

Management Software

AT-S20



User's Guide

For use with the AT-3726XL, AT-3716XL, AT-3714FXL,
AT-3726 and AT-3714F Switches

Version 3.1

PN 613-10773-00 Rev. C

 **Allied Telesyn**

Simply Connecting the World

Copyright © 1998, 1999 Allied Telesyn International, Corp.
960 Stewart Drive Suite B, Sunnyvale CA 94086

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn International, Corp.

CentreCom is a registered trademark of Allied Telesyn International, Corp.

Netscape Navigator is a registered trademark of Netscape Communications Corporation. Ethernet is a registered trademark of Xerox Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn International, Corp. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn International, Corp. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

Preface	Preface-i
Purpose of This Guide	Preface-i
How This Guide is Organized	Preface-ii
Document Conventions	Preface-iii
Related Guides	Preface-vi
Chapter 1	
Features, Menu Tree, and Defaults	1-1
Software Features	1-1
Switch Naming and Security Features.....	1-3
Switch Default Settings	1-4
Setting Switch Defaults	1-5
Menu Tree	1-6
Chapter 2	
Getting Started with Local and Remote Omega	2-1
Getting Started with Local Omega	2-1
Configuring Your Terminal Emulator Program	2-1
Starting an Omega Session.....	2-2
Entering an IP Address	2-3
Quitting a Session	2-3
Remote Management Requirements	2-4
Managing Your Switch in a TCP/IP-based Network	2-4
TCP/IP with BootP or DHCP	2-4
TCP/IP without BootP	2-5
Non-TCP/IP Networks	2-5
Configuration Options	2-5

Chapter 3

Getting Started With Browser Management	3-1
Browser Requirements	3-1
Starting a Browser Session	3-2
Navigating Around the Switch	3-3

Chapter 4

Configuration and Administration	4-1
Connecting to a Remote System	4-3
Pinging a Remote System	4-4
Enabling or Disabling a Port	4-5
Configuring IP Parameters	4-6
Naming the Switch	4-8
Change/Delete the Switch Name	4-10
Naming the Port	4-11
Changing or Deleting a Port Name	4-13
Assigning a Password to the Switch	4-14
Forgetting Your Password.....	4-14
Enabling Store-and-forward or Cut-through (Fragment-Free)	4-15
Enabling Auto-Negotiate/Half-Duplex/Full-Duplex	4-17
Enabling Transmit Pacing	4-18
Setting Up a VT100	4-19
Setting Up a Generic (Dumb) Terminal.....	4-19
Setting Full-Duplex/ Half-Duplex Mode	4-19
Setting Baud Rates	4-20
Setting Time Out Protection	4-21
Deleting a Previously Configured Timeout Value	4-21
Enabling/Disabling Omega Access	4-22
Local Omega.....	4-22
Remote Omega.....	4-22
Web-based Omega	4-22
Enabling/Disabling Backpressure	4-23
Performing Software Upgrades Via TFTP	4-24
Conditions for Network Downloads via TFTP	4-24
Using TFTP	4-24
Downloading from One Switch to Another	4-25
Broadcast Updated Software to All Systems	4-26
Using XModem to Download.....	4-27
Configuring for Bridging	4-28
Configuring Spanning Tree Parameters.....	4-29
Designating the Root Port	4-31
Selecting Global Configuration	4-33
Enabling/Disabling Port Trunking	4-34

Chapter 5

Virtual LAN Configuration	5-1
Configuration Information.....	5-5
Port Information	5-5
Adding a New VLAN	5-7
Port to VLAN Configuration.....	5-9
Deleting a Port from a VLAN or Changing Port's VLAN Assignment.....	5-10

Chapter 6

Monitoring	6-1
Activity Monitor	6-2
MAC Address Table	6-3
Show All MAC Addresses.....	6-4
Show By Port MAC Addresses.....	6-4
Get Port from MAC Address	6-5
Static MAC Addresses	6-6
Show All Static MAC Addresses.....	6-6
Show Per Port Static MAC Addresses.....	6-7
Delete/Add Static MAC Address	6-8
Add/Delete Static MAC Addresses and Selecting Ports for Multicasts.....	6-9
Clearing Static MAC Table.....	6-11
Locating Your Switch's MAC Address	6-11
Security/Source Address Table	6-12
Source Address Learning Mode.....	6-13
Security Threshold	6-15
Intruder Protection	6-17
Setting Security/Source Address Table Options	6-19
Setting Source Address Learning Mode	6-19
Setting Security Threshold.....	6-20
Setting Number of MAC Address	6-20
Setting Intruder Protection	6-21
Mirror Port	6-23
Port Status	6-25
Port Numbering	6-26
Statistics: Received and Transmitted Ethernet Frames	6-28
Viewing Switch Statistics.....	6-28
Viewing Port Statistics.....	6-33
Interpreting the Graphs	6-34
Using the Graphs as a Monitoring and Diagnostics Tool	6-35

Chapter 7

Diagnostics 7-1
Resetting the Switch 7-2
 To Reset the Switch..... 7-2
Running Diagnostics 7-3
Getting Help 7-4
Resetting Statistics Counters 7-5
 To Reset Switch (System) Counters..... 7-5

Appendix A

Spanning Tree Protocol A-1
Concepts A-1
 Features..... A-2
 Parameters A-2
 Operations..... A-3

Index Index-1

Preface

Purpose of This Guide

The purpose of this guide is to instruct network administrators on how to manage their switch by using the Omega management software to configure and monitor the device. By using the Omega software, a network administrator can manage the switch in several ways:

- Remotely
- Locally
- Web-based

Network administrators should be familiar with Ethernet switches, bridging, and the spanning tree protocol.

How This Guide is Organized

This guide is composed of the following sections:

Chapter 1, Features, Menu Tree, and Defaults, which presents the major switch features, a menu tree that displays the primary and secondary menus, and a list of switch defaults in tabular form.

Chapter 2, Getting Started with Local and Remote Omega, provides instructions on how to set up the switch for remotely or locally managing the switch.

Chapter 3, Getting Started With Browser Management, provides instructions on how to use a browser to manage the switch.

Chapter 4, Configuration and Administration, describes the management tasks according to switch, configuration, port configuration and administration.

Chapter 5, Virtual LAN Configuration, provides a brief discussion of Allied Telesyn's implementation of VLANs.

Chapter 6, Monitoring, describes the tasks related to monitoring the switch.

Chapter 7, Diagnostics, describes the testing procedures using the Omega menus.

Appendix A, Spanning Tree Protocol, provides a brief explanation of Spanning Tree Algorithm and its use with the switch

At the end of this guide is an Index according to subject matter.

Document Conventions

The conventions used in this guide are as follows:

- For DEC VT100 or ANSI (the default) terminal configuration:

When directed	You must
To select an option	Highlight the option by pressing the Up (↑) or Down (↓) arrow key; then press RETURN or Type the first character of the option you want at the prompt and then press RETURN . If two or more options have matching initial characters, type the first characters enough times until the option you want is highlighted; then press RETURN .
To enter information, for example, IP address	Type the correct IP address and press RETURN
To return to the previous screen (Omega only)	Select the option or Press ESC
To return to the previous screen (Browser)	Select the Back button
To return to Main Menu (Omega)	Highlight Return to Main menu... and then press RETURN
To return to Main Menu (Browser)	Select the Main Menu icon.

All procedures in this guide are based on the default terminal configuration.

- ❑ For generic (dumb terminal) terminal configuration:

When directed	You must
To select an option	<p>Type the first character of the option you want and then press RETURN.</p> <p>If two or more options have matching initial characters, type enough characters for Omega to distinguish your choice from the other options; then press RETURN. To guide you, the characters you must type are in uppercase.</p> <p>For example: Mirroring configuration MAC Address Table</p> <p>If options on a list are preceded by numbers (1:, 2:, 3:, etc.), type the number corresponding to your choice at the prompt; then press RETURN.</p>
To enter information, for example, IP address	Type the correct IP address at the prompt and press RETURN .
To return to the previous screen	Press RETURN after making an entry.

- ❑ Selecting a configuration:

Omega denotes a default configuration by preceding it with a >. For example, DEC VT100 configuration is shown to be the terminal type in the following screen:

```

> VT100-compatible / ANSI
Generic dumb terminal
```

The default selection in a DEC VT100 terminal configuration also appears darker. If you change the option, Omega changes the user interface by moving the > to the new selection. For example:

```
VT100-compatible / ANSI
> Generic dumb terminal
```

❑ Selecting menu options:

Menus and submenus are in courier type. Menu hierarchies are separated by a >.

Menu: Administration

Menu: Administration>IP parameters

❑ Entering variables:

Variables are information you must supply, as in IP addresses, MAC addresses, or port numbers. Variables are enclosed in angle brackets (< >).

For example, to configure a specific port:

Select Port status and
configuration><PortNumber>

where <PortNumber> can be Port 1, or 2, and so on.

Note

A note provides additional information.

Warning

A warning informs you that performing or omitting a specific action may result to bodily injury.

Caution

A caution informs you that performing or omitting a specific action may result to equipment damage or loss of data.

Related Guides

Allied Telesyn wants our customers to be well informed by providing the most up-to-date and easily accessible guides and other technical information.

Visit our website at: www.alliedtelesyn.com and download the following guide:

AT-3726XL, AT-3716XL, AT-3714FXL Installation Guide,
613-10766-00

AT-3726, AT-3714F Installation Guide,
613-10708-00

The following guides are shipped with the product:

AT-3726XL and AT-3716XL Quick Install Guide,
613-10769-00

AT-3726XL and AT-3716XL Translated Safety Information Booklet, 613-10768-00

AT-3714FXL Quick Install Guide,
613-10767-00

AT-3714FXL Translated Safety Information Booklet,
613-10770-00

AT-A10, AT-A11 Quick Install Guide,
613-10742-00

AT-3726 Quick Install Guide,
613-10668-00

AT-3726 Translated Safety Information Booklet,
PN 613-10673-00

AT-3714F Quick Install Guide,
613-10707-00

AT-3714F Translated Safety Information Booklet,
PN 613-10717-00

AT-3701, AT-3701F/SC Quick Install Guide,
613-10669-00

Chapter 1

Features, Menu Tree, and Defaults

Software Features

The switches have the following major software management features:

- ❑ Supports industry-standard 802.1Q VLAN tagging and supports a maximum of 32 port-based and tag-based VLANs (XL versions only)
- ❑ Security (XL versions only)
- ❑ Backpressure (XL versions only) and transmit pacing provide one-way flow control to relieve congested networks
- ❑ Port mirroring
- ❑ Firmware is factory-installed and ready to use
- ❑ User configuration for store-and-forward and cut-through packet switching for non-XL versions; store and forward only for XL versions
- ❑ Auto-negotiation on 10 Mbps and 10/100 Mbps UTP ports in compliance with IEEE 802.3u
- ❑ Multicast address support which allows users to specify the recipient port for multicast packets
- ❑ All UTP and fiber ports are software configurable for full- and half-duplex
- ❑ Port B (optional uplink) can be configured as either a 10/100 Mbps UTP or a 100 Mbps fiber uplink

- ❑ Port Trunking allows configuring of Ports A and B to function as a single uplink port which effectively increases the throughput of the connection.
- ❑ Spanning Tree Protocol (STP) support
- ❑ System configuration, management, and diagnostics using Allied Telesyn's Omega interface, accessible locally via an RS232 asynchronous terminal port, remotely via Telnet, or a web browser.
- ❑ Software upgrades using Xmodem via the RS232 port or TFTP to download software to switches on the network
- ❑ Broadcast software from a switch to one or all switches on the network
- ❑ Web-based management
- ❑ SNMP agent that allows the switch management from the user's network management station
- ❑ Support for BootP and Dynamic Host Configuration Protocol (DHCP) for IP parameters
- ❑ Support for DEC VT100/ANSI (the default), or generic (dumb) terminal configuration
- ❑ Internet Control Message Protocol (ICMP) Echo PING support
- ❑ Domain name service support (DNS)

Switch Naming and Security Features

The switch provides configurable options for customizing for example,

- ❑ Naming the switch and its ports

Names are more descriptive and easier to remember than addresses.

Port names can be associated with the user assigned to the port or an office location. The need to use symbolic names becomes more apparent as you add more switches and therefore multiply the number of ports you must manage.

- ❑ Enabling security features

Although passwords are not required to access the management menus, with the Omega Options menu, you can prevent (disable) either Local Omega, Remote Omega, or web-based Omega, create password protection, and enable timeout.

A timeout value automatically terminates a management session after a given period when someone leaves a current session unattended.

Switch Default Settings

Table 1-1 lists the switch default settings.

Table 1-1 Switch Default Settings

Settings	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
Get community string	public
Set community string	private
Trap community string	public
Port mirroring state	Disabled
Spanning Tree Protocol	Disabled
Omega Access	Enabled
System Name	None
Password (Omega)	No password assigned
Download Password	ATS20
Port Priority	128
Port Path Cost	100 (AT-3726)
Auto-negotiate, Full-duplex or Half-duplex (per port)	Auto-negotiate (AT-3726XL, AT-3726, AT-3716XL) Half-duplex (AT-3714FXL, AT-3714F)
Spanning Tree Priority	32768
Maximum Aging Time	20 seconds
Forwarding Delay	15
Hello Time	2 seconds
Transmit Pacing/Backpressure	Disabled
Bridge Identifier (STP)	32768 (bridge priority)
Port Priority (STP)	128
Port Cost (STP)	100 for 10 Mbps ports 10 for 100 Mbps ports
Domain Name	None
Timeout Value	5 minutes
Default VLAN Name	Default VLAN

Setting Switch Defaults

To set your switch to the factory defaults, do the following:

Warning

This operation deletes existing switch configurations.

1. Attach a terminal or PC to the RS232 port located on the front panel of the switch and start the terminal emulation program.
2. Press **RESET** located on the right side of the switch's front panel.
3. Immediately press any key when you see `Hit any key to run diagnostics or to reload system software.` A menu then displays.
4. Select `D` from the menu. The following warning message displays:

```
WARNING: This will erase all current
configuration data!
```

```
Continue? Y/N
```

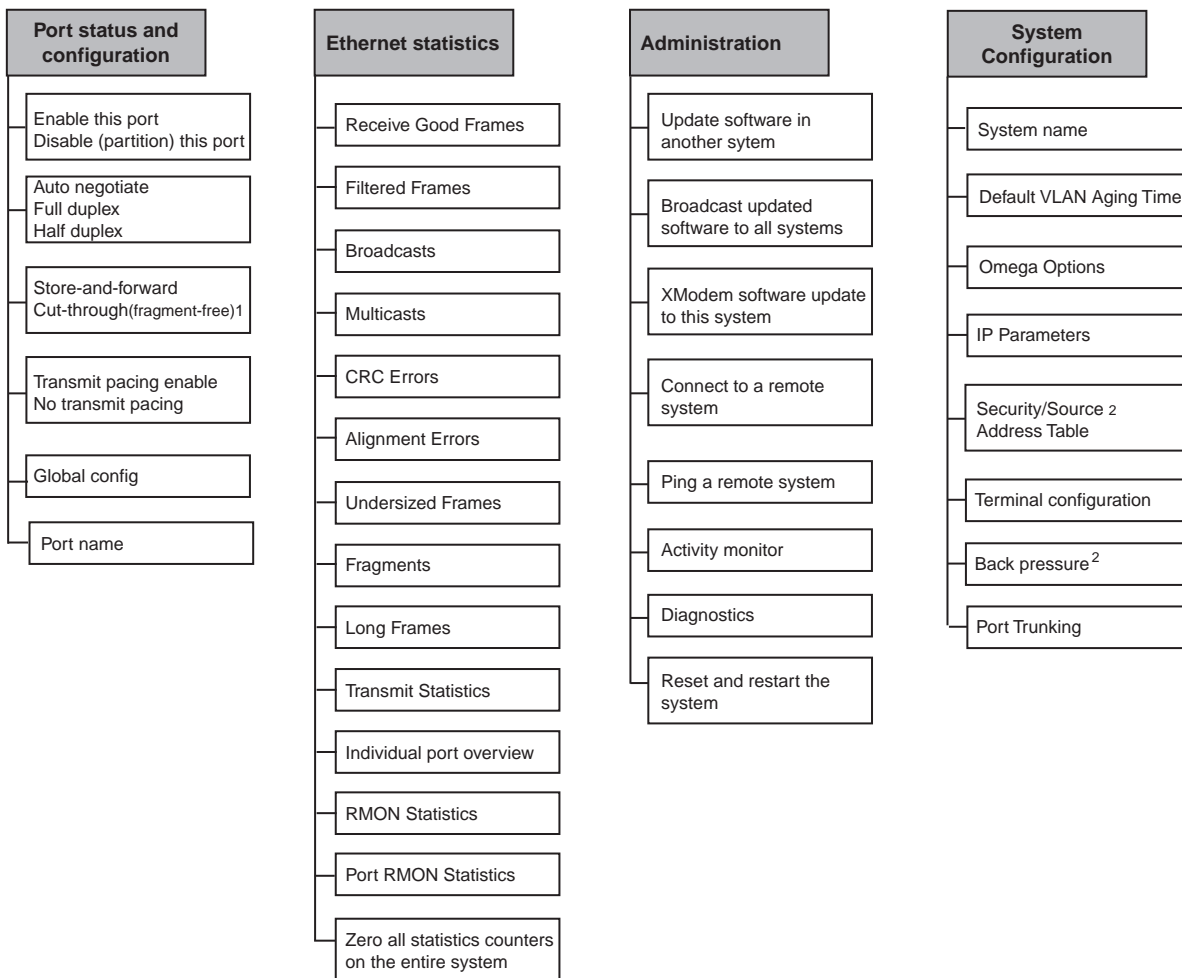
5. Select `Y`.

```
The system displays: All configuration data has
been reset to factory default values.
```

6. Press **B** to boot the switch software.

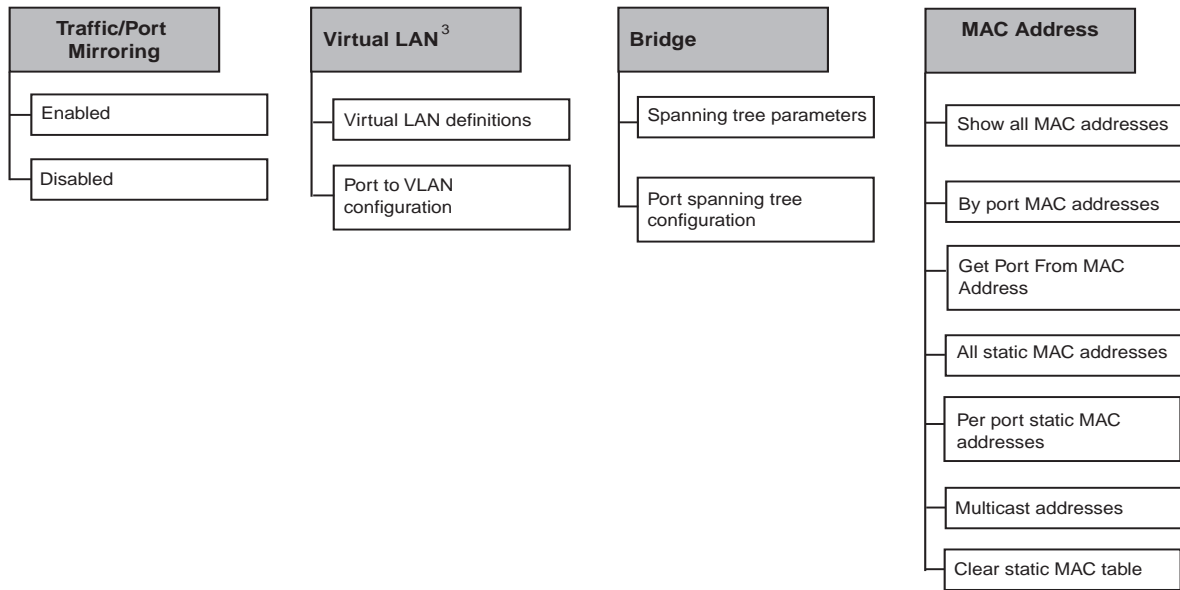
Menu Tree

The following illustration shows the Omega Menu tree.



