Management Software

AT-S41

User's Guide

FOR THE AT-8326GB FAST ETHERNET SWITCH

VERSION 1.0

Allied Telesyn

Simply connecting the (IP) world

Table of Contents

Section III
Web Browser Management 151

List of Figures

Preface

This guide contains instructions on how configure the AT-8326GB Fast Ethernet switch using the AT-S41 management software.

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section reviews the different ways that you can access the AT-S41 management software and describes the stacking features of the AT-8326GB switch.

Section II: Local and Telnet Management

The chapters in this section explain how to manage a switch from a local management session or a Telnet management session.

A local management session is established by connecting a terminal or PC to the RS-232 Terminal Port on the front panel of the switch.

A Telnet management session is established using the Telnet application protocol. This type of management session can be performed from any workstation on your network that has the application protocol.

Section III: Web Browser Management

The chapters in this section explain how to manage a switch using a Web browser, such as Microsoft® Internet Explorer or Netscape® Navigator.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Where to Find Web-based Guides

The Allied Telesyn Web site at www.alliedtelesyn.com contains PDF files of the Installation and User Guides for all Allied Telesyn products. The documents can be viewed online or downloaded onto a local workstation or server.

Contacting Allied Telesyn Technical Support

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support
You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site: **http://kb.alliedtelesyn.com**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

E-mail and Telephone Support
For Technical Support via E-mail or telephone, refer to the Support & Services section of the Allied Telesyn web site: **http://www.alliedtelesyn.com**.

For Sales or Corporate Information
You can contact Allied Telesyn for sales or corporate information at our web site: **http://www.alliedtelesyn.com.** To find the contact information for your country, select **Contact Us**, then **Worldwide Contacts.**

Obtaining Management Software Updates

New releases of management software for our managed products can be downloaded from the Allied Telesyn web site: **http://www.alliedtelesyn.com**.

Section I
Overview

The chapters in this section provide an overview of the AT-S41 management software on the AT-8326GB Fast Ethernet switch. They review the different methods for accessing the management software and describe the stacking features of the switch.

Chapter 1

Management Software Overview

The AT-S41 management software is intended for the AT-8326GB Fast Ethernet switch. The software allows you to adjust the operating parameters of the switch. Some of the functions that you can perform with the software include:

❑ Enable and disable ports

❑ Configure port parameters, such as port speed and duplex mode

❑ Create virtual LANs (VLANs)

❑ Create port trunks and port monitors

❑ Assign an Internet Protocol (IP) address

❑ Activate and configure the Spanning Tree Protocol

❑ Configure port security

The AT-S41 management software comes pre-installed on the switch with default settings for all of its operating parameters. The default settings may be adequate for some networks and may not need to be changed. If this is true for your network, then you can use the switch as an unmanaged switch by simply connecting the unit to your network, as explained in the hardware installation guide.

> **Note**
> The default settings for the management software can be found in **Appendix A, AT-S41 Default Settings** on page 235.

To actively manage a switch by changing or adjusting its operating parameters, you must access the switch's AT-S41 management software. The AT-S41 software has a menu interface that makes it very easy to use.

There are four different types of management sessions that you can use to access the AT-S41 management software on an AT-8326GB Fast Ethernet switch. They are:

❑ Local Management

❑ Telnet

❑ Web Browser

❑ SNMP

This chapter briefly describes each type of management session.

Local Management Session

You establish a local management session with an AT-8326GB Fast Ethernet switch by connecting either a terminal or a PC with a terminal emulator program to the RS232 terminal port on the front panel of the master switch, using a null-modem cable. This type of management session is referred to as "local" because you must be physically close to the switch, such as in the wiring closet where the switch is located.

Once the session is started, you will see a menu from which you can make selections to configure and monitor the switch. You can configure all of the switch's operating parameters from a local management session.

Note
For instructions on starting a local management session, refer to **Starting a Local Management Session** on page 28.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8326GB Fast Ethernet switch. In this guide, a Telnet management session is referred to as a remote management session because you can manage the switch from any workstation on your network that has the application protocol. You do not have to be physically near the switch.

Establishing a Telnet management session with an AT-8326GB stack requires that the master switch of the stack have an IP address. You cannot manage an AT-8326GB stack remotely using the Telnet application protocol if the master switch does not have an IP address. You can assign the master switch an IP address using a local management session, as described in the previous section.

Once you have established a Telnet management session with an AT-8326GB master switch that has an IP address, you have complete management access to all of the other AT-8326GB switches in the same stack.

> **Note**
> For further information on stacking, refer to the chapter on **Stacking** on page 22.

If you are just beginning to build your network and have not assigned an IP address to the switch, you might want to start by reading **When Does an AT-8326GB Switch Need an IP Address?** on page 33. This section contains a brief discussion about when it makes sense to assign an IP address to the AT-8326GB switch.

> **Note**
> For instructions on how to start a Telnet management session, refer to **Starting a Telnet Management Session** on page 31.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform the same functions in a Telnet management session as you can with a local management session, except initially assigning the switch's IP address.

Web Browser Management Session

You can also use a Web browser to manage a switch. This is another type of remote management, just as a Telnet management session is considered remote, because any workstation on your network that has a Web browser can be used to manage an AT-8326GB stack.

> **Note**
> For instructions on starting a Web browser management session, refer to **Starting a Web Browser Management Session** on page 152.

SNMP Management Session

Another way to remotely manage an AT-8326GB switch is with an SNMP management program, such as HP Openview. A familiarity with Management Information Base (MIB) objects is necessary to manage a switch with an SNMP management program, as this management method requires loading the AT-8326GB Fast Ethernet switch MIBs into the SNMP management program. For instructions, refer to your SNMP management documentation.

The AT-S41 software supports the following MIBs:

❑ SNMP MIB-II (RFC 1213)

❑ Bridge MIB (RFC 1493)

❑ 4-Group RMON MIB (RFC 1757)

❑ Allied Telesyn Enterprise MIB

Note
SNMP management does not utilize the stacking feature of the AT-8326GB switch. Consequently, you must assign an IP address to each switch that you want to manage with an SNMP program.

Chapter 2

Stacking

This chapter explains the stacking features of the AT-8326GB switch. The sections in this chapter include:

❑ **Stacking Overview** on page 23

❑ **Stacking and the Management Software** on page 24

Stacking Overview

The stacking feature can make it easier for you to manage the AT-8326GB switches in your network. It offers the following benefits:

❑ You can manage up to six AT-8326GB switches from one local or remote management session. All of the switches in a stack can be managed through one management session with the master switch of the stack. This eliminates the need to initiate a separate management session for each switch in your network.

❑ Stacking allows you to build a switch that is customized to the needs and requirements of your network.

❑ Stacking switches reduces the number of IP addresses you need to assign to the switches you are managing, since you can use one IP address for all of the switches in a stack. You assign the IP address to the master switch of the stack.

Note
You can set the IP address manually or activate the DHCP services on a master switch and have the master switch obtain its IP information from a DHCP server on your network. Initially assigning an IP address or activating the DHCP services can only be performed through a local management session.

Note
When you change the configuration of your switch stack by adding or removing a switch from the stack, the master switch will automatically reset to all parameter settings, except for the IP address, to their factory default settings. This means that any configurations or virtual LANs you have established on the master switch will be removed.

Stacking and the Management Software

If you are using the stacking feature of the AT-8326GB switch, the first thing that you should do before you perform any of the procedures in this guide is check to be sure that you are configuring the correct AT-8326GB switch in the stack. The Stack ID of the switch being managed is displayed at the top of most of the management menus.

When you start a management session on the master switch, you are by default addressing that particular switch. The management tasks that you perform effect only the master switch unless you select another switch in the stack using the management software.

Most of the menus and pages of the management software contain a Select Stack ID option that allows you to configure the parameters on another switch in your switch stack. The method of implementing the switch parameters varies for each feature of the management software. Each chapter of this manual contains instructions on how to apply the featured switch settings to another switch in your stack.

Section II
Local and Telnet Management

The chapters in this section explain how to manage an AT-8326GB Fast Ethernet switch from a local or Telnet management session. The chapters include:

Chapter 3

Starting a Local or Telnet Management Session

This chapter contains the procedures for starting local and Telnet management sessions on an AT-8326GB Fast Ethernet switch. The sections in this chapter are:

Local Management Session

On the front panel of the AT-8326GB switch is an RS232 terminal port. You use this port to establish a local management session with the switch's AT-S41 management software.

A local management session is so named because you must be close to the switch, usually within a few meters, to start this type of management session. This typically means that you must be in the wiring closet where the switch is located.

A switch does not need an IP address for you to manage it with a local management session. You can start a local management session at any time on any AT-8326GB switch in your network. Additionally, running a local management session does not interfere with the flow of Ethernet traffic through the unit.

When you start a local management session on an AT-8326GB stack, you can manage just that stack. To start a local management session on another AT-8326GB stack, you need to establish a separate local management session on that stack.

To start a local management session on an AT-8326GB stack, you connect the management cable to the RS232 port on the master switch of the stack. The master switch has a Stack ID of 1. (The STACK ID LEDs on the front of the switches will tell you which is the master switch.) Once the management session has been established, you will have management access to all the switches in the stack.

Note
For more information on stacking, refer to the chapter on **Stacking** on page 22.

Starting a Local Management Session

To start a local management session, perform the following procedure:

1. Connect one end of the null modem management cable included with the switch to the RS232 Terminal Port on a master of the stack. The master switch has a Stack ID of 1. (The STACK ID LEDs on the front of the switches will tell you which is the master switch of the stack.)
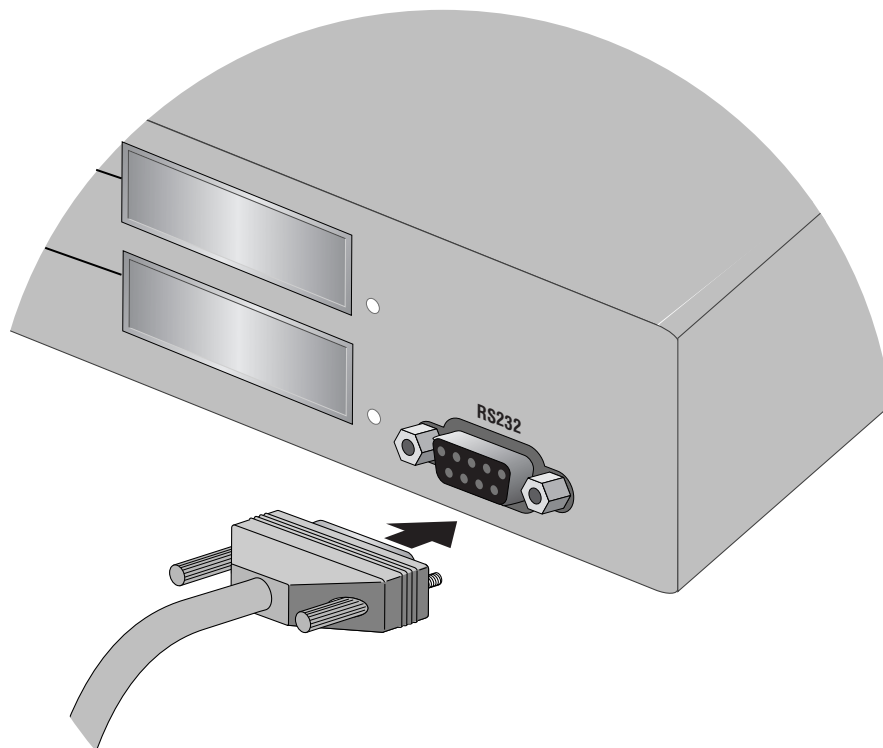
Figure 1 Connecting a Terminal or PC to the RS232 Terminal Port

2. Connect the other end of the cable to an RS232 port on a terminal or a PC with a terminal emulation program.

3. Configure the terminal or terminal emulation program as follows:

   ❑ Emulation mode: VT100

   ❑ Baud rate: 9600

   ❑ Data bits: 8

   ❑ Parity: None

   ❑ Stop bits: 1

   ❑ Flow control: None

   ❑ Key mode: Terminal keys

> **Note**
> These are the default settings for the RS232 terminal port. They are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulation program.

When the terminal session starts, it displays the management software's login prompt, as shown below. Enter the login name and password. The default login name and default password are both "manager."

```
AT-8326GB Management System Version 1.00F
Local - Console
Allied Telesyn International Corp.
Copyright, 2001
===================================================

Login Menu

Login: manager
Password: _
```

Figure 2 AT-S41 Login Prompt - Local Management Session

The switch then displays the management software's Main Menu, as shown below.

```
AT-8326GB Local Management System

Main Menu

[G]eneral Information
[B]asic Switch Configuration...
[A]dvanced Switch Configuration...
Switch [T]ools...
[S]tatistics
[Q]uit


Command>
Enter the character in square brackets to select option
```

Figure 3 AT-S41 Main Menu - Local Management Session

To select a menu item, type the corresponding letter.

Type **Q** to return to the previous menu.

Quitting from a Local Session

To quit a local session, return to the Main Menu and type **Q** for Quit.

