Labels

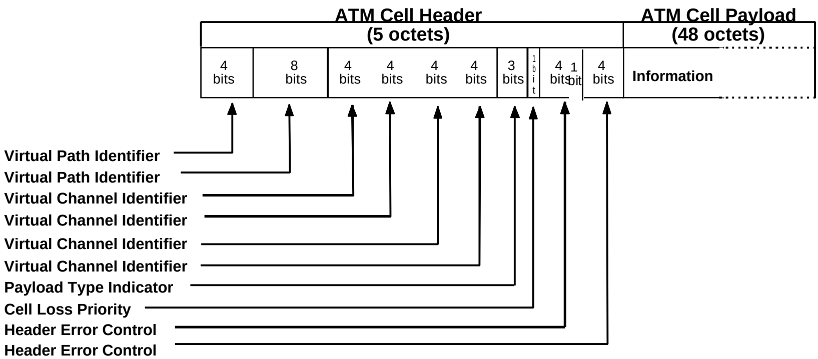


Figure 34. NNI ATM Cell Header Labels

Field	Description
Generic Flow Control (GFC)	Provides for different connections to use the same User Network Interface (UNI). The GFC used on a UNI in an ATM network must work to control the flow of cells across a data connection as well as other types of connections. It is generic, not specific to traffic type.
Virtual Path Identifier (VPI)	Identifies virtual paths between users, or users and networks. The actual number of routing bits in the VPI subfield used for routing is negotiated between the user and the network.
Virtual Channel Identifier (VCI)	Identifies virtual channels between users, or users and networks. The actual number of routing bits in the VCI subfield used for routing is negotiated between the user and the network.
Payload Type Indicator (PTI)	Indicates the type of information in the payload area, such as user and network information. It also contains an indicator to show that a cell experienced congestion while traveling through the network (EFCI). It is also used by AAL5 to indicate end of packet.
Cell Loss Priority (CLP)	Indicates the relative priority of the cell. Lower priority cells are discarded before higher priority cells during congested intervals.
Header Error Control (HEC)	Provides information for error detection and correction of single bit errors. It can also be used for cell delineation.

Table 19. Fields Description

ATM Adaptation Layer (AAL)

The ATM Adaptation Layer (AAL) runs from the end system and is transparent to the ATM network. The AAL is organized into two logical sublayers:

- Convergence sublayer
- Segmentation and Reassembly sublayer

The Convergence sublayer provides the enhanced adaptation of services provided by the ATM Layer to the requirements of the upper layers.

The Segmentation and Reassembly sublayer provides segmentation of upper layer information into a size suitable for the information field of an ATM cell, and reassembly of the contents of ATM cell information fields into upper layer information.

Figure 35 shows the positioning of the AAL in regards to a typical ATM LAN.

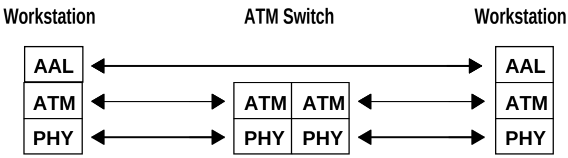


Figure 35. ATM Adaptation Layer (AAL)

There are several AAL types:

- *Type 1* provides timing information for delay- sensitive services, such as voice. Provides constant bit rate service for real-time voice and video applications.
- *Type 2* Currently not used, being redefined for potentially low speed ATM.
- *Type 3/4* provides multiplexing of common data services, not widely used.
- *Type 5* provides simple data service with no multiplexing.

The International Telecommunications Union-Telecommunications Sub-Section (ITU-T) has defined certain service classifications based on how bits are transmitted, the required bandwidth, and the types of connections required:

- Class A – Constant bit rate audio (for example 64Kbps digital voice)
- Class B – Variable bit rate (VBR) compressed video and audio
- Class C – Connection-oriented data transfer (for example Frame Relay over ATM)
- Class D – Connectionless data transfer such as CCITT.364 (SMDS) over ATM

Figure 36 summarizes the basic service classifications of the AAL Layer.

CLASS	A	B	C	D
CLOCK	Required		Not Required	
BIT RATE	Constant	Variable		
CONNECTION MODE	Connection Oriented			Connectionless

Figure 36. AAL Layer Service Classes

Virtual Connections

Virtual Connections (VCs) are composed of Virtual Channels and Virtual Paths. These Virtual Paths and Virtual Channels are used in ATM to route cells between a source and a destination.

A **Virtual Channel** is a bidirectional communication channel that transports ATM cells sequentially between two end points. Each end point uses a Virtual Channel Identifier (VCI) to identify the communication channel.

A **Virtual Path** is a group of Virtual Channels that share the same bidirectional communication channel and are assigned the same Virtual Path Identifier (VPI). Fundamentally, a Virtual Path allows an indeterminate number of Virtual Channels to be cross-connected at once.

A **Physical Link** contains one or more Virtual Paths.

Figure 37 shows the relation between a Virtual Path and Virtual Channels.

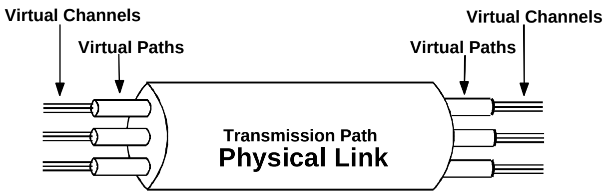


Figure 37. Virtual Connections

You can use a highway analogy to show the difference between a physical link, a virtual path, and virtual channels. A highway (physical link) has several lanes, or virtual paths. Cars (ATM traffic) travel over these virtual paths and follow a different set of directions to arrive at the same point.

When an ATM switch receives a cell on an incoming port, it looks at the cell’s header. This header information along with the switch’s routing table determines which outgoing port should forward the cell, and how the switch should set the VPI/ VCI values in the outgoing cell. There are two ways to route the cell; virtual channel switching, or virtual path switching.

Virtual Channel Switching

Virtual Channel switching is the method of switching cells on each virtual channel independently. A Virtual Channel Connection (VCC) is a set of serially cross connected Virtual Channel Links (VCL) that provide a path between two ATM devices that are physically connected to each other. Every VCL is identified by a pair of numbers called VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). This VPI/VCI pair of numbers is a local identifier. The two ATM devices directly attached over a physical wire/fiber/cable need to know (or agree on) this local identifier.

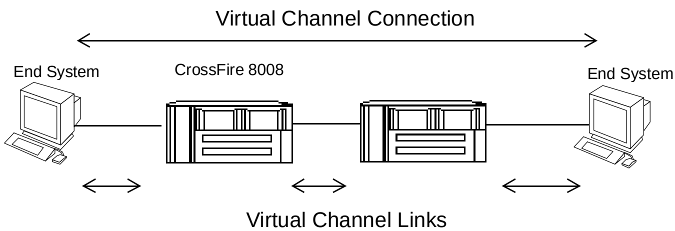


Figure 38. Virtual Channel Connection

With Virtual Channel Switching, the virtual channels are *cross connected* to different virtual channel. In figure 39, virtual channels 1 and 3 are switched to different virtual channel. This figure shows how cells come into a switch with a VPI/VCI value (such as VPI-6/VCI-3) and leave the switch with a new VPI/VCI value (VPI-15/VCI-19).

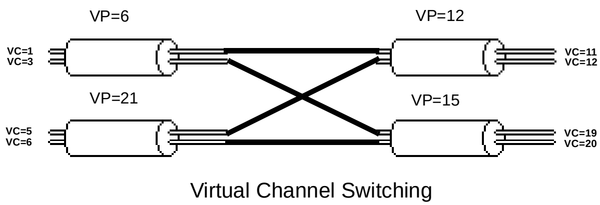


Figure 39. Virtual Channel Switching

Virtual Path Switching

Virtual Path switching is the method of switching cells with the same VPI (Virtual Path Identifier) to the same output port. A Virtual Path Connection (VPC) is a set of serially cross connected Virtual Path Links (VPL) that provide a path between two ATM devices that are physically connected to each other. When cells arrive at the switch connected to the destination end system, the switch routes the cells based on the VPI value.

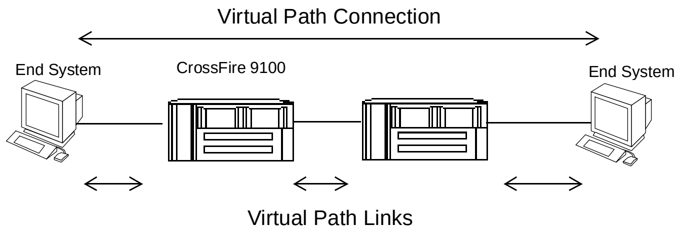


Figure 40. Virtual Path Connection

With Virtual Path Switching, figure 41 shows that all cells arriving on virtual path 6 are switched to virtual path 12, regardless of the VCI assiged to the cells. Once the cells arrive at the destination virtual path, the switch uses the VCI value to route the cells to the destination end system.

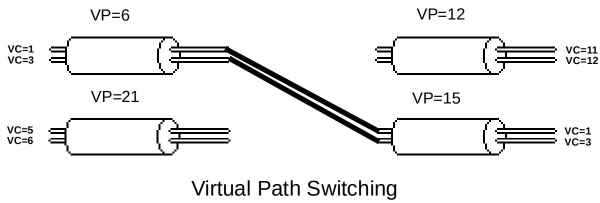


Figure 41. Virtual Path Switching

Cross Connections

The fundamental function of an ATM switch cross-connecting Virtual Connections is to accept a cell on an interface with a particular VPI/VCI identifier and forward that cell onto another interface with a new VPI/VCI identifier. The fundamental function of an ATM switch cross-connecting Virtual Paths is to accept a cell arriving on a Virtual Path Link with a particular VPI/VCI identifier and forward that cell onto another interface with a new VPI but the same VCI.

Permanent Virtual Connection (PVC)

A PVC is a provisioned virtual connection that is *permanently* available to transmit and receive cells. A Switched Virtual Connection, on the other hand, is dynamically created when an end system needs to transmit cells and is released when transmission ends.

For ATM networks, or portions of networks where the connectivity is essentially static, the configuration of PVCs and Permanent Virtual Paths (PVPs) is a straightforward and reliable mechanism. With PVCs and PVPs, there is no call setup procedure and the Quality of Service (QoS) parameters are defined when you lease the line from a carrier.

PVC links are defined manually by the network administrator, and are usually preserved in non-volatile memory. A PVC is constructed by **cross-connecting** VCC links *switch by switch* and *hop by hop* until a complete path from an end system to a destination(s) is achieved.

Switched Virtual Connection (SVC)

In contrast, SVCs are dynamically created and released as required by ATM end systems. End systems identify one another using a 20-byte ATM address (see page 62 for more information about an ATM address). A SVC is constructed when an end system **signals** through a network of ATM switches that a connection is desired. ATM switches automatically create the intermediate cross-connections required as the requested call is **routed** towards the specified destination end system(s). Quality of Service (QoS) paramters are negotiated during the call setup process.

ATM Switching Concepts

Sending ATM cells along a Permanent Virtual Circuit to an end system is easy because the system administrator has already defined all the PVC links along the way. The ATM cell leaves the sending switch with a destination VPI/VCI value in the header and each switch along the way knows exactly where to send it because the information exists in the switch's routing tables.

Sending ATM cells along a Switched Virtual Circuit is identical to using PVCs, except the call establishment is dynamic and not statically created by a network administrator. With SVCs, the switches set up the virtual connection during the call establishment process. When the connection between the sending system and the end system is complete, bandwidth is assigned to the user and the ATM cells are transmitted.

SVC Call Setup Process

In general, SVC signaling works as follows. Suppose there are two end systems (system1 and system 2) attached to an ATM switch and that system1 is going to setup a connection (a "call") to system 2. Before system1 can forward a Setup message, it must meet the following conditions:

- It must check its own status and determined that it can reserve the resources necessary to support the requested call's QoS parameters. This is accomplished through the CAC (Call Admission Control) algorithm. See page 63 for information about CAC.
- It must know through which port to forward the message. The switch maintains tables of addresses (and summary addresses) that show through which port particular addresses (or groups of address in the case of summary addresses) may be reached. Switches share this information over NNI links (such as PNNI). Or, this information can be manually configured over UNI links using IISP (Interim Inter Switch Protocol) or PNNI (Private Network-Network Interface). UNI, NNI, PNNI, and IISP are discussed in Chapter 4.

If system1 can support the QoS parameters and knows which port to forward the message through, it can start the signaling procedure. This involves the following steps:

- System1 transmits a Call Setup message over UNI to the switch. The message contains information about the requested call, including the ATM address of the device system1 wants to talk to, as well as requested QoS (Quality of Service) parameters for the call.

- The switch receives the Call Setup message and optionally returns a Call Proceeding message to system1 to inform system1 that it is capable of delivering the Setup message to the ATM address included in the Setup (the address of system 2) and that it can support the QoS parameters requested.
- The switch forwards the Setup message to system 2. System 2 checks its own condition to determine whether it is capable of the requested call. If it is capable, it (after a few intermediary steps) sends a Connect message back through the switch (or set of switches) which is delivered to system1. If system 2 is not capable of the call, it returns a Release Complete message to the switch which routes it back through the network to system1.

Cell Switching

The operation of an ATM switch is very simple. ATM cells arrive on an ATM switch's interface containing a particular Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) pair in its 5-byte header. This information uniquely identifies a traffic stream, or Virtual Channel (VC) to the ATM switch. If the ATM switch has been programmed to recognize and forward that particular stream, the ATM switch causes a new cell to be emitted on an output interface with a new VPI/VCI value. In short, an ATM switch cross-connects VCs. Figure 42 shows an ATM cell stream.

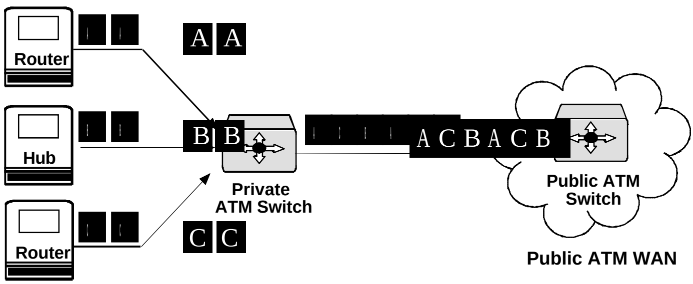


Figure 42. ATM Cell Stream

A connection table determines which output port to transfer the cell to and what VPI/VCI value should be in the cell header when it leaves the ATM switch. The connection table is organized by input port and VPI/VCI value (see Table 17). Entries on the connection table are created either manually through the use of Permanent Virtual Connections or Permanent Virtual Paths or automatically through the use of Switched Virtual Connections or Switched Virtual Paths upon request of an end system. When Switched Virtual Connections or Switched Virtual Paths are used, the connection is first routed through the ATM network (using either PNNI, CNNI, or IISP) and then locally routed at the end station to the proper application.

Figure 43 illustrates that there can be many virtual connections through an ATM switch. This is accomplished by the connection table within the ATM switch. The connection table associates a VPI/VCI value and a port number with another port number and VPI/VCI value.

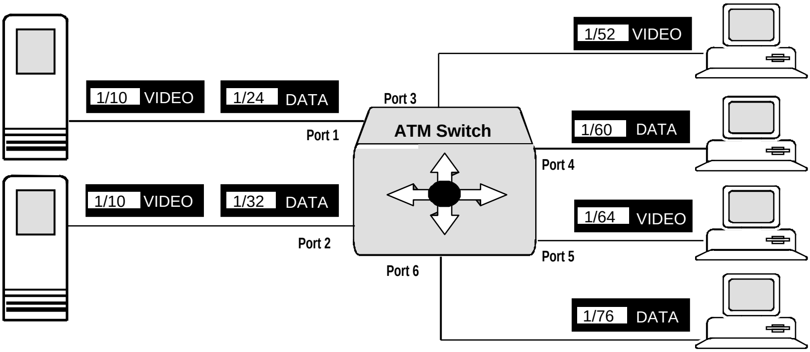


Figure 43. ATM Switching

The connection table for the ATM switch in Figure 43 would look like the following:

Port	VPI/VCI	Port	VPI/VCI
1 (VIDEO)	1/10	3 (VIDEO)	1/52
1 (DATA)	1/24	4 (DATA)	1/60
2 (VIDEO)	1/10	5 (VIDEO)	1/64
2 (DATA)	1/32	6 (DATA)	1/76

Table 20. Connection Table for the ATM Switch

Addressing

There are two types of ATM addresses; one format for ATM private networks, and one for ATM public networks. *ATM private network addresses* are commonly used for a company's private ATM network, while an *ATM public network address* would be used for an ATM public service provider.

ATM Private Network Address

An ATM private network address is always 20 bytes long and has three components:

- A Network Prefix (up to 13 bytes)
- An End System Identifier (6 bytes, normally an Ethernet MAC address)
- A Selector byte

The Network Prefix is generally assigned by the ATM switch and can carry topological information for an interswitch routing protocol. The end system identifier and selector byte is provided by the end-system. An end-system may use many ATM addresses to distinguish among different applications and services running on the end-system.

An end system informs its adjacent ATM Switch that it will accept calls for a particular ATM address by **registering** the address using the Integrated Local Management Interface (ILMI).

The UNI Management Entity **(UME)** exists on each directly connected ATM interface (such as those on an end-station and a CrossFire ATM switch) that communicate and negotiate their respective addresses, UNI services, and other signaling parameters. **ILMI** is an SNMP-based protocol for exchanging this information (particularly ATM addresses and network prefixes) between an adjacent switch and an end-system.

ATM Public Network Address

An ATM public network address is an E.164 address that is defined by ITU-T.

ATM Traffic

ATM has been designed from the start to solve many of the old traffic management problems. It enables traffic to be differentiated based on individual needs.

If you are using Available Bit Rate (ABR), ATM enables a fair allocation of bandwidth by requiring users to adjust their transmission rates according to feedback from the network.

To provide different levels of performance, the ATM standard specifies five categories of service:

- **Constant Bit Rate** (CBR) for fixed dedicated bandwidth – for example, to emulate a leased line.
- **real-time Variable Bit Rate** (rt-VBR) for high-priority communication that require a specific delivery rate, such as voice or video.
- **non-real-time Variable Bit Rate** (nrt-VBR) for high-priority communication that is not sensitive to variable time-delays.
- **Available Bit Rate** (ABR) for standard file transfers – the network makes no absolute guarantee for cell delivery, but a minimum rate of transmission is guaranteed, and cell loss is minimized.
- **Unspecified Bit Rate** (UBR) for low-priority tasks such as file transfers or print jobs. No guarantees on transmission speed are made.

When two stations on an ATM network begin a transaction, they establish an end-to-end connection, which is called a “virtual connection.” The level of service is established during the connection phase according to the requirements of the transmission and the capacity and load on the network at the time.

ATM reserves capacity to supply guaranteed bandwidth services (CBR and VBR). The remaining bandwidth is shared fairly between all other users (as ABR and UBR services). ABR and UBR services are used for carrying LAN traffic across the network.

Call Admission Control

The process by which a switch determines whether it can support a set of QoS parameters is called CAC (Call Admission Control). It guarantees the switch will not agree to a new connection unless it can support the configured QoS parameters.