1. For non-XL versions only
 2. For XL versions only

Figure 1-1 Omega Menu Tree (1 of 2)



3. For XL versions only

Figure 1-2 Omega Menu Tree (2 of 2)

Chapter 2

Getting Started with Local and Remote Omega

Getting Started with Local Omega

To locally managing your switch, simply connect a terminal or PC directly to the switch's RS232 port to access the Omega menus. See the following sections.

Configuring Your Terminal Emulator Program

To set the terminal emulator program, do the following:

1. Access the terminal emulator program on your PC (VT100) and set the following:
 - Data bits to 8
 - Stop bits to 1
 - Parity to None
 - Full-duplex (using straight-through cable)
 - Autobaud

Note

The diagnostics that run during the system boot output only at 9600 bps. Therefore, Allied Telesyn recommends this speed setting.

2. Press **<Return>** several times to ensure baud autoconfiguration.

Starting an Omega Session

Once you have established a connection to the switch, the Omega Main Menu displays.

The banner reflects the name of your switch. This example shows that the AT-3714FXL switch is operating and the switch name is Accounting.

```
Allied Telesyn AT-3714FXL Ethernet Switch
Accounting
Main Menu

Port status and configuration

Ethernet statistics

Administration

System configuration

Traffic/Port Mirroring

Virtual LANs

Bridging

MAC Address Table

Quit
```

Figure 2-1 Omega Main Menu (AT-3714FXL)

By selecting `System Configuration` from the main menu, the following screen displays. The default settings are always in bold print on the screen.

```
Allied Telesyn AT-3714FXL Ethernet Switch
Accounting
Main Menu

Password: Null (not configured)

Timeout: 5

Local Omega Enabled
Disabled Local Omega

Remote Omega Enabled
Remote Omega Disabled

Web-based Omega Enabled
Exclude Web-based omega

Return to system Configuration Menu ...
```

Figure 2-2 System Configuration Menu

Entering an IP Address

If you have a TCP/IP network but do not have a BootP server, or DHCP server, you must enter an IP address and subnet mask for the switch through Omega.

1. Select `System administration IP Parameters` from the Main Menu.
2. Select `IP address` and enter a unique IP address for the switch.
3. Select `Subnet mask` and enter the switch's subnet mask.
4. Select `Gateway address` and enter the address if you are sending packets to another IP network. The gateway address is the router that can forward packets to the other IP networks.

Once the switch has an IP address, you may initiate Omega sessions to it via Telnet. Note that you can only have one Telnet session operating at any one time. The session can be either inbound or outbound. If you have an inbound session to Omega, you do not have the option of starting a new session (outbound connection). Therefore, if you are already using Telnet, the Omega option `Connect to a remote system` will not be available (described in detail in Chapter 4, **Connecting to a Remote System** on page 4-3). In addition, a local RS232 connection blocks a Telnet session and vice versa.

Note

For non-IP environments, you can use MAC addresses to connect to remote Allied Telesyn switches only if there are no routers between the two switches. If you have assigned unique names, you may use these also.

Quitting a Session

Select `Quit` from the Main Menu to terminate the session. If you accessed the switch through the network, selecting `Quit` also cuts the connection.

It is important to select `Quit` when you are done with Omega; otherwise, you may block other remote sessions, local sessions, or software downloads. To avoid possible lockouts, see **Setting Time Out Protection** on page 4-21.

Note

After you have configured your switch using the Omega management software, you must quit the session and disconnect the RS232 cable.

Remote Management Requirements

You can remotely manage your switch, but first you must have one of the following:

- ❑ The switch's pre-configured MAC address (located below the RS232 Terminal Port label on the switch's front panel)
- ❑ A unique IP address if you use TCP/IP (by either assigning one to the remote switch or by having your BootP/DHCP server provide the needed parameters)
- ❑ A unique name for the switch that you assign via Omega (see **Naming the Switch** on page 4-8).

Managing Your Switch in a TCP/IP-based Network

To manage the switch in a TCP/IP based network, you must first:

- ❑ Configure the switch's IP parameters, or
- ❑ Automatically get an IP address via BootP or DHCP

Note

You do have the option to manage the switch using either SNMP or Omega Remote, via Telnet or web browser.

TCP/IP with BootP or DHCP

The function of the BootP utility within an IP server is to enter an IP address into the switch. Whenever you reset or power on/off the switch, the switch transmits a request packet to the server every three seconds to obtain the required IP parameters. (The BootP utility and the DHCP both make three attempts each.)

If the requesting switch does not receive a BootP or DHCP response after the third request, it will operate with a computed pseudo IP address based on the switch's MAC address for Allied Telesyn switch-to-switch communication, i.e., downloads.

If the switch receives a BootP or DHCP response, it extracts the IP address, Subnet Mask, and Gateway/Router address from the response packet and uses these parameters to configure itself until the next power-on or reset. Additionally, if the BootP response packet specifies a filename and a TFTP host address, then the switch sends a TFTP "get" request to the specified host using the specified filename. This initiates a TFTP download of operating software and allows you to maintain the downloaded server software.

TCP/IP without BootP

To manage the switch using SNMP, Telnet or web browser, you must at least enter the IP address and subnet mask using the Omega menus.

Non-TCP/IP Networks

To manage your switch on a non-TCP/IP network, you need to locally connect to one switch in the segment (see **Configuration Options** on page 2-5). You can then connect to other segments on the same segment using the techniques described in Chapter 4, **Connecting to a Remote System**.

Note

You cannot manage the switch using a web browser without configuring TCP/IP information.

Configuration Options

Network administrators can use the configurable options for their individualized switch performance. For example:

- ❑ Name the switch and its ports

Names are more descriptive and easier to remember than addresses.

Port names can be associated with the user assigned to the port or an office location. The need to use symbolic names becomes more apparent as you add more switches and therefore multiply the number of ports you must manage.

- ❑ Enable security features

Although passwords are not required to access the management menus, with the Omega Options Menu, you can prevent (disable) either Local Omega, Remote Omega, or web-based Omega, create password protection, and enable timeout.

A timeout value automatically terminates a management session after a given period when someone leaves a current session unattended.

Proceed to Chapter 4, **Configuration and Administration** and Chapter 6, **Monitoring**.

Chapter 3

Getting Started With Browser Management

Browser Requirements

To use AT-S20 software via a browser, you need the following:

- ❑ A computer connected to any network port
- ❑ A Web browser, such as Netscape Navigator®, installed on the computer
- ❑ The IP address of the switch (see Chapter 2, **Configuration Options**)

Note

While only one local or remote Omega session can be opened, there can be multiple web-based sessions opened at any time.

Starting a Browser Session

To access the switch using your browser, do the following:

1. If your network is using a proxy server, you will need to make exceptions for the switches that you want to manage. Refer to the documentation provided with your web browser.

Note

At minimum, you must have Netscape version 3.0 or any other industry-standard browser to manage the switch via a browser.

2. At the Universal Resource Locator (URL) prompt, enter the switch's IP address. The following screen is displayed.



Note

For easy access, you may want to bookmark the URL for the switches you access frequently.

Navigating Around the Switch

The switch's front panel is active. You can click anywhere on the switch and a menu or table displays. For example, if you click Port 15, that port's settings appear, as shown in Figure 3-1.

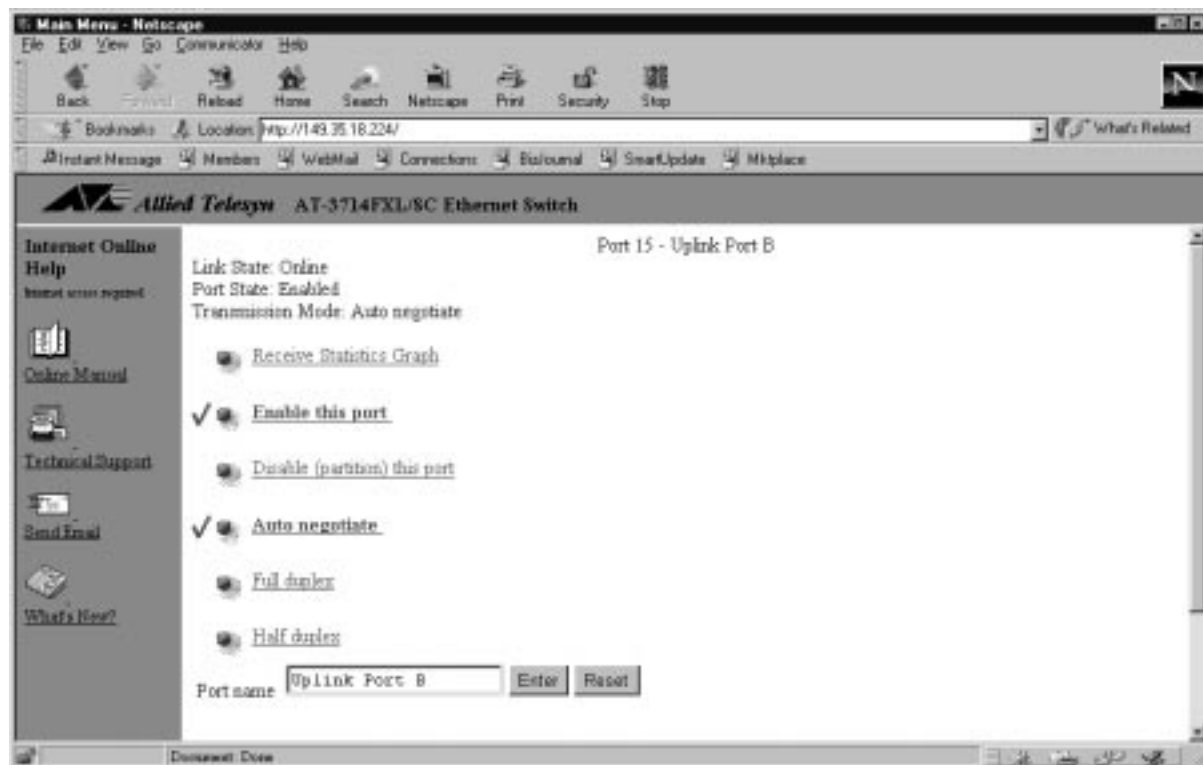


Figure 3-1 Port 15 Settings

If you click any other area other than a specified port on the switch's front panel, the following table displays.

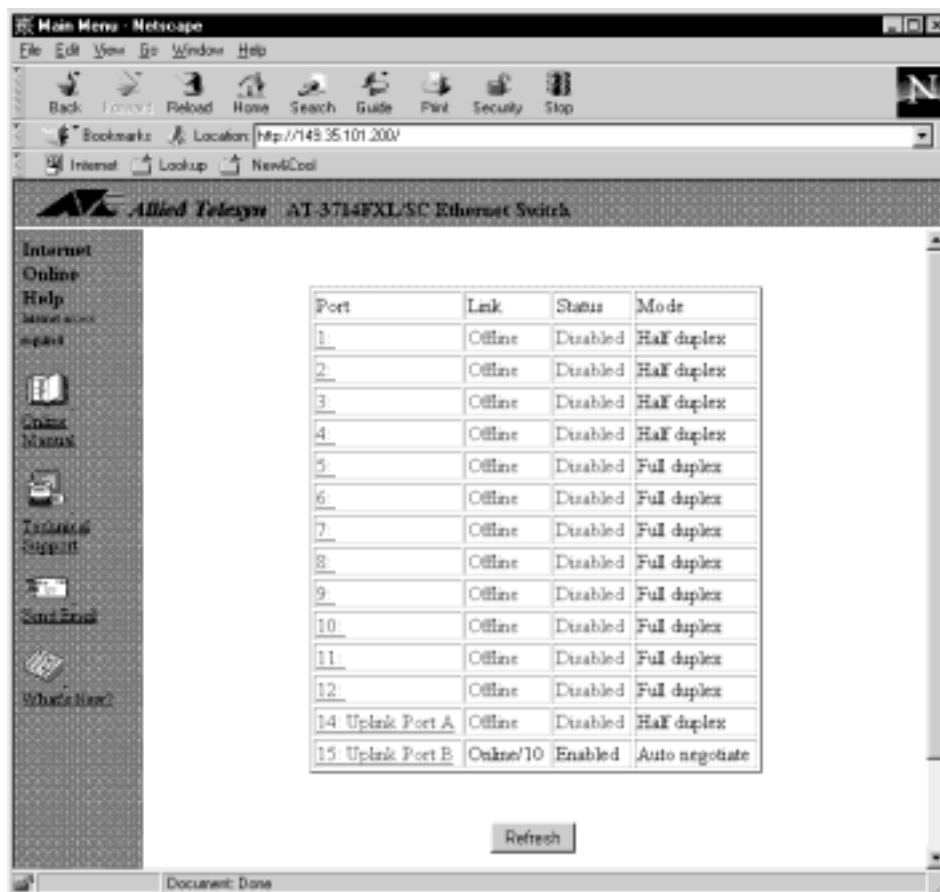


Figure 3-2 Port Link, Status, and Mode States

You also can click on the Omega Main Menu.

You are now ready to configure your switch. See Chapter 4, **Configuration and Administration**.

Chapter 4

Configuration and Administration

This chapter describes the management tasks according to switch, configuration, port configuration and administration.

Switch configuration covers the following topics:

- ❑ **Naming the Switch** on page 4-8
- ❑ **Assigning a Password to the Switch** on page 4-14
- ❑ **Setting Up a VT100** on page 4-19
- ❑ **Setting Time Out Protection** on page 4-21
- ❑ **Enabling/Disabling Omega Access** on page 4-22
- ❑ **Enabling/Disabling Backpressure** on page 4-23
- ❑ **Enabling/Disabling Port Trunking** on page 4-34

Port configuration covers the following topics:

- ❑ **Enabling or Disabling a Port** on page 4-5
- ❑ **Naming the Port** on page 4-11
- ❑ **Enabling Auto-Negotiate/Half-Duplex/Full-Duplex** on page 4-17
- ❑ **Enabling Transmit Pacing** on page 4-18
- ❑ **Selecting Global Configuration** on page 4-33

Administration covers the following topics:

- ❑ **Pinging a Remote System** on page 4-4
- ❑ **Configuring IP Parameters** on page 4-6
- ❑ **Performing Software Upgrades Via TFTP** on page 4-24
- ❑ **Using XModem to Download** on page 4-27
- ❑ **Configuring for Bridging** on page 4-28

Connecting to a Remote System

Menu. Administration> Connect to a remote system

This option allows you to use a AT-3726XL, AT-3726, AT-3716XL or AT-3714FXL, AT-3714F switch to connect to and manage another Allied Telesyn device. You can also use Telnet.

Select Administration>Connect to a remote system.

```
Please specify the system to connect to:
```

```
The system may be identified by name ('name'),  
by IP address (128.2.3.4), or by Ethernet  
address (0000F4 123456)
```

```
->_
```

3. Enter one of the following: system name or DNS name if any, IP address, or MAC address.

Once the information is validated and the connection to the remote switch is open, you immediately get the Omega menus. You may then use the Omega menus to configure the remote switch or run diagnostics.

The only option that is not available is Connect to a remote system from the Administration menu (the same is true if you used Telnet).

4. Select Quit when you are done.

Note

It is important that you select Quit after the Omega session. Otherwise, you may block other sessions or software downloads via the network to the remote switch. See also **Setting Time Out Protection** on page 4-21.

Pinging a Remote System

To ping a remote system, use the PING facility to test the reachability of receiving systems by sending them an Internet Control Message Protocol (ICMP) echo request and by then waiting for a reply.

Menu. Administration> Ping a remote system

1. Select Administration> Ping a remote system.

```
Please enter station to ping:

The system may be identified by name ('name'),
by IP address (128.2.3.4), or by Ethernet address
(0000F4 123456).
Note: Ping will repeat until a key is hit

->
```

2. Enter one of the following: system name, IP address, or Ethernet address. The following screen displays.

```
                Ping in Progress

Pinging: [Host 149.35.18.3, delay 1.000]
Ping 149.35.18.3 #1 ok RTT 0.111 seconds
Ping 149.35.18.3 #2 ok RTT 0.009 seconds
Ping 149.35.18.3 #3 ok RTT 0.001 seconds
```

Note

When using browser management, 19 pings are sent and then stop.

Enabling or Disabling a Port

Menu. Port status and configuration> <Port Number>

Ports are enabled as a default.

Disable a port if you suspect there is a problem and you want to isolate the problem to that port, therefore preventing error proliferation. You may also want to temporarily disable a port that is not in use (an unoccupied office, for example) for security reasons.