You should always exit from a management session when you are finished managing a switch. This can prevent unauthorized individuals from making changes to a switch's configuration should you leave your management station unattended.

Note
You cannot operate both a local management session and a Telnet management session on the same stack simultaneously. Failure to properly exit from a local or Telnet management session may block future management sessions.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-8326GB stack. This type of management is referred to as remote management because you do not have to be physically close to the stack to start the session, such as with a local management session. Any workstation on your network that has the Telnet application protocol can be used to manage a stack.

In terms of functionality, there are no differences between managing a stack locally through the RS232 terminal port and remotely with the Telnet application protocol. You see the same menu selections and have the same management capabilities, except that you cannot perform IP address assignment configurations in a Telnet session.

An AT-8326GB stack must have an IP address for you to manage it remotely using the Telnet application protocol. You can assign an IP address during a local management session. For instructions on how to start a local management session, refer to the previous section of this chapter.

> **Note**
> For background information on stacking, refer to **Stacking** on page 22.

Starting a Telnet Management Session

To start a Telnet management session, specify the IP address of the AT-8326GB stack in the Telnet application protocol. Enter "manager" for both the default login name and default password.

The Main Menu of a Telnet management session is the same menu that you see in a local management session, as shown in Figure 3 on page 29.

The menus also function the same way. To make a selection, type its corresponding letter. To return to a previous menu, type **Q**.

> **Note**
> You can run only one Telnet management session on a switch at a time. Additionally, you cannot run both a Telnet management session and a local management session on the same switch at the same time.

Quitting from a Telnet Management Session

To quit a Telnet session, return to the main menu and type **Q** for Quit.

Chapter 4
Basic Switch Parameters

This chapter contains a variety of information and procedures. It contains information about when to assign an IP address to a switch, resetting the switch, using the switch's default settings, and more.

Sections in the chapter include:

- ❑ **When Does an AT-8326GB Switch Need an IP Address?** on page 33

- ❑ **Configuring an IP Address** on page 34

- ❑ **Configuring System Administration Information** on page 36

- ❑ **Setting the User Interface Configuration** on page 38

- ❑ **Activating DHCP** on page 41

- ❑ **Configuring SNMP Community Strings and Trap IP Addresses** on page 42

- ❑ **Resetting the Management Software Default Values** on page 44

- ❑ **Rebooting a Switch** on page 45

- ❑ **Viewing the AT-S41 Switch Information** on page 46

- ❑ **Ping Execution** on page 47

- ❑ **Bootstrap Configuration** on page 49

When Does an AT-8326GB Switch Need an IP Address?

One of your first tasks as you begin to build your network will be to determine which of the switches in your network should be assigned unique IP addresses.

AT-8326GB Switch

Every AT-8326GB stack in your network that you want to manage remotely using the Telnet application protocol, a Web browser, or an SNMP management program must have a unique IP address. You cannot remotely manage an AT-8326GB stack if it does not have an IP address. You use the address to identify the stack when you start a remote management session.

If you assign a stack an IP address, you must also assign it a subnet mask. The stack uses the subnet mask to determine which portion of an IP address represents the network address and which portion represents the end node address.

You must also assign the stack a gateway address if there is a router between the stack and the remote management workstation. This gateway address is the IP address of the router through which the stack and management station will communicate.

You do not need to assign an IP address, subnet mask, or gateway address if you do not intend to manage an AT-8326GB stack remotely. The stack will function without these values and you can still configure all stack parameters through a local management session.

> **Note**
> For further information on stacking, refer to the chapter on **Stacking** on page 22.

How Do You Assign an IP Address?

Once you have decided which AT-8326GB stacks on your network need an IP address, you have to access the management software on the stacks and assign the addresses.

One method is to assign the IP configuration information manually. The procedure for this is explained in the next procedure, **Configuring an IP Address** on page 34. Initially assigning an IP address to a stack can only be done through a local management session.

A second method is to activate DHCP on the stack and have the stack automatically download its IP configuration information from a DHCP server on your network. This procedure is explained in **Activating DHCP** on page 41.

Configuring an IP Address

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to an AT-8326GB stack from a local or Telnet management session, as well as how to enable DHCP. If you want the stack to obtain its IP configuration from a DHCP server on your network, go to the procedure **Activating DHCP** on page 41.

To manually set a stack's IP address, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, select **I** for IP Configuration.

   The System IP Configuration Menu is displayed in Figure 4.

```
AT-8326GB Local Management System
 Basic Switch Configuration -> System IP Configuration Menu


  MAC Address:                      00:40:33:FF:01:3B
  IP Address:                       149.35.19.3
  Subnet Mask:                      255.255.0.0
  Default Gateway:                  0.0.0.0
  DHCP Mode:                        Disabled
 --------------------- <COMMAND> --------------------------


  Set [I]P Address
  Set Subnet [M]ask
  Set Default [G]ateway
  Enable/Disable [D]HCP Mode
  [Q]uit to previous menu


  Command>
  Enter the character in square brackets to select option
```

Figure 4 System IP Configuration Menu

3. Change the parameters as desired. To change a parameter, type the bracketed letter in the corresponding command and, when prompted, enter the new information.

   The commands for changing the parameters in the System IP Configuration Menu are described below:

   [I]P Address
   This command specifies an IP address of the stack. You must specify an IP address if you intend to remotely manage the switch using a Web browser, a Telnet utility, or an SNMP management program.

Subnet [M]ask

This command specifies a subnet mask for the stack.

Default [G]ateway Address

This command specifies the default router's IP address. This address is required if you intend to remotely manage the stack from a management station that is separated from the stack by a router.

Enable/Disable [D]HCP Mode

This command allows you to enable and disable DHCP mode. To learn more about DHCP mode, see **Activating DHCP** on page 41.

Configuring System Administration Information

The procedure in this section explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the AT-8326GB stack.

To set a stack's administration information, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, select **A** for System Administration Configuration.

   The System Admin. Configuration Menu is displayed in Figure 4.

```
AT-8326GB Local Management System
Basic Switch Configuration -> System Admin. Configuration
Menu


 Description: AT-8326GB
 Object ID:   1.3.6.1.4.1.207.1.4.52
 Name:
 Location:
 Contact:
-------------------------<COMMAND> --------------------
Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu



 Command>
 Enter the character in square brackets to select option
```

Figure 5 System Admin. Configuration Menu

3. Change the parameters as desired. To change a parameter, type the bracketed letter in the corresponding command and, when prompted, enter the new information.

   The commands for changing the parameters in the System Administration Configuration Menu are described below:

   Set System [N]ame
   This command specifies a name for the stack (for example, Sales). This parameter is optional and may contain up to 50 characters.

Note

It is advised that you assign each stack a name. The names can help you identify the various stacks when you manage them and can help you avoid performing configuration procedures on the wrong stack.

Set System [L]ocation

This command specifies the location of the stack. This parameter is optional and may contain up to 50 characters.

Set System [C]ontact Information

This command allows you to specify the name of the network administrator responsible for managing the stack. This parameter is optional and may contain up to 50 characters.

Setting the User Interface Configuration

The procedure in this section explains how to set the AT-S41 user interface security features, including idle timeouts, how to enable and disable the different management session options, and how to change the login user name and password.

To set a stack's user interface configuration, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, select **U** for User Interface Configuration.

   The User Interface Configuration Menu is displayed in Figure 4.

```
AT-8326GB Local Management System
Basic Switch Configuration->User Interface Configuration Menu


Console UI Idle Timeout:      5 Min.
Telnet UI Idle Timeout:       5 Min.


Telnet Server:        Enabled
SNMP Agent:           Enabled
Web Server:           Enabled
User Name:            manager
---------------------- <COMMAND> ----------------------
Set [C]onsole UI Time Out               Enable/Disable Te[l]net Server
Set [T]elnet UI Time Out                Enable/Disable [S]NMP Agent
Change Administrator User [N]ame        Enable/Disable [W]eb Server
Change Administrator [P]assword         [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 6 User Interface Configuration Menu

3. Change the parameters as desired. To change a parameter, type the bracketed letter in the corresponding command and, when prompted, enter the new information.

   The commands for changing the parameters in the User Interface Configuration Menu are described below:

   Set [C]onsole UI Timeout
   This command causes the management software to automatically end a management session if it does not detect any activity from

the local management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a stack. The default for the console timeout value is 5 minutes.You can set the timeout for between 0 and 60 minutes.

Set [T]elnet UI Timeout
This command causes the management software to automatically end a management session if it does not detect any activity from the remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a stack. The default for the Telnet timeout value is 5 minutes. You can set the timeout for between 0 and 60 minutes.

Change Administrator User [N]ame
This command changes the login name for the switch. The user name can be from 0 to 12 characters in length and can consist of alphanumeric characters (a to z, A to Z, and 0 to 9). The same user name is used for both local and remote management sessions. The default user name is "manager." The user name is case-sensitive.

Change Administrator [P]assword
This command changes the login password for the switch. The password can be from 0 to 12 characters in length and can consist of alphanumeric characters (a to z, A to Z, and 0 to 9). The same password is used for both local and remote management sessions. The default password is "manager." The password is case-sensitive.

⚠ **Caution**
Do not include spaces or special characters, such as asterisks (*) or exclamation points (!) in a user name or password. This is particularly important if you will be managing the switch from a Web browser, since most Web browsers cannot handle special characters in user names or passwords.

Enable/Disable Te[l]net Server
This command allows you to disable the Telnet management feature on the stack, and so prevent individuals from managing the stack remotely using a Telnet session.

Enable/Disable [S]NMP Agent

This command allows you to disable the SNMP management feature on the stack, and so prevent individuals from managing the stack remotely using an SNMP agent.

Enable/Disable [W]eb Server

This command allows you to disable the Web browser management feature on the stack, and so prevent individuals from managing the stack remotely using a Web browser.

Activating DHCP

This application protocol was developed to simplify network management. It is used to automatically assign IP configuration information such as an IP address, subnet mask, and, in some instances, a default gateway address to the devices on your network,.

An AT-8326GB stack supports this protocol and can obtain its IP configuration information from a DHCP server on your network. If you activate this feature, the stack will seek its IP address, subnet mask, and default gateway from a DHCP server residing on your network.

Most DHCP services allow you to specify whether the IP address assignment from the server is to be static or dynamic. If you choose static, the server will always assign the same IP address to the stack when the stack is reset or powered on. If you choose dynamic, the server will assign an unused IP address from its list of potential IP addresses each time the stack is reset or powered on.

Note
The DHCP option is disabled by default on the switch.

To activate or deactivate the DHCP protocols on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **I** to select System IP Configuration. (See the System IP Configuration Menu in Figure 4 on page 34.)

3. Type **D** to select DHCP.

   The following prompt is displayed:

   ```
   Enable or Disable DHCP mode (E/D)> _
   ```

4. Type **E** to enable DHCP services on the switch or **D** to disable the services and press Return. DHCP is disabled by default on the switch.

5. Reboot the switch using either the management software or by powering on the stack.

41

Configuring SNMP Community Strings and Trap IP Addresses

To configure the SNMP community strings for the stack and to assign up to four IP addresses of management stations to receive traps from the stack, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **N** to select SNMP Configuration.

   The SNMP Configuration Menu is displayed in Figure 7.

```
AT-8326GB Local Management System
Basic Switch Configuration -> SNMP Configuration Menu

SNMP Read Community:  public
SNMP Write Community: private
Trap Authentication:  Enabled

SNMP Trap Receivers:
 No.   Status        IP Address            Community
 ----  --------      ---------------       ------------------
 1     Deleted       <empty>               <empty>
 2     Deleted       <empty>               <empty>
 3     Deleted       <empty>               <empty>
 4     Deleted       <empty>               <empty>
------------------------------ <COMMAND> ---------------
Set SNMP [R]ead Community            [A]dd SNMP Trap Receiver
Set SNMP [W]rite Community           [D]elete SNMP Trap Receiver
[M]odify SNMP Trap Receiver          [E]nable/Disable Authentication Trap
Enable/Disable SNMP [T]rap Receiver  [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 7 SNMP Configuration Menu

3. Adjust the parameters as desired. To change a parameter, type the bracketed letter in the corresponding command and, when prompted, enter the new information.

   The commands are described below:

   Set SNMP [R]ead Community
   This command specifies the SNMP community name. The maximum length for a read community name is 20 characters.

   Set SNMP [W]rite Community
   This command specifies the SNMP write community. The parameter can be set to private or public.

   [M]odify SNMP Trap Receiver
   This command specifies trap receiver information. This allows you to modify the IP address and community name of a trap receiver.

Enable/Disable SNMP [T]rap Receiver

This command specifies the status of a trap receiver. This parameter can be set to E for enable or D to disable.

[A]dd SNMP Trap Receiver

This command allows you to add an SNMP trap receiver. The range is set of 1 to 4.

[D]elete SNMP Trap Receiver

This command deletes a specified SNMP trap receiver.

[E]nable/Disable Authentication Trap

This command specifies a community's trap authentication. This parameter can be set to E for enable or D to disable.