Olicom ATM switches use the cell rates in the traffic profile (see next section) to ensure that no ATM interface is inadvertently over-subscribed. However, you can deliberately over-subscribe or under-subscribe an ATM interface by setting the interface’s capacity parameter. By default, the interface capacity parameter is that of the physical device. For example, OC-3 is approximately 350,000 cells/second.

Figure 44 shows two virtual channels each using 100 Mbps of bandwidth. The originating path and the terminating path must have at least 200 Mbps of bandwidth allocated to prevent cells from being rejected. In Figure 44, cells from virtual channel labeled A are forwarded while cells from virtual channel B are prevented from establishing the channel set-up since the terminating path has only 155 Mbps.

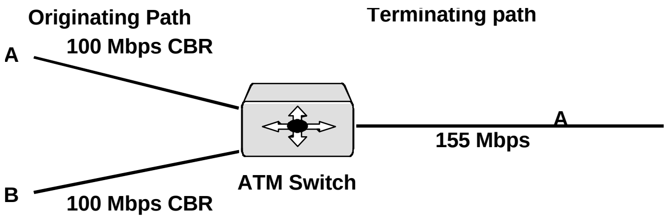


Figure 44. Bandwidth Allocation

Due to its bursty nature, over-committing bandwidth on an interface is not a problem for data traffic. However, when an interface is over committed and cells are dropped, the number of *frames* that are dropped is amplified. A frame is usually several ATM cells, and a single dropped or erred cell ruins the entire frame.

Note: You need to be very careful when over-subscribing an interface. Only over-subscribe an interface when you are certain that network traffic bursts greater than the total interface bandwidth are infrequent.

Partial Packet Discard

Another feature designed to maximize the efficiency of the CrossFire ATM switches is Partial Packet Discard for AAL5 frames. The switches can be configured to detect when one cell of the AAL5 frame that is passing through is corrupted beyond repair or lost. In this instance, the switch can discard all remaining cells in the frame. This does not interrupt end-to-end data transmission because the missing cell(s) would have caused the receiving AAL5 process to request retransmission of the entire frame. The benefit of Partial Packet Discard is that the remaining cells are discarded and bandwidth and resources are not used unnecessarily.

Cell Loss Priority

The ATM cell header also contains a field used to indicate that a particular cell is relatively unimportant. Switches should discard these cells before cells of higher importance are discarded.

This field is the one-bit Cell Loss Priority (CLP) field.

Output Buffers – Common Core Access Point

The CrossFire ATM switches are output buffered switches which guarantee wire speed performance on all receive ports. When more cells are offered to a transmit port than the port can handle, excess cells are buffered in the 32,000 cell memory (8008 and 9100 have 16,000 cell memory). For each transmit port, there are four queues where excess transmit cells are buffered, with the queues corresponding to ATM services categories (see “ATM Traffic” on page 63for more information about the service categories).

Traffic Profiles

The traffic expected in a particular direction, and/or permitted on a VC or VP, is described by a set of parameters, including Traffic Categories and one or more traffic rate parameters. Olicom groups these traffic parameters by creating Traffic Profiles that can be referenced by a single *Traffic Profiles Index* number.

The set of traffic rate parameters needed to describe a VC’s traffic profile depends on the Traffic Category parameter associated with the VC. The Olicom ATM switches ensure that all of the relevant VC or VP traffic parameters are compatible before allowing them to be cross-connected.

Olicom ATM switches support two predefined permanent traffic profiles (indexed 99 and 100); Constant Bit Rate (CBR) and real-time Variable Bit Rate (rt-VBR). To connect a CrossFire 8011/F Router or CrossFire 8005 Ethernet ATM Edge Switch through a CrossFire 8008, a VC must be specified on the device, as well as on the correct CrossFire 8008 interface.

A VC specified on a CrossFire 8011/F Router or CrossFire 8005 Ethernet ATM Edge Switch must use a traffic profile that is consistent with the traffic profile specified on a destination VC, such as a VC on a CrossFire 8008.

A switch dynamically assigns a Traffic Profile and category to a SVC.

Note: For detailed information on CrossFire 8008/9100/9200 traffic configuration see “Using Console Commands” on page 83.

Traffic Categories

Each Virtual Channel Connection (VCC) has a set of traffic characteristics which are composed of bandwidth parameters, Quality of Service (QoS) Class parameters, and priority parameters. Virtual Channel Links (VCL) and Virtual Path Connections (VPC) use the traffic characteristics that have been assiged to the VCC with which they are associated. Even though VCCs are bi-directional, the traffic characteristics may not be the same in both directions, although they can be.

Traffic Categories guarantee support for data, voice, and video simultaneously. The Olicom ATM switches offer a Traffic Categories guarantee using a four-queue priority mechanism. Managers can configure any Traffic Profile to use one of the four priority queues. Below is a sample configuration which would assign sensitive voice/video traffic a higher priority over data traffic.

Traffic Profiles Parameters	Priority Queue	Typical Use
Constant Bit Rate (CBR)	1	Real-time Voice and Video
real-time Variable Bit Rate (rt-VBR)	2	Variable Rate Video
Variable Bit Rate (VBR)	3	Client/Server
Available Bit Rate (ABR)	3	Data
Unspecified Bit Rate (UBR)	4	Data

Table 21. Traffic Profiles

When cells arrive with a higher priority Virtual Channel or Virtual Path, these cells are transmitted ahead of cells destined for lower priority Virtual Channels or Virtual Paths, regardless of how long the other cells have been waiting.

Available Bit Rate (ABR)

The ATM Forum has chosen a rate-based approach to provide flow control for Available Bit Rate (ABR) traffic. The data rate on ABR connections is dynamically controlled within the network. This is known as a *closed loop*, meaning the end station originating the call, every switch which the call traverses, and the destination end station all participate in setting the data rate of the ABR connection. Rate-based flow control uses the following method:

- After every Nth data cell, the source sends a forward Resource Management (RM) cell, which includes data rate and congestion information.
  N is typically 32.
- When the forward RM cell reaches the destination, it is turned around and sent back to the source as a backward RM cell. The destination can update any field in the RM cell. The destination does this to inform the source it is experiencing congestion.
- The ATM switches, which the RM cell traverses can also modify the cell to indicate congestion or a rate change. None of the switches can increase the values; the smallest value (signifying the weakest link) is passed to the source.
- When the source receives the RM cell it originated, the source modifies the rate of the connection. If congestion was encountered, the rate is decreased. If no congestion, the rate will be increased. Lastly, an explicit rate may be contained in the RM cell; the switch will use it as the new data rate for the ABR connection.
- For each ABR connection, there are actually two control loops of RM cells. Both ends of the connection originate forward RM cells.
- Olicom implements the Explicit Rate Control algorithm, in which the CrossFire 9100/9200 calculates the exact rate for each connection. The calculation takes into account the number of active connections on a link, the overload factor, and the rate increase or decrease. This method ensures a fair share for each connection, no queue build-up within the CrossFire 9100/9200, and efficient link utilization.

ABR Flow Control Schemes

To implement ABR services effectively, a flow-control feedback loop is required between the ATM network and the user. This enables sending stations to be alerted when the network is congested. The ATM Forum has defined two different approaches to this flow control challenge; Explicit Forward Congestion Indication (EFCI Bit) and Explicit Rate. Always use Explicit Rate when every device in the VC’s path supports ABR, and you are using a 9100/9200 with the Traffic Management module. However, use EFCI if Explicit Rate is not available.

ABR Explicit Rate

The Explicit Rate scheme makes use of a special Resource Management (RM) cell, which is inserted periodically into the data stream. The ATM switch sends the RM cell the full length of the virtual connection, from sending to receiving station and back again.

The destination station and each of the intermediate switches mark down the rate (the explicit rate allocated to the virtual circuit) in the returning RM cell. The slowest rate is therefore the value in the cell when it reaches the source. The source may then use this rate for subsequent transmissions until a new RM cell is returned. The RM cell is a standard 53-byte ATM cell, which is typically inserted after every 32nd data cell.

Explicit Forward Congestion Indicator (EFCI)

If an ATM switch experiences congestion, it can use EFCI to inform downstream ATM switches and the destination station by changing the Payload Type Indicator (PTI) field in the cell headers to “1”. The destination station reads the congestion indicators and tell the appropriate source to adjust its traffic rate. You can only use this method for traffic that can be flow patrolled on a higher protocol layer.

The advantage of EFCI flow control is that it is simple to implement in the ATM switches. The disadvantages are that the response time is dependent upon the load on the network, and the flow is not controlled by the lower layers of the transport protocols.

❑

4. Supported ATM Protocols

Signaling enables an ATM end-system to communicate across a network to a destination end-system via the use of protocols. This chapter describes the protocols used to move ATM cells to an end-system.

Sections

- ATM Signaling Protocols
- ATM Internetworking Protocols
- ATM Inter-Switch Routing Protocols

ATM Signaling Protocols

The UNI, NNI, and ILMI ATM signaling protocols are part of the ATM Layer (see page 50 for details). Remember that the ATM Layer is responsible for establishing connections and passing cells through an ATM network. The main function of the UNI, NNI, and ILMI protocols is to help set up a virtual channel across an ATM network to an end system when a request is made.

User Network Interface (UNI) and Network to Network Interface (NNI)

UNI 4.0, UNI 3.0, and UNI 3.1 are versions of the User Network Interface signaling protocol defined by the ATM Forum. This protocol is used between an ATM end system (for example CrossFire 8600 Router) and an ATM switch on an ATM network.

You can use ATM within public and private networks. There are two distinct types of ATM User Network Interfaces (UNIs) public and private.

- UNI: Public – Connects an ATM user with an ATM switch deployed in a public service provider’s network.
- UNI: Private – Interconnects an ATM user with an ATM switch that is part of a private, corporate network. A private UNI is often located in the same building as the user device.

ATM is based on the concept of two end-stations communicating via a set of intermediate switches. This includes both the UNI and the ATM Network to Network Interface (NNI). The UNI links an end-user device and a public or private ATM switch. The NNI is used on a link between two ATM switches.

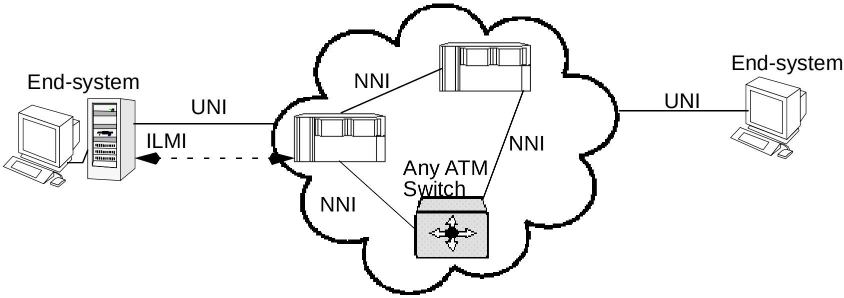


Figure 45. UNI and NNI Links

In the case of public ATM service, the UNI connects the customer premise equipment's interface to a public ATM switch. User devices can have connectivity to multiple ATM switches, however each interface must have a unique network address. Figure 46 shows an Enterprise ATM Network using both UNIs and NNIs.

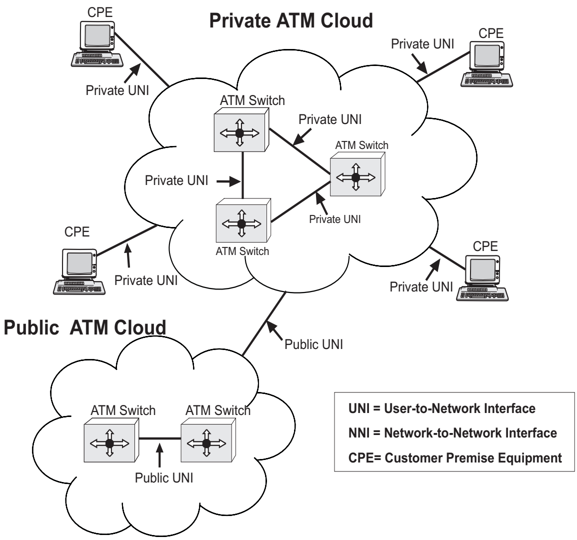


Figure 46. Enterprise ATM Network

Because ATM is a connection-oriented network, a connection between two end-points begins when one transmits a signaling request across the UNI to the network. A device responsible for signaling then passes the signal across the network to its destination. If the destination end system agrees to the connection, a virtual channel is set up across the ATM network between the two systems. Both UNIs contain mappings so the switches can route the cells correctly.

Integrated Local Management Interface (ILMI)

ILMI is an ATM Forum protocol used on UNI links (see Figure 45). The ATM switch uses this protocol to:

- Obtain the ATM address network prefix for an ATM device from the network
- Register the ATM address of each ATM device attached through a UNI link
- Query the end system to determine the maximum number of VPI and VCI bits it supports
- Query the end system to determine if the device is using UNI or NNI.
  - If the end system is using UNI, the switch also detects the UNI version (UNI 3.0, UNI 3.1, or UNI 4.0) and sets its own port accordingly. If the switch and the end system both support multiple versions, they agree to use the highest mutually supported versions.
  - If the end system is using NNI, the switch sets its own port to PNNI. See the PNNI description starting on page 78.
- Detect errors on the UNI links
- Detect a change in an attachment point; meaning is an ATM end system still connected to the same neighbor, or has the point of attachment changed.

ATM Internetworking Protocols

The CLIP and LANE protocols run on LANE Bridges (such as Olicom's CrossFire 8600 Bridge) that connect LANs to an ATM network. These protocols allow interoperability between installed LANs (and WANs) and ATM networks by mapping the Media Access Control (MAC) address to an ATM address.

Classical IP Over ATM (CLIP)

When you connect an Ethernet or Token Ring LAN to an ATM network, you need a way to map IP addresses to ATM addresses. RFC 1577 defines how to run Classical IP (or CLIP) over ATM. To achieve the address mapping or resolution, the CLIP protocol uses an ATM network as if it were an IP subnet. This subnet is referred to as a *Logical IP Subnet* (LIS). A LIS consists of a group of IP nodes that connect to the same ATM network and belong to the same IP subnet.

Within each LIS, you define one device as an ATMARP server and the rest of the nodes as LIS clients. While configuring the ATMARP server, you need to define which IP subnet the server is servicing. The function of the ATMARP server is to map IP addresses to ATM addresses for the associated clients in the LIS.

Each LIS client is configured with the ATM address of the ATMARP server. When a client within the LIS comes up, the first thing it does is establish a SVC to the ATMARP server (using the configured ATMARP server address). The ATMARP server enters the client's IP and associated ATM address in it's routing table. When the client wants to transmit data, it queries the server for the ATM address of the IP client. Once the SVC is set up between the client and end system, they can exchange information.

LAN Emulation (LANE)

LAN Emulation makes an ATM network look and behave like an extension to an Ethernet or Token Ring network. LANE is designed to support IEEE 802.3 Ethernet and IEEE 802.5 Token Ring LANs.

The basic functions of LANE are to:

- Resolve the destination MAC address into the appropriate destination ATM address.
- Segment a LAN packet into multiple ATM cells (with re-assembly at the receiving end).
- Create, use, and remove Switched Virtual Connections as necessary.
- Transmit broadcast packets to all members of the Emulated LAN.

LANE divides an ATM network into Emulated LANs (ELANs). These ELANs operate independently, but can communicate with one another through bridges and routers. Hosts and edge devices in an ELAN are referred to as LANE Clients (LECs). Within each ELAN there is a Configuration Server (LECS), a LANE Server (LES), and a Broadcast and Unknown Server (BUS). Note that multiple ELANS can share the same LECS, LES, or BUS devices.

The LECS assigns clients in an ATM network to different ELANs, the LES is responsible for mapping MAC addresses to ATM addresses, and the BUS receives all the broadcast/multicast traffic and redistributes it to all members of the ELAN. The following paragraphs explain the LEC, LECS, LES, and Bus in more detail.

Note: Unlike the CrossFire 9100/9200, the CrossFire 8008 does not have an embedded LANE Server. Your network requires an 8009 or a 9100/9200 to support LANE.

LAN Emulation Client (LEC)

One function of the LEC is to provide a LAN-like service to upper layer protocols while providing an interface to the ATM network. The LEC handles the job of interacting with the ATM network and transmitting LAN packets as ATM cells. (The LEC also receives cells from the ATM network, reassembles them into a LAN packet, and hands the packet up the protocol stack to the upper level protocols.) Each LEC has a unique ATM address and at least one MAC address.

A LEC joins an Emulated LAN (ELAN), either Ethernet or Token Ring, by contacting a LANE Server (LES) using the ATM address provided by the LANE Configuration Server (LECS). A LECS can also be bypassed by directly configuring the LEC with the ATM address of the correct LES. (See below for information on LECS and LES).

If a LEC is part of an ATM LAN bridge, it can represent several LAN stations with their own corresponding MAC addresses.

Proxy LEC

A Proxy LEC typically resides in a bridge or router. It is called a *proxy* because it is capable of representing many – perhaps thousands – of MAC addresses in the ELAN. For instance, suppose a transparent bridge joins the ELAN. On the non-ATM side of the bridge there are 100 MAC addresses. If a device in the ELAN wants to forward a MAC frame to one of those MAC addresses, it must first obtain the ATM address of the bridge LEC to set up an SVC to carry the frame as far as the bridge. In this sense the bridge ATM address is a proxy – a stand in – for the MAC address on the far side.

In a Source Route bridged environment, the LEC translation table associates the Route Descriptor of the next hop after the ELAN with the ATM address of the bridge LEC that is responsible for receiving and forwarding the frame. Each hop in a Source Route environment is uniquely identified by the concatenation of a 12-bit (three hex character) segment number and a 4-bit (one hex character) bridge ID.

LAN Emulation Servers

As noted, LANE depends on a set of software entities that provide key services. The services are requested by LANE Clients residing in edge devices or hosts of the ATM network.

The three additional LANE entities are:

- LANE Configuration Server (LECS) – defines the parameters for the emulated LAN (ELAN) and the members of the ELAN.
- LANE Server (LES) – keeps track of MAC addresses and ATM addresses for address resolution.
- Broadcast and Unknown Server (BUS) – Provides broadcast and multicast services and helps handle unknown addresses.

Every emulated LAN has one and only one each of the three entities above – but it has many LECs, and there can be many ELANs simultaneously operating. Each edge node can be a member of more than one ELAN, but the edge node requires a LEC for each LAN.

The three LANE server functions are all implemented in a single CrossFire ATM switch. A basic LANE topology with a CrossFire 9200 server and three edge nodes is shown in Figure 47.