1. Select `Port Status and configuration` to display the list of ports.
2. Select a port number, for example, `1`, from the list.

The port configuration screen appears here partially shown.

```

                                     Port 1

Link State:      Online
Port State:      Enabled
Transmission Mode: Half Duplex

Please select an option:
  >Enable this port
  Disable (partition) this port
  
```

3. Select the option to enable or disable the selected port.
4. Select `Return to Port Status Menu...` to display the list of ports with the updated information. For example, a disabled Port 1 displays.

Disabled port

```

                                     Port Status

Port      Link  Status  Mode
1:Finance Online Disabled Half duplex
2:Sales   Online Enabled  Full duplex
  
```

Configuring IP Parameters

Menu. System Configuration> IP parameters

This option applies to TCP/IP based networks only. Some IP parameters are required and others have default values you may keep. There are also optional parameters for information purposes only.

Note

If you have a BootP server and you have mapped the switch's MAC address to IP parameters, the switch will obtain its IP parameters from the server.

1. Select System Configuration, then IP parameters.

```

Ip address:                141.00.01.00
Subnet mask:               255.255.0.0
Gateway address:
Domain Name Server
Default Domain Name

Manager address:          Null (not configured)
Manager address:          Null (not configured)
Manager address:          Null (not configured)
Manager address:          Null (not configured)

Download Password:        *****

Get community string:     public
Set community string:     private
Trap community string:    public

Location:                 Null (not configured)
Contact:                  Null (not configured)
Return to System Administrator Menu ...

```

2. Select the parameter you want to configure from the following list. Then select Return to Main Menu.

Note

If you have a generic (dumb) terminal configuration, enter the letter corresponding to your choice.

IP address - This address is required.

Subnet mask - This is required.

Gateway address - This address is required if you need to send packets from one IP network to another via a router.

Domain Name Server - This address is configurable and if enabled, the DNS server will resolve names for IP commands, such as Connect (Telnet), Ping, and TFTP downloads. When entering an ASCII name at the Connect command, the switch issues a DNS name lookup request to that particular DNS configured server.

Default Domain Name - None. Optional parameter used in resolution of DNS entities.

Manager address - You may enter IP addresses for a maximum of four network management servers that will receive SNMP traps. This parameter is optional.

Download Password - ATS20 (default, uppercase)

The download process requires this password to send software from one switch to other switches in the network, provided that the switches belong to the same product series and that the download password is the same throughout the switches. You can keep the default or change it. If you change the download password of the source switch, the receiving switches cannot accept software downloads from this switch.

Note

The software automatically searches for this password during downloads without user input. This password is different from the optional system password you configured to protect the switch from unauthorized use.

SNMP community strings - The default community strings are provided: `Get=public`, `Set=private`, `Trap=public`. You have the option to keep or change them.

Location - You may enter a text string to indicate the physical location of the switch. For example, enter `First Floor, Lab`. This parameter is optional and is used for SNMP management.

Contact - You may enter a text string to indicate the name, phone number, and other useful information to help identify the person responsible for the switch. This parameter is optional and is used for SNMP management.

Naming the Switch


Menu. `System configuration> System name`

The switch has several possible unique identifiers:

- A factory-designated MAC address
- An IP address that you assign, if you have TCP/IP
- A unique name that you assign for easy management
- An assigned DNS name in the software of the DNS server for use with IP communication

Allied Telesyn recommends assigning unique names to switches to avoid unwanted or accidental software downloads.

1. Select `System configuration System name`.

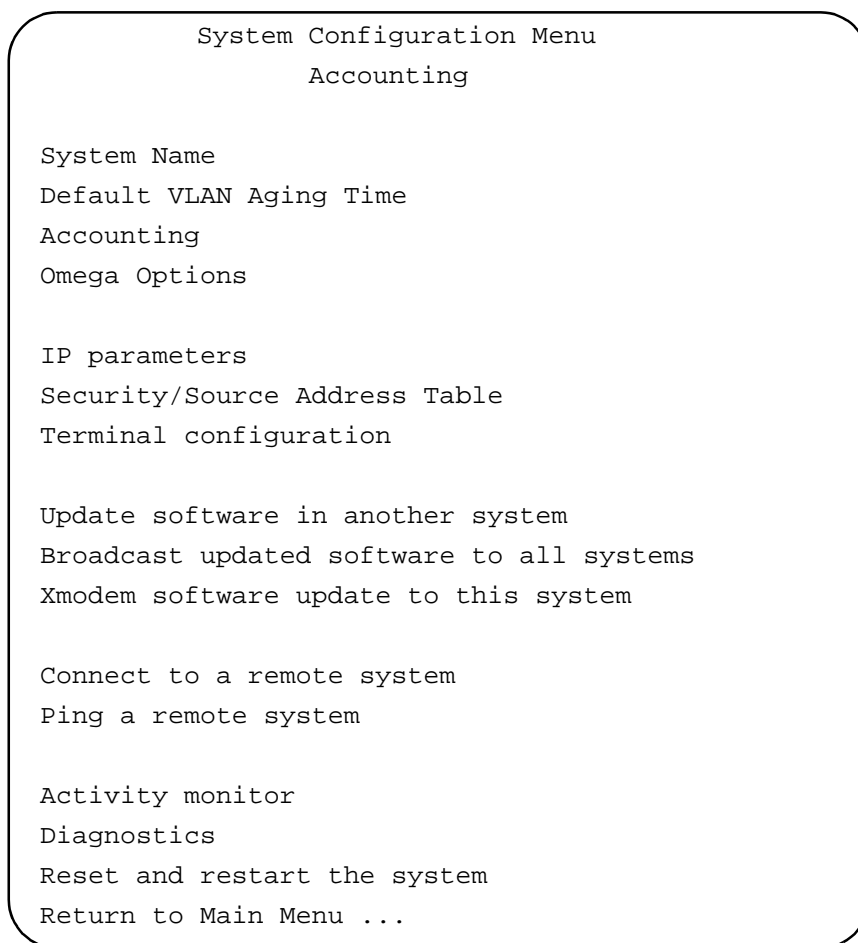


A screenshot of a terminal window showing the configuration prompt for the system name. The text is enclosed in a rounded rectangular box. The prompt is "System name" followed by "Null (not configured)" on the next line.

```
System name
Null (not configured)
```

2. Enter a name of up to 20 characters at the prompt, for example, `Accounting Switch`.

The system administration menu displays with the switch's name displayed at the top of the screen.



3. Select Return to Main Menu.

The assigned switch name will display at the top of most of the screens.

Change/Delete the Switch Name

1. Select `System configuration> System name` to display the switch's current name.

```
System name Accounting
```

2. Remove or change the current name.
3. Select the current name; press **RETURN**.

The greater-than arrow key displays indicating that the system is ready to either accept a new name or delete the existing name.

4. Press the space bar until the name has been deleted. Press **RETURN**. `Null (not configured)` displays.
5. Return to the Main Menu.

The top of the screen no longer displays the switch's name.

6. If you want to confirm the deletion, select `System Name` from the System configuration menu.

```
System name Null (not configured)
```


Naming the Port

Menu. Port status and configuration> <Port Number>

Depending on the model, the switch has the following ports, identified numerically, as listed in Table 4-1.

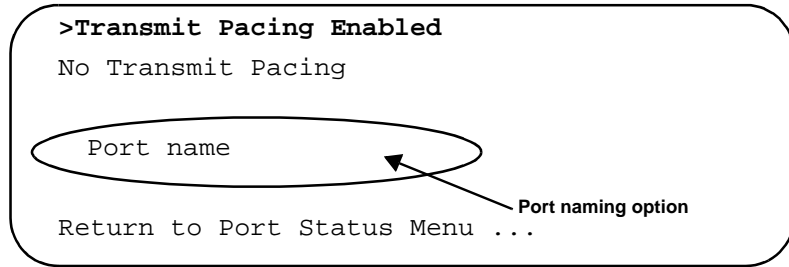
Table 4-1 Port Numbering

Switch	Port #	Port Type
AT-3726XL, AT-3726	1-24	10Base-T
	25	Remote management port for Omega
	26 (Uplink port A)	10/100Base-TX
	27 (Uplink port B)	Optional MDA (TX or FX)
AT-3716XL	1-16	10Base-T
	17	Remote management port for Omega
	18 (Uplink port A)	10/100Base-TX
	19 (Uplink port B)	Optional MDA (TX or FX)
AT-3714FXL, AT-3714F	1-12	10Base-FL
	13	Remote management port for Omega
	14 (Uplink port A)	100Base-FX
	15 (Uplink port B)	Optional MDA (TX or FX)

Because of the number of ports, you may find it more convenient to manage the ports if you assign a unique name to each port. You can associate a port number with a specific user or a location (for example, Port 1 to Room 1147).

1. Select `Port status and configuration` to display the list of ports.
2. Select a port number from the list.

The port configuration screen is partially shown.

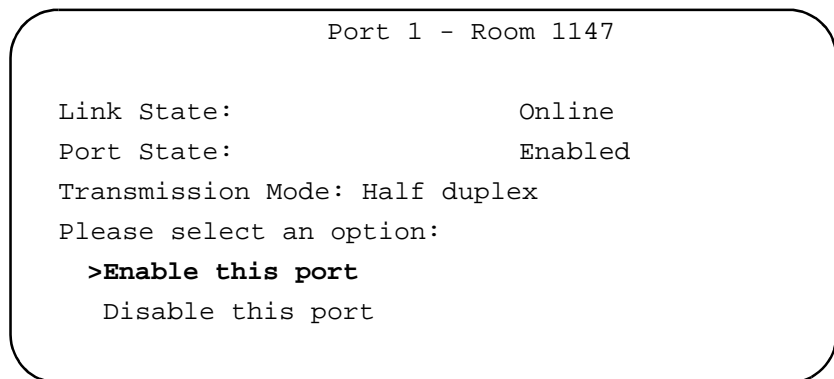


3. Enter a port name. Then press **RETURN**.

Note

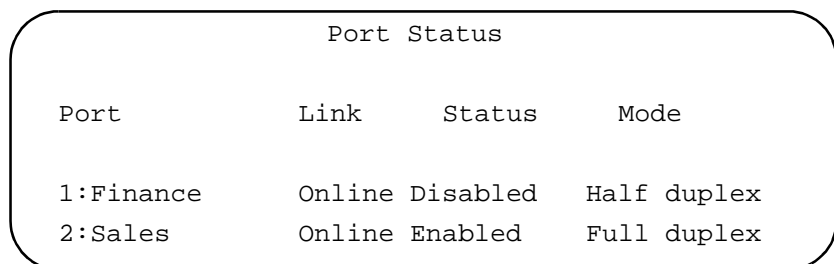
Enter a name of up to 20 characters, for example, Room 1147.

The system updates the port configuration screen by displaying the name you entered at the top of the screen, as shown in the following example.



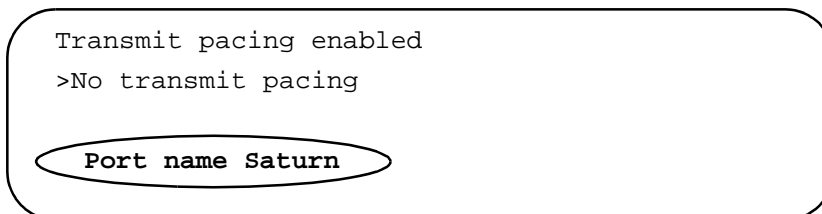
4. Select **Return to previous menu...**

A current list of newly named ports displays.



Changing or Deleting a Port Name

1. Select `Port status` and configuration to display the list of ports.
2. Select a port number, for example, 1, from the list to display the port configuration screen.
3. Select `Port name` and press **RETURN**. Type a new port name or delete the existing one. (Screen partially shown.) Press **RETURN**.



4. If deleting the port name, the system also erases the name from the top of the screen.
5. Return to the Main Menu and select `Port Configuration` to see the name deletion or change for the specified port.

The system displays an updated port list.

Assigning a Password to the Switch

Menu . System configuration> Omega options>
Password

Assigning a password protects the switch management software from unauthorized configuration changes. Once you configure a password, you need to enter it at the start of an Omega session.

1. Select System configuration> Omega options> Password.

```
Password:                               ->  
Null (not configured)  
Timeout: 5
```

2. Highlight Null (not configured), press **RETURN**, then enter a password (maximum 20 characters). Press **RETURN** again.

See **Setting Time Out Protection** on page 4-21 for additional information.

3. Select Return to Main Menu.

Forgetting Your Password

If you forget or lose your password, either reset the switch to factory defaults (see **Setting Switch Defaults** on page 1-5) or contact Allied Telesyn's Technical Support.

Enabling Store-and-forward or Cut-through (Fragment-Free)

Menu. Port Status and configuration<PortNumber>

Forwarding method determines how the port handles packets. The options you see on the port configuration screen is related to how the switch is configured to forward packets as a whole. The default setting for the switch is Store-and-Forward.

1. Select Port status and configuration to display the list of ports.
2. Select a port number from the list.

The port configuration screen appears. Depending on the switch's forwarding method, your options for the port can be:

```
>Store-and-forward
Cut-through (fragment-free)
```

A: Port options if the switch uses store-and-forward method

```
Store-and-forward
>Cut-through (fragment-free)
```

B: Port options if the switch uses fragment free method

3. Select the forwarding method you want for the port.

Store-and-forward. In this default mode, the switch stores the incoming packet until it has the entire packet, then forwards it onto its destination.

The switch software checks for a valid CRC before forwarding the packet and allows the switch to store the packet until network resources, for example, an unused link, are available for forwarding. This allows complete error checking. Store-and-forward ensures data integrity and prevents packet errors from being propagated in the network. On the other hand, every store-and-forward device in the path from the sender to the receiver adds a small delay due to the time spent in storing and checking the packet before forwarding it.

Select this forwarding method if you are running applications where data integrity is more important than small delays.

Cut-through (fragment-free). This option is available for non-XL versions only. In this method, the switch starts to forward the incoming packet to its destination while the packet is still being received.

Cut-through (fragment-free) provides low latency for forwarding frames and also filtering fragment frames by not transmitting a frame until 64 bytes have been received by the switch. In cut-through (fragment-free) mode, fragment frames or runts (frames less than 64 bytes) are filtered, thus providing some network error protection.

Select the cut-through (fragment-free) method if you are running time-sensitive applications.

Enabling Auto-Negotiate/Half-Duplex/Full-Duplex

Menu. Port status and configuration> <Port Number>

The port's transmission mode defines the direction that data can move. The switch provides the following port transmission modes:

- Auto-negotiate (AT-3726XL, AT-3716XL, AT-3726 default)
- Full-duplex
- Half-duplex (AT-3714FXL, AT-3714F default)

1. Select `Port Status and configuration` to display the list of ports.
2. Select a port number from the list of ports.

The port configuration screen appears (partial screen shown only).

```
Link State: Online
Port State: Enabled
Transmission Mode: Full duplex
Please select an option:
```

```
>Enable this port
```

```
Disable (partition) this port
```

```
>Auto negotiate
```

```
Full duplex
```

```
Half duplex
```

Transmission mode options

3. Select the transmission mode you want for the port.

If you select `Auto-negotiate`, the switch detects the speed and duplex settings of the connected device.

If the switch and end device are not set to the same setting, a high collision rate could occur which may degrade network performance.

Note


Make sure that both ends of the connect are set to the same mode. If only one end of the connection is capable of auto-negotiation, then both ends of the connection must be manually set for speed and half- or full-duplex.

Enabling Transmit Pacing

Transmit Pacing is the switch's capability to inject transmit delays and is selectable on a per port basis. Transmit pacing introduces delays into the normal transmission of packets, which delays transmission attempts between stations thereby reducing the probability of collisions during heavy traffic (as indicated by packet deferrals and collisions). This situation applies in cases where congestion exists within the switch. For example, all ports on the switch are queuing up to send traffic out through only one uplink port. When the congestion clears, the switch stops sending the delays so that devices can begin retransmitting. This mode then increases the chances of successful transmission.

1. Select `Port status and configuration` to display the list of ports.
2. Select a port number from the list.

The port configuration screen displays. (Partial screen is shown here.)



```
Transmit pacing enabled
>No transmit pacing
```

3. Select `Transmit pacing enabled`.

Setting Up a VT100

Menu. System configuration> Terminal configuration>VT100-compatible/ANSI

The system displays the default terminal configuration settings.

```

> VT100-compatible / ANSI
  Generic "dumb" terminal

> 8 data bits
  7 data bits

> 1 stop bit
  2 stop bits

> No parity
  Odd parity
  Even parity

> Full duplex (echo)
  Half duplex (no echo)
  Data rate ("baud rate") ...

```

To make your terminal selections, simply select the setting of your choice, then select Return to previous menu... or Return to Main Menu.

Setting Up a Generic (Dumb) Terminal

Menu. System configuration> Terminal Configuration> Generic **dumb** terminal

Setting Full-Duplex/ Half-Duplex Mode

Menu. System configuration> Terminal Configuration> Generic **dumb** terminal Full duplex

Setting Baud Rates

Menu. System configuration> Terminal Configuration> Generic **dumb** terminal> (Data rate **baud** rate)...

Note

The default is automatic baud rate detection.

You can also select from the following fixed baud rates. Allied Telesyn recommends 9600 bps.

Table 4-2 Fixed Baud Rates

19200 bps	600 bps
9600 bps	300 bps
4800 bps	150 bps
2400 bps	75 bps
1200 bps	

Setting Time Out Protection

Menu. System configuration> Omega Options

A timeout value is one way to protect the switch from unauthorized use in case you forget to exit from Omega and then leave the switch unattended. If you configure a timeout value, the software clocks the elapsed time between the last time any key was pressed during an Omega session and the current time. If the elapsed time exceeds the timeout value, the software automatically terminates the session.

1. Select System administration> Omega Options.

```
Omega Options menu
Password: Null (not configured)
Timeout: 5
```

2. Enter a timeout value from 0 to 32,767 minutes. Press RETURN.

If the timeout value is set to zero, you must always quit after a management session. Otherwise, subsequent Telnet sessions and software uploads will be blocked to the switch. To avoid blocking any Telnet sessions or software uploads, you must manually enter Quit.

Deleting a Previously Configured Timeout Value

If you want to delete a previously configured timeout value, repeat the above procedure and enter 0 (zero) as the new value.