Changes to the SNMP parameters are immediately activated on the stack.

Resetting the Management Software Default Values

The procedure in this section returns all management parameters in a stack to their default values. This procedure also deletes any VLANs that you have created in the stack.

> **Note**
> The management software default values can be found in **Appendix A** on page 235.

To return the management software to its default settings, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.

2. From the Switch Tools Configuration Menu, type **R** to select System Reboot.

   The System Reboot Menu is displayed in Figure 8.

```
AT-8326GB Local Management System
Main Menu -> System Reboot Menu

Reboot Status:          Stop
Reboot Type:            Normal



------------------------ <COMMAND> --------------------

Set Reboot [O]ption
Start [R]eboot Process
[Q]uit to previous menu


Command>
 Enter the character in square brackets to select option
```

Figure 8 System Reboot Menu

3. From the System Reboot Menu, type **O** and then select Factory Default.

4. Type **R** to Start Reboot Process.

   The following prompt is displayed:

   Are you sure you want to reboot the system (Y/N) ->

5. Type **Y** for yes or **N** for no.

   If you type **Y** for yes, the stack settings are reset to the factory default values.

Rebooting a Switch

To reboot a switch, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.

2. From the Switch Tools Configuration Menu, type **R** to select System Reboot.

   The System Reboot Menu is displayed in Figure 9.

```
AT-8326GB Local Management System
Main Menu -> System Reboot Menu

Reboot Status:          Stop
Reboot Type:            Normal




----------------------- <COMMAND> --------------------

Set Reboot [O]ption
Start [R]eboot Process
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Figure 9 System Reboot Menu

3. Type **O** and then set a Reboot Option: Factory Default, Factory Default Except IP, or Normal. The default reboot option is Normal. The three Reboot options are described below:

   Normal
   Resets the switch and saves your configuration changes.

   Factory Default
   Resets the switch to its factory default settings. If you select this option, all of your configuration changes will be erased.

   Factory Default Except IP
   Resets the switch to its factory default settings except for the IP address you assigned to the switch.

4. Type **R** to Start Reboot Process.

   The switch immediately reloads its operating system. This process will take a few minutes.

   ⚠ **Caution**
   The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Viewing the AT-S41 Switch Information

The procedure in this section explains how to display general information about the stack, including:

❑ Administration information

❑ Bootcode version number

❑ Hardware information

❑ System information, including MAC address

To display the stack information, perform the following procedure:

1. From the Main Menu, type **G** to select General Information.

The General Information Menu is displayed in Figure 10.

```
AT-8326GB Local Management System
Main Menu -> General Information

 System up for:   01hr(s), 38min(s), 58sec(s)

Boot Code Version/Date:              1.00B / Dec 22 2001 16:23:12
Runtime Code Version/Date:           1.00F / Jan 15 2002 19:40:11
Hardware Information
  Version:             1.00         DRAM Size:           8MB
  Fixed Baud Rate:   9600bps        Flash Size:          4MB
Administration Information
  Switch Name:
  Switch Location:
  Switch Contact:
System Address Information
  MAC Address:       00:40:33:FF:01:3B
  IP Address:        149.35.19.192
  Subnet Mask:       255.255.0.0
  Gateway:           0.0.0.0
Automatic Network Features
  DHCP Mode:         Disabled


 Press any key to continue...
```

Figure 10 General Information Menu

There are no configuration options on this page; it is for informational purposes only.

Ping Execution

To configure the ping execution settings on the switch, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.

2. From the Switch Tools Configuration Menu, type **P** to select Ping Execution.

   The Ping Execution Menu is displayed in Figure 11.

```
AT-8326GB Local Management System
Main Menu -> Ping Execution

Target IP Address:     0.0.0.0
Number of Requests:    10
Timeout Value (sec):   3
=============== Result ===============




-------------------------------- <COMMAND> ------------------
Set Target [I]P Address                 [E]xecute Ping
Set [N]umber of Requests                [S]top Ping
Set [T]imeout Value                     [Q]uit to previous menu
Command> _
Enter the character in square brackets to select option...
```

Figure 11 Ping Execution Menu

3. Adjust the parameters as desired. To change a value, type its corresponding bracketed letter and, when prompted, enter the new value. The parameters are described below.

   Set Target [I]P Address
   This command specifies the IP address of the end node you are pinging.

   Set [N]umber of Requests
   Number of ping attempts the switch should make before it stops pinging if it does not receive a response. The default number of ping requests is 10.

   Set [T]imeout Value
   The length of time for which the switch will continue to send pings if it does not receive a response. The default timeout setting is 3 seconds.

4. Select one of the two ping test options by typing the corresponding bracketed letter: Execute Ping or Stop Ping.

[E]xecute Ping
Starts the ping process and displays ping test results. Also allows you to clean out the ping test configuration cache by typing **C** for Clean Ping Data. When you clean out the ping data, you will remove the ping test results from view.

[S]top Ping
Ends the ping process and displays ping test results gathered before the pinging was stopped.

The Ping Execution Menu with ping test results is displayed in Figure 12.

```
AT-8326GB Local Management System
Main Menu -> Ping Execution

Target IP Address:      0.0.0.0
Number of Requests:     10
Timeout Value (sec):    3
=============== Result ===============

   No. 1                      60 ms
   No. 2                     100 ms
   No. 3                     100 ms
   No. 4                     100 ms




------------------------------ <COMMAND> -----------------
Set Target [I]P Address                [E]xecute Ping
Set [N]umber of Requests               [S]top Ping
Set [T]imeout Value                    [Q]uit to previous menu
Command> _
Enter the character in square brackets to select option...
```

Figure 12 Ping Results

The number in the results display designates the number of the ping attempt. For example, No. 1 represents the first ping attempt.

The milliseconds value represent the time taken for the ping attempt. For example, the first ping test was completed in 60 milliseconds.

Bootstrap Configuration

The bootstrap feature allows you to download new software and configuration settings when you boot up the switch.

To configure the bootstrap settings on the switch, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.

2. From the Switch Tools Configuration Menu, type **B** to select Bootstrap Configuration.

   The Bootstrap Configuration Menu is displayed in Figure 13.

```
AT-8326GB Local Management System
Switch Tools Configuration -> BootStrap Configuration Menu


Boot Load Mode :     Local
Boot Mode :          TFTP
File Type :          IMAGE


----------------------- <COMMAND> ----------------------
Set [B]oot Load Mode
Set Boot [M]ode
Set [F]ile Type
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Figure 13 Bootstrap Configuration Menu

3. Adjust the parameters as desired. To change a parameter, type the bracketed letter in the corresponding command and, when prompted, enter the new information. The commands are described below:

   Set [B]oot Load Mode
   Allows the user to determine how the stack should boot up. There are two boot load options: local and remote.

   Local
   If you choose the local boot load mode, the stack boots using the management software that is saved in the stack's memory. This is the default boot load mode. If you are going to use the local boot load mode, you do not need to configure any of the other parameters on the Bootstrap Configuration Menu.

Remote
If you choose the remote boot load mode, the stack downloads software from a TFTP server and boots using the newly downloaded management software.

Set Boot [M]ode
If you are using the remote boot load mode, you need to specify how the stack should download the new management software. There are two boot mode options: DHCP and TFTP.

When downloading the image:

DHCP
The stack will get an IP address, TFTP server IP address, and a filename from the DHCP server. The stack will then use this information to connect to the TFTP server and download the filename it received and boot the downloaded file as the image. If this file does not exist, it uses the file which it last booted off of successfully.

TFTP
The stack will use the IP address it had prior to reboot to download the image file from the server through TFTP using the information configured in "Switch Tools -> Software Upgrade -> TFTP Software Upgrade".

When downloading the configuration:

The stack will get the TFTP server and file information from what is configured in the menu; "Switch Tools -> Configuration File Upload/Download -> TFTP Configuration File Upload/Download". This information cannot be learned from the DHCP server.

DHCP
The stack will get an IP address from a DHCP server which will then be used to TFTP the configuration file from the server. If the configuration file has a static IP address assigned in it, then the IP address would be overwritten after the configuration file has been loaded.

TFTP
The stack will use the IP address it had prior to reboot to download the configuration file from the server through TFTP.

Set [F]ile Type

If you selected the remote boot load mode, you can choose what kind of files the switch will download while it is booting up. There are three file type options:

Image

An image file is the management software for the stack.

Configuration

A configuration file is a file that contains all of the existing configurations and settings for a stack. You can upload the configuration file and modify the stack settings and then download the configuration file back to the stack or onto multiple stacks that you want to have the same configurations. The stack(s) will then update their configuration(s) based on the settings in the configuration file.

Image and Configuration

This option allows you to download both the management software and the configuration file.

Chapter 5
Port Parameters

This chapter contains procedures for viewing and changing the parameter settings for the individual ports on a stack.

This chapter contains the following procedures:

❑ **Configuring Port Parameters** on page 53

❑ **Configuring Gigabit Port Type** on page 56

Configuring Port Parameters

To configure the parameter settings for a port on the stack, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **P** to select Port Configuration.

   The Port Configuration Menu is displayed in Figure 14.

```
AT-8326GB Local Management System
 Basic Switch Configuration -> Port Configuration Menu
 Stack ID: 1
 Port  Trunk      Type      Link     Status          Mode           Flow Ctrl
 ----  -----    --------    ----   ----------    ---------------     ---------
   1    ---     10/100TX    Down    Enabled      Auto                Enabled
   2    ---     10/100TX    Down    Enabled      Auto                Enabled
   3    ---     10/100TX    Down    Enabled      Auto                Enabled
   4    ---     10/100TX    Down    Enabled      Auto                Enabled
   5    ---     10/100TX    Down    Enabled      Auto                Enabled
   6    ---     10/100TX    Down    Enabled      Auto                Enabled
   7    ---     10/100TX    Down    Enabled      Auto                Enabled
   8    ---     10/100TX    Down    Enabled      Auto                Enabled
   9    ---     10/100TX    Down    Enabled      Auto                Enabled
  10    ---     10/100TX    Down    Enabled      Auto                Enabled
  11    ---     10/100TX    Down    Enabled      Auto                Enabled
  12    ---     10/100TX    Down    Enabled      Auto                Enabled
 ------------------------------ <COMMAND> -------------------------
[N]ext Page                 Set [S]tatus          Set [F]low control
[P]revious Page             Set [M]ode            Select Stack [I]D
[Q]uit to previous menu

 Command> _
 Enter the character in square brackets to select option
```

Figure 14 Port Configuration Menu

Note
By default, the management software initially displays the ports on the master switch. To view the ports on another switch in a stack, use the Select Stack ID command.

The columns on the Port Configuration Menu are described below.

Port
The port number.

Trunk
The trunk group number. A number in this column indicates that the port is a member of a trunk.

Type
The port types. Ports 1-24 are 10/100Base-TX and can operate at 10/100 Mbps. Ports 25-26 are 1000Base-TX and can operate at 10/100/1000 Mbps.

Link
The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Status
The current operating status of the port.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. Possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for all of the ports on the switch.

Disabled - The port has been manually disabled.

Mode
The current operating settings of the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode. This is the default setting for all of the ports.

10-HDx - 10 Mbps in half-duplex mode

100-HDx - 100 Mbps in half-duplex mode

10-FDx - 10 Mbps in full-duplex mode

100-FDX - 100 Mbps in full-duplex mode

1000-FDx - 1000 Mbps in full-duplex mode

1000-HDx - 1000 Mbps in half-duplex mode

The 1000 Mbps settings can only be applied on Ports 25-26.

Flow Ctrl
The current flow control setting on the port. A stack uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Possible values are:

Enabled - The port is allowed to use flow control. This is the default setting for all of the ports on the stack.

Disabled - The port is not configured to use flow control.

Port status, mode, and flow control can be configured from the Port Configuration Menu.

3. To configure port status, type **S** to select the Set Status option.

The following prompt is displayed:

```
Set Status-> Enter port number>
Port number is in range of 1 to 26, 0 to set all
ports.(Except giga port)
```

Enter a port number. Press Enter and type **E** for Enable or **D** for Disable. The new port status is activated immediately and displayed in the Port Configuration Menu.

4. To configure port mode, type **M** to select the Set Mode option.

The following prompt is displayed:

```
Set Mode-> Enter port number>
Port number is in range of 1 to 26, 0 to set all
ports.(Except giga port)
```

Enter a port number.

The following prompt is displayed:

```
Enter new mode for port 3 (a/h/H/f/F)>
a:Auto; h:10-HDx; H:100-HDx; f:10-FDx; F:100-FDx
(case sensitive)
```

Enter the new operating mode for the port and press Enter. The new port mode is activated immediately and displayed in the Port Configuration Menu.

5. To configure flow control, type **F** to select the Set Flow Control option.

The following prompt is displayed:

```
Set flow control-> Enter port number>
Port number is in range of 1 to 26, 0 to set all
ports.(Except giga port)
```

Enter a port number. Press Enter and type **E** for Enable or **D** for Disable. The new flow control setting is activated immediately and displayed in the Port Configuration Menu.