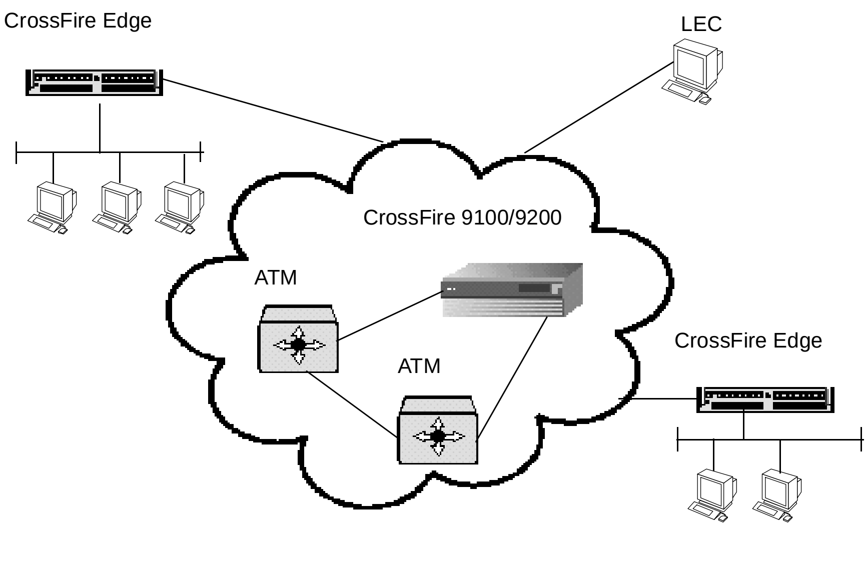


Figure 47. CrossFire ATM Switch with LANE Server

LAN Emulation Configuration Server (LECS)

The LANE Configuration Server assigns LANE clients (LECs) to the correct emulated LANs, and provides LECs with the values of configured parameters, such as type of emulated LAN (Ethernet or Token-Ring) and maximum frame size.

The LECS has a well-known ATM address that LANE clients (LECs) use when they first join an ELAN (Emulated LAN). The LECS receives the configuration request from the LEC. The LECS then returns the ATM address of the LANE Server (LES) that manages the ELAN the LEC wants to join. Regardless of the number of ELANs present, only a single LECS is needed to provide the ATM address of the LES associated with each ELAN.

Note: The well-known LECS ATM address assigned by the ATM Forum is: 47.0079000000000000000000000.00A03E000001.00

LAN Emulation Server (LES)

There is one LES per ELAN and each LES is identified by a unique ATM address. The LES keeps track of the ATM addresses (and MAC addresses) of all ELAN members. When a LEC wants to set up a SVC to another LEC, it provides the MAC address of the destination to the LES, and the LES returns the relevant ATM address, allowing SVC setup, or distributes the request to the other ELAN members so they can respond.

Note: The CrossFire 9100/9200 can support up to 32 ELANs because you can configure up to 32 logical LESs in each ATM switch.

Broadcast and Unknown Server (BUS)

The Broadcast and Unknown Server provides two important services:

- It applies the broadcast and multicast capabilities of a LAN to the point-to-point connection structure of the ATM network
- It also supplements the LES for unknown destinations by broadcasting unknown packets to all LANE clients on the ELAN

Each LEC is connected to only one BUS per ELAN. The BUS to which a LEC connects is identified by a unique ATM address. In the LES, this unique ATM address is associated with a broadcast MAC address. Each ELAN consists of a LES/BUS pair.

ATM Inter-Switch Routing Protocols

Inter-switch routing is the process by which an ATM switch, in conjunction with other ATM switches, determines the sequence of hops (the path) through the ATM network that should be created in response to a **switched** virtual channel (or path) signaling request. In this mode of ATM switch operation, the ATM network elements are required to cooperate in establishing, maintaining and dismantling Virtual Channels and Paths, as required by end-system applications. SVCs depend on:

- **Signaling** - ATM devices communicate that a Virtual Channel (or Path) is requested (or rejected).
- **UME/ILMI** - ATM end systems and switches exchange ATM addressing and other information.
- **Routing** - A network of ATM switches determine the path a Virtual Channel connection should traverse.

To allow multi-vendor ATM networks to work together, the ATM Forum produced a very simple interim routing specification called **IISP** (Interim Inter-Switch Signaling Protocol), which requires users to manually configure the “routing database” on each switch.

Later on, the ATM Forum produced the Private Network to Network Interface (PNNI) inter-switch routing protocol, which has its roots in OSPF, a Layer 3 routing protocol.

Olicom has implemented IISP, PNNI

Interim Interswitch Protocol (IISP)

Olicom’s CrossFire 8008/9100/9200 software implements Inter-switch Signaling Protocol (IISP) to allow interoperation with IISP switches from other vendors (Figure 48).

IISP has limited functionality. In its simplest terms, IISP is a manually configured UNI without ILMI. Using IISP requires manual configuration of the address tables in each switch in the network. The configured address tables are used to forward only the appropriate SVC signaling requests to another ATM switch (also running IISP on its interface). Configuring the address tables can be laborious and inaccurate because IISP has no detection/prevention of routing loops.

.

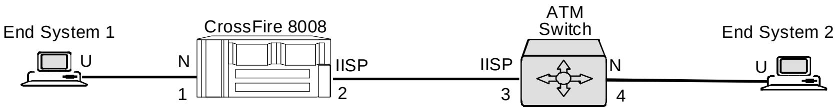


Figure 48. Connecting CrossFire 8008 to Other Vendor's Switches

In Figure 48, IISP requires that the CrossFire 8008 be manually configured to know that End System 2 is reachable via its interface 2, and that the other switch be configured to know that End System 1 is reachable via its interface 3. End systems are identified by their 20 byte ATM address.

Using hierarchical ATM addressing, you can specify many end systems by a "group address" (similar to an ATM network prefix). Therefore, you can specify many end systems with a single entry in the switch's connection table.

Private Network to Network Interface (PNNI)

ATM networks rely on some form of NNI (network-to-network interface) protocol to communicate between switches and to establish routes across the ATM network. PNNI is the routing protocol defined by the ATM Forum. Some of the reasons to use PNNI are:

- PNNI is an approved standard that allows interoperability between vendors' ATM switches
- Scales well to very large networks when hiearchy is implemented
- Saves resources by choosing a single path, and allocates resources over this path exclusively
- Well defined management information base (MIB) makes it easy to manage and monitor switches

How PNNI Works

PNNI creates SVCs with two protocols. The first protocol distributes topology information between switches and clusters of switches to compute the best path between two endpoints. The second protocol defines the signaling used to create point-to-point and point-to-multipoint connections.

Every new call takes the form of a Setup message that contains the requested QoS parameters for the call, as well as the ATM address of the called end system. When a switch receives such a Setup message over a UNI connection, it:

- Looks up the destination address in PNNI tables
- Chooses the path that best fits the QoS request from the set of possible paths
- Writes the path into the Setup message and forwards the message

Each switch along the way determines whether it can support the requested QoS parameters and, if it can, reserves the necessary resources for the call and forwards the Setup message along the path specified. As noted previously, the process by which a switch determines whether it can support a set of QoS parameters is called Connection Admission Control (see page 58).

The first switch – the switch connected to the source end system over a UNI link – is responsible for generating the path through the network. This path consists of a series of nodes. Each node can represent either a physical switch or a network of switches. Thus, the path generated by the first switch must be correct, but it may contain generic portions that switches will make specific farther along the path. ATM switches along the SVC cannot change this path. This ensures that loops are not introduced in the call establishment process.

If a switch along the way cannot support the requested QoS parameters – if its CAC process rejects the call – it returns the Setup message backwards along the path to a switch closer to the beginning of the path. The switch to which the Setup message is returned chooses another path from its set of possible paths and forwards the Setup message along. This process of finding a new route is called *crank back*.

If a route through the network that satisfies the QoS request is not found, the source end system is informed that the call cannot be completed. If a route through the network that satisfied the QoS request is found, the Setup message reaches the destination end system. If that system can also support the QoS request, it returns a connect message back along the same path. As this message returns through the network, the switches lock in the resources needed for the call (VPI and VCI values, as well as buffers to support the QoS parameters).

Peer Groups

Switches using PNNI are organized into *peer groups*. Peer groups consist of a set of switches that have the same *peer group ID*.

PNNI switches send *Hello messages* out each port and thereby discover any neighboring PNNI switches they are connected to. These Hello messages contain, among other items, the switch's peer group ID. This allows connected switches to determine if they are in the same or in different peer groups. (The Hello protocol is used by switches that are physically attached, as well as by switches that are attached through special SVC's).

Switches that are in the same peer group exchange complete information about all ATM addresses, switches and links inside the peer group. After these exchanges, every switch in the peer group has identical and complete information about all paths in the peer group, as well as the states of all switches in the peer group. As conditions change or as links come up or go down, switches continuously update each other. So, even in changing network conditions, all switches in a peer group maintain an identical view of the peer group.

PNNI runs best when the addressing scheme reflects the nework topology. You can simplify network configuration if you assign all switches in a peer group (network) an address that starts with the same unique 9 octet prefix. This eliminates the need to configure node and peer group IDs individually.

Note: Olicom switches are all shipped with the same 9 octet prefix already configured. This means that Olicom switches are already set up to be in the same peer group.

In addition, if network prefixes configured for a particular switch are the same for all its ports and unique among different switches, all reachability information can be contained in the default summary. This decreases the volume of service traffic between switches.

Peer Group Levels

Peer groups are defined by a specified number of bits in the switch's ATM address prefix (the address prefix is the first 13 bytes of the switch's ATM address). Thirteen bytes equals 104 bits, so there are 104 possible *peer group levels* in PNNI. For example:

- You can specify a peer group that is defined by the first 16 bits of the switch's ATM address. That peer group is said to be in level 16.
- You can specify a peer group that is defined by the first 104 bits of the switch's ATM address. That peer group is said to be in level 104.

Note: The CrossFire ATM switches support five peer group levels. These five peer groups can be defined using any level between one and 104 (including one and 104). That is, you can define a total of five peer groups in any one switch using different numbers of the first 104 bits of the switch's ATM address.

Two Peer Group Examples

Suppose you have two switches that are connected, and the switches' peer groups are defined as follows:

	Level	Beginning of ATM address in hex	Peers?
Switch 1	24	39.11.22…	No
Switch 2	24	39.11.33…	

Table 22. Two Peer Group Examples

Switch 1 and Switch 2 use the Hello protocol to exchange their peer group ID's and determine that they are not in the same group. (The first 24 bits of their ATM addresses are not the same.) Because the switches are not in the same group, they do not exchange full information about their knowledge of their peer groups with each other. Switch 1 and Switch 2 form a link called an *outside link*.

Now, suppose you have two switches that are connected, and the switches' peer groups are defined as follows:

	Level	Beginning of ATM address in hex	Peers?
Switch 1	32	39.11.22.33…	Yes
Switch 2	32	39.11.22.33…	

Table 23. Outside Link Connection

Switch 1 and Switch 2 use the Hello protocol to exchange their peer group ID's and determine that they are in the same group. (The first 32 bits of their ATM addresses are the same.) Because the switches are in the same group, they exchange information about this peer group with each other. This information is used to route Setup messages according to QoS requests in or through the peer group. Switch 1 and Switch 2 form a link called a *horizontal link*.

By default CrossFire ATM switches are predefined to be members of level 72. That means that the first 72 bits of all CrossFire ATM switches are used to determine the switch's peer group ID. By default, all CrossFire switches' ATM addresses have the same first 72 bits. Therefore, by default, CrossFire ATM switches are in the same peer group at level 72.

Separating Two Dynamically Routed PNNI Networks

Note: You can use an IISP link to separate two dynamically routed PNNI networks. An ATM service provider may use PNNI to route SVCs, and a local network manager can also use PNNI to route SVCs. Because the service provider would want to limit the scope of its PNNI network, an IISP link would be used between the two PNNI networks.

❑

5. Using Console Commands

This chapter provides information about using console commands to manage your CrossFire ATM Switch. You can also use ClearSight, a graphical interface to configure and manage your switch. To configure all the parameters on your switch, use Clearsight. The console commands are limited to commands that you might use to maintain your switch or do a minor change.

Sections

- Supported Console Commands
- Entering ATM Commands on Your Console
- General System Commands
- Rebooting Your Switch
- Modifying the Baud Rate
- ATM Interface Commands
- Configuring Traffic Descriptors
- Configuring the BridgeID Broadcast Feature
- Configuring the IISP Port
- Configuring Classical IP Over ATM (CLIP)
- Configuring LAN Emulation Client (LEC)
- Configuring Q.SAAL
- Configuring SNMP over Serial Links Protocol (SLIP)
- Proxy User Mode Configuration
- LAN Emulation Console Commands
- Using the Call Out Feature
- Using the Call Back Feature
- SNMP Management Commands
- LAA Console Commands

Supported Console Commands

Several console commands have been implemented to let you enter commands instead of using ClearSight. The following table lists the available console commands.

Topic	Command	See page
General System Commands	`system set <options>`	94
	`system show <options>`	96
	`system delete <options>`	
Reboot Commands	`system reboot`	97
	`system hboot`	97
	`system mboot`	97
Serial Interface Commands	`baud set <options>`	98
	`baud show`	98
ATM Interface Commands	`atm show <options>`	99
	`atm stop <interface>`	101
	`atm start <interface>`	101
	`atm cycle <interface>`	101
	`atm test <interface>`	101
PVC Command	`atm create pvc <options>`	102
PVP Command	`atm create pvp <options>`	103
VPLP Command	`atm create vplp <options>`	103
Deleting Virtual Connections	`atm delete <options>`	104
Address Prefix Command	`atm set prefix <prefix in hex>`	104

Topic	Command	See page
DS3 Parameters	atm set ds3<interface><options>	104
Traffic Descriptor Commands	atm trafficdesc show <options>	108
	atm trafficdesc set <options>	114
	atm trafficdesc activate	118
	atm trafficdesc delete <descriptor index>	118
BridgeID Broadcast	bridgeid set <options>	119
	bridgeid show	119
IISP Port Commands	ume disable <interface>	120
	ume add address <interface> <address>	120
	ume set addr_reg <options>	121
	ume show	121
CLIP Interface Commands	clip server set <options>	122
	clip client set <options>	122
	clip server show	122
	clip client show	122
Proxy User Commands	signaling set <options>	127
	signaling show <options>	127
	signaling clear <options>	127
LAN Emulation Console Commands	lane <options>	129
LANE Services Commands	lane services <options>	129
Super ELAN Commands	lane set lesbusid	129
	lane show lesbusid	129

Topic	Command	See page
ELAN Commands	`lane show elan`	130
	`lane set elan`	130
Call Out Commands	`call out <options>`	131
Call Back Commands	`call back <options>`	132
SNMP Management Commands	`snmp add <options>`	133
	`snmp set <options>`	133
	`snmp show <options>`	133
	`snmp delete <options>`	133
LAA Console Commands	`system show laa`	135
	`system set <mac>`	135
	`system delete laa`	135
LEC	`lec set <options>`	123
	`lec show <options>`	124
Q.SAAL	`link set ifIndex <options>`	125
	`link show ifIndex <options>`	125
SLIP	`slip set <options>`	126
	`slip show`	126

Table 24. Console Commands

Entering ATM Commands on Your Console

This chapter describes the command line interface for managing and configuring your switch. This line oriented user interface is available through:

- The Console Serial Interface Port on the switch. This port uses a small microphone jack connector for the CrossFire 8008 or a DB-9 connector for the CrossFire 9100/9200.
- Telnet via the switch Management Ethernet Port. The switch has a UTP Ethernet interface for out–of–band management and configuration using IP. You can “Telnet” to a switch via the Ethernet Management Interface and create a console session via TCP/IP. You can also use the Ethernet management interface for SNMP access via a network management tool, such as Olicom’s ClearSight.

Multiple console interfaces can be running simultaneously. This is useful when several people are monitoring the switch. However, it can become a problem if more than one person is configuring a switch simultaneously.

Note: If you are using Olicom’s ClearSight graphical user interface to configure and manage the switch, refer to the ClearSight Documentation Set.

Getting Started

The switch commands use the following syntax:

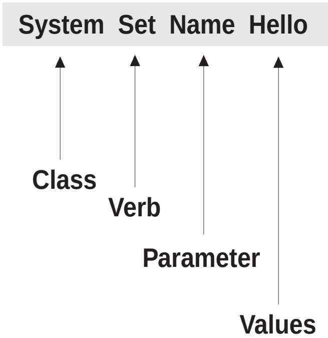
```
<class> <verb> {locator} {parameter} {{value} {<value|value>}}
```

Note: Tokens surrounded by “<” and “>” are mandatory, tokens surrounded by “{” and “}” are optional. Tokens with bars between listed values specify the only entries allowed by a locator, parameter, or another value, such as ON|OFF.

1. The first word, or *token*, in a command line is the command *class*, or *object*. The command class is a category of related commands.
2. The second token in the command line is a *verb*. It defines the action to be performed by the command. The most common verbs are `show` and `set`.
3. The third token in the command line is most often a *locator*. A locator further defines the class or object, specifying which interface, device, or other entity is to be acted upon.
4. The final tokens in the command line are *parameters* and *values*. Typing the parameter followed by a question mark (?) provides context sensitive help showing what value is expected.

The following example changes the system name of the switch. As the prompt consists of the system name it too will be changed. On the CrossFire 9100/9200, the display on the front panel will also reflect the system name.

```
prompt> system set name hello
```



Command Line Editing

A set of editing commands allows you to modify a command line. For example, you can display the previous command, delete characters forward or backward, type in the new, modified command, and execute the command. The following table explains the line editing commands.

Note: These are standard UNIX line editing commands. The ^ stands for the Ctrl key

.

Key Strokes	Action
<tab> or ?	If you have typed a fragment of a token, the token is completed. If you are between tokens, a list of all available subsequent tokens is displayed.
^p (or up arrow)	Scrolls backwards through the list of previous commands.
^n (or down arrow)	Scrolls forward through the list of previous commands.
^f (or right arrow)	Moves the cursor forward one character.
^b (or left arrow)	Moves the cursor backward one character.
^e	Moves the cursor to the end of the line.
^a	Moves the cursor to the beginning of the line.
^d	Deletes the next character.
Back space	Deletes a character.
^k	Deletes (kills) all characters from the cursor to the end of the line.
^u	Removes all characters on the line leaving just the command prompt.

Table 25. Editing Commands

Classes

Classes, or object tokens, indicate the general category for a command.

Class	Description
system	Commands related to generic system functions, such as passwords, date and time, and non–volatile parameter storage.
baud	Lets you modify the baud rate for you switch.
atm	Commands related to the ATM Layer. These commands are used for creating, deleting, and displaying Virtual Channels, Virtual Paths, cross connections, and ATM Layer interface parameters.
bridgeid	Lets you set the BridgeID broadcast feature.
clip	Commands related to the Classical IP over ATM protocol.
signaling	Commands related to manipulating signaling parameters.
ume	Commands related to manipulating UNI Management Entity (UME) parameters.
snmp	Commands related to the Simple Network Management Protocol (SNMP).

Table 26. Class Description

Verbs

Verbs specify the action the switch command executes.

Verb	Description
show	Displays information.
start	Enables an interface on a switch.
stop	Disables an interface on a switch.
cycle	Stops and restarts an interface on a switch.
test	Puts an interface on an ATM switch into test mode.
clear	Clears an interface on a switch.
set	Sets or modifies specified parameters.
create	Creates a new connection, Virtual Circuit, Virtual Path, and so on.
delete	Deletes an existing connection, Virtual Circuit, Virtual Path.
add	Adds a new connection, Virtual Circuit, Virtual Path, and so on.