Enabling/Disabling Omega Access

Local Omega The default for Local Omega is `Enabled`. This means you can access the Omega menus from a terminal or PC connected to the switch's RS232 port.

Remote Omega The default for Remote Omega is `Enabled`.
You still can use SNMP to manage the hub remotely. To change the setting again, use Local Omega.

Web-based Omega The default for Web-based Omega is `Enabled`.

Menu. System configuration> Omega Options

```
Omega Options Menu
Brandy
Password:      Null (not configured)
Timeout:      5

> Local Omega Enabled
Disable Local Omega

> Remote Omega Enabled
No Remote Omega

> Web-based Omega Enabled
Exclude Web-based Omega

Return to System Configuration Menu ...
```

Figure 4-1 Enabling/Disabling Omega

Enabling/Disabling Backpressure

This feature is available for the XL versions only. For backpressure to be implemented, the ports must be in half-duplex mode. Backpressure is useful when a port's input buffer is running low on memory resources. For example, outbound packets are traversing a single uplink port. When backpressure is enabled, the switch simulates a collision when its input buffers are nearly filled so that sending devices will defer transmissions. These sending devices will retry transmissions according to the Ethernet back-off algorithm. Once switch resources are available again, the switch stops sending the collision signals and devices can freely transmit again. Figure 4-2 shows backpressure enabled.



Figure 4-2 Enabling Backpressure

Performing Software Upgrades Via TFTP

You can download software upgrades from a switch to one or more switches on the network, or download onto a switch via Trivial File Transfer Protocol (TFTP) from a TFTP server.

The switches initially use a factory-configured default download password, **ATS20** to authorize software downloads. You do not need to manually enter this password to download software successfully.

Note

This download password can be changed to prevent unauthorized changes to the switch firmware.

Conditions for Network Downloads via TFTP

The switch uses TFTP of the TCP/IP protocol suite to download software to other switches whether or not your network uses TCP/IP. TFTP is transparent to other devices on the network.

The switch can download software within the following conditions:

- ❑ The switches must be directly connected to the same network cable or joined by switches or bridges and routers, if the gateway addresses in both switches are properly configured.
- ❑ All switches receiving the same software must use the same download password (ATS20). See **Configuring IP Parameters** on page 4-6).

Using TFTP

If you have TFTP, you can use it to download an image file from the switch with the upgraded software. When issuing the TFTP get or put command, take note of the following variables:

Image file name. Get the latest from Allied Telesyn's website at **www.alliedtelesyn.com**.

IP address. This is the IP address of the switch that is the source or destination of the file.

Download password. The default download password is **ATS20** in uppercase.

File type. The file type is octet or binary.

Note

TFTP platforms vary. Some have graphical user interfaces while other platforms require you to type the commands.

Downloading from One Switch to Another

Menu. Administration> Update software in another system

Follow this procedure:

- ❑ To download software to another switch on the network without physically being at the destination switch
- ❑ To ensure that all the switches on the network you intend to upgrade will be upgraded, since you will be manually upgrading one switch at a time

1. Select Update software in another system.

Please specify the system to be downloaded:

The system may be identified by name ('name'),
by IP address (128.2.3.4), or by Ethernet
address (0000F4 123455).

2. Enter either the destination switch's name, its IP address, or its MAC address (also known as the Ethernet address printed above the switch's RS232 management port). Then press **RETURN**.
3. Select the Return to Main Menu icon to see a confirmation similar to the following screen.

Activity monitor

load request received from Second Floor Computer
Room
loading... 000287-02A8C
completed.

Repeat this procedure to download software to every switch on the network.

Broadcast Updated Software to All Systems

Menu. Administration> Broadcast Updated Software to All Systems

Note

Plan a software broadcast during times when your network is not busy.

1. Select Administration> Broadcast updated software to All systems.

The switch announces the availability of the software to all switches; in turn, the switches that need the upgrade respond with a request message.

The screen immediately turns on the Activity Monitor screen and displays the information as switches on the network request and then receive the software.

Activity monitor

```
Broadcast notification sent  
Broadcast notification sent  
Broadcast notification sent
```

Note

You cannot undo this command once executed.

2. Select Return to Main Menu... without interrupting the software download.

If you have many switches requesting the download, not all of them may receive the download, especially if the network is busy. Repeat the procedure to ensure that all switches receive the software upgrade.

Note

Switches on your network with different download passwords will not receive the software upgrades.

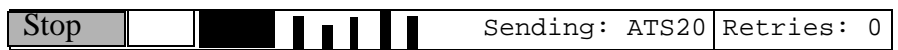
Using XModem to Download

1. Select Administration > XModem software update to this system.

```
Accounting
Ready to receive software upgrade via XModem.
Warning: During software update Management activity
is disabled.
Do XModem update now? (Yes or No):
```

2. Enter Yes.

```
The System host is now ready for download. Please
start your XMODEM transfer.
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```



The above screen displays the downloading progress and that there were no retries.

Configuring for Bridging

Menu. Bridging

The options under the Bridging Menu item are for configuring and enabling spanning tree.

As a bridge, the switch:

- ❑ Learns source and destination MAC addresses of incoming packets by storing the information in a forwarding table (see also Activity Monitor on page 6-2).
- ❑ Forwards the packet to the destination's network segment if the source is from a different network segment; or discards the packet if the source and destination address are on the same segment because all stations on the segment have already received the packet.
- ❑ Ages out the addresses (deletes the information from the table) if undetected by any port within a user-defined or a default elapsed time.
- ❑ Updates the MAC address table automatically as you add, remove, or relocate devices on the network.
- ❑ Prevents loops with spanning tree.
- ❑ Updates other bridges with topology information by periodically sending bridge protocol data units (BPDUs).

When you select `Bridging` from the Main Menu, the following screen displays:

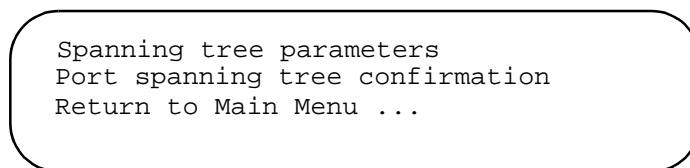


Figure 4-3 Bridging Submenu

You are now ready to configure or disable spanning tree. Note that Spanning Tree is on by default. See [Configuring Spanning Tree Parameters](#).

If you want an overview of the Spanning Tree Protocol (STP) before proceeding, go to Appendix A, **Spanning Tree Protocol**.

Note

Although defaults are adequate for most installations, changing defaults should be done only if the network administrator understands the IEEE 802.1d standard.

Configuring Spanning Tree Parameters

Menu. Bridging Spanning tree parameters

Default spanning tree parameters are provided; you do not need to change them.

1. Select **Bridging, spanning tree parameters** to display the bridging options, as shown in the following screen.

```

                                Bridge configuration Menu
Bridge Identifier (Mac Address: Priority)      f32c20 5474b5: 32768
Root Bridge Identifier (Mac Address: Priority) f32c00 535b97: 32768
Cost to the root                             0
Port closest to the root                     1
Max Age                                       20
Forwarding Delay                             15