Configuring Gigabit Port Type

Ports 25 and 26 can operate as either GBIC ports or as 10/100/1000 Mbps twisted pair ports. The default port type setting is twisted pair. In order to change the use of these ports from one type to another, the port type must be changed in the AT-S41 management software.

To configure the gigabit port type, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **G** for Select Giga Port Type.

   The Select Giga Port Type Menu is displayed in Figure 15.

```
AT-8326GB Local Management System
 Basic Switch Configuration -> Select Giga Port Type Menu
 Stack ID: 1
 Giga Port NO.        Port Type
 -------------     ---------------
      25                  TP
      26                  TP


 ------------------------------- <COMMAND> ------
 [S]et giga port type
 Select Stack [I]D
 [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Figure 15 Select Giga Port Type Menu

3. Type **I** to choose Select Stack ID and enter the ID number of the switch in the stack whose gigabit port type you want to change. (You can skip this step if you are changing the gigabit port type on the master switch, which is selected by default.)

4. From the Select Giga Port Type Menu, type **S** to select Set giga port type.

   The following prompt is displayed:

   Enter giga port number >

   Port number is in range of 25 to 26

5. Enter the number of the gigabit port whose type you want to change.

   The following prompt is displayed:

   Set giga port type for port 25 (G/T)>

   G for GBIC; T for TP

6. Enter your selection. Type **G** to make the port a GBIC port or **T** to make the port a twisted pair port.

    The port type change is displayed immediately in the Select Giga Port Type Menu.

    Note
    When a gigabit port has been set to operate as a GBIC port instead of a twisted pair port, the port mode cannot be changed in the Port Configuration Menu. The GBIC port is in a forced 1000 Mbps full-duplex mode.

Chapter 6

Port Security

This chapter contains the procedures for setting port security. The sections in this chapter include:

❑ **Port Security Overview** on page 59

❑ **Configuring Port Security** on page 61

❑ **Setting a Threshold** on page 63

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control the number of MAC addresses learned on the ports, and so control the number of network devices that can forward frames through the stack.

An AT-8326GB stack has three levels of port security: Normal (default), Limited, and Secure. You can set the security level on a per port basis. The security levels are briefly described below.

Normal
This is the default port security setting and indicates that port security is disabled on the port. The switch learns and adds addresses to its dynamic MAC address table as it receives frames on the port.

Limited
You use this security level to specify the maximum number of dynamic MAC addresses a port can learn. Once a port has learned its maximum limit of MAC addresses, it will discard any frames that it receives with a source MAC address not already learned and stored in the MAC address table. When a port is set to Limited security, any MAC addresses it learned prior to being set to Limited security are retained in the MAC address table and included in the threshold count. The threshold levels apply only to dynamic MAC addresses. You can continue to add static MAC addresses to a port operating under Limited security.

This security level can prevent unauthorized individuals from connecting to your network and gaining access to network resources. For example, if an AT-8326GB port is connected to an Ethernet hub with four workstations attached, you can configure the switch port to learn only four MAC addresses. Once those addresses are learned, any one else attempting to connect to the network through the Ethernet hub would be denied access.

The MAC aging time for the port remains active under this security level. Inactive dynamic MAC addresses learned on the port are aged out from the MAC address table.

Secure
This security level causes the port to immediately stop learning new dynamic MAC addresses. The port forwards frames based on the dynamic MAC addresses that it has already learned and any static MAC addresses that the network administrator enters.

The MAC aging time is disabled under this security level. The dynamic MAC addresses learned on a port and added to the MAC address table remain in the table and are never purged, even when the end nodes are inactive.

Configuring Port Security

To set a port's security level, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **P** to select Port Security Configuration.

   The Port Security Configuration Menu is displayed in Figure 16.

```
AT-8326GB Local Management System
 Advanced Switch Configuration -> Port Security Configuration Menu
 Stack ID: 1
 Port    Secure Level      Threshold         Intrusion Detection Status
 ----    --------------    -----------       ------------------------------
    1         Normal          -----            -----
    2         Normal          -----            -----
    3         Normal          -----            -----
    4         Normal          -----            -----
    5         Normal          -----            -----
    6         Normal          -----            -----
    7         Normal          -----            -----
    8         Normal          -----            -----
    9         Normal          -----            -----
   10         Normal          -----            -----
   11         Normal          -----            -----
   12         Normal          -----            -----
 -------------------------- <COMMAND> ----------------------------
 [N]ext Page               [S]et Secure Level      Set [T]hreshold
 [P]revious Page        Select Stack [I]D      Set Intrusion[D]etection
 [Q]uit to previous menu

 Command> _
 Enter the character in square brackets to select option
```

Figure 16 Port Security Configuration Menu

3. Type **I** to choose Select Stack ID and enter the ID number of the switch in the stack where you want to configure port security. (You can skip this step to configure port security on the master switch, since the master switch is selected by default.)

4. Type **S** to select Set Secure Level.

5. At the prompt, enter the port number whose security you want to set. Press Enter.

   The following prompt is displayed:

   ```
   Limited or Secure port N <L/S/N>>
   L for Limited; S for Secure; N for Normal
   ```

6. Select the desired security level.

❑ To disable security on the port, type **N** to select Normal mode. This is the default security setting. A port operating in Normal mode does not have any restrictions on the number of MAC addresses it can learn. The port continues to learn addresses until it reaches the 254 address maximum of MAC address table.

❑ To specify a maximum number of dynamic MAC addresses each port can learn, type **L** to select Limited mode. To specify the limits, refer to the next procedure.

❑ To stop the port from learning new dynamic MAC addresses and have it forward frames based only on static MAC addresses and on those dynamic addresses that it has already learned, type **S** to select Secure mode.

Note
Only one security level can be active on a port at a time.

A change to the security level is immediately activated on the port and the new setting is displayed in the Port Security Configuration Menu.

Setting a Threshold

The Limited security mode lets you set a maximum number of dynamic MAC addresses a port on a switch can learn. Once the maximum number of MAC addresses have been learned by a port, frames with new source MAC addresses are discarded and are not forwarded by the port.

Static MAC addresses are not included in the count of the maximum MAC addresses a port can learn. You can continue to add static MAC addresses even after a port has learned its maximum number of dynamic MAC addresses.

To configure Limited security mode for a port, perform the following procedure:

1. Perform the procedure **Configuring Port Security** on page 61 to configure the port with Limited security.

2. Type **T** to select Set Threshold.

   The following prompt is displayed:

   ```
   Set threshold->Enter port number >
   Port number is in range of 1 to 26
   ```

3. Enter the number of the port you want to configure. Press Return.

   The following prompt is displayed:

   ```
   Set threshold->Enter port number >
   Threshold is in range of 1 to 170
   ```

4. Enter the number of dynamic MAC addresses you want the port to be able to learn. This will be the new threshold for the port and will be displayed immediately in the Port Security Configuration Menu.

   Note
   Threshold is not supported in Normal and Secure modes.

Setting Intrusion Detection

The Limited and Secure security modes let you determine how the switch responds when it receives MAC addresses in excess of its threshold.

1. Perform the procedure **Configuring Port Security** on page 61.

2. Type **D** to select Set Intrusion Detection.

   The following prompt is displayed:

   ```
   Set intrusion detection status->Enter port number >
   Port number is in range of 1 to 12
   ```

3. Enter the number of the port to configure. Press Enter.

   The Intrusion Detection Status Menu is displayed in Figure 17

```
AT-8326GB Local Management System
Select item number for intrusion detection status

Advanced Switch Configuration -> Intrusion Detection Status Menu


Item                Description
------   ------------------------------------
1                 No action
2                 Disable the port only
3                 Notify with trap only
4                 Notify with trap and disable the port


Set intrusion detection status->Enter item number >
Select item number for intrusion detection status
```

Figure 17 Intrusion Detection Status Menu

4. Type the number associated with the desired setting for Intrusion Detection Status. The following parameters are available:

   1 - No action
   2 - Disable the port only
   3 - Notify with trap only
   4 - Notify with trap and disable the port

   A change to detection status is immediately activated on the port.

Chapter 7
Port Trunking

This chapter contains the procedures for configuring port trunks. Sections in the chapter include:

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between an AT-8326GB switch and another network device, such as a server, router, workstation, or another Ethernet switch.

A port trunk can consist of up to four 10/100 Mbps ports or two 10/100/1000 Mbps ports that have been grouped together to function as one logical path to an end node. A port trunk increases the bandwidth between a stack and an end node and can be useful in situations where a single physical data link between a stack and an end node is insufficient to handle the traffic load.

The port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

Observe the following guidelines when creating a port trunk:

❑ Each AT-8326GB switch in a stack can support up to four port trunks at a time.

❑ A port trunk can consist of up to four 10/100 Mbps ports or two 10/100/1000 Mbps ports.

❑ The ports of a port trunk must be of the same type. For example, they can be all twisted pair ports or all fiber optic ports.

❑ The ports of a port trunk must reside on the same switch in a stack.

❑ The ports on the switch are divided into four port trunk groups. The port members of each port group are shown below:

> Port Group 1: ports 1-8
> Port Group 2: ports 9-16
> Port Group 3: ports 17-24
> Port Group 4: ports 25-26

❑ Trunk port members must be within the same port trunk group.

❑ Slave switches in a switch stack only have the first three port trunk groups. The 10/100/1000 Mbps ports on slave switches cannot belong to port trunks.

❑ The duplex mode, speed, and flow control settings must be the same for all the ports in a trunk.

❑ When cabling a trunk, the order of the connections should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

For example, assume that you are connecting a trunk between two AT-8326GB switches. On the first AT-8326GB switch you had chosen ports 12, 13, 14, 15 for the trunk. On the second AT-8326GB switch you had chosen ports 21, 22, 23, and 24. To maintain the order of the port connections, you would connect port 12 on the first AT-8326GB switch to port 21 on the second AT-8326GB, port 13 to port 22, and so on.

❑ The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.

❑ You can create a port trunk of optional GBIC modules installed in the Port 25 and Port 26 slots of an AT-8326GB switch.

Figure 18 shows an example of a port trunk between an AT-8326GB switch and a network server. The server is connected to the switch with four data links. The links are connected to ports 1 through 4 on the switch.
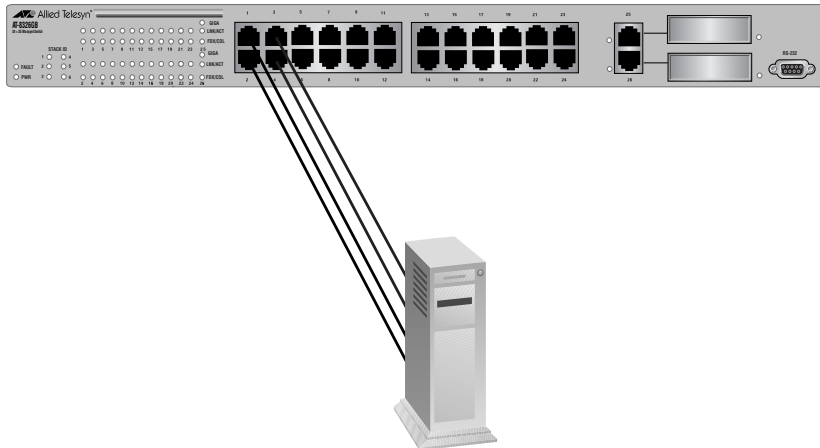

Figure 18 Port Trunk Example 1

You can also use port trunks to increase the bandwidth between switches. The example in Figure 19 shows a port trunk of four data links between two AT-8326GB switches.
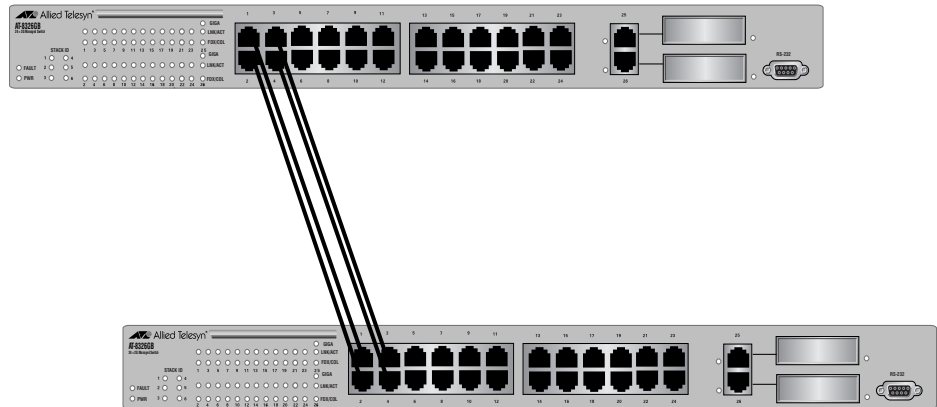

Figure 19 Port Trunk Example 2

Creating a Port Trunk

This section contains the procedure for creating a port trunk on a stack. Be sure to review the guidelines in the **Port Trunking Overview** on page 66 before performing this procedure.

⚠ **Caution**

Do not connect the cables to the trunk ports on the stack until after you have configured the trunk with the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note

Before adding member ports to a port trunk, examine the parameter settings of the ports that will make up the trunk. Check to be sure that the settings, such as speed and duplex mode, are the same for all the ports of the trunk. You should also check to be sure that the ports are members of the same VLAN.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **T** to select Trunk Configuration.

   The Trunk Configuration Menu is displayed in Figure 20.