Table 27. Verb Description

Locators

Locators designate the specific item to be acted upon by the switch command. For example, **port 3** is the locator in the following example:

```
olicom atm switch>atm start 3
```

The following table shows some of the locators used in ATM console commands.

Locator	Selects
interface <n>	An ATM interface.
vc <i vpi vci>	A Virtual Circuit for the specified interface.
vp <i vpi>	A Virtual Path for the specified interface.
traffic <n>	A Traffic Profile.

Table 28. Locators Designated Item

Parameters

Parameters designate a particular feature(s) that is available for a given class and locator. In the following example, **`name`** is the parameter. The command sets the system name to `Marketing`.

```
prompt> system set name marketing
```

Typing a parameter followed by a question mark (?) provides context sensitive help showing what value should be entered immediately following the parameter.

Values

Values further define the parameter entered on a command line. Context sensitive help showing what value should be entered immediately following a parameter is available by typing the parameter followed by a question mark (?).

Console Help

You can enter a question mark (?) at any time to see a list of all valid switch commands for the level under which you are currently operating. For example, entering just a ? provides a list of all command *classes*. Entering a class name, such as **system**, followed by a ? provides a list of all verbs that can be used in the **system** command.

Password Protection

The current values of all parameters can be displayed at any time from any command line console session. However, values can only be changed after entering **ACCESS mode WRITE**.

Note: The default password for the Olicom ATM switch is ‘AaBbCcDd’.

You can enter **ACCESS mode WRITE** by entering the following command:

```
prompt> system set access write
```

You are then prompted for the write access permission password.

General System Commands

The CrossFire ATM system commands are used to set and show ATM system parameters, such as passwords, location, and system IP address.

```
SYSTEM SET <options>
```

For example, `system set ip address 128.100.104.016` sets the IP address for the ATM switch.

Option	Description
`time <mm/dd/yy{:hh:mm}>`	System date and time
`name <string>`	System name – you can enter a string of 1 to 32 ASCII characters. Only A to Z, and 0 to 9 are supported. Example: `system set name 8008_marketing`
`location <string>`	Location of your switch. You can enter a string of 1 to 32 ASCII characters. Only A to Z, and 0 to 9 are supported.
`contact <string>`	Person to contact in case of switch problems. You can enter a string of 1 to 32 ASCII characters. Only A to Z, and 0 to 9 are supported.
`access <none | write>`	System access mode. Write mode requires a write permission password (you are prompted for the password). Default is none.
`password <string>`	System write permission password – you can enter a string of 1 to 32 ASCII characters. Only A to Z, and 0 to 9 are supported Default is AaBbCcDd.

Option	Description

`ip <address|mask|gateway>`	System IP Address, mask, and default gateway. The system prompts you for each address.
	
	IP addresses are entered by typing four integers between 0 and 255 inclusive, separated by periods; for example nnn.nnn.nnn.nnn.
	
	Examples:
	`system set ip address 128.100.104.016`
	`system set ip mask 255.255.000.000`
	`system set ip gateway 128.100.250.020`

`tftp/bootp <host_ip|filename |start>`	host_ip – sets the TFTP host IP address. Use the format nnn.nnn.nnn.nnn.
	
	filename – sets the TFTP filename. Use the format filename.extension.
	
	start – initiates a TFTP transfer.
	
	Example:
	`system set tftp host_ip 128.100.104.016`
	`system set tftp filename test.mcf`
	`system set tftp start`

`image <current|test>`	current <image_#> – indicates the image to use for the next boot. test <image_#> – indicates the image to boot once for the next boot.
`diagnostics <on|off>`	Sets the diagnostics feature for the ATM switch on and off.
`laa <mac_address>`	sets mac address of Locally Administrated Address (see LAA Console Commands for details)

Table 29. General System Commands

System Show Command

The `system show` command lets you view information that you entered using the `system set` command.

```
system show time|name|location|contact|address|ip|version|
     tftp/bootp|diagnostics| laa
```

If you enter `system show version`, you see output similar to the following:

```
Olicom Crossfire ATM Switch
ROM Revision:                  5.00.00
Olicos Revision:               05.00.99.09 - ECO
Level:                         X
```

ROM Revision–indicates the version of firmware running on your switch.

Olicos Revision–indicates the version of software running on your switch. Olicos stands for Olicom Operating System.

ECO Level–indicates a patch version of software that may be running on your switch if you requested a feature modification for your particular network environment. “X” as shown in the example above indicates that there are no patches installed on your switch.

System Delete Command

```
system delete laa
```

Deletes Locally Administrated Address of the switch (see LAA Console Commands for details).

Rebooting Your Switch

There are three console commands for rebooting your system.

System Reboot Command

The `system reboot` command causes the ATM switch to reboot as if power had been cycled. The switch uses the settings stored in non-volatile memory when rebooting.

System Hboot Command

The `system hboot` command causes the ATM switch to clear its non-volatile storage, and reboot as if the system were being booted for the first time. When rebooting, the switch replaces the user setting in non-volatile memory with the factory default settings.

Note: The `system hboot` command permanently erases all parameter and configuration information stored in non-volatile memory.

System Mboot Command

Use the `system mboot` command to do a total reboot and uses bootp to get the most current software image.

Modifying the Baud Rate

To modify the baud rate for the ATM switch, use the following command:

```
baud set <baud_rate>
```

Valid baud rates are 1200, 2400, 4800, 9600, 19200, 38400.

To see the baud rate set for the ATM switch, use the following command:

```
baud show
```

ATM Interface Commands

Use the ATM command to configure parameters related to the ATM layer.

ATM Show Command

Use the `atm show <options>` command to display information about the:

- ATM Layer Interface
- Permanent Virtual Circuits
- Permanent Virtual Paths
- Virtual Path Logical Ports

Option	Description
`status`	Shows the status of each port on your switch (up or down) and the type of interface cable connected to the port.
`prefix`	Shows the ATM network prefix configured for the ATM switch. This prefix is used for the ILMI address registration process.
`ds3 <interface>`	Shows the DS3 parameters configured for a port. For example: Port 10: Up C-BIT Parity Encoding is enabled Clock is INTERNAL (TCLOCK) XOR with 55 is enabled SCRAMBLING is enabled PLCP delineation is enabled HCS passthru is disabled 8k reference is enabled as MASTER Short Cable

Option	Description
`pvc {<interface> {<vpi> {<vci>}}}`	Displays a list of currently configured Permanent Virtual Connections available on the switch and settings related to these connections. For example, you can see the VPI/VCI value of both ends of the PVC and the cross connection ID. • If you want to view information for a specific PVC, make sure you enter the interface and the VPI/VCI values for the configured PVC. • If you enter the command without any arguments (`atm show pvc`) all PVCs are displayed.
`pvp {<interface> {<vpi>}}`	Displays a list of currently configured Permanent Virtual Paths available on the switch and settings related to these connections. For example, you can see the VPI value of both ends of the PVP and the cross connection ID. • If you want to view information for a specific PVP, make sure you enter the interface and the VPI values for the configured PVP. • If you enter the command without any arguments (`atm show pvp`) all PVPs are displayed.
`vplp {<interface> {<vpi>}}`	Displays a list of currently configured Virtual Path Logical Ports available on the switch, and settings related to these connections. • If you want to view information for a specific VPLP, make sure you enter the interface (or port number) and the VPI values for the configured VPLP. • If you enter the command without any arguments (`atm show vplp`) all VPLPs are displayed.

Table 30. ATM Console Commands

Stopping and Starting an ATM Interface

You can disable, enable, and cycle (disable and then enable) an ATM interface using the following commands.

Command	Description
`atm start <interface>`	This commands restarts an ATM interface after it has been stopped. For example, `atm start 3` enables interface 3.
`atm stop <interface>`	This command stops an ATM interface. No ATM cells are permitted into or out of the ATM interface when you enter this command. For example, `atm stop 3` disables interface 3.
`atm cycle <interface>`	This command stops and restarts an ATM interface. For example, `atm cycle 3` stops and then restarts interface 3.
`atm test <interface>`	This command puts the interface on an ATM switch into test mode. For example, `atm test 3` puts port 3 into test mode.

Table 31. Disabling or Enabling an ATM Interface

Creating a Permanent Virtual Connection (PVC)

Use the following command to define a PVC on a switch and then cross connect it to another PVC.

```
atm create pvc <in_interface> <vpi> <vci> <out_interface>
     <vpi> <vci> traffic <tx> {<rx>}
```

For example, `atm create pvc 1 1 33 2 2 34 traffic 99`

This command defines and cross connects two PVC endpoints; one on interface 1 with a VPI/VCI value of 1/33, and the other on interface 2 with a VPI/VCI value of 2/34. The transmit (Tx) and receive (Rx) traffic profile indexes are the same and equal 99.

General PVC Information

Permanent Virtual Connections (PVC's) are manually created ATM connections. These connections must be created and defined in:

- Both end stations (they terminate the PVC)
- All switches along the route connecting the end stations (they cross connect the PVC's into an end-to-end connection)

The key point regarding PVC configuration is that the encapsulation must be the same at both end stations connected by the PVC. The specific encapsulation type used on a PVC is not relevant to a switch because switches merely receive ATM cells on a given channel, look up the destination VPI/VCI and interface, rewrite the VPI/VCI values in the ATM cell header as needed, and switch the cell out the specified interface.

Note: VCI values of 31 and lower are reserved on every VP (Virtual Path). For instance, 0/5 is the well-known signaling channel, 0/16 the ILMI, 0/17 the LECS, and 0/18 the PNNI. Therefore your VCI values must be 32 or higher.

Creating Permanent Virtual Paths (PVP)

Use the following command to define a PVP on a switch and then cross connect it to another PVP.

```
atm create pvp <in_interface> <vpi> <out_interface> <vpi>
     traffic <tx> {<rx>}
```

For example, `atm create pvc 1 1 2 2 traffic 99`

This command defines and cross connects two PVP endpoints; one on interface 1 with a VPI value of 1, and the other on interface 2 with a VPI value of 2. The transmit (Tx) and receive (Rx) traffic profile indexes are the same and equal 99.

General PVP Information

Permanent Virtual Paths (PVP's) are similar to PVC's. A PVP can be thought of as a bundle of PVC's that all share the same VPI value (for any given link).The switch forwards cells based only on the cell's VPI value and it ignores the VCI value. This is referred to as *path switching,* whereas full PVC configuration is referred to as *channel switching.* The CrossFire ATM switches perform channel switching and path switching.

PVP's provide a simple way to create a path through a network of switches that contains many PVC's. Without a PVP, all PVC's would have to be individually configured in every switch.

Creating a Virtual Path Logical Port (VPLP)

Use the **atm create vplp** command to define a VPLP. VPLP runs a set of ATM protocols (like ILMI, signaling, and PNNI/CNNI) within a single VPI range. As a result, all connections established by these protocols have the same VPI value assigned to them. VPLP, used in conjunction with PVPs, allows VP tunneling over an ATM network. VP tunneling provides a way to run ATM protocols transparently over a network that does not support them.

You can also use VPLPs with a VP multiplexer to connect multiple end stations to a single ATM switch port. The VP multiplexer does VP switching of VPI 0 on the end station ports to different VPIs on the ATM switch port. Configuring VPLPs on these VPIs lets the switch handle connections from all connected end stations.

```
atm create vplp <port> <vpi> traffic <tx> {<rx>}
```

For example, `atm create vplp 1 1 traffic 99` creates a logical port on interface 1 with an assigned VPI value of 1. The transmit (Tx) and receive (Rx) traffic profile indexes are the same and equal 99.

Deleting PVCs, PVPs and VPLPs

Use the atm delete <options> command to delete an existing PVC, PVP, VPLP, or SPVC. When deleting a PVC or PVP, keep in mind that deleting a PVC or PVP releases system resources back to the CrossFire switch.

Option	Deletes
pvc <interface> <vpi> <vci>	A PVC
pvp <interface> <vpi>	A PVP
vplp <interface> <vpi> <vci>	A VP logical port

Table 32. Deleting PVC or PVP

Setting the Address Prefix

Use the atm set prefix command to set a new ATM address prefix when you cannot use the default prefix (39333233343536373839303030).

```
atm set prefix <prefix in hex>
```

The prefix you enter should be 8 or 13 hex digits.

Setting DS3 Parameters

Use the atm set ds3 command to set DS3 parameters for an interface.

```
atm set ds3 <interface> <options>
```

The following table describes the options you can set for a DS3 interface.

Option	Description
`noxor_55` `xor_55`	Turns off and on the xor-55 option. The default is xor_55.
`no scrambling` `scrambling`	Turns off and on cell payload scrambling for transmitted cells and does not attempt to descramble for received cells. The default is scrambling.
`hec` `plcp`	Specifies the type of deliniation. `hec` indicates hec delineation. `plcp` indicates that plcp framing is used for transmit and receive. See "Using the Reference Clock with DS3 PLCP Framing" on page 107. Note that PLCP framing is the default for DS3

`8k_ref dis-able|slave|master`	`disable`
	The 8KHz reference clock is ignored and the DS3 interface uses internal plcp framing. Note that internal plcp framing is the default for DS3.
	
	`slave`
	The 8KHz reference clock is taken from the "master" DS3 interface.
	
	`master` (default)
	The recovered 8KHz reference clock from this interface becomes the "master" clock for the other DS3 interfaces set in "slave" mode.

Option	Description
short_cable long_cable	short_cable (default) Sets the line equalization to be compatible with a "short" coax cable. long_cable Sets the line equalization to be compatible with a "long" coax cable.
hcs_stop hcs_pass	hcs_stop (default) All cells with Header Checksum Errors are dropped. However, statistics are kept for the number of cells with Header Checksum Errors. hcs_pass Allows cells with Header Checksum Errors to be passed to the upper layers. Statistics are kept for the number of cells with Header Checksum Errors.
m23 c_bit	m23 Selects the M23 application, where the C-bits are forced to 1, except for the first C-bit of a frame. c_bit (default) Selects C-bit parity mode for modifying the C-bits of the frame.

Option	Description
no_loop line_loop pay_loop	no_loop (default) Does not perform any loopback on the DS3 interface. line_loop The electrical signals received by this interface are looped back to the transmit side.(This loopback bypasses the entire DS3 Framer). pay_loop The received payload is looped back to this interface's transmitter, with the overhead bits being regenerated by the DS3 Framer.
tclock	The atm set ds3 <interface> tclock command sets the interface’s transmit clock (DS3 rate) source. An interface is defined as a single DS3 transmit/receive connection to the CrossFire switch module.
loop_time	Uses the recovered 44.736 MHz clock from the interface’s receiver as the transmit clock.

Table 33. Options for Setting a DS3 Interface

Using the Reference Clock with DS3 PLCP Framing

When you select plcp framing (`atm set ds3 <interface> plcp`), the 8k reference clocking option becomes significant.

- `atm set ds3 <interface> 8k_ref disable` – this command means the 8k framing is generated internally.
- `atm set ds3 <interface> 8k_ref slave` – this command means the 8k reference is taken from the “master”, which must be one of the other interfaces on the same PHY Module.
- `atm set ds3 <interface> 8k_ref master` – this command means the “master” is the source of the 8k reference.

Configuring Traffic Descriptors

Use the `atm trafficdesc` command to set traffic descriptors for the configured PVCs and PVPs.

Each PVC and PVP has certain connection parameters associated with it. For instance, each PVC and PVP is defined as a certain ATM service Category (CBR, UBR and so forth). Each PVC and PVP must also have Quality of Service (QoS) parameters defined that are appropriate for its service category. This bundle of QoS and bandwidth parameters are referred to as the Traffic Descriptor.[1]

When creating a PVC or PVP on a switch you must supply:

- VPI and VCI values (VPI only for PVP's)
- Input and output interfaces
- Traffic descriptors for both directions of the VCC

Note: A VCC (Virtual Channel Connection) is a set of serially cross connected PVC's (Virtual Circuits) sharing the same VPI/VCI values on each hop linking two end systems through a network of switches. PVC's are bi-directional, being composed of two circuits, one in each direction. Each circuit can have the same *or different* Traffic Descriptors. Non-symmetrical Traffic Descriptors on the same VCC reflect the fact that much network traffic is itself non-symmetrical.

Displaying Cell Rates

Use the `atm trafficdesc show list` command to display a list of configured traffic descriptors. Figure 49 shows a sample display.

		PCR		SCR		MBS			Frm		
Idx:	Class:	0:	0+1:	0:	0+1:	0:	0+1:	Tag:	Dsc:	BEF:	Status:
0099	rtVBR	-1	7000	-1	5208	-1	50	NO	NO	NO	Active
0100	CBR	-1	167	-1	-1	-1	-1	NO	NO	NO	Active

Figure 49. List of Configured Traffic Descriptors

1.Most of the information for this section was taken from the *Traffic Management Specification, Version 4.0* (document number af-tm-0056.000) written by the ATM Forum.

The following table describes the fields on this report.

Report Field	Shows
`idx`	Descriptor index
`class`	ATM service category
`pcr`	Peak Cell Rate for cells that do not have the Cell Loss Priority set (PCR 0), and for cells regardless of the setting for Cell Loss Priority (PCR 0+1).
`scr`	Sustainable Cell Rate – shows the upper limit of the average transmission speed, in cells/second of an ATM connection. If an application uses SCR, the network only guarantees the SCR and not the higher PCR.
`mbs`	Maximum Burst Size – the maximum number of cells a switch can send above the SCR setting.
`tag`	YES indicates that CLP tagging is allowed; NO indicates that CLP tagging is not allowed.
`frm dsc`	Frame Discard – YES indicates Partial Packet Discard is enabled; NO indicates Partial Packet Discard is disabled.
`bef`	Best Effort – YES indicates Best Effort (or UBR class) is enabled; NO indicates Best Effort is disabled. When BEF is enabled, the switch will make a “best effort” to forward traffic, but will not guarantee PCR or any of the QoS settings.
`status`	The current status. `Active` means the traffic descriptors are configured and available for a PVC and PVP to use. `NotInSrv` means the traffic descriptors are not available for a PVC or PVP to use. `NotReady` means the traffic descriptors are configured but are not available for a PVC or PVP to use.

Table 34. Report Fields

Displaying Quality of Service (QoS) Parameters

Use the `atm trafficdesc show qos` command to display Quality of Service (QoS) parameters for configured traffic descriptors. Figure 49 shows a sample display.

		PCR		SCR				-log	
Idx:	Class:	0:	0+1:	0:	0+1:	CTD	CDV	(CLR):	Status:
0099	rtVBR	-1	7000	-1	5208	-1	1/10	NO	Active
0100	CBR	-1	167	-1	-1	-1	1/10	NO	Active

Figure 50. QoS Parameters for Configured Traffic Descriptors

The following table describes the fields on this report.