Bridge Priority:                             32768
  Max age time:                              20
  Hello time:                                2
  Forwarding delay:                          15
  Return to bridge Menu ...

```

Figure 4-4 Spanning Tree Screen

2. Select **Bridge Priority** and enter a priority number.

The number can be from 0 to 65,535 with 0 being the highest priority. The number consists of a 2-byte bridge priority number and a 6-byte MAC address. Bridges use this number to determine the root bridge for a loop-free implementation. If bridges happen to have equal priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

When the root bridge malfunctions, the bridge with the next priority number (the next lowest MAC address) automatically takes over as root bridge.

3. Enter `Max age time` to get the next screen and enter the aging time in seconds at the prompt.

The aging time can be from 6-40 seconds, with 20 seconds as a default. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs).

For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds.

Note

Aging time for BPDUs are different from aging time in the MAC address table.

4. Enter `Hello time` and enter the time in seconds at the prompt.

Hello time can be from 1-10 seconds, with 2 seconds as the default. Bridges use this parameter to determine the time interval between generating and sending configuration messages.

5. Enter `Forwarding delay` value and enter the time in seconds.

The default is 15 seconds. The time indicates the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change; therefore, loops may result.

6. Select `Return to Main Menu` and repeat the procedure if you want to reconfigure the spanning tree parameters for Administration.

Designating the Root Port

Menu. Bridging> Port spanning tree configuration

In this procedure, you identify the root port and the path cost for the spanning tree. Default values will work for the majority of the users; but for purposes of illustration, Port 1 will be the root. All ports have priority 128 and cost values are 100 by default.

1. Select Port spanning tree configuration from the Bridging Menu to get a similar list shown on the screen.

Port	Charlie Priority	Cost
1:	128	100
2:	128	100
3:	128	100
4:	128	100
5:	128	100
6:	128	100
7:	128	100
8:	128	100
9:	128	100
10:	128	100
11:	128	100
12:	128	100
More...		
Enable Spanning Tree for All Ports		
Disable Spanning Tree for All Ports		
Return to Bridge Menu ...		

2. Select a port number, for example, 1, to get a screen similar to the following.

Bridge Menu	
Port 1 - Finance	
>Enable Spanning Tree	
Disable Spanning Tree	
Priority:128	
Cost:	100
Return to previous menu ...	

3. Select `Priority` to get the next screen and enter 0 as the priority number at the prompt to make Port 1 the root port.

The range is 0-255. When the designated root port is disabled or the cable connection breaks, the STP algorithm reconfigures an alternate path to the LAN by identifying the port with the next lowest priority number.

4. Select `Cost` to get the next screen and enter a cost parameter ranging from 1-65,535; or keep the default value.

The spanning tree algorithm uses the cost parameter in combination with the priority to decide which bridges provide the lowest cost path to the root bridge for that LAN.

Higher port costs are associated with ports of lower bandwidth, and vice versa. For example, 100 is the cost for a 10 Mbps port, 10 for a 100 Mbps port, and 1 for a 1 Gbps port.

You are done with spanning tree configuration. Now that the required parameters have been configured, bridges can make a determination on the best single path to a destination.

A formula determines the amount of time it takes for the topology to reconfigure, depending upon the spanning tree values you use. Refer to the IEEE specification for details.

Selecting Global Configuration

Menu. Port Status and configuration> <Port Number> >Global Config

Selecting this option copies the displayed port configuration (enable, auto-negotiate, etc.) to all regular (non-uplink) ports on the switch without changing the port names or VLAN assignments. Port names and VLAN assignments remain as originally defined.

1. Select Port Status and configuration to display the list of ports.
2. Select a port number, for example, 1 , from the list.
3. Select the Global Config option.
4. Confirm your action.
5. Select Return to Port Status Menu... to display the list of ports with the updated information.

Enabling/Disabling Port Trunking

Port Trunking configures Ports A and B to function as a single uplink port to increase the bandwidth of the connection. Communication streams between two devices across the trunked uplink port will always be passed on the same physical port. If one trunk port becomes inactive, the other continues to operate and handle all uplink traffic. When the inactive port recovers, the switch automatically resumes its operation; no reset is required.

This option displays only when both uplink ports are installed.

Note

Port Trunking requires that both uplink ports be of the same type and operate in the same mode.

When enabled, this option copies the port configuration parameters and the port VLAN assignments of Port A to Port B. All changes to Port A parameters or VLANs assignments also change Port B. Both ports operate as a single uplink until this option is disabled.

The Port name field in the Port Status and Configuration menu displays the ports as "Trunk #1/active" or "Trunk #1/inactive" for each of the ports, according to their status.

1. Select `System configuration > Enable Port Trunking`.
2. Select `Return to System Configuration Menu...`, then select `Port Status and configuration Menu...` to display the list of ports with the updated information.

Chapter 5

Virtual LAN Configuration

This chapter introduces VLAN configuration as it applies to Allied Telesyn's implementation of VLANs. VLAN features are provided only on the XL versions of the switches. The XL versions support port-based VLANs and 802.1Q (draft 8) VLAN tagging.

Menu.Virtual LANs.

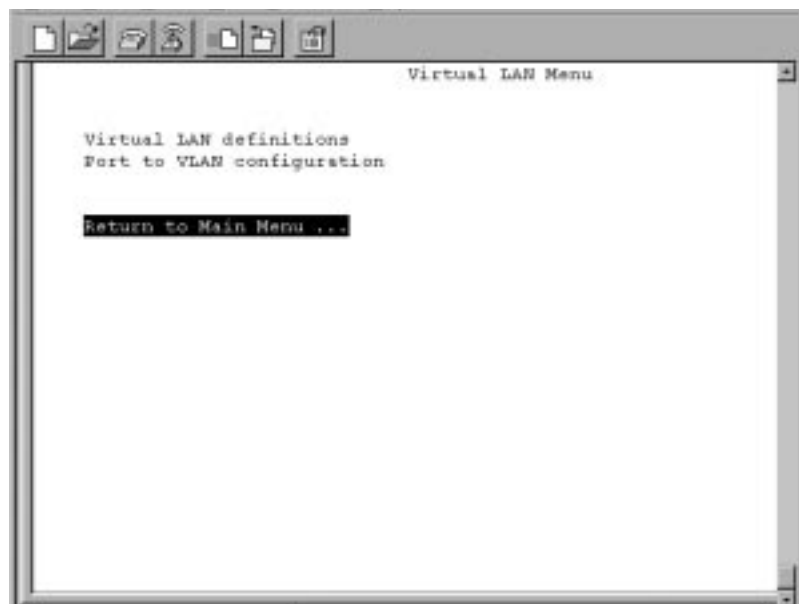


Figure 5-1 Virtual LANs Menu

By default, the switch has one port-based VLAN (all ports' VLAN assignment showing as Default VLAN) and one spanning tree domain. In most situations, users find the defaults acceptable and do not require further configuration; however, your network may require assigning end stations into logical groupings, regardless of their physical location.

You can group your end stations logically through VLANs. Information exchange is confined within the members of a given VLAN. A VLAN constitutes one broadcast domain; therefore, broadcast packets from an end station only go to other stations within the same VLAN.

Port-based VLANs cannot communicate with each other through the switch; they require a router to do this (Figure 5-2).

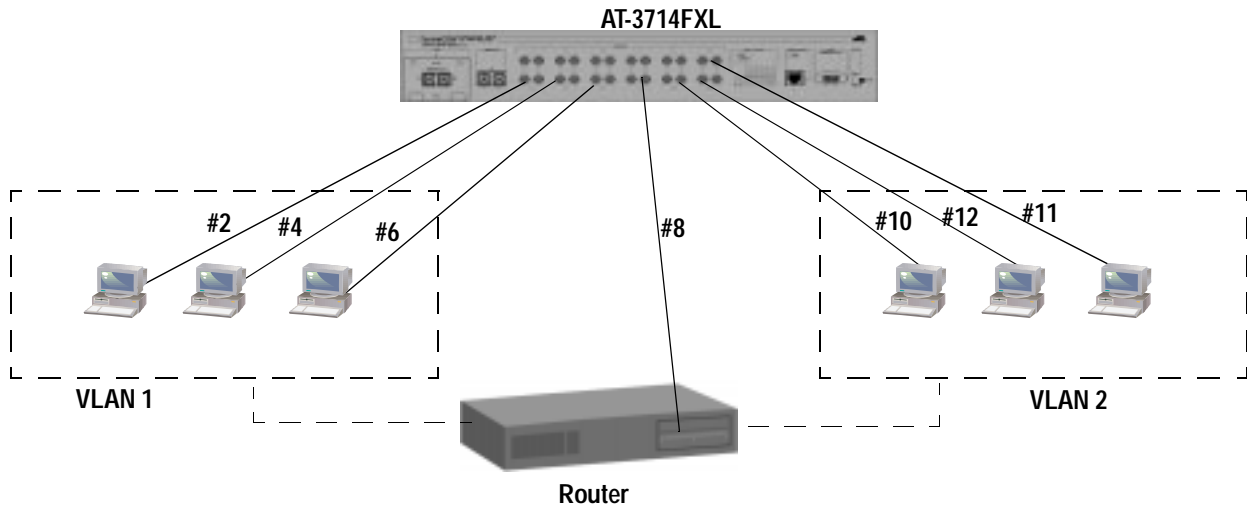


Figure 5-2 VLAN Example

Advantages of Using VLANs

- ❑ You have the flexibility of grouping workstations logically or functionally, regardless of their physical location on the network.
- ❑ You can change VLAN memberships anytime by software configuration without moving the workstations physically, or change group memberships by simply moving a cable from one port to another.
- ❑ With VLAN tagging, the ability to group workstations into logical work groups is more versatile. You can assign a port to be an uplink to another 802.1Q-compatible switch and enable it to carry all VLAN traffic instead of using one uplink port per each VLAN port configured.

The VLAN ID used to tag incoming packets without a tag is called the Port Virtual LAN (PVID) for the specified port.

When a port is a member of a port-based VLAN, it is internally assigned a unique Port VLAN ID or PVID. This PVID is added as a VLAN tag as frames enter this port. This PVID is used to route the frame through the switch and through 802.1Q-based switches. This enables legacy (non-802.1Q compliant) devices connected to the switch to take advantage of the VLAN capabilities of the switch.

Note

The manager is a legacy device. It cannot interpret VLAN tags. The management agent responds only to pings from any device that is located within the same VLAN, defined by the management port's PVID.

Figure 5-3 shows how VLANs are used across uplink ports and between two different manufacturer's equipment. The switches have the following VLAN configurations:

AT-3714FXL Configuration

- ❑ Port 1 is a member of the "Default VLAN"
- ❑ Ports 2 and 14 are members of VLAN #2

The AT-3714FXL is configured as follows:

- ❑ The AT-3714FXL will have a VLAN named "Default VLAN". Port 1 will be both tagged and a port-based member of "Default VLAN" with a PVID and a VLAN ID of 1. Port 15 is added as a tag member so that "Default VLAN" will have access to the uplink between switches.
- ❑ The AT-3714FXL will have a VLAN named "VLAN 2". Ports 2 and 14 will be both a tagged and a port-based member of VLAN #2 with a PVID and a VLAN ID of 2. Port 15 is added as a tag member so that "VLAN 2" will have access to the uplink between switches.
- ❑ The AT-3714FXL will have a VLAN named "Uplink". Port 15 will be both tagged and a port-based member of VLAN "Uplink" with a PVID and a VLAN ID of 3. See Figure 5-3.

AT-8518 Configuration

- ❑ Ports 1 and 3 are members of the "Default VLAN"
- ❑ Ports 2 is a member of VLAN #2

The AT-8518 is configured as follows:

- ❑ The AT-8518 will have a VLAN named “Default VLAN”. Ports 1 and 3 will be both tagged and a port-based member of “Default VLAN” with a PVID and a VLAN ID of 1. Port 10 is added as a tag member so that “Default VLAN” will have access to the uplink between switches.
- ❑ The AT-8518 will have a VLAN named “VLAN 2”. Port 2 will be tagged and a port-based member of VLAN #2 with a PVID and VLAN ID of 2. Port 10 is added as a tag member so that “VLAN 2” will have access to the uplink between switches.
- ❑ The AT-8518 will have a VLAN named “Uplink”. Port 10 will be tagged and a port-based member of VLAN “Uplink” with a PVID and a VLAN ID of 3. See Figure 5-3.

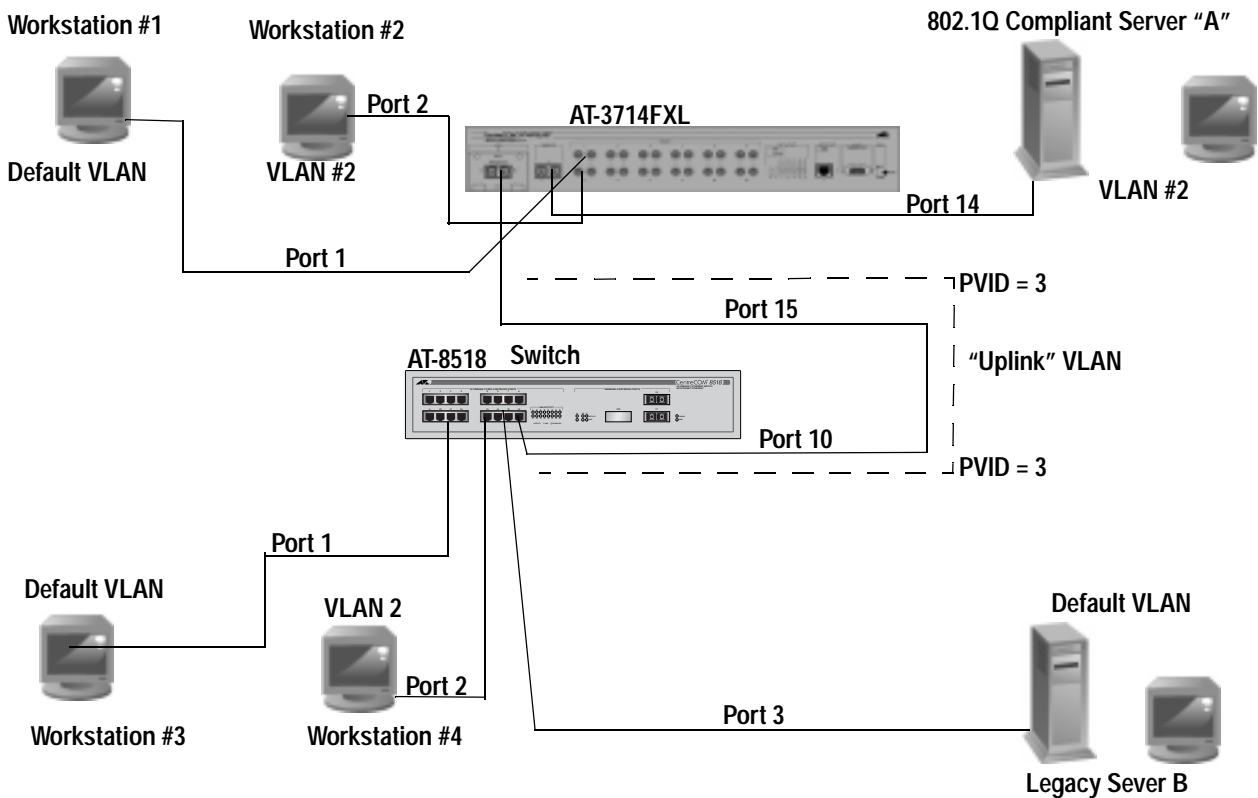


Figure 5-3 Typical Configuration

Note

The PVIDs must match on the trunk or uplink port between the AT-8518 switch and the AT-3714FXL switch. For example, they both must have IDs of 1.

Uplink ports (15 and 10 on both switches) are used to connect the two switches. To allow VLANs to span across switches, these uplink ports are output enabled for every configured VLAN on the switch. Therefore, when a broadcast packet is received on any port (representing a packet on any VLAN), it is transmitted through the uplink port. Note that since the uplink port on the AT-3714FXL has PVID of "3", packets transmitted on the uplink port from VLAN 2 or the "Default VLAN" will be transmitted with their VLAN tag in place. This scheme preserves the VLAN information across the uplink port.

In this example, Workstation #4 can talk with Server A because its VLAN information is preserved across the uplink. In turn, Workstation #1 can talk with Server B for the same reason. Workstation #2 is precluded from talking to Server B since Server B has a different VLAN, and any packets generated from Workstation #2 that traverse the uplink port will continue to be associated with VLAN 2.

Configuration Information

By default, only one VLAN is defined in a 3700XL switch. Up to 32 VLANs can be defined in the unit. A VLAN is defined when the following occurs:

- Name the VLAN
- Assign a VLAN ID number
- Define a port configuration to be used for that VLAN

By default, the VLAN named "Default VLAN" is assigned and given a VLAN ID and PVID of 1, and all ports receive packets for this VLAN.

Port Information

Each port must be assigned a PVID. The VLAN can be chosen from one of the VLANs defined in the VLAN configuration. By default, all ports belong to the "Default VLAN" which has a PVID of 1.

The following Omega configuration screens show VLAN and port to VLAN definitions.



Figure 5-4 Virtual LAN Main Menu



Figure 5-5 Default VLAN Menu

Adding a New VLAN

Menu. Virtual LANs><Virtual LAN definitions><Add new table entry>

1. Select Add new table entry>. The following screen displays.



Figure 5-6 Adding New VLAN Descriptors

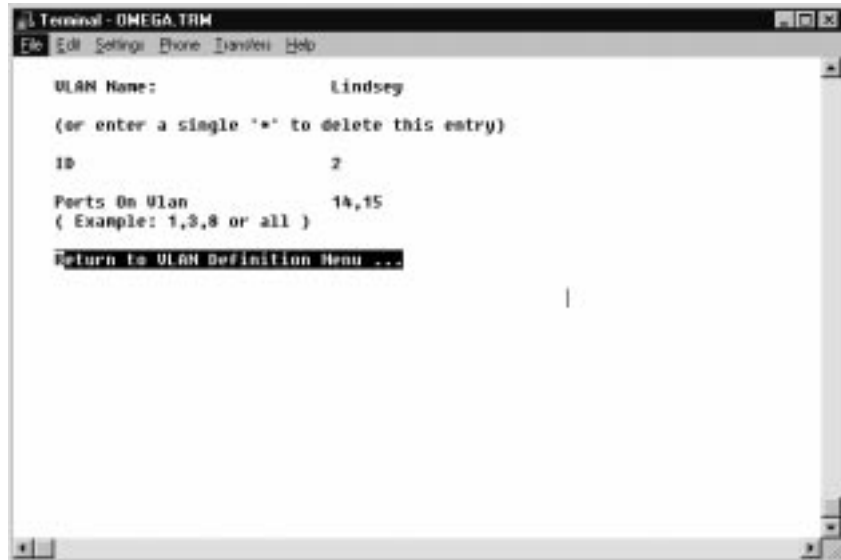
2. Enter the following VLAN descriptors:

- New VLAN name (in this example Lindsey)

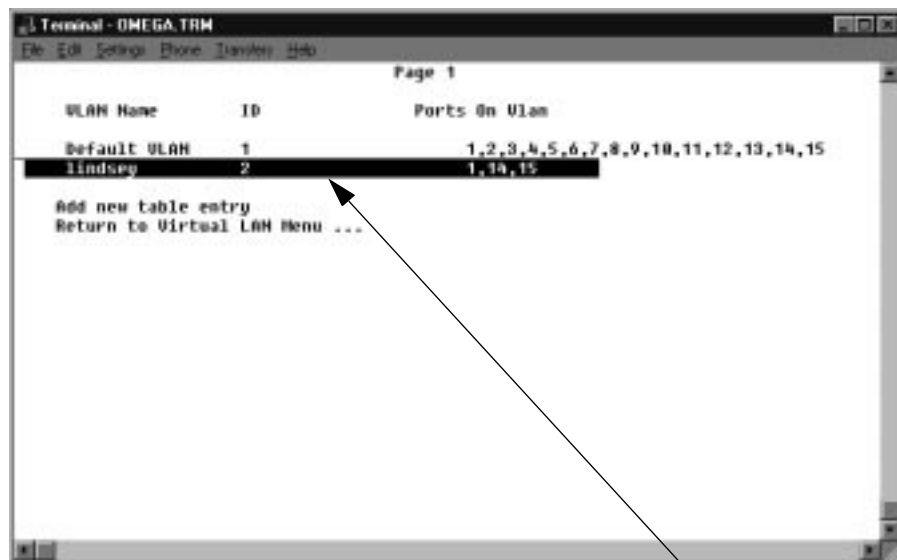
When you enter a new VLAN name, for example Lindsey, the ID number automatically increments to the next VLAN ID number, for example from 1 to 2. See following screen.

- VLAN ports (in this example 14, 15)

By default, the uplink ports are included in the VLAN ports. A port can belong to any number of VLANs, maximum of 32 VLANs.



3. Select Return to VLAN Definition Menu. The following screen displays showing the new VLAN descriptors.



automatically increments

Figure 5-7 New VLAN Descriptors

Note

Allied Telesyn highly recommends that you use the VLAN ID (default) supplied by the system. Although you can change VLAN IDs to suit your specific needs, changing them requires a more advanced understanding of VLAN tagging.

Port to VLAN Configuration

Menu. Virtual LANs><Port to VLAN configuration>

1. Select Port to VLAN configuration.

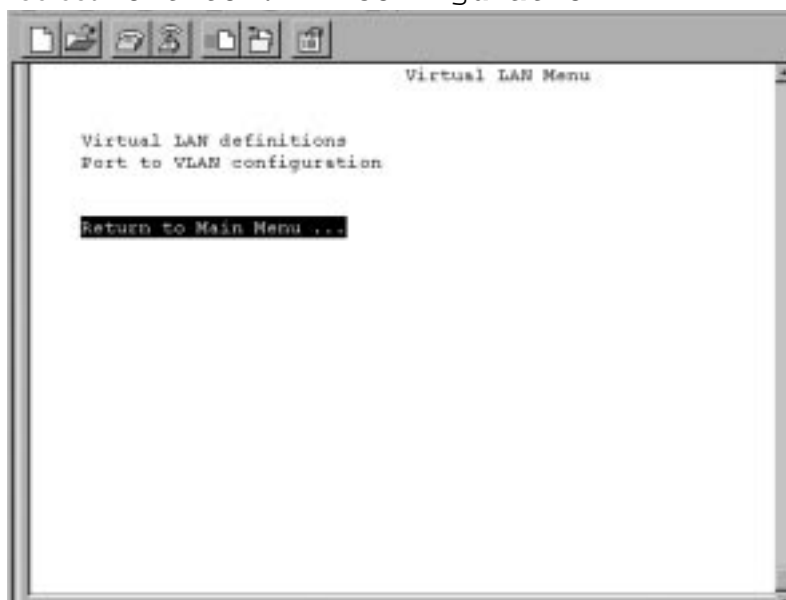


Figure 5-8 Virtual LAN Menu

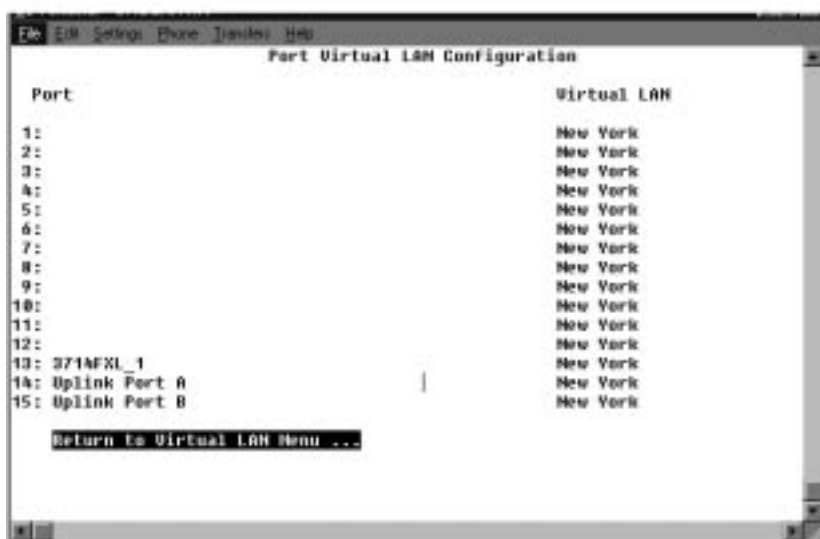


Figure 5-9 Port-To-VLAN Configuration

If you select Port 6 for example, the screen will show that Port 6 is now associated with the Default VLAN.

**Deleting a Port
from a VLAN or
Changing Port's
VLAN
Assignment**

1. Select `Port VLAN` configuration from the `Virtual LANs` menu to display the port list with VLAN assignments.
2. Select the port number you want to delete or change.
The screen displays the port's VLAN configuration and a list of available VLANs).
3. Do one of the following:
 - To reassign the port to another VLAN, select the new VLAN name from the list.
 - To delete the port from a VLAN, select `Default VLAN` from the list.

The screen displays the list of ports with the updated VLAN assignment.

Chapter 6

Monitoring

This chapter describes the tasks related to monitoring the switch. The tasks are shown in the following order:

- ❑ **Activity Monitor** on page 6-2
- ❑ **MAC Address Table** on page 6-3
- ❑ **Static MAC Addresses** on page 6-6
- ❑ **Security/Source Address Table** on page 6-12
- ❑ **Mirror Port** on page 6-23
- ❑ **Port Status** on page 6-25
- ❑ **Port Numbering** on page 6-26
- ❑ **Statistics: Received and Transmitted Ethernet Frames** on page 6-28

For illustration purposes, the procedures throughout this chapter are based on a switch named Accounting. Some of the ports have names.

Activity Monitor

Menu. Administration> Activity Monitor

The Activity Monitor option is useful in troubleshooting or in monitoring software broadcasts. You can observe ongoing system activity, if any.

The following screen displays when you select Administration> Activity monitor.

```
Accounting
Activity monitor

Broadcast notification sent.
Broadcast notification sent.
```

The activity monitor also automatically activates when you download software to switches on the network (System administration, Broadcast updated software to all systems). The system displays the MAC address of a switch as software downloads to it.

```
Accounting
Activity monitor

load request received from Second Floor Computer
Room
loading... 000f4-02A8CE
completed.

load request received from Third Floor
Administration
loading... 0000F4 D0D070
completed.

load request received from Third Floor SysLab
loading... 0000F4 C00520
completed.
```

Figure 6-1 Activity Monitor During Software Downloads

MAC Address Table

The MAC address table (also referred to as the forwarding table) is a snapshot of source MAC addresses that the switch has learned and static MAC addresses which have been stored in the switch's volatile memory until the addresses have aged. The information on the table dynamically changes as packets appear on any port.

The software deletes a MAC address from the table after the aging time of 300 seconds (5 minutes). If you reset the switch or remove power, the table clears the learned addresses but gets updated as soon as the switch is operational and the ports start to detect packets.

Menu. MAC Address Table

```
MAC Address Menu
Accounting

Show all MAC addresses
By port MAC addresses
Get port from MAC Address
---Static addresses display and configuration---
All static MAC address
Per port static MAC address
Get Port from MAC Address
Multicast addresses
Clear static MAC table
Return to Main Menu...
```

Figure 6-2 Sample MAC Address Table

Show All MAC Addresses

Select MAC Address Table> Show all MAC addresses.

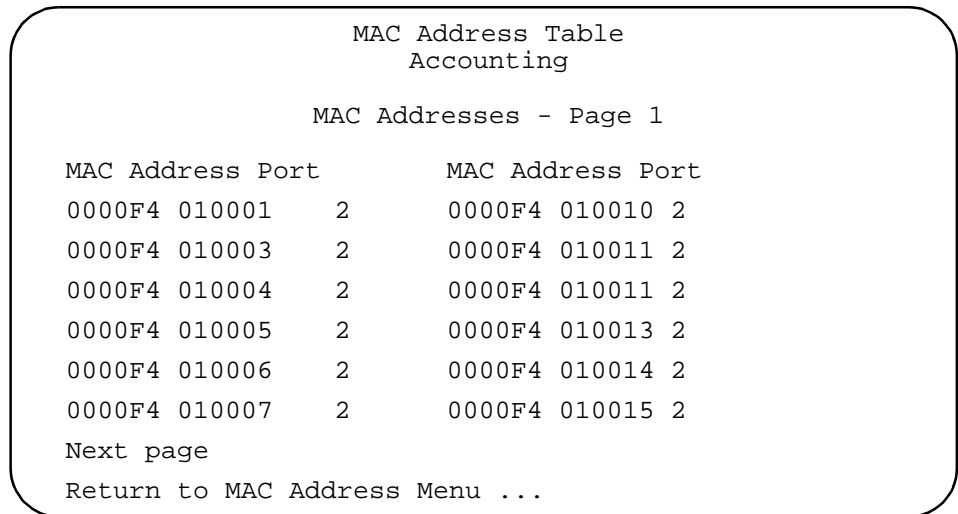


Figure 6-3 Show All MAC Addresses

Show By Port MAC Addresses

Menu. By port MAC addresses

1. Select MAC Address Table from the main menu. The MAC address menu displays.
2. To learn the MAC address of a specific port, select By port MAC addresses.
3. Select a specific port number to learn the MAC addresses for that port. The following screen displays as an example, Port 5's MAC addresses.

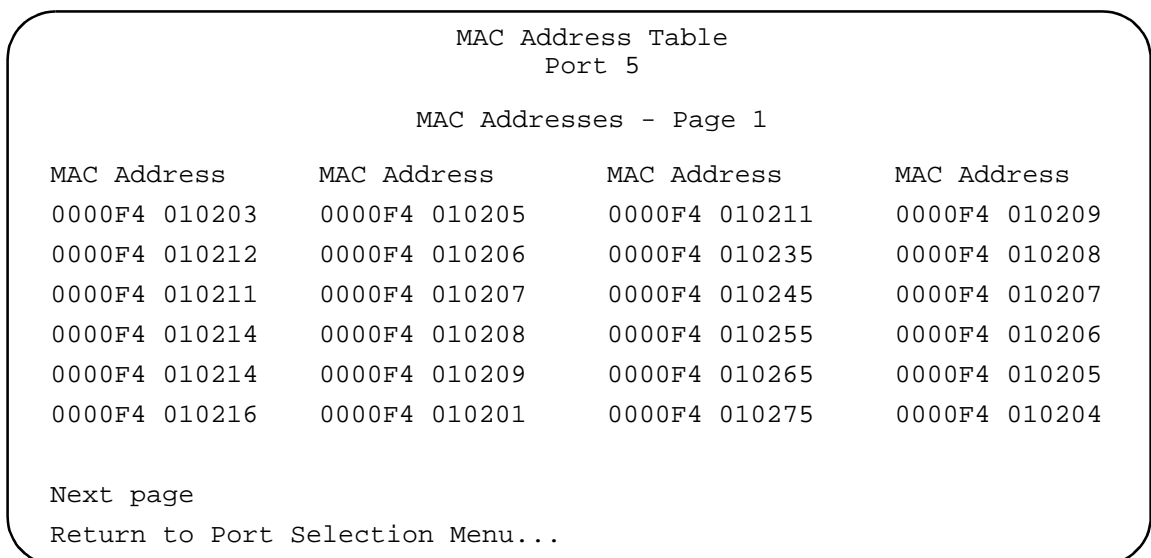


Figure 6-4 By Port MAC Address (Port 5)

Get Port from MAC Address

Users can enter a MAC address and the program returns the port number associated with the MAC address.

Menu. Get Port from MAC Address

1. Select `MAC Address Table` from the main menu. The MAC address menu displays.
2. Select `Get Port from MAC Address`.
3. In the MAC Address field, using the Up Arrow key, enter the MAC Address, for example `0000F4 010203`. Then press **RETURN**.

The following screen shows that the MAC Address of `0000F4 010203` is associated with Port 5.



Figure 6-5 Get Port from MAC Address (Port 5)

Static MAC Addresses

Static MAC addresses are associated with only one port, the port assigned to the device with that MAC address. Static addresses remain in the table and are not aged in 5 minutes like other learned MAC addresses.

Show All Static MAC Addresses

Menu. MAC Address Table> All static MAC addresses