```
AT-8326GB Local Management System
 Advanced Switch Configuration -> Trunk Configuration Menu
 Stack ID: 1
 Group    Status    Port Members
 -----    --------  ------------------------------
   1      Disabled   1,  4
   2      Disabled
   3      Disabled
   4      Disabled

 Note: The trunk port members must be within the same port group.
       The port members of each port group are shown below.
       Port group 1: port 1-8  , group 3: port 17-24
       Port group 2: port 9-16 , group 4: port 25-26


 ------------------------------- <COMMAND> --------------------
 [A]dd Trunk Member                      [S]et Trunk status
 [R]emove Trunk Member                   Select Stack [I]D
 [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 20 Trunk Configuration Menu

3. Type **I** to choose Select Stack ID and enter the ID number of the switch in the stack where you want to create the port trunk. (You can skip this step to create the port trunk on the master switch, since the master switch is selected by default.)

4. From the Trunk Configuration Menu, type **A** to select Add Trunk Member.

    The following prompt is displayed:

    ```
    Enter trunk group number->
    ```

5. Enter the port trunk group containing the ports you want to use in the trunk.

    The following prompt is displayed:

    ```
    Enter port members (up to 4 ports) for trunk 1>
    ```

6. Enter the ports that will constitute the port trunk. You can specify the ports individually (e.g., 1,2,3,4) or as a range (e.g., 7-10). Press Enter.

    The port trunk members will appear in the Trunk Configuration Menu.

7. To set trunk status, type **S** to select Set Trunk Status.

    The following prompt is displayed:

    ```
    Enter trunk group number->
    ```

8. Enter the number of the port trunk group that you want to enable or disable.

    The following prompt is displayed:

    ```
    Enable or Disable trunk group 1 (E/D)>
    ```

9. Type **E** to enable the port trunk group or type **D** to disable the port trunk group.

10. Configure the ports on the remote end node for port trunking. Refer to the instructions included with the node for directions on how to create a port trunk.

11. Connect the cables to the ports of the trunk on the switch.

    The port trunk is ready for network operations.

AT-S41 User's Guide

Deleting a Port Trunk

> ⚠ **Caution**
> Disconnect the cables from the port trunk on the switch before performing the following procedure. Removing a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **T** to select Trunk Configuration.

    The Port Trunking menu in Figure 20 on page 69 is displayed.

3. Type **I** to choose Select Stack ID and enter the ID number of the switch in the stack where you want to delete the port trunk. (You can skip this step to delete a port trunk on the master switch, since the master switch is selected by default.)

4. From the Trunk Configuration Menu, type **R** to select Remove Trunk Member.

    The following prompt is displayed:

    ```
    Enter trunk group number->
    ```

5. Enter the port trunk group for the port(s) you want to remove from the trunk.

    The following prompt is displayed:

    ```
    Enter port members (up to 4 ports) for trunk 1>
    ```

6. Enter the ports of the port trunk that you want to delete. You can specify the ports individually (e.g., 1,2,3,4) or as a range (e.g., 7-10). Press Enter.

    > **Note**
    > You must remove all port members of a port trunk from their trunk group in order to fully delete the port trunk. You can also disable the trunk group, but this will not remove the port members from the port trunk and may cause data loops in your network.

7. The port trunk members are deleted from the port trunk group. The Trunk Configuration Menu is updated immediately.

71

Setting Port Trunk Status

To enable or disable a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **T** to select the Trunk Configuration Menu.

3. Type **I** to choose Select Stack ID and enter the ID number of the switch in the stack containing the port trunk you want to enable or disable.

4. From the Trunk Configuration Menu, type **S** to select Set Trunk Status.

   The following prompt is displayed:

   ```
   Enter trunk group number->
   ```

   Enter the number of the port trunk group that you want to enable or disable.

   The following prompt is displayed:

   ```
   Enable or Disable trunk group 1 (E/D)>
   ```

5. Type **E** to enable the port trunk group or type **D** to disable the port trunk group.

Chapter 8

Port Monitoring

This chapter contains the procedures for configuring port monitoring. Sections in the chapter include:

Port Monitoring Overview

The port monitoring feature allows you to unobtrusively monitor the traffic being received and transmitted on a port on the switch by having the traffic copied to another switch port. You can connect a network analyzer to the port functioning as the monitoring port to monitor the traffic without impacting network performance or speed.

Observe the following guidelines when configuring port monitoring:

❑ You can monitor only one port on a switch at a time.

❑ You can monitor only one port in a switch stack at a time.

❑ The port to be monitored and the monitoring port must be located on the same switch.

Enabling Port Monitoring

To enable port monitoring, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **M** to select Port Monitoring Configuration.

   The Port Monitoring Configuration Menu is displayed in Figure 21.

```
 AT-8326GB Local Management System
 Advanced Switch Configuration -> Port Monitoring Configuration Menu

Stack ID Monitoring Port     Stack ID     Monitored Port Status
--------- --------------     ----------   --------------   -----------
     1         3                 1                8         Enabled


 ----------------------------- <COMMAND> ------------------------
 [S]et Monitoring Port
 Set [M]onitored Port
 [E]nable/Disable Port Monitoring
 [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 21 Port Monitoring Configuration Menu

3. Type **S** to select Set Monitoring Port.

   The following prompt is displayed:

   ```
   Set monitoring port->Enter port number>
   ```

4. Enter the number of the port you want to function as the monitoring port. The default monitoring port is Port 2. You can specify only one monitor port. Press Enter.

   Note
   When you have created a switch stack, you will be prompted to enter the Stack ID before entering the port number.

   The port number you have just entered is displayed under the Monitoring Port heading on the Port Monitoring Configuration Menu.

5. Type **M** to select Set Monitored Port.

   The following prompt is displayed:

   ```
   Set monitored port->Enter port number>
   ```

6. Enter the number of the port whose traffic is to be monitored. The default monitored port is Port 1. You can specify only one port to be monitored. Press Enter.

   The port number you have just entered is displayed under the Monitored Port heading on the Port Monitoring Configuration Menu.

7. Type **E** to select Enable/Disable Port Monitoring.

   The following prompt is displayed.

   ```
   Enable or Disable monitoring (E/D)>
   ```

8. Type **E** to enable port monitoring. The status will change to Enabled on the Port Monitoring Configuration Menu.

   Port monitoring is now functional.

Modifying Port Monitoring

To modify the port monitoring configuration, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **M** to select Port Monitoring Configuration.

   The Port Monitoring Configuration Menu is displayed, as shown in in Figure 21.

3. To change the monitoring port, type **S** to select Set Monitoring Port.

   The following prompt is displayed:

   ```
   Set monitoring port->Enter port number>
   ```

4. Enter the number of the port you want to function as the monitoring port. You can specify only one monitor port. Press Enter.

   The port number you have just entered is displayed under the Monitoring Port heading on the Port Monitoring Configuration Menu instead of the previous monitoring port's number.

5. To change the monitored port, type **M** to select Set Monitored Port.

   The following prompt is displayed:

   ```
   Set monitored port->Enter port number>
   ```

6. Enter the number of the port whose traffic is to be monitored. You can specify only one port to be monitored. Press Enter.

   The port number you have just entered is displayed under the Monitored Port heading on the Port Monitoring Configuration Menu instead of the previously monitored port's number.

7. Type **E** to select Enable/Disable Port Monitoring.

   The following prompt is displayed.

   ```
   Enable or Disable monitoring (E/D)>
   ```

8. Type **E** to enable port monitoring. The status will change to Enabled on the Port Monitoring Configuration Menu.

   Note
   If you change either the monitoring port or the monitored port, the port monitoring function will reset itself to Disabled. You must Enable port monitoring each time you make a change to the port monitoring configuration.

AT-S41 User's Guide

Disabling Port Monitoring

To disable port monitoring, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **M** to select Port Monitoring Configuration.

   The Port Mirroring Menu is displayed, as shown in Figure 21 on page 75.

3. Type **E** to select Enable/Disable Port Monitoring.

   The following prompt is displayed:

   ```
   Enable or Disable monitoring (E/D)>
   ```

4. Type **D** for Disable.

5. The port monitoring status will change to Disabled on the Port Monitoring Configuration Menu.

   The port monitoring on the switch is disabled. The port that was functioning as the monitoring port is now available for normal network operations.

Chapter 9

Spanning Tree Protocol

This chapter provides introductory information on the Spanning Tree Protocol (STP) and explains how to adjust the STP bridge and port parameters. The sections in this chapter include:

❑ **STP Overview** on page 80

❑ **Configuring a Bridge's STP Settings** on page 84

❑ **Configuring STP Port Settings** on page 87

Note
For detailed information on the Spanning Tree Protocol, refer to Section 4 of IEEE Std 802.1D, ISO/IEC 10038: 1993.

STP Overview

The AT-8326GB Fast Ethernet switch supports the Spanning Tree Protocol, as specified in the IEEE 802.1D standard. STP can be an important part of large networks where loops, either planned or unplanned, exist in the network topology.

A loop exists when two or more nodes on your network can transmit data to each other over more than one data link. A network loop can pose a danger to network performance and operability. Data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and often significantly reduce network performance.

STP prevents data loops from forming in your network by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, STP places the extra paths in a standby or blocking mode, leaving only one main active path.

The redundant paths can be activated by STP if the main path goes down. So not only does STP guard against multiple links between end nodes, but it can also activate backup redundant paths in case a main link fails.

Selecting a Root Bridge

The first task that bridges perform when STP is activated on a network is the selection of a root bridge. The root bridge is used by the other bridges to determine if there are redundant paths in the network. The root bridge also distributes network topology information to the other network bridges.

A root bridge is selected by a combination of a bridge's priority number, also referred to as the bridge identifier, and sometimes its MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number is adjustable on the AT-8326GB switch. By adjusting the value, you can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You should probably also consider which bridge should function as a backup in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

Finding and Resolving Redundant Paths

Once the root bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and a root bridge, the bridge is referred to as the designated bridge and the port through which the bridge is communicating with the root bridge is referred to as the designated port.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an evaluation of port costs. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

The port costs for the ports on the AT-8326GB Fast Ethernet switch are adjustable through the management software. Below are standard default port cost values.

Table 1 Standard Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

The port costs for the ports on the AT-8326GB Fast Ethernet switch are adjustable through the management software. Below are the default port cost values.

Table 2 AT-8326GB Port Costs

Port Speed	Port Cost
10 Mbps	19
100 Mbps	19
1000 Mbps	4

The cost of a path is cumulative; the final cost of a path is the value of all ports between a bridge and the root bridge.

If two paths have the same port cost, the preferred path is selected through port priority. This is a value that you can adjust on a per port basis on the switch.

Handling Topology Changes

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. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the forwarding delay value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the AT-8326GB Fast Ethernet switch through the management software. The appropriate value for this parameter will depend on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Communicating Between Bridges

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought online, it will issue a BPDU in order to determine whether a root bridge has already been selected on the network and, if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge will periodically transmit a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the Hello Time. This is a value that you can set on the AT-8326GB Fast Ethernet switches. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8326GB switch is selected as the root bridge of a spanning tree domain, it will transmit a BPDU every 2 seconds.

Configuring a Bridge's STP Settings

This section contains the procedure for configuring a bridge's STP settings.

⚠ **Caution**

STP on a bridge is disabled by default. If you enable STP, the bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **S** to select Spanning Tree Configuration.

   The Spanning Tree Configuration Menu is displayed in Figure 22.

```
AT-8326GB Local Management System
Basic Switch Configuration -> Spanning Tree Configuration Menu

 STP Status:         Disabled

 Root Port:          N/A
 Root Path Cost:     N/A

 Designated Root: N/A      Bridge ID:             8000 004033FF013B
 Hello Time:      N/A      Bridge Hello Time:    2     Sec.
 Maximum Age:     N/A      Bridge Maximum Age:   20    Sec.
 Forward Delay:   N/A      Bridge Forward Delay: 15    Sec.


 ----------------------- <COMMAND> ---------------------------
Enable/Disable [S]TP            Set Bridge Maximum [A]ge
Set Bridge Pr[i]ority           Set Bridge Forward [D]elay
Set Bridge [H]ello Time      Spanning Tree [P]ort Configuration
[Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 22 Spanning Tree Configuration Menu

The Spanning Tree Configuration Menu displays the current STP operating parameters in two columns labeled Designated Root and Bridge ID. The Designated Root column displays the STP parameters from the root bridge. The Bridge ID column displays the STP parameters of the switch you are currently managing.

3. Adjust the bridge STP settings as needed. To change a parameter, type its corresponding bracketed letter and, when prompted, enter the new information. The parameters are described below.