Report Field	Description
idx	Descriptor index
class	ATM service category
pcr	Peak Cell Rate for cells that do not have the Cell Loss Priority set (PCR 0), and for cells regardless of the setting for Cell Loss Priority (PCR 0+1).
scr	Sustainable Cell Rate – shows the upper limit of the average transmission speed, in cells/second of an ATM connection. If an application uses SCR, the network only guarantees the SCR and not the higher PCR.
ctd	Cell Transfer Delay – the amount of time it takes a cell to go from source to destination through the ATM network.
cdv	Cell Delay Variation – for the traffic descriptor. This parameter is applicable only for CBR and rt-VBR traffic descriptors. A value of -1 means this parameter is not used.
-log (clr)	Negative base 10 logarithm of Cell Loss Ratio for the traffic descriptor. This parameter is applicable only for CBR and VBR traffic descriptors. A value of 0 means this parameter is not used.
status	The current status. Active means the traffic descriptors are configured and available for a PVC and PVP to use. NotInSrv means the traffic descriptors are not available for a PVC or PVP to use. NotReady means the traffic descriptors are configured but are not available for a PVC or PVP to use.

Table 35. Report Fields for QoS

Displaying ABR Parameters

Use the **atm trafficdesc show abr** command to display ABR-specific parameters for configured ABR traffic descriptors. Figure 51 shows a sample display.

Idx:	MCR:	ICR:	TBE:	FRTT:	RIF:	RDF:	Nrm:	Trm:	CDF:	ADTF:
0096	1000	1000	16777215	1000	1	1/32768	32	100	1/16	50

Figure 51. ABR-Specific Parameters for Configured Traffic Descriptors

The following table describes the fields on this report.

Report Field	Description
`idx`	Descriptor index
`mcr`	Minimum Cell Rate – the rate, in cells/second at which the source can always send.
`icr`	Initial Cell Rate – the rate, in cells/second used to send an initial cell or after an idle period.
`tbe`	Transient Buffer Exposure – number of cells a source can send during the start-up period; before the first RM-cell returns.
`frtt`	Fixed Round-Trip Time – the “best case” time for a cell to traverse the network from the source to a destination and back.
`rif`	Rate Increase Factor – controls the amount of cell transmission rate increase when a source receives an RM-cell.
`rdf`	Rate Decrease Factor – controls the decrease in the cell transmission rate.
`nrm`	Maximum number of cells a source can send for each forward RM-cell.
`trm`	An upper bound on the time, in milliseconds between forwarded RM-cells for an active source.
`cdf`	Cutoff Decrease Factor – controls the decrease in ACR associated with CRM.
`adtf`	ACR Decrease Time Factor – the time, in seconds permitted between sending RM-cells before the rate is decreased to ICR.

Table 36. Report Fields for ABR

Setting Traffic Descriptors

Use the `atm trafficdesc set <options>` command to set traffic descriptors for an CrossFire ATM switch.The following table describes the options you can set for traffic descriptors.

Option	Description
`class <cbr|rtvbr|nrtvbr|abr|ubr|other>`	`cbr` (Constant Bit Rate) – indicates fixed dedicated bandwidth; similar to an emulated leased line. `rtvbr` (real-time Variable Bit Rate) – use for high-priority communication that does requires a specific delivery rate, such as voice or video. `nrtvbr` (non-real-time Variable Bit Rate) use for high-priority communication that is not sensitive to variable time delays. `abr` (Available Bit Rate) – use for standard file transfers. The network makes not absolute guarantee for cell delivery but a minimum rate of transmission is guaranteed, and cell loss is minimized. `ubr` (Unspecified Bit Rate) – for low-priority tasks such as file transfers or print jobs. This class does not guarantee any specific transmission speed. `other` – this
`pcr0` `pcr1`	Peak Cell Rate for cells that do not have the Cell Loss Priority set (PCR 0), and for cells regardless of the setting for Cell Loss Priority (PCR 0+1).

Option	Description
`scr0` `scr1`	Sustainable Cell Rate – shows the upper limit of the average transmission speed, in cells/second of an ATM connection. If an application uses SCR, the network only guarantees the SCR and not the higher PCR.
`mbs0` `mbs1`	Maximum Burst Size – the maximum number of cells a switch can send above the SCR setting.
`tagging enable` `tagging disable`	YES indicates that CLP tagging is allowed; NO indicates that CLP tagging is not allowed.
`discard enable` `discard disable`	Enables and disables Partial Packet Discard.
`ctd <value>`	Cell Transfer Delay – sets the amount of time allowed for a cell to go from source to destination through the ATM network.
`cdv <value>`	Cell Delay Variation – sets the amount of variation (difference between maximum and minimum CTD) allowed for CTD. This parameter is applicable only for CBR and rt-VBR traffic descriptors.
`logclr <0...15>`	Sets the Cell Loss Ratio for the traffic descriptor. This parameter is applicable only for CBR and VBR traffic descriptors.

Option	Description

`abr<mcr|icr|tbe|frtt|rif |rdf|nrm|trm|cdf|atdf>`	`mcr`
	Minimum Cell Rate, in cells/second at which the source is allowed to send. See Note 1 on page 118.
	
	`icr`
	Initial Cell Rate, in cells/second at which a source should send initially and after an idle period. See Note 1 on page 118.
	
	`tbe`
	Transient Buffer Exposure is the number of cells a source can send during the start-up period; before the first RM-cell returns. The source and ATM network negotiate this number, which can be between zero and 16,777,215.
	
	`frtt`
	Fixed Round-Trip Time is the sum of the fixed and propagation delays from the source to a destination and back.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>abr<mcr|icr|tbe|frtt|rif |rdf|nrm|trm|cdf|atdf></code></td><td><code>rif</code>
Rate Increase Factor – controls the amount of cell transmission rate increase when a source receives an RM-cell. This rate is a power of two, ranging from 1/32,768 to one.

<code>rdf</code>
Rate Decrease Factor – controls the decrease in the cell transmission rate. This rate is a power of two, ranging from 1/32,768 to one.

<code>nrm</code>
Maximum number of cells a source can send for each forward RM-cell. Enter a power of two, in the range of two to 256.

<code>trm</code>
An upper bound on the time, in milliseconds between forwarded RM-cells for an active source. Trm is 100 times a power of two, in the range of $100*2^{-7}$ to $100*2^{0}$.

<code>cdf</code>
Cutoff Decrease Factor controls the decrease in ACR associated with CRM. CDF is zero or a power of two in the range of 1/64 to 1.

<code>adtf</code>
ACR Decrease Time Factor is the time, in seconds permitted between sending RM-cells before the rate is decreased to ICR. The ADTF range is .01 to 10.23 seconds, with a granularity of 10 milliseconds.</td></tr>
</table>

Table 37. Report Fields for Traffic Descriptors

Note: Rates are signaled as 24-bit integers which have a minimum value of zero and a maximum value of 16,777,215. However, RM-cells use a 16-bit floating point format which has a maximum value of 4,290,772,992.

Activating Traffic Descriptors

Use the `atm trafficdesc activate` command to enable traffic descriptor parameters you have already configured.

Deleting Traffic Descriptor Indexes

Use the `atm trafficdesc delete <descriptor index>` command to delete a configured traffic profile.

Configuring the BridgeID Broadcast Feature

Use the `bridgeid set` commands if you want your ATM switch to broadcast BridgeIDs. The first command enables (or disable) the BridgeID broadcast feature, and the second command indicates the time interval you want the switch to send out the BroadcastIDs.

```
bridgeid set enable|disable
bridgeid set interval <interval value>
```

To see how the BridgeID parameters are set on an ATM switch, enter the following command:

```
bridgeid show
```

Configuring the IISP Port

By configuring border interfaces on the CrossFire ATM switches to be IISP with the appropriate connection table(s), a switched virtual connection (SVC) can extend from the Olicom cloud across the border and through another vendor's routing domain.

Figure 52 shows an SVC crossing such a border and connecting two end stations.

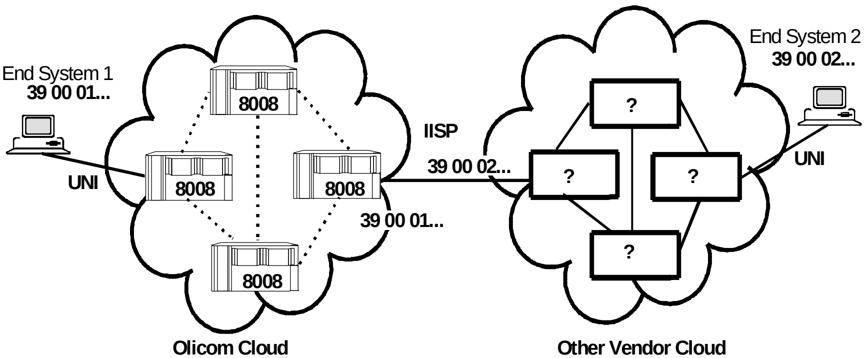


Figure 52. Connecting Olicom Cloud to Other Vendor Cloud

Each port on an ATM switch must be properly configured for IISP to ensure that the IISP protocol runs properly between ATM switches. Configuring a port for IISP involves:

- enabling and disabling UME on IISP ports
- adding the switch’s ATM address to the routing table
- enable address registration on an interface

Enabling and Disabling UME on an IISP port

To enable and disable UME on an IISP interface, use:

```
ume enable <interface>
```

and

```
ume disable <interface>
```

commands.

Configure Routing Tables

You can create static routes by adding all addresses that exist in the ATM cloud to which you are connecting. Use the following command to add addresses to the table:

```
ume add address <interface> <address>
```

You can also use the `ume add address` command if an end system switch on the other side is not capable of registering its own ATM address or a Network Administrator would like to enter an ATM group address.

Note: You can add many addresses simultaneously with this command. For example, if you have a series of addresses that begin with 39, enter the following command to add all of these addresses:

```
ume add address <interface> <39>
```

39 would be considered a prefix or mask. An ATM switch sends all addresses that begin with 39 down the specified interface. Remember that you only want to add addresses to create static routing tables.

To delete an address from a routing table, enter the console command:

```
ume delete address <interface> <address>
```

Setting UNI Management Entity (UME) Parameters

To enable or disable address registration on an interface, enter the following command:

```
ume set addr_reg <port> <on|off>
```

For example, if you enter `ume set addr_reg 8 on` turns on the address registration feature for interface 8, and sets the ATM address for the switch.

Displaying UME Parameters

To display the configured UME parameters for an interface, use the following command:

```
ume show <interface>
```

The information displayed looks like:

```
ume parameters for port 8:

status:                              full
device type:                         node
uni type:                            private
state:                               nopolling
protocol version:                    uni 4.0
addr registration:                   supported
address(es):
390000000000000000000000000000000008800
end of addresses
```

Where:

- Status–indicates the status of the ILMI connectivity. The status can either be *full* or *off*.
- Device Type–indicates the type of device using the ATM interface. The type can either be *node* or *user*.
- State–indicates the state the ILMI protocol is in. The state can be *stopped, link failing, establishing, configuring, retrieving, registering, verifying*, or *cleanup*. ILMI goes through these stages while creating, maintaining and deleting connections between ports.

Configuring Classical IP Over ATM (CLIP)

IP over ATM is used to configure Classical IP over ATM (RFC 1577) in-band management on an Olicom ATM switch. The switch can function as a CLIP client and as an CLIP server. The CLIP client and CLIP server software work together to send IP packets through an ATM network. For more information about CLIP, refer to page 72.

Setting ATM Address Information for a CLIP Server

To set the server's ATM address, type the following command:

```
clip server set atm_addr <atm address>
```

In some CLIP environments, the server has a predefined ATM address. This prevents the possibility of the server being assigned a different ATM address and forcing all the clients to be reconfigured.

One device per Logical IP Subnet (LIS) is an ARP server and is used by the other devices to find the destination ATM address that was mapped from the IP address in the IP packet.

To set the IP subnet address and mask of the CLIP Server, enter the following commands:

```
clip server set subnet_addr <ip subnet address>
clip server set subnet_mask <ip subnet mask>
```

Setting ATM Address Information for a CLIP Client

To use the CLIP client, you must configure an ATM address for the ARP server. The command is:

```
clip client set server_addr <atm address>
```

You should make sure the client and server are in the same IP subnet.

To set the IP address and the IP mask of the CLIP Client, enter the following commands:

```
clip client set ip_addr <ip address>
clip client set ip_mask <ip_mask>
```

Displaying the CLIP Client and Server Information

To display the configured ATM address, IP subnet address, and IP subnet mask for a CLIP client or server, enter one of the following commands:

```
clip client show
clip server show
```

Configuring LAN Emulation Client (LEC)

LEC is a client for LAN Emulation – protocol that allows to emulate Ethernet networks on ATM. All those LEC commands changing and showing the internal client configuration.

Setting LEC configuration parameters

To set the name of Emulated LAN that client is to join type the following command:

```
lec set ELANName {string}
```

Internal LEC is capable to join both EtherNet and Token-Ring ELAN so we can choose the type of ELAN by typing the command:

```
lec set type {ethernet | token_ring}
```

Token-Ring ELAN’s could have few kind of frame sizes so we have to choose one if the LEC is of Token-Rig type:

```
lec set size {1516 | 4544 | 9234 | 18190 }
```

To set the IP address and netmask for LEC we have to type commands:

```
lec set ipaddr <nnn.nnn.nnn.nnn>
lec set netmask <nnn.nnn.nnn.nnn>
```

Showing LEC configuration parameters

You can see all configuration parameters by typing single command:

```
lec show all
```

After typing that command you can see the result as follows:

```
LEC parameters:
ELAN name:      Some_ELAN_Name
ELAN type:      Ethernet        after reboot: Ethernet
Frame size:     1516            after reboot: 1516
LEC state:      Operational
IP Address:     99.99.99.99
P Netmask:     255.255.255.0

LEC Vccs:                     (Interface/VPI/VCI)
Config Direct:          0/0/400
Control Direct:         0/0/403
Control Distribute:     0/0/404
Multicast Send:         0/0/405
Multicast Forward:      0/0/406
```

If you do not want to see all of the parameters you can type one of these commands:

```
lec show ELANName
```

(shows name of Emulated LAN)

```
lec show type
```

(shows type of Emulated LAN)

```
lec show size
```

(shows size of Emulated LAN)

```
lec show state
```

(shows state of Internal LEC)

```
lec show ip
```

(shows IP address and netmask of internal LEC)

```
lec show Vccs
```

(shows internal VCC’s of LEC if in operational state).

Configuring Q.SAAL

Q.SAAL uses HDLC-like protocol that is responsible for proper transmission on the link between two ports.

Setting Q.SAAL configuration parameters

On the specified interface (ifIndex) we can set the value of maximum receive window used by Q.SAAL (maxRcvWindow). Larger value is preferred during transmitting of large size data.

Note: If on specified interface there are sent large numbers of small portions of data we should try to set small value.

To do this we can type the following command:

```
link set ifIndex {InterfaceNumber} {maxRcvWindow}
```

It is recommended to cycle specified interface to make sure that both sides made changes to that parameter via negotiation at the beginning of establishing the connection.

Showing Q.SAAL configuration parameters

We can see all Q.SAAL parameters on specified interface by typing single command:

```
link show ifIndex <InterfaceNumber>
```

This command is very useful if user wants to know what is complete status of specified link. The result of that command will be as follows:

```
Link 5 parameters:

maxRcvWindow:    256

rcvWindow:       256

vrH:             11

vtS:             10                vtA:           131

vtPS:            10                vtPA:          131

vrR:             11                vtPA:          1

vrMR:            267               vtMS:          266

rcvNs:           11                rcvNr:         10

rcvNps:          131               rcvNmr:        266
```

For complete description of all that parameters look at Q.2110 ITU-T Specification.

Configuring SNMP over Serial Links Protocol (SLIP)

SLIP allows fully configuring the switch by the Simple Network Management Protocol with use only RS-232 connector.

Setting SLIP configuration parameters

To set SLIP parameters type the following commands:

```
bdrate     slip set bdrate <bdrate number>
ipmask     slip set IP mask
ipaddr     slip set ipaddr <W.X.Y.Z>
interface  slip set interface on|off
```

After setting all this parameters we can use SLIP to manage the switch.

Showing SLIP configuration parameters

We can see all actual configuration parameters by typing single command:

```
slip show
```

After typing that command we can see the result as follows:

```
baudrate:             9600 bps
parity:               none
stop bits:            1
IP Address:           99.99.99.99
IP Netmask:           255.255.255.0
Modem Init:           AT&C1 S0=1 E0
Header Comression:    DISABLED
Slip is:              ENABLED
```

Proxy User Mode Configuration

Adding ATM switches to existing networks normally requires you to reconfigure existing ATM equipment on the network to recognize the new CrossFire ATM switches. Reconfiguration is required due to interoperability issues associated with IISP or PNNI. This can be especially time consuming on large networks. Using the CrossFire 8008/9100/9200 interfaces connected to the network as a proxy user allows you to avoid this reconfiguration. When connected to a network using proxy user mode, the CrossFire ATM switches appear to the network as a single user interface with multiple ATM addresses. The CrossFire ATM switches provide ATM switching functions for stations on CrossFire 8008/9100/9200 interfaces that you attach to the network via the proxy.

To configure proxy user mode, identify the interface to act as proxy and each interface for which you will use the proxy. Connect the proxy interface to the ATM network. Connect each interface that must access the network to its end station(s). Use the following command for each end station interface that will use the proxy interface:

```
signaling set proxy_user <end station interface>
     <proxy interface>
```

The switch displays a message like **"port 1 will proxy for port 10"** after you enter this command.

Each configured end station interface uses the proxy interface to access the network.

Displaying a Proxy User

To see the interface (or port) that is acting as a proxy user for a port, enter the following command:

```
signaling show <end station interface>
```

The switch displays a message indicating which port is the proxy user for the `<end station interface>` you entered in the command.

Clearing a Proxy User

To clear an interface (or port) that is acting as a proxy user for a port, enter the following command:

```
signaling clear proxy_user <end station interface>
```

The switch displays a message like **"proxy for port 10 cleared"** after you enter this command.

Creating Multiple Proxy Interfaces

You can create multiple proxy interfaces on a single CrossFire ATM switch. This allows you to connect the CrossFire ATM switches to many different networks and proxy end station interfaces to networks on an individual basis. The logical limit to the number of proxy interfaces is 1/2 the number of interfaces on the switch (one proxy interface for each end station interface).

You can also cascade multiple CrossFire ATM switches via proxy interfaces. You simply connect each switch proxy interface as an end station to the proxy interface of the CrossFire ATM switches downstream toward the network. After connection, perform the above command on each ATM switch based on the end station to proxy interface sequence.

Figure 53 shows three proxy user mode configurations. End station 1 (on CrossFire 8008 A interface 4) uses interface 1 on CrossFire 8008 A as proxy to network 1. End station 2 (on interface 5, CrossFire 8008 A) uses interface 2 on CrossFire 8008 A as proxy to network 2, demonstrating a case of multiple proxies on a single switch. End station 3 (on interface 6, CrossFire 8008 A) uses interface 3 on CrossFire 8008 A as proxy to CrossFire 8008 B. End station 3 (now on interface 2, CrossFire 8008 B) then uses interface 1 on CrossFire 8008 B as proxy to network 3, thereby cascading the proxy configuration through two CrossFire 8008s.