```

Static Address Configuration Menu
Accounting
MAC Addresses - Page 1

MAC Address      Port  MAC Address      Port
0000F4 010001    2    0000F4 000010    2
0000F4 01000F    2    00A0D2 56002C    2
0000F4 01001F    2    01A0D2 02F01C
0000F4 01002D    2

Next page
Return to MAC Address Menu ...
    
```

Figure 6-6 Show All Static MAC Addresses

Show Per Port Static MAC Addresses

Menu. MAC Address Table>Per Port Static MAC
Addresses> Port number

See Figure 6-7 and Figure 6-8.

```

Port Selection Menu
Accounting

Port 1
Port 3
Port 5
Port 7
Port 9
Port 11
Port 13
Port 15
Port 17
Port 19
Port 21
Port 23
Port 26 - Uplink Port A

Port 2
Port 4
Port 6
Port 8
Port 10
Port 12
Port 14
Port 16
Port 18
Port 20
Port 22
Port 24
Port 27 - Uplink Port B

Return to MAC Address Menu ...

```

Figure 6-7 Per Static MAC Addresses

The static MAC addresses for Port 2 display, as shown in Figure 6-8.

```

Add MAC Address Menu
Accounting

Port 2

MAC Addresses      MAC Address      MAC Address      MAC Address
0000F4 010203     0000F4 010205     0000F4 010211     0000F4 010209
0000F4 010212     0000F4 010206     0000F4 010235     0000F4 010208
0000F4 010211     0000F4 010207     0000F4 010245     0000F4 010207
0000F4 010214     0000F4 010208     0000F4 010255     0000F4 010206
0000F4 010214     0000F4 010209     0000F4 010265     0000F4 010205
0000F4 010216     0000F4 010201     0000F4 010275     0000F4 010204

Add MAC address      Null (not configured)
Delete MAC address   Null (not configured)
Next page
Return to Port Selection Menu...

```

Figure 6-8 Per Port Static MAC Address (Port 2)

Delete/Add Static MAC Address

Menu. MAC Address Table> Per port static MAC addresses> Port number> Add MAC address

1. Select Per port static MAC address screen, then <Port Number>.
2. Enter your six digit static MAC address. Figure 6-9 shows that the static MAC address table has been added to Port 19 (Randy).

```

Static Address Configuration Menu
Accounting

MAC Addresses - Page 1

MAC Address      Port          MAC Address      Port
000010 000001      2                0000F4 00001013
000002 00000B   Port 19 - Randy 00A0D2 56002C17
0000D2 56001F      2
0000D2 56002D      7

Please select an option:
Next page
Add Mac Address 000002 00000B
Delete this entry
    
```

Figure 6-9 Add Static MAC Address (Port 19)

Add/Delete Static MAC Addresses and Selecting Ports for Multicasts

Menu. Multicast addresses> Add MAC address>
Ports for Multicasts

Multicast addresses are a type of static address. When you clear the static address table, all multicast addresses are discarded. However, if you add a multicast address, this address appears in the static address table.

Note

You add or delete a MAC address from the Muticast Addresses menu.

Add Static MAC Address Menu	
Accounting	
MAC Addresses	
MAC Address	Ports for Multicast Packets
0100F4 010243	14,15
0100F4 397492	all
0100F4 070697	7,8
0100F4 643476	2,3
0100F4 365454	4,5
Add MAC address	Null (not configured)
Ports for multicast	Null (not configured)
(Example: 1, 3, 8, or all)	
Delete MAC address	Null (not configured)
Next page	

Figure 6-10 Muticast Addresses (Add/Delete MAC Addresses)

1. Select Multicast addresses, Add MAC address.

Note

Prior to MAC addresses being added, you must enter both the MAC address and ports to receive multicast packets.

2. As an example, enter the six digit multicast MAC address (010002 00000B) and the ports (5,10,12) that you want to receive multicast packets from that device. See Figure 6-11.

```

                                Add Static MAC Address Menu
                                Accounting
                                MAC Addresses

MAC Address                      Ports for Multicast Packets
0100F4 010243                    14,15
0100F4 397492                    all
0100F4 070697                    7,8
0100F4 643476                    2,3
0100F4 365454                    4,5
Add MAC address                   010002 00000B
Ports for multicast               5,10,12
(Example: 1, 3, 8, or all)
Delete MAC address               Null (not configured)
Next page
Return to MAC Address Menu ...
    
```

Figure 6-11 Add MAC Address and Multicast for Ports 5, 10, and 12

3. To see your newly added MAC address and ports that are to receive multicast packets, press **RETURN**. This simply refreshes the screen.

Note

If you want to change any of the ports that have already been assigned a multicast, you must re-add the new ports designated to receive multicast packets.

Clearing Static MAC Table

When you clear the static address table, all multicast addresses are discarded. However, if you add a multicast address, this address appears in the static address table.

Menu. MAC Address Table Clear> Clear static MAC table

1. Select MAC Address Table, then select Clear static MAC table.

Clear Static MAC table now? (Yes or No):

2. Enter `y` to clear the MAC address table.

Locating Your Switch's MAC Address

- Look at the MAC address label directly above the RS232 management port on the switch's front panel, or
- Select `Diagnostics` from the System Administration Menu to read the address from the screen.

Security/Source Address Table

The Security/Source Address Table menu defines two options:

- ❑ Source Address Learning Mode (Secure or Automatic)
- ❑ Intruder Protection Action (SNMP Trap/No Trap; Port Disabled/Not Disabled)
- ❑ Threshold Security

Figure 6-12 shows the Security/Source Address Table menu and defaults.

```
Please select an option:
Source Address Learning Mode:
  Automatic: source address learning enabled; no intruder protection
  Secure: source address table locked; intruder protection enabled
  > Threshold: intruder protection when port MAC address limit exceeded

  Config MAC address limit per port

Intruder Protection:
  Transmit an SNMP Trap if an intruder is detected
  > No SNMP Trap if an intruder is detected

  Disable the port if an intruder is detected
  > Port state unchanged if an intruder is detected

  Return to System Configuration Menu ...
```

Figure 6-12 Security/Source Address Table

Table 6-1 briefly lists the options in the Security/Source Address Table menu. For complete definitions of this options, see the sections that follow this table.

Table 6-1 Security/Source Address Table

Options	States	Definition
Source Address Learning Mode	Automatic	Source address learning is enabled, and the intruder protection is disabled.
	Secure	The source address table is locked, and the intruder protection is enabled.
	Threshold	Learning is enabled. Intruder protection is enabled if threshold is exceeded.
Intruder Protection	Send Trap	Trap is transmitted.
	No Trap	Trap is not transmitted when an intruder is detected.
	Disable Port	The port is disabled when an intruder is detected.
	Port State Unchanged	The port remains ON when an intruder is detected.

Source Address Learning Mode

The Source Address Table (SAT or MAC forwarding table) is a database of MAC addresses and their associated port of entry learned by the switch. The Source Address Learning Mode allows you to control it as a "secure" or "automatic" state.

Secure: Learning Off/Security On

In the "secure" mode, the learning feature is disabled and the source address table is in a "locked" state. This setting is used when the MAC address learning is completed and when any new MAC address entries are to be entered manually. When the SAT is locked, no new addresses will be learned. If a packet is received with an address that is not already in the SAT, the packet is dropped and the new MAC address is not learned.

Automatic: Learning On/Security Off

The automatic mode is the default setting. When in “automatic” mode, the SAT is in an “unlocked” state and is updated each time a port receives a packet from a new source address. The SAT address table can store 2K of MAC addresses.

When the switch is in a learning mode, the software:

- ❑ Monitors the MAC source address as frames come into each port
- ❑ Compares the incoming source addresses to entries in the SAT table
- ❑ Updates the SAT table by storing the new MAC address

Note

If you do not lock the SAT table, it will not be saved when the switch is reset.

Most users typically keep the source address learning mode ON to continuously update the MAC address table. Information in the table is useful for inventory control, based on MAC addresses of the devices connected to the module. As an option, you can manually turn learning OFF and go to a secure mode if you want to restrict the module only to specific MAC addresses. Once this process is complete, all MAC addresses become static addresses and will stay in the MAC address table until the table is cleared or until the address is deleted.

Security Threshold

Security Threshold allows the user to limit or set the number of MAC addresses for any port or all ports. In addition, when threshold is enabled; intruder protection also is enabled. The port continues to learn new MAC addresses until it is disabled. In a busy network, the port may accumulate more MAC addresses than the specified limit if MAC addresses are learned between the time the threshold is exceeded and the time the port is disabled. See Figure 6-13.

```

Please select an option:

Source Address Learning Mode:

    Automatic: source address learning enabled; no intruder protection
    Secure: source address table locked; intruder protection enabled
    > Threshold: intruder protection when port MAC address limit exceeded

    Config MAC address limit per port

Intruder Protection:

    Transmit an SNMP Trap if an intruder is detected
    > No SNMP Trap if an intruder is detected

    Disable the port if an intruder is detected
    > Port state unchanged if an intruder is detected

    Return to System Configuration Menu ...
  
```

Figure 6-13 Security Threshold

To set the number of MAC addresses associated for a specified port or for all ports, use the Config MAC address limit per port command.

```

Port                MAC Address Limit
1:                  0
2:                  0
3:                  0
4:                  0
5:                  0
6:                  0
7:                  0
8:                  0
9:                  0
10:                 0
11:                 0
12:                 0

More ...
Return to Security / Source Address Table ...
  
```

Figure 6-14 Configure MAC Address Limit

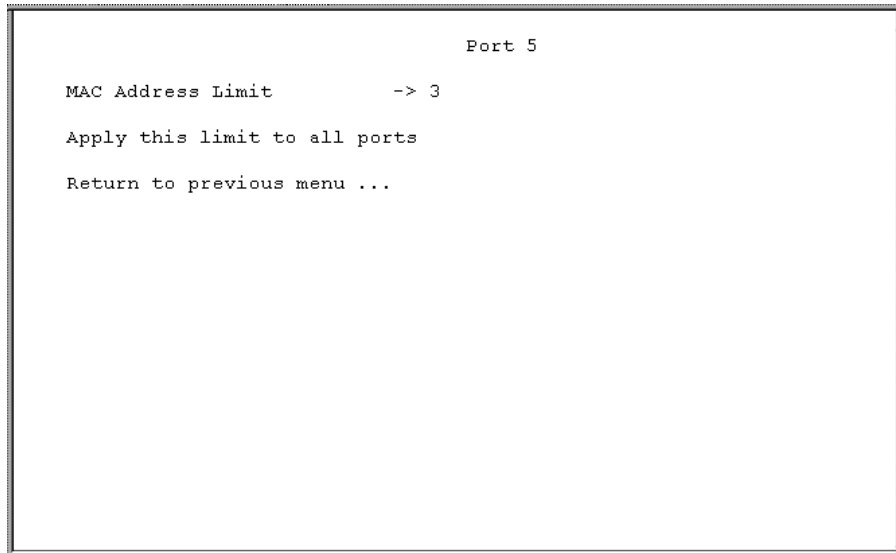
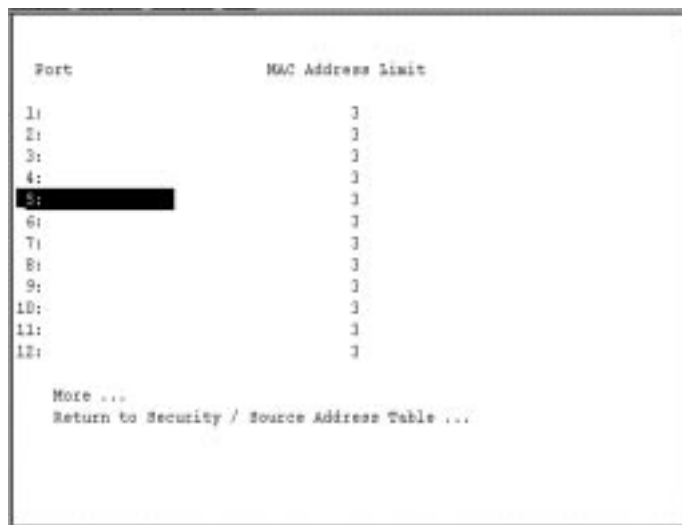


Figure 6-15 MAC Address Limit on Port 5



All ports
with the limit
of three MAC
Addresses

Figure 6-16 MAC Address Limit on All Ports

Intruder Protection

The Intruder Protection feature resides in the lower-half of the Security/Source Address Table menu and is shown in Figure 6-12. This screen does not appear until you first enable Secure : source address table locked; intruder protection enabled option.



Figure 6-17 Intruder Protection Screen Section

The Intruder Protection option determines how the switch handles transmissions from MAC addresses not found in the SAT. These options are available when the switch is set to the “secure” mode.

The switch detects intruders by comparing incoming source MAC addresses to entries in the SAT table. Intruders are transmissions from addresses not found in the table. There are several possibilities for configuring a port in relationship to intruders:

- Transmit SNMP trap message (port state unchanged)
- Disable the port (no SNMP trap)
- Transmit SNMP trap and disable the port
- No action (default)--(No trap; port state unchanged)

Transmit SNMP Trap Message (port status unchanged)

Use this configuration to send an SNMP trap message to the SNMP manager when an intruder is detected. (See Configuring IP Parameters on page 4-6. The IP parameters is a submenu of the System Configuration menu.)

The message contains enough SNMP MIB information to help you identify the port where the intrusion took place. Regardless of the mode you select for Transmit SNMP Trap, SNMP statistics gathering continues.

Disable the Port (no SNMP trap)

Use this configuration when you want the switch to automatically disable the port when an intruder is detected. Once the switch software disables a port because of an intruder, no source address can use that port. The port remains disabled until you manually enable it.

Note

When the Security feature is used to disable a port, the MAC addresses are not deleted until the port is re-enabled. This allows the user to check the MAC address display to see which MAC addresses came in on the specified port.

Transmit SNMP Trap and Disable port

Use this configuration if you want to send an SNMP trap message and disable the port at the same time during an intrusion. Once the switch software disables a port because of an intruder, no source address can use that port. Note that when the port becomes disabled by enabling the securing feature, the MAC addresses associated with the specified port are not removed immediately from the table. However, the addresses will be removed from the table as the MAC addresses age out.

No Action (default) (No trap; port state unchanged)

In this default setting, an SNMP trap is not sent and the port state remains unchanged when an intruder is detected.

Setting Security/Source Address Table Options

Security options are enabled or disabled on a system-wide basis.

To set any of the options within the Source Address Learning Mode menu, simply select the desired option using the UP and DOWN arrow keys and then press Enter. Options on the menu that are in bold print are the defaults.

Menu. System configuration<Security/Source Address Table>

```

Please select an option:
Source Address Learning Mode:

  Automatic: source address learning enabled; no intruder protection
  Secure: source address table locked; intruder protection enabled
  > Threshold: intruder protection when port MAC address limit exceeded

  Config MAC address limit per port

Intruder Protection:

  Transmit an SNMP Trap if an intruder is detected
  > No SNMP Trap if an intruder is detected

  Disable the port if an intruder is detected
  > Port state unchanged if an intruder is detected

  Return to System Configuration Menu ...
  
```

Figure 6-18 Security/Source Address Table Screen (defaults)

Setting Source Address Learning Mode

1. Select <Secure: source address learning enabled; intruder protection disabled>. The Secure: Source Address Learning Enabled screen displays.