Enable/Disable [S]TP
Enables and disables STP on the switch. The default setting is disabled.

Set Bridge Pr[i]ority
The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65535, with 0 being the highest priority.

The default value for bridge priority on the AT-8326GB is 8000. The current bridge priority is displayed in the Bridge ID field on the Spanning Tree Configuration Menu and is followed by the switch's MAC address.

Bridge [H]ello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Maximum [A]ge
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. 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. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Forwarding [D]elay
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, resulting in network loops. The default is 15 seconds.

Spanning Tree [P]ort Configuration
Allows configuration of Port Priority, Path Cost, Trunk Priority, and Trunk Path Cost. Refer to the next section for instructions on how to configure these parameters.

Configuring STP Port Settings

To configure the STP port parameters, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **S** to select Spanning Tree Configuration.

3. From the Spanning Tree Configuration Menu, type **P** to select Spanning Tree Port Configuration.

   The Spanning Tree Port Configuration Menu is displayed in Figure 23.

```
AT-8326GB Local Management System
Spanning Tree Configuration->Spanning Tree Port Configuration Menu
Stack ID: 1
Port  Trunk   Link    State     Speed  Priority  Path Cost   MAC Address
----  ------- ----  ----------  -----  --------  ---------  -----------
  1    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:3C
  2    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:3D
  3    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:3E
  4    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:3F
  5    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:40
  6    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:41
  7    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:42
  8    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:43
  9    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:44
 10    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:45
 11    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:46
 12    ---    Down  Forwarding   10      128        19       00:40:33:FF:01:47
--------------------------- <COMMAND> ---------------------------

[N]ext Page            [S]et Port Priority    Set [T]runk Priority
[P]revious Page        Set Path [C]ost        Set T[r]unk Path Cost
Select Stack [I]D      [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Figure 23 Spanning Tree Port Configuration Menu

4. Adjust the parameter settings as desired. To change a parameter, type its corresponding bracketed letter and, when prompted, enter the new information. The parameters are described below.

Set Port Pr[i]ority
Sets the parameter used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0-255. The default value for priority is 128.

Note
Port priority cannot be set on ports that are part of a trunk group.

Set Path [C]ost
Sets the cost parameter used in deciding which port provides the lowest cost path to the root bridge for that LAN. The range is 1 to 65535.

Set [T]runk Priority
Sets the parameter used as a tie breaker when two or more trunk groups are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-255.

Set Trunk Path [C]ost
Sets the cost parameter to decide which trunk group provides the lowest cost path to the root bridge for that LAN. The range is 1 to 65535.

The following information is for display purposes only and cannot be changed from the Spanning Tree Port Configuration Menu.

Port
The port number.

Trunk
The trunk group number. A number in this column indicates that the port is a member of a port trunk.

Link
The link status between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

State
This parameter indicates the current STP status of the port. Possible values are:

❑ Forwarding

❑ Listening

❑ Learning

❑ Blocking

Speed
The operating speed of the port.

MAC Address
The MAC addresses of the ports on the switch.

Chapter 10

Virtual LANs

This chapter contains basic information about virtual LANs (VLANs). It also contains the procedures for creating, modifying, and deleting VLANs from a local or Telnet management session.

This chapter contains the following sections:

VLAN Overview

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent broadcast domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you can segment your network through the switch's management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

❑ Improved network performance

Network performance often suffers as networks grow in size and as data traffic increases. The more nodes on each LAN segment vying for bandwidth, the greater the likelihood overall network performance will decrease.

VLANs improve network perform because VLAN data traffic stays within the VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them. It also frees up bandwidth within all the logical workgroups.

Additionally, since each VLAN constitutes a separate broadcast domain, broadcast traffic remains within the VLAN. This too can improve overall network performance.

❑ Increased security

Since data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

❑ Simplified network management

VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to been made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the wiring at the switches.

But with VLANS, you can change the LAN segment assignment of an end node connected to the switch through the switch's AT-S41 management software. VLAN memberships can be changed any time through the management software without moving the workstations physically, or having to change group memberships by moving cables from one switch port to another.

Additionally, a virtual LAN can span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch and so are not restricted to being in the same physical location.

VLAN Modes   An AT-8326GB stack features two VLAN modes: 802.1Q and port-based. The 802.1Q VLAN mode complies with the IEEE 802.1Q standard and supports two types of VLANs:

❑ Untagged VLANs

❑ Tagged VLANs

Untagged and tagged VLANs are described in the next section. The Port-based VLAN mode is described on page 106.

Tagged and Untagged VLAN Overview

As explained in the **VLAN Overview** section, a VLAN consists of a group of ports on one or more Ethernet switches that form a logical Ethernet segment and an independent broadcast domain. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is a connection device, such as a router or Layer 3 switch.

A VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A VLAN can also span switches and consist of ports from multiple Ethernet switches.

The parts that make up a VLAN are:

❑ VLAN name

❑ VLAN Identifier

❑ Untagged ports

❑ Tagged ports

❑ Port VLAN Identifier

VLAN Name   Every VLAN in your network should be given a name. The name should reflect the function of the network devices that are be members of the VLAN. Examples include Sales, Production, and Engineering. You will be required to specify a name when you create a VLAN.

VLAN Identifier   Each VLAN in a network must be assigned a number. This number is called the VLAN identifier (VID). This number will uniquely identify each VLAN in your network. You assign the VID number when you create the VLAN.

If a VLAN consists of ports located on only one physical AT-8326GB stack, you must assign it a VID unique from all other VLANs in your network.

In instances where a VLAN spans multiple AT-8326GB stacks, the VID for the VLAN must be the same must on each stack. This enables the stacks to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple devices.

For example, if you had a VLAN titled Marketing that spanned three AT-8326GB stacks, you would assign the Marketing VLAN on each stack the same VID.

Untagged and Tagged Ports

There are two kinds of ports that you can assign to an IEEE 802.1Q-compliant VLAN: tagged ports and untagged ports. The basic difference between the two is that an untagged port can be a member of only one VLAN at a time while a tagged port can be a member of multiple VLANs.

Untagged Ports

When the ports on an Ethernet switch are divided into independent VLANs, the switch needs to have a mechanism for determining which ports belong to which VLANs. For instance, if a switch needs to broadcast a frame to the ports of a particular VLAN, it needs to know which ports comprise the VLAN.

In a VLAN that consists of untagged ports, port membership is determined by what is referred to as the port VLAN identifier (PVID). This is a number that you must assign to a port when you assign it as an untagged member of a VLAN. The PVID of a port will be the same as the VID of the VLAN in which the port is to be an untagged member.

Here is an example. Let's assume that you are creating a new VLAN called Sales and that you assigned the VLAN a VID of 4. You have decided that Ports 1 through 4 on a switch will be untagged members of the new VLAN. Consequently, you would assign Ports 1 to 4 PVIDs of 4, the same as the VID. Now, when the switch receives a frame on one of the ports on the Sales VLAN and it needs to broadcast the frame to the other ports of the VLAN, it will know that the VLAN consists of Ports 1 to 4.

A VLAN that consists of only untagged ports is referred to as an untagged VLAN. In order for frames from untagged VLANs to cross a VLAN boundary, there must be a Layer 3 switch or router providing a connection between the VLANs.

You can assign each port only one PVID. Consequently, a port can be an untagged member of only one VLAN at a time.

Note

An AT-8326GB stack is pre-configured with one untagged VLAN, called the Default VLAN. All ports on the switch are members of this VLAN. The Default VLAN has a VID of 1. Consequently, all the ports in the VLAN have a PVID value of 1.

The ports are called untagged because the switch assumes that the frames received on this type of port will not contain any information that indicates VLAN membership and that VLAN membership will be determined solely by a port's PVID. (This contrasts with tagged ports,

explained next, where VLAN membership is determined by information within the frames themselves.) Frames received on untagged ports and lacking any VLAN identifying information are referred to as untagged frames.

When a switch receives a frame on an untagged port, it first examines the PVID of the port on which the frame was received and then adds the PVID to the frame itself. It then examines the destination MAC address of the frame. If the destination address is in the MAC address table and if the switch port where the destination node is located is part of the same VLAN as the port that received the frame, the switch sends the frame out the port to the destination node.

If the destination MAC address is not in the MAC address table, the switch broadcasts the frame to all the ports that share the same PVID as the port that received the frame.

Tagged Ports

The second type of port that can be a member of a VLAN is called a tagged port. There are several principal differences between a tagged port and an untagged port.

As explained earlier, a switch determines the VLAN membership of a frame received on an untagged port by examining the PVID that you assigned to the port.

But when a frame is received on a tagged port, the switch examines the frame itself to determine VLAN membership. The VLAN information within an Ethernet frame is referred to as a tag or tagged header. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard).

When a switch receives a frame with a VLAN tag, referred to as a tagged frame, the switch forwards the frame only to those ports that share the same VID.

Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of tagged ports is that they can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, an IEEE 802.1Q-compliant server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

So how do you indicate which ports are to be tagged and which are to be untagged when you create a VLAN? The rule is straightforward. If you assign a port to only one VLAN, the switch assumes it is to be an untagged port. If you assign a port to more than one VLAN, the switch assumes that the port is to be both a tagged and untagged port.

A VLAN that contains only tagged frames or that contains a combination of tagged and untagged ports is referred to as a tagged VLAN. And, as explained previously, any device that you connect to a tagged port of a tagged VLAN must be IEEE 802.1Q-compliant.

General Rules to Creating an Untagged or Tagged VLAN

Below are general rules to observe when creating a VLAN.

❑ An AT-8326GB switch can support up to256 tagged and untagged VLANS.

❑ Each VLAN must be assigned a unique VID. However, if a particular VLAN spans multiples AT-8326GB stacks, each part of the VLAN on the different stacks must be assigned the same VID.

❑ A port can be an untagged member of only one VLAN at a time.

❑ A port can be a tagged member of multiple VLANs.

❑ You must assign each untagged port a PVID. The PVID of an untagged port must match the VLAN's VID. You must assign this value manually when you create the VLAN.

❑ An untagged VLAN that spans multiple stacks requires a port on each stack where the VLAN is located to function as a connection between the various parts of the VLAN reside.

❑ If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to connect the VLANs.

Creating a Tagged or Untagged VLAN

The procedure for creating a new VLAN is divided into the following phases:

❑ Phase 1: Assigning a VID and name and specifying the port members

❑ Phase 2: Converting tagged ports into untagged ports

Performing Phase 1 is required whenever you create a new VLAN. Every VLAN must have a name, VID, and, of course, ports. You will need to perform Phase 2 if some or all of the ports of a VLAN will be untagged ports. Ports that you want to function as untagged ports must be converted by changing their PVIDs, as explained in Phase 2.

To create a new VLAN, start by performing the procedure in Phase 1.

Phase 1 This phase assigns a VID and a name to your VLAN, and also designates the VLAN port members.

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

The VLAN Management Menu is displayed in Figure 24.

```
AT-8326GB Local Management System

Advanced Switch Configuration -> VLAN Management Menu


VLAN Type : 802.1Q        GVRP Status :Disabled
VLAN ID    VLAN Name                        VLAN Type
-------   -------------------------------  ----------
1         Default VLAN                      Permanent




-------------------------- <COMMAND> ----------------------------
[N]ext Page              [C]reate VLAN      C[o]nfig VLAN Member
[P]revious Page          [D]elete VLAN       [S]et Port Config
[R]eset VLAN to Default  Set [G]VRP Status  Set VLAN [T]ype
[Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 24 VLAN Management Menu

> **Note**
> Check to make sure the VLAN Type is set to 802.1Q. 802.1Q is the
> default VLAN Type. You can create tagged and untagged VLANs
> only when the switch is operating in the 802.1Q mode. For
> instructions on how to change the switch's VLAN mode, see **Setting
> the VLAN Type** on page 114.