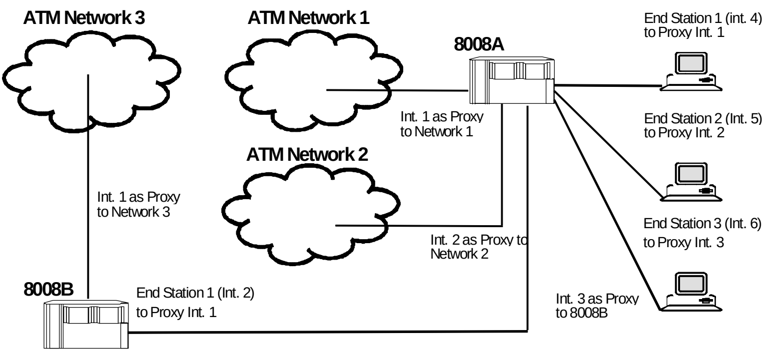


Figure 53. Multiple and Cascaded Proxy User Configuration

LAN Emulation Console Commands

You can enable and disable LAN Emulation (LANE) services on a CrossFire 9100 and 9200 using the following `lane services` commands.

```
lane services enable
lane services disable
```

Note: The `lane services` commands are not available on the CrossFire 8008.

Displaying Current SuperELAN LES/BUS ID

To display current value of SuperELAN LES/BUS ID enter the following command:

```
lane show lesbusid
```

The switch displays a messages like “`SuperELAN LES/BUS ID: 0x0B`” after you enter this command.

Changing Current SuperELAN LES/BUS ID

To change current value of SuperELAN LES/BUS ID enter the following command:

```
lane set lesbusid <newID>
```

`<newID>` must be in range 0 to 30 and should be entered as hex value.

Note: This command cannot be entered on CrossFire 9X00 acting as Backup RXLES.

Note: This command causes release of all LANE Clients attached to all ELANs on both Primary and Backup RXLESs. Reason of this behavior is that this command changes LEC_ID range allowed for all LES/BUS pairs on this device and associated Backup RXLES. Starting from this moment all old LEC_IDs are invalid and the only way to change assigned LEC_ID is to force re-join of this LEC.

Displaying List of ELANs Defined on This Device

To list all ELANs defined on this device use the following console command:

```
lane show elan
```

Sample Display:

```
List of defined ELANs:
IDX   ELAN Name
     0 "EtherNet"
     1 "TokenRing 1516"
     2 "TokenRing 4544"
     3 "TokenRing 9234"
     4 "TokenRing 18190"
```

Displaying Details of ELAN

To display all details of ELAN defined on this device use the following console command:

```
lane show elan <idx>
```

Sample display:

```
Idx                                = 0
LAN Type                           = 802.3 (Ethernet)
ELAN Name                          = "EtherNet"
Max Frame Size                     = 1516
TLVS:Target-Less-NARP TLV          = enabled (1)
```

Changing Value of Target-Less-NARP TLV

To change the value of Targt-Less-NARP TLV for a particular ELAN defined on this device use the following console command:

```
lane set elan <idx> target-less-narp { disable |  enable }
```

Disabling of Sending of Target-Less-NARP TLV

To disable sending of Target-Less-TLV in LE_CONFIG_RESPONSE frames use the following console command:

```
lane set elan <idx> target-less-narp delete
```

Using the Call Out Feature

The ATM Call Out feature automatically sends a CLI message to a specified console when an ATM switch detects a hardware problem. For example, if you enable the Call Out feature for a switch and a fan fails, the modem connected to the switch experiencing the problem dials the configured phone number.

This phone number will most likely be the number a modem connected to a PC in the central network monitoring location.Then the switch sends a text message to the destination console. This message contains the IP address of the switch experiencing the problem and a brief explanation of the problem.

The Call Out feature notifies you when the following events occur:

- Power Supply Unit (PSU) failure
- Fan failure
- Temperature warning (temperature is above or below the configured range)
- Port auto disabled

To enable this feature complete the following steps:

1. Enter the following console commands:

   ```
   call out enable
   call out number <phone_number>
   ```

   The phone_number is the number the modem dials when the ATM switch detects a hardware problem.

2. Disconnect the console and plug a modem into the serial port. Make sure you connect the modem into the serial port located on the front panel; the serial port on the back side of the switch is used for debugging.

To see the phone number the modem will dial, or if this feature is enabled or disabled, enter `call out show`.

The display message will look like:

```
callout is on
callout phone 5085551212
```

To disable this feature, enter `call out disable`.

Note: The `call out` commands are not available on the CrossFire 8008.

Using the Call Back Feature

The ATM Call Back feature lets you monitor and configure an ATM switch from a remote location. A network administrator might use this feature to fix a problem while at another location, or Olicom Technical Support might request you to enable this feature to help them determine a problem with your switch.

To enable this feature complete the following steps:

1. Enter the following console commands:

   ```
   call back enable
   call back number <phone_number>
   ```

   The phone_number is the number of the remote modem to dial out to.

2. Disconnect the console and plug a modem into the serial port. Make sure you connect the modem into the serial port located on the front panel; the serial port on the back side of the switch is used for debugging.

3. Reboot the switch to cause the modem to dial out to the configured phone number.

To see the phone number the modem will dial, or if this feature is enabled or disabled, enter `call back show`.

The display message will look like:

```
callback is on
callback phone 6175551212
```

To disable this feature, enter `call back disable`.

Note: The `call back` commands are not available on the CrossFire 8008.

SNMP Management Commands

Simple Network Management Protocol (SNMP) is used to remotely configure an ATM switch. The following SNMP console commands are supported in this release:SNMP Management Commands

Command	Description
`snmp add client <address> <community_name>`	Adds a trap client. A trap is a message that a CrossFire switch sends to Olicom's Integrated Management System (IMS) when an unusual event, such as a cold or warm start occurs, or link goes up or down. The trap messages are used for troubleshooting purposes. Example: `snmp add client 128.100.110.111 test` where *128.100.110.111* is the IP address of an IMS workstation, and *test* is the community password needed to access the desired CrossFire switch.
`snmp set access <readonly|readwrite>`	Sets access for the client to the appropriate access level.

`snmp set community <read|write>`	Sets the access level for a community. You must also supply a community index number (1-4), a community name, and a community IP address with this command.
	
	`read <index> <name> <ip address>`
	This argument sets readonly access for the specified community.
	`write <index> <name> <ip address>`
	This argument sets read/write access for the specified community.

Command	Description
`snmp show <clients|communi-ties>`	Displays information about the trap clients or communities.
`snmp delete client <index>`	Deletes a trap client. Enter the *index* of the trap client you want to delete.

Table 1. SNMP Management Commands

LAA Console Commands

Displaying LAA

To display the current MAC address used by the device and configured MAC address of the device which will be used after soft reboot use the following console command:

```
system show laa
```

Sample display:

```
Current MAC address:      00:00:24:90:70:DE (burned-in)
Burned-in MAC address:    00:00:24:90:70:DE
Configured MAC address    02:00:00:23:23:23 (LAA)
to be used after
soft reboot:
```

Changing LAA

To change MAC address used by the device use the following console command:

```
system set laa <mac>
```

Note: The change will take place after soft reboot of the device.

Note: Bit0 in most significant byte has to be set to “0”. Bit1 in most significant byte has to be set to “1”. These conditions are checked by procedure serving this console command.

Returning to Burned-in MAC Address

To return to MAC address burned-in MAC address use the following console command:

```
system delete laa
```

Note: The change will take place after soft reboot of the device.

❑

6. Configuring LANE and PNNI

This chapter provides some additional information about configuring a LANE Server and a hierarchical PNNI network.

Sections

- Changing the Well-Known ATM Address
- LANE Redundancy
- Support for IBM MSS SuperELAN
- Configuring PNNI

Changing the Well-Known ATM Address

In most instances, the LANE server does not require any configuration–it's already configured for "plug and play" operation. The LANE server is configured with an ATMF well-known address to which any LEC can join. The LANE server is also configured to support Ethernet and Token Ring LANs supporting 1516, 4544, 9234 and 18190 frame sizes.

If you are installing a LANE server in a pre-existing network, and the network has a specific ATM addressing scheme, you might have to change the default well-known ATM address to accomodate the addressing scheme in effect. If the address is anything other than the well-known address, then all clients wishing to join must manually configure the LECs address, or configure the new address on the Service Registry on the ATM switches.

LANE Redundancy

To provide true redundancy, you need at least two CrossFire 9100/9200 ATM switches in your ATM network, with one designated the *primary* server and the other designated the *backup* server.

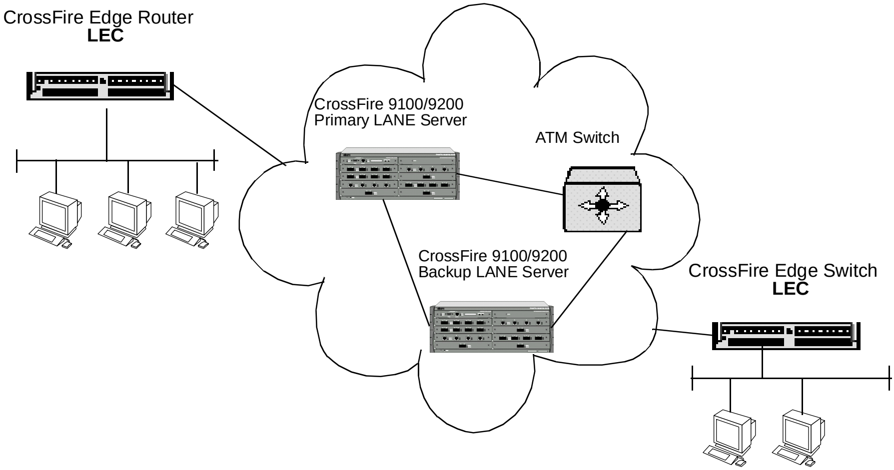


Figure 54. LANE Redundancy

The primary LANE component is configured like any LANE server, with the well-known ATM address to which any LANE client can join. Since the backup provides a dedicated function to the primary, LANE clients are not aware of its existence, and thus cannot join it.

Once the roles are deteremined, the backup establishes a control connection to the primary. This control connection is made to an ATM address designated for the redundant feature. The default address for the redundancy feature is the multicast address, which also identifies of the vendor allowed to use this address.

The only configuration required to provide LANE redundancy is to enable the redundancy feature in each component and designate the primary and backup servers. To ensure smooth operation you can also verify the configuration of the well-known address and the control multicast address.

Support for IBM MSS SuperELAN

One LES/BUS pair theoretically can handle 65277 LAN Emulation Clients (LECs), but in practice it can handle only about 250-300, so that a large network must be split among more than one LES/BUS pair. For example, a network with 1000 LECs should be split among 4 LES/BUS pairs. To allow connectivity between those 4 parts of one ELAN, IBM developed the *Super ELAN* concept.

To understand Super ELAN functionality, assume that we have two ELANs, ELAN1 and ELAN2, which should communicate. An MSS with Super ELAN functionality joins ELAN1 and ELAN2 as a proxy LEC and then replicates LE_ARPs and broadcast & unknown traffic from any ELAN to all other ELANs. When LEC1 in ELAN1 wants to establish a Data Direct SVC to LEC2 in ELAN2, it issues an LE_ARP to LANE Server serving ELAN1. The server does not know the ATM address of LEC2 so it forwards the LE_ARP to all LECs that registered as proxy (MSS is one of them). When MSS receives an LE_ARP from LANE Server ELAN1 it forwards it to all ELANS that belong to the same Super ELAN (ELAN2 is one of them). When the LANE Server serving ELAN2 receives the ARP, it either already knows the ATM address of LEC2 or forwards the ARP to LEC2.

The LE_ARP_RESPONSE goes all the way back through MSS to LEC1. Then LEC1 establishes an SVC to LEC2.

Avoiding LEC_ID Duplication

When LEC1 and LEC2 are assigned the same LEC_ID (which is possible because they join different servers/ELANs), LE_ARP between them does not work and all data traffic is dropped.

Olicom ATM switches enable you to avoid this problem by letting you assign a unique LEC_ID range per device, so that each LANE server on that device assignes a LEC_ID within that range.

All LEC_IDs are divided into 32 ranges, with each range assigned a unique range number from 0 to 31.

- To determine the range for a device, set the value of SuperELAN LES/BUS ID to a number between 0 and 30 (31 is reserved).
- The default value is 0x0B, which was chosen to maintain compatibility with previous versions of the Olicom CF9x00 switch.

Configuring PNNI

Typically, a CrossFire ATM switch is pre-configured and ready to run "out-of-the-box". This means that all CrossFire switches are configured to be members of the same peer group. If you are installing a CrossFire switch in a hierarchical network, you must change the switch configuration.

Creating a Peer Group

When using PNNI, each ATM switch is referred to as a node. Each node is automatically given a node ID, which is based on a switch's ATM address.

You can group PNNI nodes into peer groups. Each member of a peer group should have:

- The same peer group ID, which is derived from the switches' ATM addresses.
- A common prefix in the ATM address that is unique to a peer group. The administrator can also use this prefix as a means for identifying where the switches in the peer group are located.
- The same length address prefix. This prefix is referred to as a PNNI level. This level is used to indicate the number of bytes in an ATM address that must be identical for all the members in a peer group.

Example:

Here's an example of how to create a peer group of ATM switches. Suppose a network administrator decides to assign level 24 to the members in a peer group. This means the first 3 bytes in the ATM address assigned to members of the peer group will be the same. In Figure 55, switches A and B are in the same peer group because the first 3 bytes are the same. Switches C and D are in a different peer group than switches A and B.

Peer Group 2

Peer Group 1

9200 - D

ATM address 40.12.23...

Assigned level 24

9200 - C

ATM address 40.12.23...

Assigned level 24

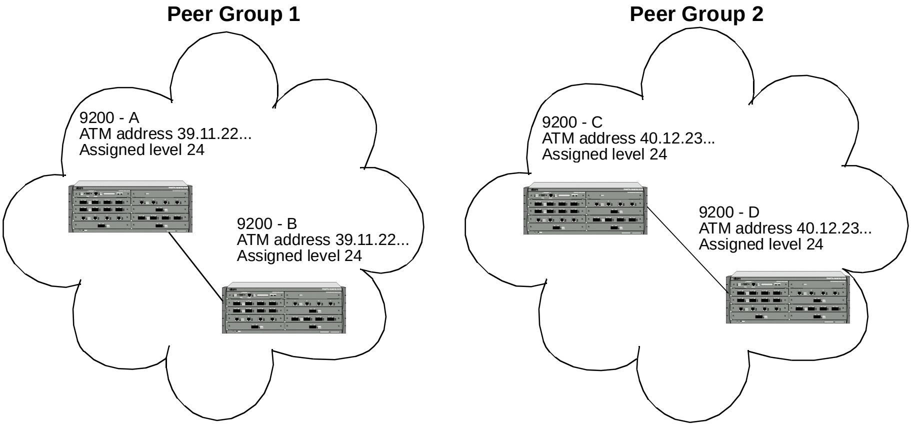


Figure 55. Two Peer Groups

As mentioned above, all CrossFire switches are preconfigured to be in the same peer group at level 72 (ATM address whose first 13 bytes are significant and whose first 9 bytes are exactly the same). This means that if you are creating an ATM network with CrossFire switches, no configuration changes are needed, unless you want to establish two peer groups.

Configuring for a Multi-level Hierarchical Network

In ATM networks with more than forty switches, you should create a multi-layer network. Multi-layer PNNI networks consist of peer groups that can communicate with each other.

Peer groups must communicate with one another at the same "level," and must have ATM addresses which place them in the same peer group. To accomplish this, we need to create another *level* and assign *like* ATM addresses for the nodes at this level. These new nodes are *logical group nodes* and are the only entities allowed to communicate between peer groups.

In Figure 56, the Logical Group Nodes from each subnet create a virtual link to allow the subnets to talk.

Level 8

Level 8

LGN 39

LGN 39

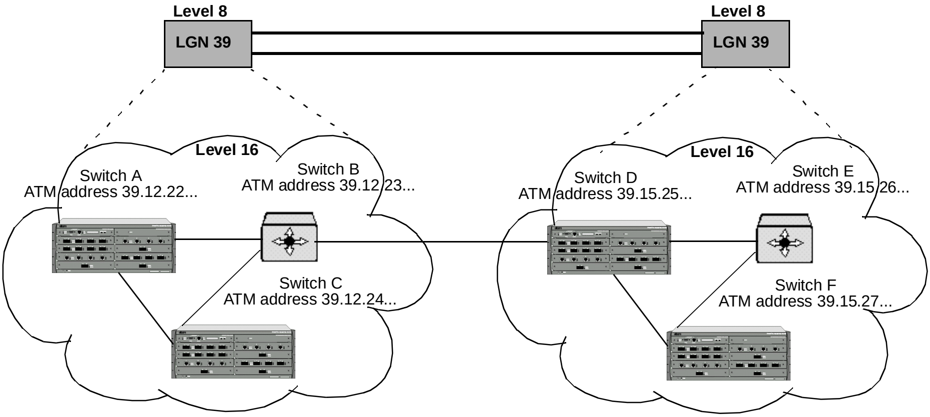


Figure 56. PNNI Logical Group Nodes

One switch in each peer group must be selected to talk to the next level. This switch is referred to as a *Peer Group Leader*. Normally, the nodes in a peer group elect the node with the highest Node ID as the peer group leader who will join the next level up. However, a network administrator can configure one node with a higher priority than the rest so that when it is running, it will be elected as the leader. A network administrator may want a node with more processing power to be the leader.

Typically, "edge nodes" are designated peer group leaders, but any node can be designated as a peer group leader. Edge nodes are switches that are physically connected on the edge of two peer groups. In Figure 56, switches B and D are edge nodes.

Note: To allow all of the definitions and configuration changes to take effect you should reboot your switches. Once each node (A,B,C D, E and F) comes up, arbitration occurs for the selection of the peer group leaders. When the Peer group leader in each group has been identified, each peer group leader then initiates the creation of the respective "logical node" at the new level, which will represent the group in all communications with other peer groups.

❑

7. Configuration Backup

This chapter describes how to back up and restore switch configuration.

Sections

- Overview
- Backing Up a Configuration
- Uploading a Configuration

Overview

ATM switch configuration data stored in non-volatile memory (battRAM) can be backed up and restored via TFTP. You can use this capability to:

- **Prevent configuration loss**
  Use the backup function to store a copy of the switch configuration in a safe file. If the switch configuration is ever corrupted, you can then TFTP the backup configuration to the switch.
- **Configure multiple switches**
  For example, to configure three switches, A, B, and C, first configure switch A, then use the backup function to store a copy of switch A's configuration in a file, and then TFTP the file to switches B and C.

See: Backing Up a Configuration and Uploading a Configuration for details.

Backing Up a Configuration

To download a configuration file from the ATM switch, enter the following commands on your console:

```
tftp <ip_address>
bin
get olicom/<password>/config <MAC address>.bin
     <filename>
```

Parameters:

ip_address is the IP address of the switch you want to back up.

password is the write-access password of the switch.

MAC address is the MAC address of the switch. In this case, be sure to enter the MAC address without periods (full stops) between the digits.

filename is the file name (on your local machine) under which you want to store the configuration data.

Note: Only configuration data are downloaded. Fatal information (when the switch rebooted and what it was doing at the time) is not included in the download.