```

Please select an option:
Source Address Learning Mode:

  Automatic: source address learning enabled; no intruder protection
  > Secure: source address table locked; intruder protection enabled
  Threshold: intruder protection when port MAC address limit exceeded

  Config MAC address limit per port

Intruder Protection:

  Transmit an SNMP Trap if an intruder is detected
  > No SNMP Trap if an intruder is detected

  Disable the port if an intruder is detected
  > Port state unchanged if an intruder is detected

  Return to System Configuration Menu ...
  
```

Figure 6-19 Secure: Source Address Learning Enabled

Setting Security Threshold

1. Select <Threshold:intruder protection when port MAC address limit exceeded>

When enabled, this feature displays in bold print on your screen.

Setting Number of MAC Address

Select <Config MAC address limit per port> The following screen displays.



Figure 6-20 Five MAC Addresses Assigned to Port 1

2. Select the specified port and enter the maximum number of MAC addresses assigned to that port, for example three MAC addresses for Port 5.



Figure 6-21 MAC Address Limit on Port 5

- To apply the same number of MAC address limits to all ports, select <Apply this limit to all ports>. The following screen displays.

Port	MAC Address Limit
1:	3
2:	3
3:	3
4:	3
5:	3
6:	3
7:	3
8:	3
9:	3
10:	3
11:	3
12:	3

More ...
Return to Security / Source Address Table ...

All ports
with the limit
of three MAC
Addresses

Figure 6-22 MAC Address Limit on All Ports

Setting a port(s) to 0 (default) indicates that there is no limit of MAC addresses for the specified port(s). In threshold mode, the port disable option must be enabled to stop intruder traffic since the switch is in learning mode.

Setting Intruder Protection

When a packet with an unknown address is received, the port on which the packet is received is disabled. This feature can be enabled or disabled.

When a packet with an unknown address is received, an SNMP trap is generated to notify the network administrator of such event. This feature can be enabled or disabled.



Figure 6-23 Intruder Protection

The defaults for Intruder Protection are:

- No SNMP Trap if an intruder is detected
 - Port state unchanged if an intruder is detected
1. Select <Transmit an SNMP Trap if an intruder is detected>
 2. Select <Disable the port if an intruder is detected>

For detailed MAC address information, see **MAC Address Table** on page 6-3. All other related MAC address information follows the MAC Address Table section.

Mirror Port

Menu. Traffic/Port Mirroring

The Mirror Port allows you to monitor traffic on any port with the use of a monitoring device.

Traditionally, users had to sacrifice one other port to mirror another; for example, to monitor traffic on Port 2 (the source port), you had to configure another port (for example, Port 3), as the destination port to mirror it. Port 3 therefore could not perform its primary function, switching packets, while it is mirroring Port 2. The Mirror Port is an extra port designated as the fixed destination port. It can mirror any source port you identify.

The mirror port will mirror both receive and transmit activity on the mirrored port.

For the non-XL versions of the switch, the receive and transmit activities can be monitored selectively. For the XL versions, both receive and transmit activities are monitored simultaneously.

When you physically connect a monitoring device to the Mirror Port, the Mirror Port LINK LED lights green. Make sure you also refer to the monitoring device's manual.

1. Select `Traffic/Port Mirroring` from the main menu. The Port Mirroring screen is displayed.

```
Port mirroring state:
>Enabled
Disabled
Note: Both transmit and receive activity will be
mirrored.
```

2. Select `Enabled` to display additional options on the same screen.
3. Select a source port number.

The software displays a list of ports, similar to the following screen (some ports have been named in the example):

```
Please select a port:
Port 1-Room 1148      Port 2-Room 1149
Port 3-Room 1150      Port 4-Room 1151
Port 5                Port 6
Port 7                Port 8
Port 9                Port 10
Port 11               Port 12
Port 13               Port 14
Port 15               Port 16
Port 17               Port 18
Port 19               Port 20
Port 21               Port 22
Port 23               Port 24
Port 26-Uplink Port A  Port 27-Uplink Port B

Return to Port Mirroring Configuration...
```

4. Select Return to Main Menu...
5. Go to your monitoring device to see the traffic.

Port Status

Menu. Port status and configuration

Selecting Port Status and configuration from the Main Menu for the first time displays the list of ports similar to the following screens.

Note

For the AT-3714FXL and AT-3714F, Ports 14 and 15 are the uplink ports (Port A and Port B).

Accounting			
Port	Link	Status	Mode
1:	Online	Enabled	Half duplex
2:	Online	Enabled	Half duplex
3:	Online	Enabled	Autonegotiate
4:	Online	Enabled	Half duplex
5:	Online	Enabled	Autonegotiate
6:	Online	Enabled	Autonegotiate
7:			
8:			
9:			
10:			
11:			
12:			
More ...			
Return to Mai			

Accounting			
Port	Link	Status	Mode
13:	Online	Enabled	Half duplex
14:	Online	Enabled	Half duplex
15:	Online	Enabled	Half duplex
16:	Online	Enabled	Half duplex
17:	Online	Enabled	Half duplex
18:	Online	Enabled	Half duplex
19:	Online	Enabled	Half duplex
20:	Online	Enabled	Half duplex
21:	Online	Enabled	Half duplex
22:	Online	Enabled	Half duplex
23:	Online	Enabled	Half duplex
24:	Online	Enabled	Half duplex
25:	Online	Enabled	Half duplex
26:	Uplink Port A	Online	Half duplex
27:	Uplink Port B	Online	Half duplex
More...			

Standard uplink port → 26: Uplink Port A
Optional uplink port (MDA) → 27: Uplink Port B

Figure 6-24 Port List from Port Status (for AT-3726XL, AT-3726)

Port Numbering

Table 6-2 shows the port numbers for the switch.

Table 6-2 Port Numbering

Switch	Port #	Port Type
AT-3726XL, AT-3726	1-24	10Base-T
	25	Remote management port for Omega
	26 (Uplink port A)	10/100Base-TX
	27 (Uplink port B)	Optional MDA (TX or FX)
AT-3716XL	1-16	10Base-T
	17	Remote management port for Omega
	18 (Uplink port A)	10/100Base-TX
	19 (Uplink port B)	Optional MDA (TX or FX)
AT-3714FXL, AT-3714F	1-12	10Base-FL
	13	Remote management port for Omega
	14 (Uplink port A)	100Base-FX
	15 (Uplink port B)	Optional MDA (TX or FX)

Selecting a port number, for example, 1, from the list displays the port configuration screen for Port 1, as shown in Figure 6-25.

```
Accounting

Port 1

Link State: Online
Port State: Enabled
Transmission Mode:                Half duplex

Enable this port
Disable (partition) this port

Auto negotiate
Full duplex
Half duplex

Store-and-forward
Cut-through (fragment-free)

Transmit pacing enabled
No transmit pacing

Port Name
Return to Port Status Menu ...
```

Figure 6-25 Port Configuration for Port 1

The following options at the top of the screen are for information only.

- ❑ Link State indicates the presence or absence of a physical link on the port.
- ❑ Port State indicates if the port has been enabled, disabled, blocked, affording, or listening. The state changes depending on software or user intervention.

Normal means the port is ready but not necessarily active.

Disabled means someone has manually disabled the port using the Omega software.

Partitioned means the software has detected an error in the network and therefore automatically disables the port to prevent the error from propagating.

- ❑ Transmission Mode indicates the speed and direction by which packets can be transmitted either by enabling auto-negotiate, (10 or 100 Mbps) half- duplex (one direction only), or full-duplex (both directions simultaneously).

Statistics: Received and Transmitted Ethernet Frames

Menu. Ethernet statistics

You can view statistics on received and transmitted frames in two ways:

- ❑ At the switch level, where you see the total of each frame type on all ports taken together; or
- ❑ At the port level, further broken down into:
 - Per port, all frame types
 - Per frame type

Statistics are useful if you are trying to diagnose a problem and would like to isolate it to a specific port. You can view graphs that show information on the switch as a whole. From this total picture, you have the option to view statistics on a per-frame type or a per-port basis.

Viewing Switch Statistics

1. Select `Ethernet Statistics` from the Main Menu to display the Receive Statistics Graph.

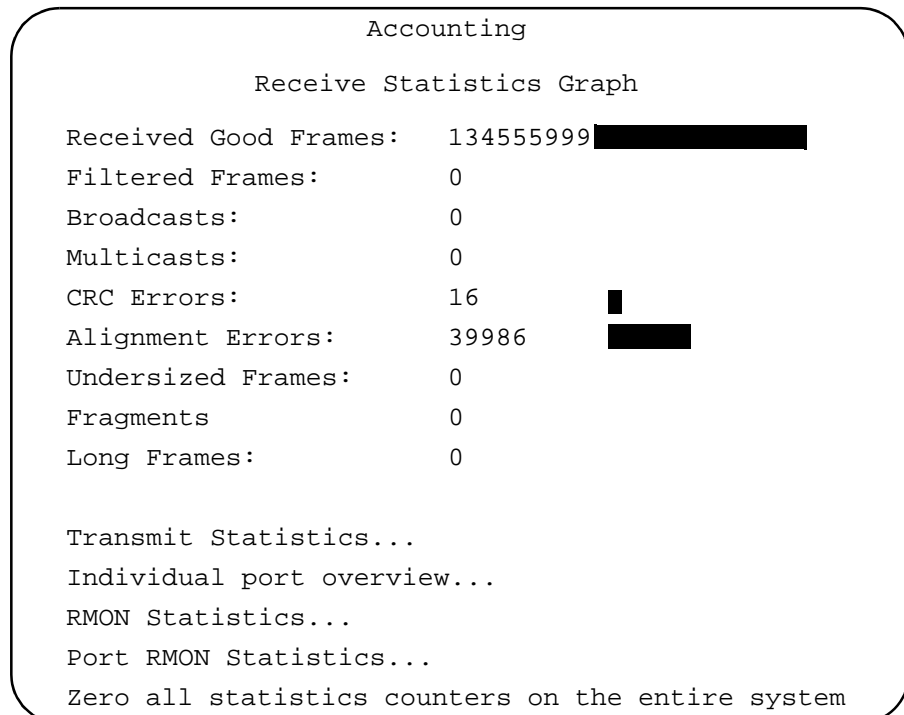


Figure 6-26 Received Frames Graph

The graph shows the types of frames received by the switch over a period since the switch's last reset or since the counters have been reset to zero. Table 6-3 lists and defines the types of received frames.

2. Select `RMON Statistics` from the `Receive Statistics Graph` to display the `RMON Statistics Graph`.
3. Select a port, for example `Port 1`. Figure 6-28 displays the `RMON Statistics` for `Port 1`.

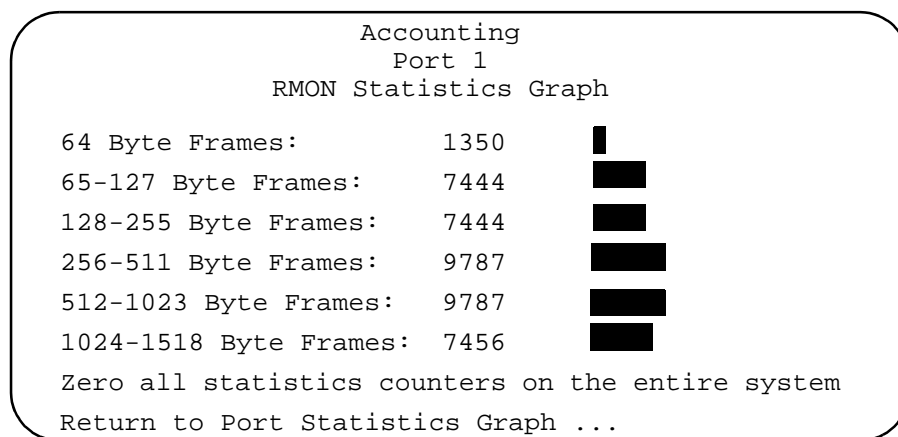


Figure 6-27 RMON Statistics for Port 1

Table 6-3 Received Frames

Frame Type	Description
Received Good Frames	Total number of frames received by the switch since the last reset.
Filtered Frames	Frames received by the switch but not forwarded because the destination is within the same LAN segment, therefore, the frame was already seen by all nodes on the segment.
Broadcasts	Frames received and then forwarded by the switch destined for nodes on the network.
Multicasts	Frames received and then forwarded by the switch destined for multiple but specific addresses.
CRC Errors	Frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes).
Alignment errors	Frames with a non-integral number of bytes, that is, frame length in bits are not evenly divisible by 8, but with the proper length (64-1518 bytes).
Undersized Frames	Frames less than the minimum specified by IEEE 802.3 (64 bytes including the CRC).
Fragments	Frames that are shorter than 96 bits, including 64 bits of preamble and may occur because of a collision or from a failed transceiver transmitting bad packets.
Long frames	Frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC).
RMON	The following frames relate to RMON.
64 Byte Frames	Total number of transmitted/received frames (including bad frames) that were 64 octets (excluding framing bits but including FCS octets).
65-127 Byte Frames	Total number of transmitted/received frames (including bad frames) that were between 65 and 127 octets (excluding framing bits but including FCS octets).
128-255 Byte Frames	Total number of transmitted/received frames (including bad frames) that were between 128 and 255 octets (excluding framing bits but including FCS octets).
256-511 Byte Frames	Total number of transmitted/received frames (including bad frames) that were between 256 and 511 octets (excluding framing bits but including FCS octets).
512-1023 Byte Frames	Total number of transmitted/received frames (including bad frames) that were between 512 and 1023 octets (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	Total number of transmitted/received frames (including bad frames) that were between 1024 and 1518 octets (excluding framing bits but including FCS octets). If the LONG bit is set, this statistic counts frames that are between 1024 and 1536 octets (excluding framing bits but including FCS octets).

4. Select Transmit Statistics to display the Transmit Statistics Graph, as shown in Figure 6-28.

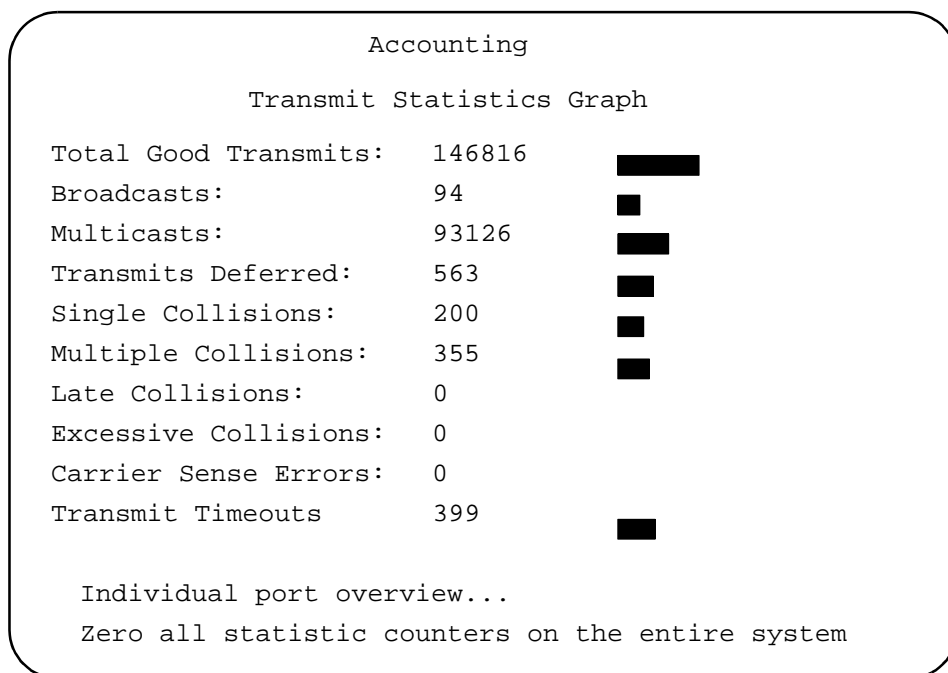


Figure 6-28 Transmitted Frames Graph

The graph shows the types of frames transmitted by the switch over a period since the switch's last reset or since the counters have been reset to zero. Table 6-4 lists and defines the types of transmitted frames.

Table 6-4 Transmitted Frames

Frame Type	Description
Total Good Transmits	Total frames transmitted by the switch without errors.
Broadcasts	Total number of received/transmitted good packets that were directed to the broadcast address. This does not include multicast packets.
Multicasts	The total number of received/transmitted packets that were directed to the multicast address. This does not include packets directed to the broadcast address. For the 100 Mbps ports, the counter records the sum of alignment and code errors (frames received/transmitted with RX/TX error signal).
Transmits Deferred	Frames whose transmission has been deferred by the switch due to lack of resources; they are not stored in the buffer and eventually dropped.
Single Collisions	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collisions	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Late Collisions	Collisions that occur after 64-byte times of the frame had elapsed.
Excessive Collisions	A count of frames for which the first transmission on a particular interface fails due to excessive collisions.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count is incremented at most once per transmission attempt even though the carrier sense condition fluctuates during a transmission attempt.
Transmit Timeouts	Number of times the switch has stopped trying to transmit due to collisions

Viewing Port Statistics

1. Select **Ethernet statistics**, then select **Receive Statistics Graph**.
2. Select **Individual port overview** to display a screen similar to Figure 6-29, listing each port and the corresponding total number of frames received:

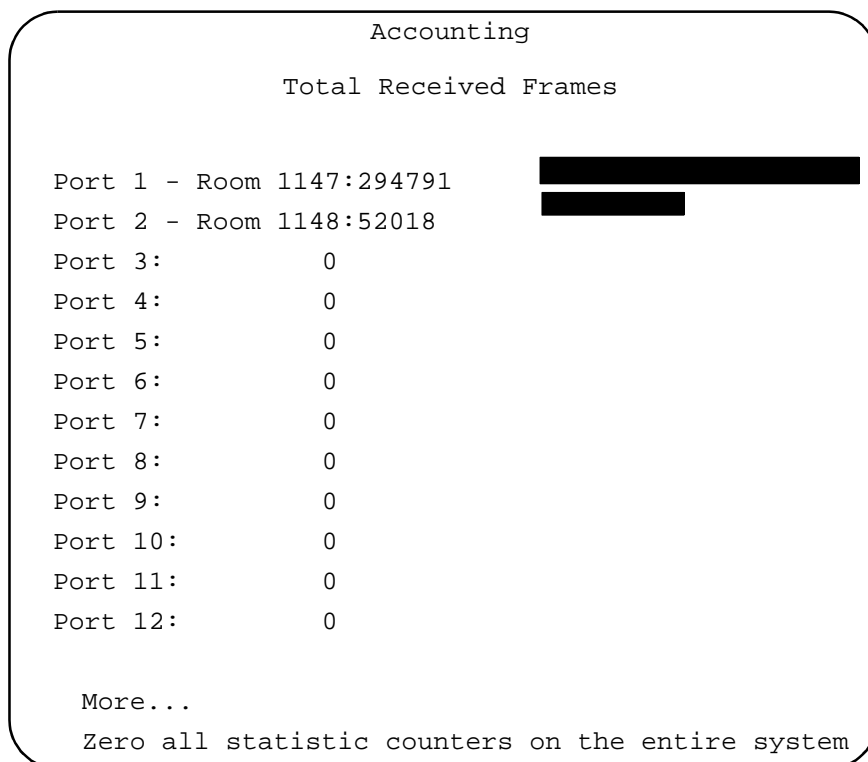


Figure 6-29 Total Received Frames Per Port Graph

3. Select a port number, for example, **Port 1**, to display a screen similar to Figure 6-30, showing the types of frames received by Port 1.

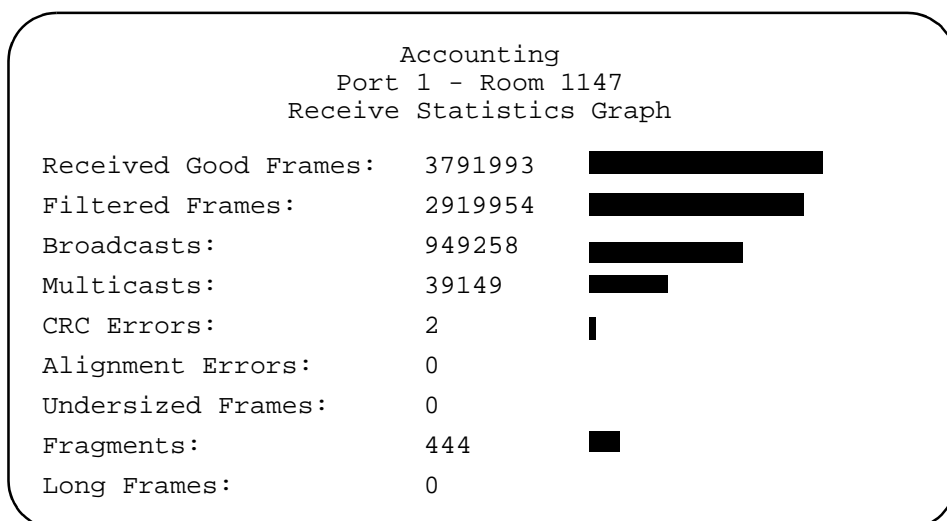


Figure 6-30 Received Frames Graph for Port 1

The graph shows the frames Port 1 has received over a period since the switch's last reset or since someone has last set the counters to zero.

4. Select Transmit statistics to display a screen similar to Figure 6-31, showing the frames transmitted by Port 1.

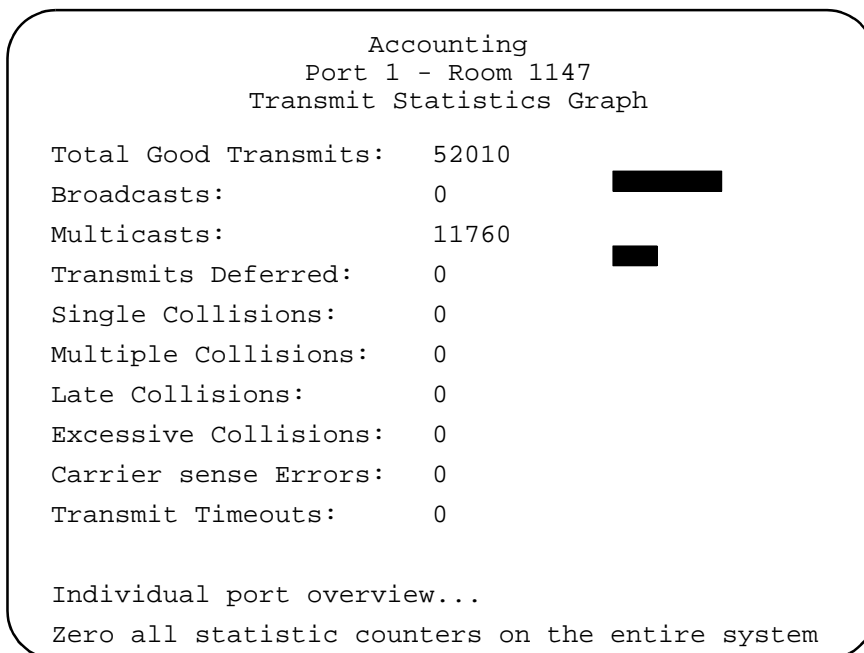


Figure 6-31 Transmitted Frames Graph for Port 1

Expect transmit errors to be very small. The switch may receive a number of bad frames, but the switch must drop those and send only good frames.

Interpreting the Graphs

The sample graphs show the types of frames received or transmitted by a switch or its individual ports since the last time the counters or the switch were reset. The software keeps count of the number of frames and creates a graph. The counters and the graph dynamically increment as the switch processes frames over a period of time.

When the individual counters reach a maximum of 2^{32} (over 4 billion), then the counters reset to zero. Because each counter resets independently; your graph may become inaccurately skewed; therefore, you need to reset the counters to get a new baseline on frame statistics.

Using the Graphs as a Monitoring and Diagnostics Tool

1. Display any of the Ethernet statistics graphs by selecting `Ethernet statistics` from the Main Menu.
2. Observe the counters and the graph.

The graph helps you visually monitor the proportion of good and bad frames the switch has detected. Good frames consist of filtered and forwarded unicasts, broadcasts, and multicasts. Bad frames are runts and long frames or those with CRC or alignment errors. It is normal to have a number of error packets occasionally. If the network seems to be slow, this graph is one of the areas you can check to help isolate the problem.

3. Identify and fix the problem.

Note that the problem may be external to the switch, and the statistics may just indicate an error condition somewhere on the network you need to fix. You may also need additional monitoring devices specifically designed for that purpose, such as a network analyzer, to identify the problem.

4. Select `Zero statistics counters` from any of the Statistics screens after fixing the problem.

You need to reset counters to get a new baseline on frame statistics. That is because the counters and graphs still depict the information during the error condition and will continue to increment from there until you reset the counters.

Note

For more details on resetting statistics counters, see Chapter 7, **Diagnostics**.

Chapter 7

Diagnostics

This chapter describes the following topics:

- ❑ **Resetting the Switch** on page 7-2
- ❑ **Running Diagnostics** on page 7-3
- ❑ **Getting Help** on page 7-4
- ❑ **Resetting Statistics Counters** on page 7-5

Also see AT-3726XL, AT-3716XL, and AT-3714FXL Installation Guide and AT-3726, AT-3718, and AT-3714F Installation Guide that explains in detail the different ways to diagnose error conditions by interpreting the LEDs on the switch's front panel.

Resetting the Switch

Menu. Administration> Reset and restart the system

You reset the switch:

- ❑ As a first attempt to fix an error condition; for example, the FAULT LED is on
- ❑ To download software through a modem
- ❑ To reset all statistics counters to zero

To Reset the Switch

Menu. Administration> Reset and restart the system

Optionally, you can press **Reset** on the switch's front panel, or unplug its power cord and then plug it in.

The **Reset** button is recessed; you must use a pointed object to press it. The switch first undergoes a power-on self test (POST) process that takes only a few moments; then the switch becomes operational again.

Running Diagnostics

Menu. Administration> Diagnostics

Select **Diagnostics** from the System Administration Menu to display the Diagnostics screen. The example in Figure 7-1 shows the Diagnostics screen on a switch named Accounting.