3. From the VLAN Management Menu, select **C** for Create VLAN.

    The VLAN Creation Menu is displayed in Figure 25.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option


Advanced Switch Configuration -> VLAN Creation Menu

VLAN Index :
VLAN Name :

Device          Member
--------        ------------------------------------------------------
    1
    2
    3


--------------------------- <COMMAND> ---------------------------
Set VLAN [I]D/[I]ndex                    [S]elect Port Member
Set VLAN [N]ame                          [A]pply
[Q]uit to previous menu



Command> _
Enter the character in square brackets to select option
```

Figure 25 VLAN Creation Menu

4. Type **I** to select Set VLAN ID/Index.

    The following prompt is displayed:

    ```
    Enter VLAN ID ->Enter VLAN ID >
    ```

5. Enter a VID for the new VLAN. The VID can be between 2 and 4094.
    Press Enter.

    If this VLAN will be unique in your network, then its VID must also be
    unique from all other VIDs in the network.

    If this VLAN will be part of a larger VLAN that spans multiple AT-
    8326GB stacks, than the VID value for the VLAN should be the same
    on each stack. For example, if you are creating a VLAN called Sales
    that will span three AT-8326GB stacks, you must assign the Sales
    VLAN on each stack the same VID value.

6. Type **N** to select Set VLAN Name.

   The following prompt is displayed:

   ```
   Enter VLAN Name ->Enter VLAN Name >
   ```

7. Enter a VLAN name of up to 32 characters. Press Enter

   The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

   If the VLAN will be unique in your network, then the name should be unique as well.

   If the VLAN will be part of a larger VLAN that spans multiple stacks, then the name for the VLAN should be the same on each stack where nodes of the VLAN are connected.

8. Type **S** to choose Select Port Member.

   The following prompt is displayed:

   ```
   Enter Stack ID >
   ```

9. Enter 1 to select the master switch.

   Note
   The VLAN must contain at least one port from the master switch. Furthermore, when creating a new VLAN, you cannot add ports from the slave switches. Ports from the slave switches can only be added to a VLAN only after the VLAN has been created, by modifying the VLAN, as explained in the procedure **Viewing or Modifying a Tagged or Untagged VLAN** on page 101.

   The following prompt is displayed:

   ```
   Enter port number>
   ```

10. Enter the ports, both tagged and untagged, on the master switch that are to be members of the new VLAN. Press Return.

    You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

11. Type **A** to select Apply.

    You have now created a new VLAN. You gave it a VID and a name. You also specified which ports were to be members of the new VLAN.

However, it is important to note that, by default, all of the ports that you just added to the new VLAN are tagged ports, meaning they are shared ports. The ports are still members of their current VLANs.

If you want to convert the ports into untagged ports, you must perform the procedure in Phase 2.

Phase 2   This phase of creating a new VLAN converts the tagged ports that you added to the new VLAN into untagged ports. This involves changing the PVIDs of the ports so that they match the VID of the new VLAN. For example, if you assigned the new VLAN a VID of 4, you must change the PVIDs of the untagged ports to 4. The following procedure explains how this is accomplished.

The following procedure assumes that you are continuing directly from Phase 1.

1. From the VLAN Creation Menu, type **Q** to select Quit to Previous Menu.

   The VLAN Management Menu is displayed again.

2. Type **S** to select Set Port Config.

   The VLAN Port Configuration Menu is displayed in Figure 26.

```
AT-8326GB Local Management System
VLAN Management -> VLAN Port Configuration Menu

 Stack ID: 1

 Port    PVID
 ----    ----
   1       1
   2       1
   3       1
   4       1
   5       1
   6       1
   7       1
   8       1
------------------------------- <COMMAND> ------------------------

 [N]ext page                             Set Port [V]ID
 [P]revious Page                    Set Stack [I]D
 [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 26 VLAN Port Configuration Menu

This menu lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 8 on the switch all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

The menu, when initially displayed, lists the PVIDs for the ports on the master switch of the stack.

3. Type **I** to choose Select Stack [I]D and enter the number of a switch in the stack containing a port whose PVID you need to change. (You can skip this step if you want to change to the master switch, since the master switch is displayed by default.)

    The VLAN Port Configuration Menu for the selected switch is displayed.

4. To set a PVID, type **V** to select the Set Port VID option.

    The following prompt is displayed:

    ```
    Set PVID->Enter port number>
    ```

5. Enter the port number whose PVID you want to change.

    A prompt similar to the following is displayed:

    ```
    Enter PVID for port 1>
    ```

6. Enter the new PVID for the port.

    Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the new VLAN as an untagged port.

    If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

7. Repeat Steps 3 to 6 to assign new PVIDs to any other ports that are to be untagged members of the new VLAN.

8. Once you have changed all of the appropriate PVIDs, type **Q** to select Quit to Previous Menu.

    The VLAN Management Menu in Figure 24 on page 96 is displayed again.

This completes the procedure for creating a new VLAN.

Viewing or Modifying a Tagged or Untagged VLAN

There are two phases to modifying a VLAN. You might need to perform both phases or just one of them, depending on what it is you want to change in the VLAN. The phases are:

❑ Phase 1: In this phase, you can view a VLAN's configuration, as well as change a VLAN's name and add or remove tagged ports.

❑ Phase 2: In this phase, you can add or remove untagged ports.

Phase 1

This phase explains how to display the Config VLAN Member Menu of a VLAN. This menu displays a VLAN's configuration. You can also use the menu to change a VLAN's name and add or remove tagged ports.

Note
If you do not want to change a VLAN's name or add or remove tagged ports, then skip this procedure and go straight to Phase 2 to add and remove untagged ports.

---

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, select **O** for the Config VLAN Member option.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VID of the VLAN you want to view or modify.

The Config VLAN Member Menu for the VLAN is displayed, as shown in Figure 27. This menu contains all the current information about the VLAN.

```
AT-8326GB Local Management System
VLAN MAnagement-> Config VLAN Member Menu

Stack ID: 1      VLAN ID: 3                 VLAN Name: Engineering

Port              Participation           Tagging
----              -------------           -------
8                 Static                  No
9                 Static                  No
10                Static                  No
11                Static                  No
16                Static                  No
23                Static                  No


----------------------------Command---------------------------

[N]ext Page            [C]hange VLAN Name     [A]dd VLAN Member
[P]revious Page        [M]odify Participation [R]emove VLAN Member
Select Stack [I]D    [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 27 Config VLAN Member Menu

This menu, when initially displayed, lists the ports on the master switch that belong to the selected VLAN. The columns in the menu are defined below:

Port
This column lists the ports on the selected switch that are members of the VLAN.

Participation
This column indicates whether the port is participating in GVRP.

Tagging
This column indicates whether the port is a tagged or untagged port of the VLAN. No indicates that the port is an untagged member while Yes indicates that it is a tagged member.

5. To change the VLAN's name, type **C** to select Change a VLAN Name and enter the new name when prompted.

6. To add or remove tagged ports from the VLAN, do the following:

Note
To add or remove untagged ports from the VLAN, perform **Phase 2** below.

a. Type **I** to choose Select Stack ID and enter the number of the switch in the stack containing ports that you want to add or remove from the VLAN. (You can skip this step if the ports are located on the master switch, since the default selection is the master switch.)

b. To add tagged ports to the VLAN, type **A** and then specify the ports that you want to add as tagged ports to the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Press Enter.

c. To remove tagged ports from a VLAN, type **R** and specify the tagged ports that you want to remove. Press Enter. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

Phase 2   You perform this phase whenever you need to add or remove an untagged port from a VLAN. This phase explains how to change the PVIDs of the ports so that they match the VID of a different VLAN. For example, if you want to assign Port 2 as an untagged member of a VLAN with a VID of 4, you must change the PVID of the port to 4.

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. Type **S** to select Set Port Config.

   The VLAN Port Configuration Menu is displayed in Figure 28.

```
AT-8326GB Local Management System
VLAN Management -> VLAN Port Configuration Menu

 Stack ID: 1

 Port    PVID
 ----    ----
   1       1
   2       1
   3       1
   4       1
   5       1
   6       1
   7       1
   8       1
------------------------------ <COMMAND> ----------------------

 [N]ext page                          Set Port [V]ID
 [P]revious Page                      Set Stack [I]D
 [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 28 VLAN Port Configuration Menu

This menu lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 8 on the switch all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

The menu, when initially displayed, lists the PVIDs for the ports on the master switch of the stack.

4. Type **I** to choose Select Stack ID and enter the number of a switch in the stack containing a port whose PVID you need to change.

The VLAN Port Configuration Menu for the selected switch is displayed.

5. To set a PVID, type **V** to select the Set Port VID option.

The following prompt is displayed:

```
Set PVID->Enter port number>
```

6. Enter the port number whose PVID you want to change.

A prompt similar to the following is displayed:

```
Enter PVID for port 1>
```

7. Enter the new PVID for the port.

Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the new VLAN as an untagged port.

If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

8. Repeat Steps 3 to 6 to assign new PVIDs to any other ports that are to be untagged members of the new VLAN.

9. Once you have changed all of the appropriate PVIDs, type **Q** to select Quit to Previous Menu.

The VLAN Management Menu in Figure 24 on page 96 is displayed again.

This completes the procedure for modifying a VLAN.

Deleting a Tagged or Untagged VLAN

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, select **D** for Delete VLAN.

4. At the command prompt, enter the VLAN ID of the VLAN you would like to delete. Press Enter.

   The VLAN is removed from the switch. The PVIDs of the untagged ports in the VLAN are changed to 1, making the ports untagged members of the Default VLAN.

   Note
   You cannot delete the Default VLAN, which has a VLAN ID of 1.The Default VLAN is a permanent VLAN.

Port-based VLAN Mode Overview

The AT-8326GB switch features a special Port-based VLAN mode. This VLAN mode allows you to create VLANs that are slightly different than the tagged and untagged VLANs described earlier in this chapter.

> **Note**
> For those of you who are familiar with Allied Telesyn products, please note that the port-based VLAN described here is not the same as the port-based VLANs featured in our other managed switches, such as the AT-8024 Fast Ethernet switch. The untagged VLAN described earlier in this chapter is analogous to the port-based VLAN featured in other Allied Telesyn switch products.

Port-based VLANs are just lists of ports that belong to different VLANs on the switch. To create a port-based VLAN, you simply indicate which ports you want in it. You do not configure PVIDs, as you do for untagged ports, and, while you do specify a unique VID when you create a port-based VLAN, its use is limited to within the switch. A VID is not used across multiple switches to identify different port-based VLANs.

Port-based VLANs do have a couple of advantages over tagged and untagged VLANs described earlier in this chapter. For instance, port-based VLANs are easier to configure, mainly because you do not have to worry about setting PVIDs.

Plus, it can be easier to share network resources. Ports can be shared in port-based VLANs and the shared devices do not need to be IEEE 802.1Q-compliant, as required with a tagged VLAN.

The major disadvantage to port-base VLANs is VLAN leakage, where frames that originate in one VLAN end up in another. This can occur where port-based VLANs share ports.

Here is how this can occur. Let's assume that a frame arrives on a switch port that is shared among three different VLANs. If the destination MAC address in the frame has not been learned by the switch, the frame will be broadcast out the ports of all three VLANs. Hence, the frame crosses the boundaries of the VLANs.

This might not be a problem for you if network security is not a major concern. However, if it is a high priority, then either the VLANs that you create with the port-based VLAN mode should not contain shared ports, or you should instead create tagged VLANs, as described earlier in this chapter.

Creating a Port-based VLAN

To create a new port-based VLAN, perform the following procedure:

> **Note**
> This procedure assumes that the switch is set to the Port-based VLAN Type. For instructions on how to change the VLAN Type on the switch, refer to **Setting the VLAN Type** on page 114.

1. From the Main Menu, type **A** to select Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

   The VLAN Management Menu is displayed.

3. From the VLAN Management Menu, type **T** to select Set VLAN Type.

   The following prompt is displayed.

   ```
   Set VLAN type (P/8)>
   ```

4. From the VLAN Management Menu, type **C** to Create VLAN.

   The VLAN Creation Menu is displayed in Figure 29.

```
AT-8326GB Local Management System

Advanced Switch Configuration -> VLAN Creation Menu

VLAN Index :
VLAN Name :

Port Member
--------------------------------------------------------



-------------------------- <COMMAND> ---------------------------

Set VLAN [I]D/[I]ndex                    [S]elect Port Member
Set VLAN [N]ame                          [A]pply
[Q]uit to previous menu



Command> _
Enter the character in square brackets to select option
```

Figure 29 VLAN Creation Menu

5. Type **I** to select Set VLAN ID/Index.

   The following prompt is displayed:

   ```
   Enter VLAN ID ->Enter VLAN ID >
   ```

6. Enter a unique VLAN ID for the VLAN. Press Enter.

   Since the stack does not examine the VID in tagged headers of tagged frames when operating in the Port-based VLAN mode, this VID value does not need to be unique from all other VLANs in your network. It only needs to be unique from the other VLANs in the stack on which you are creating the VLAN.

   The value can be from 2 and 256.

7. Type **N** to select the Set VLAN Name option.

   The following prompt is displayed:

   ```
   Enter VLAN Name ->Enter VLAN Name >
   ```

8. Enter a VLAN name of up to 32 characters. Press Enter

   The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

9. Type **S** to Select Port Members.

   ```
   Enter Stack ID >
   ```

10. Enter the number of a switch in the stack which has one or ports that are to be members of the VLAN.

    The following prompt is displayed:

    ```
    Enter port number>
    ```

11. Enter the ports on the selected switch that are to be members of the new VLAN. Press Return.

    You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

12. If the VLAN will consist of ports from different switches in the stack, repeat Steps 9 to 11 to add ports to the VLAN from other switches.

13. Type **A** to select Apply.

    You have now created a new VLAN. You gave it a VID and a name. You also specified which ports were to be members of the new VLAN.

Note
The ports that you just added to the new VLAN are not removed from their current VLAN assignments. You must remove the ports manually from the other VLANs if you do not want them to be shared. For instructions, refer to **Modifying a Port-based VLAN** on page 110.

You can repeat this procedure to create additional port-based VLANs.

Modifying a Port-based VLAN

The following procedure explains how to change the name of a port-based VLAN, as well as add or remove ports.