Note: To list files available for download from the switch, first download the file *dir.txt* from the device. For security reasons, the field *Password* is not shown in filenames listed in the *dir.txt* file.

Uploading a Configuration

Downloaded configuration data can be uploaded to any switch – not only to the source one. Whether you are restoring a lost configuration or configuring several switches, this can save you a lot of work.

The procedures for restoring a backed up configuration file to the device from which it came and for copying a backed up configuration file to another device are similar but not identical. Be sure to follow the correct procedure.

Because a backed up configuration file contains IP settings, however, you must be sure to avoid giving the same IP settings to multiple switches. The command syntax for copying a configuration to another switch instructs the target switch to retain its current IP settings instead of adopting the uploaded IP settings.

Restoring a Configuration to the Same Switch

To restore a configuration from a backup file, simply TFTP the backup to the switch by entering the following commands on your console:

```
tftp <ip_address>
bin
put <filename> olicom/<password>/config.
     <MAC address>.bin
```

Copying a Configuration to Another Switch

To upload a backed up configuration file to a different switch (preserving the target switch’s IP configuration):

```
tftp <ip_address>
bin
put  <filename> olicom/<password> config.SaveIP.
     <MACaddress>.bin
```

Parameter definitions for both procedure:

ip_address is the IP address of the switch to which you want to copy the configuration.

password is the write-access password of the switch.

MAC address is the MAC address of the switch. In this case, be sure to enter the MAC address without periods (full stops) between the digits.

filename is the name of the file (on your local machine) containing the configuration data.

Note: Only configuration data are uploaded. Fatal information (when the switch rebooted and what it was doing at the time) is not included in the upload.

Note: Because this operation changes all configuration data (except IP settings), you should always back up the target switch before uploading a configuration to a different device.

While uploading a configuration:

- Data size is controlled – the upload is rejected if its size exceeds 250K.
- Received image is checked – only valid configuration records will be accepted.
- Software version compatibility is controlled – you cannot upload a configuration file from a switch that was running newer software than the target switch.
- Transfer status is indicated – the message “WRITEFLS” is displayed while configuration records are beign written into non-volatile memory.

If all of the above finishes correctly, the switch will soft reboot and the uploaded configuration will become the active image.

❑

8. Contacting Technical Support

If support is not provided by your organization or the local vendor, you can at any time relay information to or contact Olicom Technical Support via one of the listed services. In addition, e-mail, FTP or WWW provide up-to-date software updates, application notes, quick fixes and various utilities which may solve your problem.

Before You Contact Olicom Technical Support

- Boot the switch to run the power-on diagnostics. Capture and print the diagnostics (note that any traffic through the switch will be disrupted). . ☐
- Print messages from the Message Log in the OpenView or Network Node Manager . . . . ☐
- Print the Support Log and e-mail it to Technical Support. (See instructions below.) . . . . ☐
- Display the Event Log on your console before you call Technical Support. (See instructions below.). . . . . ☐
- If possible, attach a display summary screen captured from the console or telnet . . . . ☐
- If possible, simplify the environment by removing other devices. . . . . ☐
- Fill in as much as possible in the included Problem Report Form . . . . ☐
- Contact your place of purchase . . . . ☐

Printing the Support Log

The Support Log lists errors that occurred before a switch crashed. This log lists system, hardware, and IP configuration information, and contains a stack dump if a fatal error occurred.

To print the Support Log, complete the following steps.

1. Reboot the switch that experienced the error condition.
2. Enter the following commands on your console:

```
tftp <ip_address>
get /olicom/support.<mac_address>.txt
```

IP_address is the IP address of the switch that crashed.

mac_address is the MAC address assigned to the switch that crashed. For the “get” command shown above, enter the MAC address without periods.

3. E-mail the text file to:

Europe: support@olicom.dk

USA: support@olicom.com

Printing the Event Log

The Event Log shows when system reboots occur, as well as stack traces if a fatal error occurs. You can use this log to help determine a problem if you can’t tftp to a failed switch.

With the CrossFire 9100 and 9200s, the event log is stored in volitile memory. Therefore, the log information is erased when you reboot the switch. With the CrossFire 8008, events are stored in volitile and non-volitile memory. The log stored in non-volitile memory contains fatal error information, if applicable.

To view the Event Log, complete the following steps.

1. Make sure you have a console connected to the switch encountering the error condition.
2. Enter the evlog show console command.
   - If you are connected to a **CrossFire 9100 or 9200** switch, enter the following console command:

     ```
     evlog show {<event>}
     ```

     If you do not enter an event number, the list of events begins with the first entry in the log. If you enter an event number, the list begins with the event number you entered.
   - If you are connected to a **CrossFire 8008** switch, enter the following console command:

     ```
     evlog show <n|v> {<event>}
     ```

     The <n|v> arguments are used to display event logs stored in non-volitile versus volitile memory.
3. Contact Technical Support to help you determine the switch’s problem.

To clear an event log on a **CrossFire 9100 or 9200**, enter **evlog clear**. If you are connected to a **CrossFire 8008**, use the following console command:

```
evlog clear <n|v|b>
```

Where n is for non-volitile memory, v is for volitile memory, and b is for both non-volitile and volitile memory.

Hotline Support

Call the following numbers for help with *any* problem you may encounter when installing Olicom software and hardware products:

Europe: (+45) 4527 0102 (Denmark, Monday to Friday, 7 am to 6 pm GMT + 1)
(+48) 58 348 15 20 (Poland, Monday to Friday, 8 am to 6 pm GMT + 1)

USA: (+1) 1-800-OLICOM-1 (24 hours a day, 7 days a week)
(+1) 972 907-4200 (24 hours a day, 7 days a week)

Fax Support

For assistance with any problem you may encounter when installing Olicom software and hardware products, Olicom's Support department will reply either by fax or by telephone within 24 hours, Monday to Friday. Use one of the following fax numbers:

Europe: (+45) 45 27 02 40 (Denmark)

(+48) 58 348 15 01 (Poland)

USA: (+1) 972 671 7524

Bulletin Board Service

All of Olicom's support services are available via our BBS: software updates, application notes, quick fixes, various utilities, etc. The Bulletin Board Service (BBS) can be contacted using either a standard modem or an ISDN modem.

Standard Modem Requirements

Modem speed:	2400, 4800, 7200, 9600, 12000, 14400, 28800 bps
Modem standard:	CCITT V21/V22/V22bis/V32/V34/V42bis/HST/MNP5
Parity:	N (none)
Databits:	8
Stop bits:	1
Transfer protocols:	Xmodem, Ymodem, Zmodem, Kermit and Sealink.

Use one of the following numbers:

Europe: (+45) 45 27 01 00 (Denmark) (and create your own account)

USA: (+1) 972 422 9835

ISDN Modem

Use the following number:

Europe: (+45) 45 96 32 48 (Denmark)

Internet E-Mail

Olicom customer support is available on e-mail through Internet. Use one of the following e-mail addresses:

Europe: support@olicom.dk

USA: support@olicom.com

Anonymous Internet FTP Server

All Olicom's support services can be obtained from our anonymous FTP server: software updates, application notes, quick fixes, etc. To connect, open an FTP session to:

Europe: ftp.olicom.dk

USA: ftp.olicom.com

Internet World Wide Web Server (WWW)

The Olicom WWW server contains up-to-date information about Olicom products, newsletters and press releases. It also contains addresses of all Olicom offices and support centers worldwide. Our software library contains the latest driver and software revisions. The WWW server can be accessed using the following web addresses:

Europe: http://www.olicom.dk

USA: http://www.olicom.com

Olicom Support WEB

The Olicom Support WEB contains technical support hints, driver and software updates, a problem report form and support news.

Europe: http://www.olicom.dk

Select "Services" from the main menu.

Problem Report Form

Fill in both sides of this Problem Report Form, print out the relevant system configuration files and fax or mail to Olicom Technical Support. You can also fill in and send a Problem Report Form from Olicom's web site on the Internet.

Switch Information	
Switch type:	
Hardware revision:	
Software version:	
Switch Configuration	
Port configuration:	
Stack Configuration:	
UEM Configuration:	
Adapter Information	
Adapter type:	
Operating system:	
Network OS:	
Driver name:	
Driver version:	

Company: ______________________________ Name: ________________________

Address: ____

Country: _________________________ Phone/Fax: __________________________

E-mail: _______________________.

Problem Description
Network Installation Sketch

Appendix A. Chassis Maintenance

This appendix describes the procedures for inserting a CrossFire 8008 into a CrossFire 8000 Chassis, calculating the power supply requirements for the CrossFire 8000 Chassis, and general CrossFire 8000 Chassis maintenance considerations.

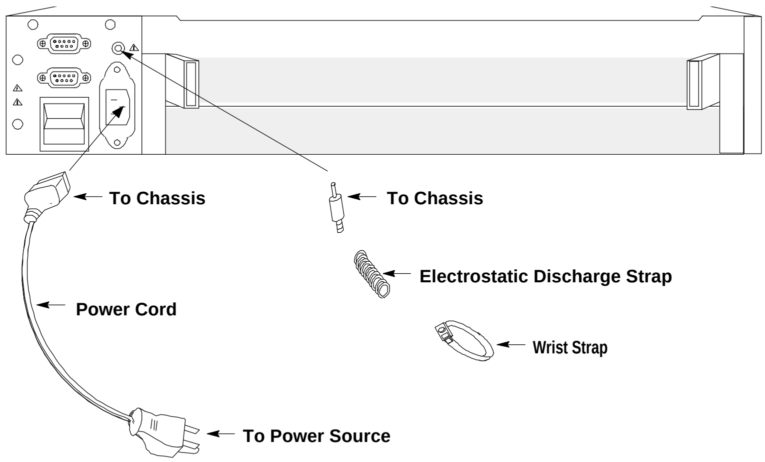
Sections

Inserting a CrossFire 8008 Into a CrossFire 8000 Chassis

Before inserting the CrossFire 8008 into a CrossFire 8000 Chassis, you must be properly grounded. This is necessary to avoid electrostatic discharge damage to the equipment. To be properly grounded, follow these steps:

1. Connect one end of the power cord to the CrossFire 8000 Chassis and the other end to the power source to ground the CrossFire 8000 Chassis.
2. Fasten one end of the electrostatic discharge strap around your wrist and connect the other end to the plug on the CrossFire 8000 Chassis back panel to ground yourself to the CrossFire 8000 Chassis.

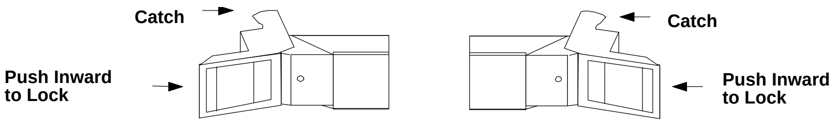
Note: The CrossFire 8000 Chassis (1-slot) is used for illustration in this description, but the grounding procedure is the same for the CrossFire 8000 Chassis (2-slot) and CrossFire 8000 Chassis (8-slot).



To insert a CrossFire 8008 into a CrossFire 8000 Chassis, do the following:

1. Insert the CrossFire 8008 into the CrossFire 8000 Chassis by sliding the top module board into the top guides of the slot in the enclosure. To seat the module, the card ejectors must be in the unlock position.
2. Making sure the CrossFire 8008 is inserted all the way into the CrossFire 8000 Chassis, lock it into place by pushing the card ejectors inward. The catch on the card ejectors should lock into the tabs on the sides of the enclosure.

Note: If the catch does not lock into the tabs or if the module does not seem to fit, **do not force it.** It may not have been properly inserted into the guides.



3. When the CrossFire 8000 Chassis is powered on, the indicators on the CrossFire 8008 light as the power-on diagnostics begin.

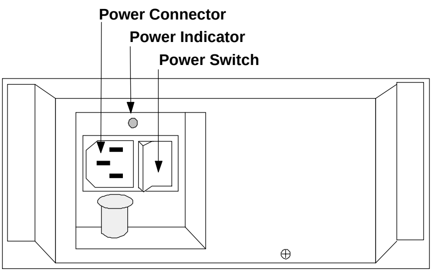
CrossFire 8000 Chassis Power Supplies

The number of power supplies that you need in a CrossFire 8000 Chassis (2-slot) and CrossFire 8000 Chassis (8-slot) depends on the number and type of modules installed, and the type of power supply you are using: 175 Watt or 250 Watt.

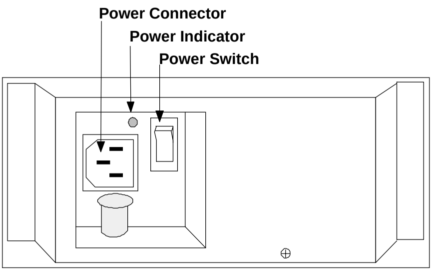
Note: The 175 Watt Power Supply provides 150 watts at 5 V.

The CrossFire 8000 Chassis (2-slot) and CrossFire 8000 Chassis (8-slot) chassis support either 175 or 250 Watt power supplies. Keep in mind that each slot cannot exceed a 75 Watt draw.

Warning: You cannot combine 175 and 250 Watt power supplies in the same chassis.



175 Watt Power Supply



250 Watt Power Supply

The Power Indicator (green) is lit when the power supply is turned on and functioning properly.

Note: If you are upgrading to a 250 Watt Power Supply, you must turn off the unit before removing the old 175 Watt Power Supply.

Calculating Power Supply Requirements

To calculate the power supply requirements:

1. Determine your CrossFire 8008 configuration. If you are unsure of your configuration, refer to your *Assembly and Configuration Test Sheet.*
2. Refer to the CrossFire Configuration Power Consumption table and determine how much power your CrossFire 8008(s) will consume.
3. Note the power consumed by your CrossFire 8008(s).

CrossFire 8008 Configuration	Power Consumed
CrossFire 8008 with 8 DS3 ports	56 Watts
CrossFire 8008 with 12 DS3 ports	62 Watts
CrossFire 8008 with 8 OC-3 MM SC ports	69 Watts
CrossFire 8008 with 12 OC-3 MM SC ports	84 Watts
CrossFire 8008 with 8 UTP ports	69 Watts
CrossFire 8008 with 12 UTP ports	84 Watts
CrossFire 8008 with 8 OC-3 SM ST ports	80 Watts
CrossFire 8008 with 12 OC-3 SM ST ports	101 Watts

Table 38. CrossFire 8008 Configuration Power Consumption

4. Refer to the Power Consumption by Module table to determine how much power will be consumed by other modules in your chassis.

Module	Power Consumption	Module	Power Consumption
CF 8011/F Router RRRR	66 Watts	XLM RRRR	46 Watts
CF 8011/F Router RREE	63 Watts	XLM RREE	43 Watts
CF 8011/F Router RRWW	62 Watts	XLM RRWW	42 Watts
CF 8011/F Router EEEE	60 Watts	XLM JJJ	50 Watts
CF 8011/F Router EEWW	59 Watts	XLM JJEE	44 Watts
CF 8011/F Router WWWW	58 Watts	XLM JJW	43 Watts
CF 8011 Router RRRR	66 Watts	XLM EEEE	40 Watts
CF 8011 Router RREE	63 Watts	XLM EEWW	39 Watts
CF 8011 Router RRWW	62 Watts	XLM WWWW	38 Watts
CF 8011 Router EEEE	60 Watts	XLP RWWW	19 Watts

CF 8011 Router EEWW	59 Watts	XLP EWWW	18 Watts
CF 8011 Router WWWW	58 Watts	XLH 16R	18 Watts

Table 39. Power Consumption by Module

5. Referring to the Power Consumption by SIM Table, determine the number of watts consumed for each WAN SIM (if any) on your modules. If you are unsure of which SIMs are installed, refer to your *Assembly and Configuration Test Sheet.*

Power Consumption for WAN SIMS			
SIM	**Power Consumption**	**SIM**	**Power Consumption**
Serial Compression	6 Watts	RS-232/V.24/ V.28	1 Watt
Basic Rate ISDN (BRI)	2 Watts	V.35	1 Watt
Universal	1 Watt	T1	1 Watt
RS-422/X.21	1 Watt	DDS DSU/CSU	1 Watt

Table 40. Power Consumption by SIM

6. Add the total power consumed by all modules to the total power consumed by all SIMS to obtain the total power consumption on your chassis.
7. Using the total power consumption for your configuration, refer to the appropriate Power Supplies Required table for the type of power supply you will be using to determine the number of power supplies required for your configuration.

Power Supply Requirements Using 175 Watt Power Supplies		
If your power consumption is:	**You must have:**	**For redundancy, you need:**
Up to 150 Watts	1 power supply	2 power supplies
Between 151 and 300 Watts	2 power supplies	3 power supplies
Between 301 and 400 Watts	3 power supplies	4 power supplies

Table 41. 175 Watt Power Supplies Required

Power Supply Requirements Using 250 Watt Power Supplies		
If your power consumption is:	**You must have:**	**For redundancy, you need:**
Up to 250 Watts	1 power supply	2 power supplies
Between 251 and 500 Watts	2 power supplies	3 power supplies
Between 501 and 750 Watts	3 power supplies	4 power supplies

Table 42. 250 Watt Power Supplies Required

Note: If you are upgrading to a 250 Watt Power Supply, you must turn off the unit before removing the old 175 Watt Power Supply.

Replacing or Adding a Power Supply

The CrossFire 8000 Chassis (2-slot) and CrossFire 8000 Chassis (8-slot) power supplies are hot-swappable. When replacing or adding a power supply, the amount of power supplied to a chassis cannot fall below the power requirements for the number of modules that are installed. It may be necessary to temporarily remove modules to meet the power requirements until replacement power supplies are available.

Reasons for inserting a new power supply include:

- Adding a power supply unit in a blank slot.
- Replacing a power supply that has failed.

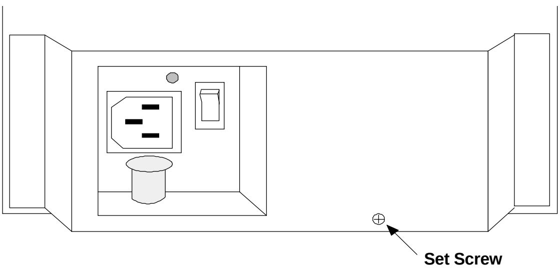
Note: Only Olicom personnel and end users who have been trained are allowed to remove and insert components.

Warning: You should not remove a power supply or a blank panel until you are ready to replace it. Leaving a power supply slot open, with no blank panel, adversely affects the air flow in the unit.

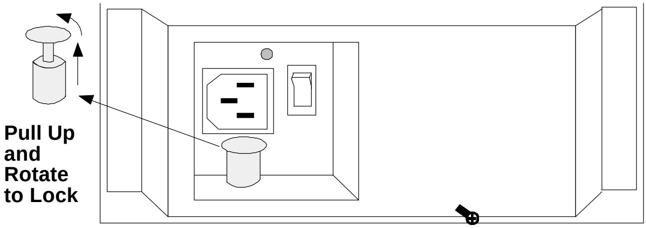
Removing a failed power supply

1. Turn off the power switch.
2. Remove the power cable.
3. Loosen the set screw on the power supply (or blank panel, if you are adding a power supply).