```
Accounting
Allied Telesyn AT-3714FXL
MAC Address 0000F4 010203 RJ45/MII Applique, MAU
AT-S20 Ethernet Switch Software: Version 3.0 981104
Running 2 days, 20 minutes, 10 seconds
Diagnostics Results:
  Flash PROM                Good
  RAM                        Good
  Serial Interface           Good
Optional Extended Diagnostic Tests:
  Extended Diagnostic Test will disrupt normal system
  These tests should be run only when the network is
  inactive.
Run Extended Diagnostic Tests now? (Yes or No):
```

Figure 7-1 Diagnostics Screen

The Diagnostics Menu allows you to run a limited set of diagnostics test on the switch. There are only two results on a diagnostics test: Good or Failed.

You also see the following information:

- The switch model and version number
- The switch's MAC address
- The software model and version number
- The type of MDA (applique) if installed and whether a MAU is installed (Medium Attachment Unit)
- The time the switch has been up and running

Getting Help

Contact Allied Telesyn's technical support at **www.alliedtelesyn.com**. Be prepared to give the following information:

- Serial number
- Software version
- A description of the problem

Resetting Statistics Counters

Menu. Ethernet statistics> Zero all statistics on the entire system

You reset the statistics counters because:

- ❑ The counters no longer reflect the current information.

For example, disabling a port to fix a problem does not reset its counters. After the error clears and you manually re-enable the port, you may want its statistics to accumulate from a fresh start. Otherwise, the counters and the graph not only still reflect information associated with the error condition; the counters continue to increment from the wrong baseline.

- ❑ As each frame type reaches the maximum of 2^{32} (over 4 billion), the statistics for that frame type resets to zero. Once this happens, the counters and graph become inaccurately skewed.

To Reset Switch (System) Counters

1. Select `Ethernet Statistics` from the Main Menu to display the Receive Statistics Graph.
2. Select `Zero all statistics on the entire system`.

Both Receive and Transmit counters and graphs are reset to zero.

Appendix A

Spanning Tree Protocol

This appendix provides a brief explanation of Spanning Tree Algorithm and its use with the switch.

For detailed information on the operation of the Spanning Tree Algorithm, consult IEEE Std 802.1D, ISO/IEC 10038: 1993.

Concepts

The switch, which runs the AT-S20 software, also implements the IEEE 802.1D Spanning Tree Protocol (STP). The STP provides a network with robustness and allows network administrators to easily change their network topology. Its implementation reduces complex network topologies (networks with multiple paths between source and destination nodes) to a single active topology. This technique guarantees that loops do not occur between source and destination nodes of the network. Loops are eliminated by placing some of the redundant ports in a blocking state, in which they do not forward packets but continue to execute the protocol. If the network topology changes, for example by the failure, removal, or addition of an active network node, a blocked port may be included in the new active topology and begin forwarding frames.

Features

The switch provides the following STP features:

- ❑ Compensates automatically for the failure, removal, or addition of any bridge in an active data path.
- ❑ Achieves port changes in short time intervals, which establishes a stable active topology quickly with a minimum of network disturbance.
- ❑ Uses a minimum amount of communications bandwidth to accomplish the operation of the STP.
- ❑ Reconfigures the active topology in a manner which is transparent to stations transmitting and receiving data packets.
- ❑ Manages the topology in a consistent and reproducible manner through the use of STP parameters.

Parameters

Several configuration parameters control the operation of the Spanning Tree Protocol. Table A-1 describes the parameters and lists each parameter's default settings for the switch. The port numbers include the 10Base-T ports, the management port, the standard 100 Mbps uplink port, and an optional expansion port, dependent upon the switch model.

Table A-1 Spanning Tree Protocol Parameters

Parameter and Description	Default
Bridge Group Address Unique MAC group address, recognized by all bridges in the network	N/A
Bridge Identifier Identifier for each bridge, consisting of two parts: a 16-bit bridge priority and a 48-bit network adapter address. Ports are numbered in absolute numbers; for example from 1-27 for a 24-port switch with expansion modules. The network adapter address is the same address as the first port of the bridge.	32768 (bridge priority)
Port Priority	128
Port Cost The spanning tree algorithm calculates and ensures that an active topology generates minimal path costs.	100 for 10 Mbps ports 10 for 100 Mbps ports

Operations

When spanning tree is enabled for the first time or when the network topology changes due to a failure, the addition, or removal of a component, the spanning tree algorithm automatically sets up the active topology of the current network.

Communication between bridges. Periodically, all devices running STP on a network transmit packets to each other through the Bridge Group Address which all bridges share. When a bridge receives a packet sent to the Bridge Group Address, the bridge's STP processes the packet. The packet is ignored by application software and other LAN segments. Bridges communicate between each other in order to determine the Root Bridge.

Selecting a root bridge and designated bridges. During communication between bridges, one bridge is determined to have the lowest bridge identifier. This bridge becomes the Root Bridge.

After the Root Bridge has been selected, each LAN segment looks for the bridge that has the lowest cost relative to the Root Bridge. These bridges become Designated Bridges.

Selecting designated ports. Each Designated Bridge selects a Designated Port. This port is responsible for forwarding packets to the Root Bridge.

Handling duplicate paths. When the active topology of the network is determined, all packets between any two nodes in the network use only one path. Where a duplicate path exists, the non-designated port is put into a blocking state.

Remapping network topology. If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports.

The blocked ports do not forward packets immediately. They first pass through two states, listening and learning, to verify that they may begin forwarding. A port remains in each of these two states for the time defined by the Forwarding Delay parameter. This algorithm ensures that no temporary loops exist in the active network topology and is a safeguard against packet forwarding during a network topology change period.

Index

A

activity monitor 4-26, 6-2
address aging 4-28
administration, switch, list of tasks 4-2
ANSI terminal, *see also* DEC VT100 terminal emulation
ATS20 download password 4-7
automatic mode 6-14
auto-negotiation 1-1

B

backpressure 4-23
baud rates, supported, terminal emulation 4-20
BootP 4-6
BootP server 4-6
BootP utility 2-4
bridge group address parameter A-2
bridge identifier parameter A-2
bridge protocol data unit (BPDU) 4-28, 4-30

C

configuration, global 4-33
configuration, switch and ports, list of tasks 4-1
contact parameter 4-7
conventions, document Preface-iii
cost parameter 4-32
counters, reset 7-5
counters, statistics, resetting 6-34, 7-2, 7-5
cut-through 4-16

D

DEC VT100 terminal emulation Preface-iii, 4-19
default
 VLAN, 5-1
default domain name parameter 4-7
destination port 6-23
DHCP 2-4
disabling, port 4-5
discarding, packet 4-28
Domain Name Server (DNS) 4-7
download password 4-7, 4-26
downloading software 4-25
dumb terminal 4-6

E

enabling, port 4-5
Ethernet 6-28
Ethernet frames, received 6-28
Ethernet frames, transmitted 6-28

F

features, software 1-1, 2-4
forwarding table, *see also* MAC address
fragment-free 4-16
frames, received 6-30
frames, transmitted 6-32

G

gateway address 4-7
generic terminal 4-6
get request 2-4

global configuration 4-33
graphs, statistics, interpretation of 6-34

H

half-duplex 4-17
hello time 4-30

I

intruder protection 6-12, 6-17, 6-17–6-18
IP address 2-4, 4-6
IP commands 4-7
IP parameters
 IP address 2-3
 setting through Omega 4-6–4-7
 SNMP strings 4-7

L

learning mode 6-14
learning, bridge 4-28
limit, MAC Address 6-21
link state, port 6-27
location parameter 4-7

M

MAC address 6-13, 6-15, 6-20
 aging in table 4-28, 6-3
 limit 6-21
 location 7-3
 location of 6-11
 port 6-4
 remote connection for non-IP 2-3
 sample table 6-3
 setting 6-20
 stored in memory 6-3
 updating 4-28
management software
 quitting 1-3, 2-3, 2-5
 session, starting 2-2, 3-2
manager address 4-7
maximum aging time 4-30
memory capacity 6-3
menu options, selecting Preface-v
menu tree, Omega 1-4
menus
 source address table (SAT) 6-12–6-18
mirroring, port 6-11–6-24

N

name restriction 4-12
naming
 port 4-11–4-13
 switch 4-8–4-10
network downloads, software 4-24

O

Omega 6-18
 source address table (SAT) 6-12–6-18

P

password
 to download software 4-26
password protection 1-3, 2-5
password, ATS20 4-7
PING facility 4-4
port configuration
 mirroring 6-11–6-24
port configuration, task list 4-1
port cost parameter A-2
port list, screen sample 6-25
port MAC address 6-4
port name, deleting 4-13
port naming 1-3, 2-5
port numbering 6-26
port priority and cost 4-31–4-32
port priority parameter A-2
port state 6-27
port status 6-25–6-27
port trunking 1-2, 4-34
ports
 disabling 6-18

Q

quitting a session 4-4
quitting, Omega 1-3, 2-3, 2-5

R

received frames 6-30
remote switch
 connecting to 4-3
 downloading software to 4-24–4-26
reset, switch 7-2
router
 for VLAN communication, 5-2
RS232 cable 2-3

S

- SAT (Source Address Table) 6-13
- secure mode 6-13
- security 6-18
- Security Threshold 6-20
- security threshold 6-15
- security threshold, setting 6-20
- Security/Source Address Table 6-12
- setting, MAC Address 6-20
- setting, security threshold 6-20
- setting, source address 6-19
- SNMP
 - community strings 4-7
- SNMP MIB 6-17
- SNMP trap message 6-17
- software upgrades
 - network downloads 4-24–4-26
- source address learning Mode 6-12
- source address learning mode 6-19
- source address setting 6-19
- source address table (SAT) 6-12–6-18
- Source AddressTable (SAT) 6-13
- source port 6-23
- sourceaddress learning mode 6-13
- spanning tree
 - concepts Preface-ii, A-1–A-2
 - parameters, configuring 4-29–4-32
- spanning tree protocol
 - features A-2
 - operations A-3
 - parameters A-2
- static MAC Address, clearing 6-11
- statistics, viewing 6-28, 6-33
- store-and-forward 4-15
- subnet mask 2-4, 4-7
- switch configuration, task list 4-1
- switch identifiers 4-8
- switch name, deleting 4-10
- switch naming 1-3, 2-5

T

- Telnet 2-3
- terminal settings 2-1
- TFTP, get request 2-4
- TFTP, software downloads 4-24
- threshold security 6-12
- timeout value 1-3, 2-5

- transmission mode 6-27
- transmitted frames, Ethernet 6-31–6-32
- trap message
 - intruder protection 6-17–6-18
- trunking, port (sharing) 4-34

V

- variables, entering Preface-v
- Virtual LAN Configuration 5-1
- virtual local area networks (VLANs)
 - about,
 - local area network
 - virtual, 5-1
 - advantages, 5-2
 - default, 5-1
- VLAN
 - communication, 5-2
 - maximum number 5-5
- VT100 4-19