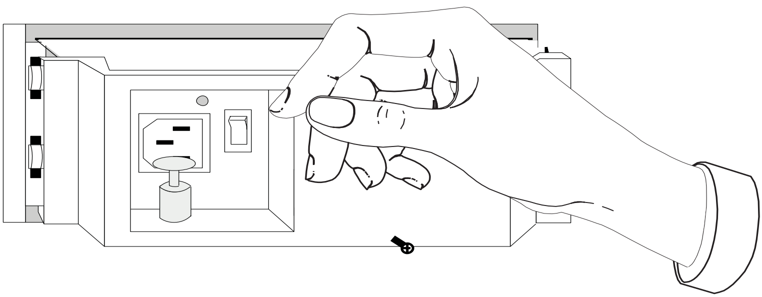
.



4. If you are replacing a power supply, pull up on the head of the locking pin and rotate it a quarter turn to lock in position.



5. Grip the power supply and slide it out of the enclosure. (If you are removing a blank panel, grip it on the bottom, below the set screw and slide it out of the enclosure). Handle the power supply from the bottom. It is normal for the bottom of the power supply to be very warm.



Warning: Hazardous circuitry is accessible with the power supply or blank panel removed. Do not insert your hand or any other object other than a power supply or blank panel in the open enclosure.

Warning: Do not leave the power supply slot open. A new power supply or a blank panel must be installed within two minutes of removing a power supply. Operating a system with an open power supply slot, adversely affects the air flow in the unit and causes the other power supplies to overheat and shut off.

Inserting a New Power Supply:

1. Make sure the locking pin on the new power supply is in the up position. If it is not, pull up on the head and rotate it a quarter turn to the lock in position.

2. Insert the new power supply into the enclosure by sliding the rails on the bottom of the power supply into the guides on the enclosure. **If your power supply has plastic tabs on the sides, push the plastic tabs inward as you are inserting the power supply.** Make sure that the power supply is firmly inserted into the enclosure.
3. Rotate the locking pin a quarter turn to drop it to its original position.
4. Tighten the set screw.
5. Connect the power cable to the unit and to the power source.
6. Power on the new power supply. The power supply indicator should light.

CrossFire 8000 Chassis Does Not Power-On

If the CrossFire 8000 Chassis does not power-on when the power switch is turned on:

1. Turn off the power switch.
2. Make sure that the power cable is securely attached to the unit and to the power supply outlet.
3. Make sure that the power supplied to the unit meets the requirement.
4. Power-on the unit again.
5. If the problem persists, contact the Olicom Technical Resources Center.

Replacing a Module

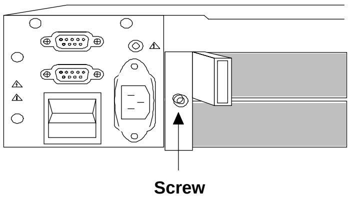
Reasons for inserting a new module include:

- Replacing a module that has failed
- Adding a module in a blank slot to increase the number of ports

The procedure to replace or add a module is the same for the CrossFire 8000 Chassis (2-slot) and the CrossFire 8000 Chassis (8-slot).

Removing a Module or Blank Panel

1. Remove any network or terminal cables connected to the module.
2. Loosen the screw that secures the module or blank panel. If performing this procedure on a CrossFire 8000 Chassis (2-slot) or CrossFire 8000 Chassis (8-slot), you must first loosen the screw to the locking door before you can loosen the module or blank panel screw.



3. Unlock the card ejectors on the module or blank panel by pushing outward.

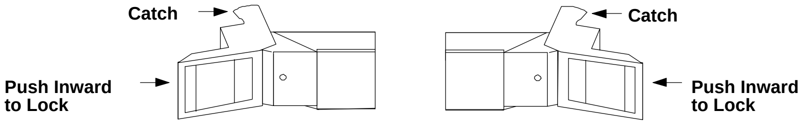
4. Slide the module or blank panel out of the enclosure. Place the module in a protective antistatic bag.

Warning: Hazardous circuitry is accessible with a module removed. Do not insert your hand or any object inside the open enclosure of the chassis.

Inserting a Module:

1. Insert the module into the enclosure by sliding the top module board into the top guides of the slot in the enclosure. To seat the module, the card ejectors must be in the unlocked position.

2. Make sure the module is inserted all the way into the enclosure. Lock the module into place by pushing the card ejectors inward. The catch on the card ejectors should lock into the tabs on the sides of the enclosure. If the catch does not lock into the tabs, or if the module does not seem to fit, **do not force it**. It may not have been properly inserted into the guides. Remove the module and reinsert.



3. Power on the CrossFire 8000 Chassis. The indicators on the module(s) will light as the power-on diagnostics begin. For information about the power-on sequence of a module, refer to Chapter 2, "Installation"

4. After you have verified that the module is operational, tighten the screw to secure the module. If performing this procedure on a CrossFire 8000 Chassis (2-slot) or CrossFire 8000 Chassis (8-slot), you must now also tighten the screw to the locking door.

5. Connect any network or terminal cables to the module. For information on how to connect devices, refer to Chapter 2, "Installation"

6. Replacing a Fan Module

The CrossFire 8000 Chassis (2-slot) and CrossFire 8000 Chassis (8-slot) support a fan module that operates with a 175 or 250 Watt power supply. Any fan module installed in the chassis must be of the same type. Keep in mind that the fan module used with the 175 Watt power supply rotates in a different direction than the fan module used with the 250 Watt power supply.

Reasons for inserting a new fan module include:

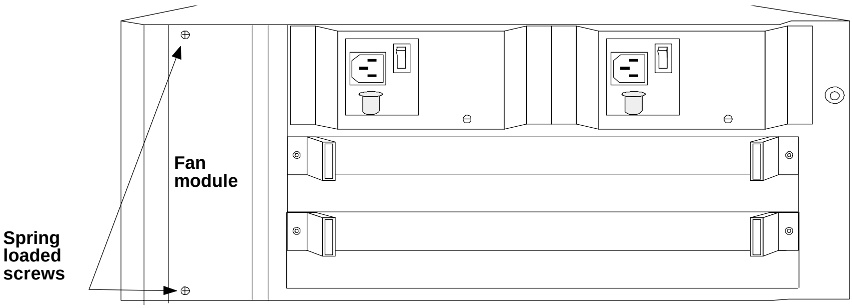
- The fan module fails
- The fan module becomes noisy in an office environment.

Note: Only Olicom personnel and end users who have been trained are allowed to remove and insert fan modules.

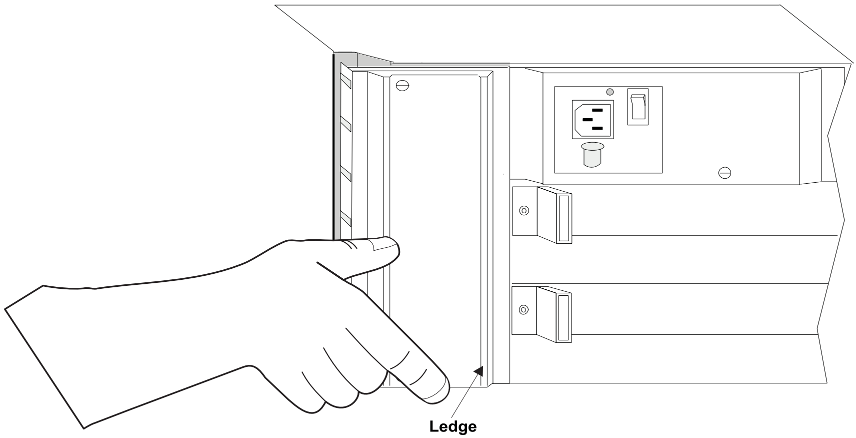
Warning: You should not remove a fan module until you are ready to replace it. Removing a fan module adversely affects the air flow in the unit.

Removing the Fan Module:

1. Loosen the spring loaded screws.



2. Grip the fan module under the ledge as shown and slide it out of the enclosure.



Warning: Hazardous circuitry is accessible with the fan module removed. Do not insert your hand or any other object inside the open enclosure.

Inserting the New Fan Module:

1. Slide the rails on the top and bottom of the fan module into the guides on the enclosure. Make sure that the fan module is firmly inserted into the enclosure. The fans should begin rotating. You can verify this by looking through the vents on the side of the chassis.

2. After you have verified that the new fan module is operating, tighten the spring-loaded screws.

❑

Appendix B. Error and Status Messages

The alphanumeric display on the CrossFire 9150/9250 Processor Module will normally show the system name that has been configured in the management applications. However, if an error occurs, the display will switch to an alternating numeric and alphabetic display of error codes.

Sections

- Bootstrap ROM Messages
- Launcher Program Messages
- Messages from Online Operation
- Error and Fault Messages

The numeric error display may be as follows:

E	0	1		2	:	0	4

The "E" is a type indication. It may have the following values:

B Message from the bootstrap ROM

L Message from launcher program

M Message from online operation

E Errors and faults

The "01" is the error code. This is listed in the table below. In this example error 01 indicates that a port has been automatically disabled.

The "2:04" is the so-called extended code. This provides additional information about the fault. In this case it means that the faulty port is port number 4 on expansion module number 2.

The alphanumeric display shows an abbreviated error text. In the example used here (the automatic disabling of an ATM port), the alphanumeric display will show:

P	O	R	T	A	D	S	B

This is an abbreviation of "Port Auto-Disabled".

Each error has a "Severity level". If there are two errors, only the most severe one is displayed.

Errors with a severity level of 3 or less are not considered serious. The error will be removed from the display after 15 minutes.

Severity levels are shown below.

Severity level	Explanation
0	Information
1	Notice, this is not an error condition but may require special handling
2	Warning
3	Error, the system continues with this error
4	Critical, must be corrected, the system continues in a degraded state
5	Alert, immediate correction required
6	Panic, the system will close down or restart

Table 43. Severity levels

Bootstrap ROM Messages

The table below lists possible bootstrap ROM messages.

Code	Severity	Extended code	Text	Description
BOOT			BOOTING	Switch start up
01	0		INITBOOT	Initializing bootstrap software
02	0		TEST CPU	Testing CPU
03	0		TESTMRAM	Testing minimum RAM
04	0		TEST ITR	Testing interrupts
05	0		TEST TIM	Testing timer
06	0		TEST UAR	Testing UART
07	0		TEST ETH	Testing Ethernet controller
08	0		TESTARAM	Testing all RAM
09	0		ACT LOAD	Activating loader
10	0		CHK SWD	Checking software status word
11	0	N	LOADIMG	Downloading image N (N=1 or 2) from flash memory
21	0		REQ BOOT	Requesting software via BOOTP
22	6		CHKSUMER	Flash memory microcode checksum error, requesting software via BOOTP

Code	Severity	Extended code	Text	Description
23	4		SWDCORR	Two images present and both software status words corrupted or inconsistent, starting BOOTP
24	0	NNNN	LOADING	Downloading via BOOTP, NNNN is a packet counter
25	0		BOOTCPLT	BOOTP completed
26	4		BOOTABRT	BOOTP aborted due to TFTP timeout, restarting BOOTP
27	5		BOOTFILE	BOOTP terminated, the file in BOOTP response is not present, retrying
31	6		ETHOFAIL	Ethernet operation failure, retrying
41	0		STARTIMG	Starting normal image
42	0		STARTTIM	Starting test image
43	0		STARTBIM	Starting BOOTP loaded image
51	6		BPROMCKS	Bootstrap ROM checksum error, system halted
52	6	NNNN	CPUFAIL	CPU test failure, NNNN is the subtest ID, system halted
53	6	NNNN	RAMFAIL	RAM test failure, NNNN is the subtest ID, system halted
54	6		TIMFAIL	Timer test failure, system halted

Code	Severity	Extended code	Text	Description
55	6		UARFAIL	No UART present, system halted
56	4		ETHFAIL	Ethernet chip test failure, system halted
57	6		NO MRAM	No minimal RAM detected or RAM is faulty, system halted
58	6		IMPLOAD	Software load from flash memory failed but the checksum was okay, system halted
59	6		EEPROM?	Backplane EEPROM is invalid, system halted
60	6		MINRAM	Not enough RAM to execute the image loaded via BOOTP, system halted
61	6		EXP IMG	Bootstrap ROM expected software in flash memory after BOOTP and first activation of the launcher program, system halted
62	6		BCKPLANE	Invalid backplane hardware product ID in EEPROM
70	5	1	MCHEADER	Corrupted magic cookie in the multichunk header, retrying
		2	MCHEADER	Incorrect pad field in the multichunk header, retrying

Code	Severity	Extended code	Text	Description
		3	MCHEADER	Incorrect or inconsistent number of chunks in the multichunk file, retrying
		4	MCHEADER	Incorrect or inconsistent total checksum, retrying
		5	MCHEADER	Received file is too short, retrying
		6	MCHEADER	Received file is too long, retrying

Table 44. Bootstrap ROM Messages

Launcher Program Messages

The table below lists possible launcher program messages.

Code	Severity	Extended code	Text	Description
01	0		LAUNCHER	Launcher started
02	0	N	LOADIMG	Loading image N from flash memory
03	0	N	SAVEIMG	Saving image N to flash memory
04	0		STARTSW	Starting software
10	6	1	MCHEADER	Corrupted magic cookie in the multichunk header in RAM, system halted
		2	MCHEADER	Incorrect pad field in the multichunk header in RAM, system halted
		3	MCHEADER	Incorrect or inconsistent number of chunks in the multichunk file in RAM, system halted
		4	MCHEADER	Incorrect or inconsistent total checksum, system halted
11	6	N:1	FLHEADER	Incorrect marker field in a chunk in RAM, N is the chunk number, system halted

Code	Severity	Extended code	Text	Description
		N:2	FLHEADER	First file in RAM is not launcher program file as expected, N is the chunk number, system halted
		N:3	FLHEADER	Second file in RAM is not the main CPU program file as expected, N is the chunk number, system halted
		N:4	FLHEADER	Checksum error in a file in RAM, N is the chunk number, system halted
		N:5	FLHEADER	Incorrect pad fields in the file header in RAM, N is the chunk number, system halted
21	6	1	MCHEADER	Corrupted magic cookie in the multichunk header in flash memory, system halted
		2	MCHEADER	Incorrect pad field in the multichunk header in flash memory, system halted
		3	MCHEADER	Incorrect or inconsistent number of chunks in the multichunk file in flash memory, system halted

Code	Severity	Extended code	Text	Description
		4	MCHEADER	Incorrect or inconsistent total checksum, system halted
22	6	N:1	FLHEADER	Incorrect marker field in a chunk in flash memory, N is the chunk number, system halted
		N:2	FLHEADER	First file in flash memory is not launcher program file as expected, N is the chunk number, system halted
		N:3	FLHEADER	Second file in flash memory is not the main CPU program file as expected, N is the chunk number, system halted
		N:4	FLHEADER	Checksum error in a file in flash memory, N is the chunk number, system halted
		N:5	FLHEADER	Incorrect pad fields in the file header in flash memory, N is the chunk number, system halted

Table 45. Launcher Program Messages

Messages from Online Operation

The table below lists possible messages from online operation.

Code	Severity	Extended code	Text	Description
00	0		STARTING	The actual switch software is starting
01	0		TESTEPRO	Testing EEPROM
02	0		CPUSWAP	Processor module swapped
03	0		DEFCONFI	Using default configuration
04	0		TMPCONFI	Using temporary configuration
06	0		DTCXMODU	Detecting expansion modules
07	0	N	NEWXMODU	Detected new expansion module in slot N
08	0	N	MISXMODU	Detected missing expansion module in slot N
09	4		MISFEATU	Detected missing traffic management module but the module is enabled
21	0	S:NN	PORTDSBL	Port NN in expansion module S disabled by management

Code	Severity	Extended code	Text	Description
22	0	S:NN	PORTLOOP	Port NN in expansion module S has loop-back enabled by management
23	0	S	MODUDSBL	Expansion module S disabled by management
31	1	C	WRITEFLS	Rewriting flash memory, C= 1:config1, 2:config2, 3:SW1, 4:SW2
32	1	NNNN	LOAD SW	Downloading software, NNNN is the packet counter
51	2		CONGEST	Global congestion
52	2		INVCELLS	Invalid cell rate
53	2	NN	PORTCNGS	Core Access Point congestion, Core Access Point=NN
54	3	NN	TEMPWARN	Temperature warning, NN is the temperature in Celsius
61	4		SNMPAUTH	SNMP message authentication failure
62	5		ILGLLOGI	OBM illegal login attempt (max. login attempts exceeded)

Code	Severity	Extended code	Text	Description
63	4		ILGLCALO	OBM call-out failed due to illegal password
64	4		CLBFAIL	OBM call-back failed due to illegal password

Table 46. Possible Messages from Online Operation

Error and Fault Messages

The table below lists possible error and fault messages.

Code	Severity	Extended code	Text	Description
01	4	S:NN	PORTADSB	Port NN in expansion module S automatically disabled
02	5		FANFAIL	Fan failure
03	5		NPSUFAIL	Power supply failure, N is the power supply number
04	6		CPUEEPRO	Processor module EEPROM corrupted
05	6		FTREEPRO	Traffic management module EEPROM corrupted
06	6		BCKEEPRO	Backplane EEPROM corrupted
07	5	N	XMDEEPRO	Expansion module EEPROM corrupted, module number is N
08	6		TEMPCRIT	Temperature has reached critical level, the switch will be powered down
09	6	NN	IPRTFAIL	Core Access Point loop-back failure, the switch will halt, NN is the Core Access Point number
10	6		SWCHSTOP	The switching system has an unrecoverable fault, system halted

Code	Severity	Extended code	Text	Description
11	6		HWCAPAB	The image loaded via BOOTP requests hardware capabilities which cannot be fulfilled, system halted
12	6		HW CONS	Hardware consistency check has detected invalid expansion module configuration (i.e. more than three 622 modules), system halted
13	6	N	PCI STOP	PCI error interrupt detected N=1 SERR N=2 PERR, system halted
14	6	N	FPGASTOP	Download of FPGA ‘N’ failed. N=1 EPD N=2 SARMUX N=3 ATLANTIC N=4 PACIFIC, system halted
15	4	N	XMDUNKNO	Unknown expansion module type in slot N
16	6		SAR MUX	SAR MUX FIFO full, system halted
17	6		SWTCHERR	Switching system error, system halted
18	4		ETHFAIL	Ethernet chip test failure, system halted

Code	Severity	Extended code	Text	Description
19	6		EEPROM?	Backplane EEPROM is invalid, system halted
20	6		DSP STOP	Download of code to traffic management module failed

Table 47. Possible Error and Fault Messages

❑

Index

Numerics

A

B

C

D

M

N

O

P

Q

R

S

T

U

V

W

X

Olicom A/S
Nybrovej 114
2800 Lyngby
Denmark
Tel: (+45) 45 27 00 00
Fax: (+45) 45 27 01 01

Olicom, Inc.
1680 North Prospect Drive
Richardson, TX 75081
USA
Tel: (+1) 972 907 4600
Fax: (+1) 972 671 7525

World Wide Web URLs

http://www.olicom.com
http://www.olicom.dk

DOC-6990/5.1.5