To modify a port-based VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, select **O** for the Config VLAN Member option.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VID of the VLAN you want to view or modify.

   The Config VLAN Member Menu for the VLAN is displayed in Figure 30. This VLAN contains all the current information about the VLAN.

```
AT-8326GB Local Management System
VLAN MAnagement-> Config VLAN Member Menu

Stack ID: 1  VLAN ID: 3    VLAN Name: Engineering


Group Members
-------------------------------------------------------
1, 2, 3, 4, 5




---------------------------Command---------------------------
[N]ext Page            [C]hange VLAN Name     [A]dd VLAN Member
[P]revious Page        [M]odify Participation [R]emove VLAN Member
[Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 30 Config VLAN Member Menu

5. To modify the VLAN, use the commands at the bottom of the screen.

    The commands are described below:

    [C]hange a VLAN Name
    This command is used to change a VLAN's name. Type **C** and enter the new name at the command prompt.

    [M]odify Participation
    This command is disabled when the switch is operating in the port-based VLAN mode.

    [A]dd VLAN Member
    This command adds ports to the VLAN. Type **A** and then specify the ports that you want to add as members of the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Press Enter.

    Note
    Any port that you add to a VLAN remains a member of the VLAN(s) in which it is currently assigned. If you do not want the port to be a shared port, you must remove it from the other VLANs.

    [R]emove VLAN Member
    This command removes ports from the VLAN. Type **R** and specify the tagged ports that you want to remove from the VLAN. Press Enter. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

    Note
    You cannot remove a port if it is not already a member of another VLAN.

Setting GVRP Status

To set the GVRP status, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, select **G** for Set GVRP Status.

   The following prompt is displayed.

   ```
   Enable or Disable GVRP status (E/D)>
   E for Enable; D for Disable
   ```

   Type **E** to select Enable. The default setting is Disabled.

   The GVRP Status in the VLAN Management Menu is immediately changed to reflect the new setting.

Resetting the VLAN Parameters to Default

This command deletes all VLANs that you created. All ports are returned back to the Default VLAN.

To reset the default VLAN parameters of the switch, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, select **R** for Reset VLAN to Default.

   The following prompt is displayed.

   ```
   Are you sure you want to reset VLAN configuration
   to factory default (Y/N)>
   Y for Yes; N for No
   ```

   Type **Y** to select Yes.

   The following prompt is displayed.

   ```
   Are you sure you want to reset VLAN configuration to
   factory default (Y/N)>
   Reset to factory default completed, press any key to
   continue...
   ```

   The default VLAN settings are immediately displayed in the VLAN Management Menu.

Setting the VLAN Type

The AT-8326GB switch can operate in either the 802.1Q VLAN mode for creating tagged and untagged VLANs or the port-based VLAN mode.

Note
The VLAN Type default is 802.1Q.

The change the VLAN mode, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.

2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

3. From the VLAN Management Menu, type **T** to select Set VLAN Type.

   The following prompt is displayed.

   ```
   Set VLAN type (P/8)>
   ```

4. Enter **P** for the Port-based VLAN Type or **8** for the 802.1Q VLAN Type.

Note
Changing the VLAN type setting deletes all VLANs except the Default VLAN.

Chapter 11

MAC Address Table

This chapter contains the procedures for viewing the MAC address table. The sections in this chapter include:

- ❑ **MAC Address Overview** on page 116
- ❑ **Displaying MAC Addresses** on page 118
- ❑ **Viewing MAC Addresses by Port** on page 120
- ❑ **Viewing the MAC Addresses by MAC** on page 121
- ❑ **Viewing the MAC Addresses of a VLAN** on page 122
- ❑ **Adding Static MAC Addresses** on page 123
- ❑ **Deleting Static MAC Addresses** on page 124
- ❑ **Changing the Aging Time** on page 125

MAC Address Overview

Every hardware device on your network has a unique MAC address. This address is assigned to the device by the device's manufacturer. For example, when you install a network interface card (NIC) in a computer so that you can connect it to the network, the NIC already has a MAC address assigned to it by its manufacturer.

The AT-8326GB Fast Ethernet switch contains an 8 kilobyte entry MAC address table. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned.

The switch learns the MAC addresses of the end nodes by examining the source address of each packet received on a port. It adds the address and port on which the packet was received to the MAC table if the address had not already been entered in the table. The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When the switch receives a packet, it also examines the destination address and, by referring to its MAC address table, determines the port on which the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each packet to the appropriate port where the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments, increasing network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port

on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

The type of MAC address described above is referred to as a dynamic MAC address. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node over a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the aging timer. This value is adjustable on the AT-8326GB switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 125.

The MAC address table can also store static MAC addresses. A static MAC address, once entered in the table, remains in the table indefinitely until you delete it, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch will not learn in its normal dynamic learning process, or if you want a MAC address to remain permanently in the table, even when the end node is inactive.

Displaying MAC Addresses

To display the MAC address table, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

   The Forwarding Database Menu is displayed in Figure 31.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Forwarding Database Menu

[S]tatic Address Table
Display MAC Address by [P]ort
Display MAC Address by [M]AC
Display MAC Address by [V]ID
[Q]uit to previous menu



Command> _
Enter the character in square brackets to select option
```

Figure 31 Forwarding Database Menu

3. To display the MAC addresses, select from the options below. To select an option, type its corresponding bracketed letter.

   [S]tatic Address Table
   This displays the static address table, which lists all static addresses assigned to ports on the switch.

   Display MAC Address by [P]ort
   This displays both the static and dynamic MAC addresses on a selected port.

   Display MAC Address by [M]AC
   This displays all static and dynamic MAC addresses on a switch.

   Display MAC Address by [V]ID
   This displays all MAC addresses by VLAN ID.

The management software displays the MAC addresses based on your selection. Figure 32 is an example of the Display MAC Address by MAC option, which displays both static and dynamic MAC addresses.

```
AT-8326GB Local Management System
Forwarding Database Menu -> Display MAC Address by MAC

 Age-Out Time:  300 Sec.

   MAC Address         Stack ID      Port
 -----------------     ----------    ----
00:40:33:FF:01:59         2           4
00:40:33:FF:01:5A         2           5
00:40:33:FF:01:5B         2           6
00:40:33:FF:01:5C         2           7
00:40:33:FF:01:5D         2           8
00:40:33:FF:01:5E         2           9
00:40:33:FF:01:5F         2           10
00:40:33:FF:01:60         2           11
00:40:33:FF:01:61         2           12
00:40:33:FF:01:62         2           13
----------------------------- <COMMAND> --------------------

[N]ext Page                            Set [A]ge-Out time
[P]revious Page                        [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

Figure 32 Display MAC Address by MAC Menu

The Forwarding Database is for viewing purposes only except for Set Age-Out Time. The columns on the menu are defined below.

MAC Address
The MAC addresses of the end nodes connected to the switch.

Stack ID
The stack ID of the switch on which the MAC address was learned.

Port
The port on the switch where the MAC address was learned.

Set [A]ge-Out Time
This allows you to manually set the MAC address age-out time. The range is 10 to 1048 Seconds. The default setting is 300.

Viewing MAC Addresses by Port

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You can also use this procedure to view any static MAC addresses that have been assigned to a port.

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database Menu, type **P** to select View MAC Addresses by Port.

    The following prompt is displayed:

    ```
    Add new entry->Enter Stack ID >
    Stack ID is in range of 1 to X
    ```

    X equals the Stack ID of the last switch in your switch stack.

4. Enter the Stack ID of the switch for the port whose static and dynamic MAC addresses you want to view and press Enter.

    The following prompt is displayed:

    ```
    Enter port number >
    Port number is in range of 1 to 26
    ```

5. Enter the number of the port whose static and dynamic MAC addresses you want to view and press Enter.

    A window is displayed with the MAC addresses of the nodes on the port. The columns in the window and the definitions of the columns are the same as for the **Display MAC Address by MAC Menu** on page 119.

Viewing the MAC Addresses by MAC

This section contains the procedure for viewing the dynamic MAC addresses learned on the ports of a switch. They are displayed in numerical order. This procedure will also let you view all static MAC addresses that have been assigned to any port(s) on the switch.

To view the MAC addresses on the switch in numerical order, perform the following procedure.

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database Menu, type **M** to select Display MAC Address by MAC.

   The management software displays a window with a list of all static and dynamic MAC addresses of the end nodes connected to the switch. For an example of the window and for definitions of the columns, refer to the **Display MAC Address by MAC Menu** on page 119.

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

Note
To perform this procedure, you need to know the VLAN ID number of the VLAN whose MAC addresses you want to view.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database Menu, type **V** to select Display MAC Address by VID.

    The following prompt is displayed:

    ```
    Enter VLAN ID>
    VLAN ID is in range of 1 to 4094
    ```

4. Enter the VLAN ID of the desired VLAN and press Return.

    The management software displays a window with a list of the MAC addresses of the end nodes in the VLAN. For an example of the window and for definitions of the columns, refer to the **Display MAC Address by MAC Menu** on page 119.

Adding Static MAC Addresses

The management software allows you to assign up to 256 static MAC addresses on an AT-8326GB Fast Ethernet switch.

To add a static address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database Menu, type **S** to select Static Address Table.

4. From the Static Address Table Menu, type **A** to Add New Entry.

    The following prompt is displayed:

    ```
    Enter MAC Address(xx:xx:xx:xx:xx:xx) >
    ```

5. Enter the static MAC address in the following format:

    ```
    xx:xx:xx:xx:xx:xx
    ```

    Once you have specified the MAC address, the following prompt is displayed:

    ```
    Add new entry->Enter Stack ID >
    Stack ID is in range of 1 to X
    ```

    X equals the Stack ID of the last switch in your switch stack.

6. Enter the Stack ID of the switch for the port you want to assign a static MAC address.

    Once you have entered the Stack ID, the following prompt is displayed:

    ```
    Add new entry->Enter port number >
    Port number is in range of 1 to 26
    ```

7. Enter the port number you want to assign a static MAC address.

    Once you have specified the port number, the following prompt is displayed:

    ```
    Add new entry->Enter VLAN ID>
    VLAN ID is in range of 1 to 4094
    ```

8. Enter the VLAN ID of the VLAN the port belongs to.

    Once you have specified the VLAN ID, the management software adds the static address to the MAC address table.

9. Repeat steps 4 through 8 to enter additional static MAC addresses.

Deleting Static MAC Addresses

To delete a static MAC address, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database menu, type **S** to select Static Address Table.

4. From the Static Address Table Menu, type **D** to Delete Entry.

    The following prompt is displayed:

    ```
    Enter MAC Address(xx:xx:xx:xx:xx:xx) >
    ```

5. Enter the static MAC address in the following format:

    ```
    xx:xx:xx:xx:xx:xx
    ```

    Once you have specified the MAC address, the following prompt is displayed:

    ```
    Delete entry->Enter VLAN ID>
    VLAN ID is in range of 1 to 4094
    ```

6. Enter the VLAN ID of the VLAN in which the port for this static address is a member

    Once you have specified the VLAN ID, the management software deletes the static address from the MAC address table.

7. Repeat steps 4 through 6 to delete additional static MAC addresses.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

> **Note**
> The aging time can be adjusted from the following menus: Display MAC Address by Port, Display MAC Address by MAC, and Display MAC Address by VID. It cannot be adjusted on the Static Address Table Menu.

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database.

3. From the Forwarding Database menu, type **P** to select View MAC Addresses by Port, **M** to select Display MAC Address by MAC, or **V** to select Display MAC Address by VID.

4. Once you have made your selection, follow the prompts until you are able type **A** to select MAC Aging Time.

   The following prompt is displayed:

   ```
   Enter your new value ->
   Age-out time is in range of 10 to 1048 Sec
   ```

5. Enter a new value in seconds. The aging setting is in range of 10 to 1048 seconds. The default setting is 300 seconds.

   The management software immediately activates the new aging time value on the switch.

Chapter 12
Quality of Service

This chapter contains the procedures for configuring the Quality of Service (QoS) feature of the AT-S41 software. Sections in the chapter include:

❑ **Quality of Service Overview** on page 127

❑ **Configuring QoS** on page 128

Quality of Service Overview

The AT-8326GB switch supports QoS as specified in the IEEE 802.1p and 802.1Q standards. QoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to QoS, network traffic was handled in a best-effort manner. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can prove problematic. For example, transfer delays of voice transmission can result in poor audio quality.

QoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest.

The AT-8326GB switch has two priority queues, 1 (low) and 0 (high). When a tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues according to following assignments:

IEEE 802.1p Traffic Class	AT-8326GB Queue
0	1
1	1
2	1
3	1
4	0
5	0
6	0
7	0

For example, a tagged packet with a priority tag of 6 is placed in the high priority queue, while a packet with a priority tag of 1 is placed in the low priority queue.

These priority-to-queue assignments can be overridden using the AT-S41 management software on a per port basis.

Note
QoS is disabled by default on the switch.

Configuring QoS

To configure QoS on the switch, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **S** to select Quality of Service Configuration.

   The Quality of Service Configuration Menu is displayed in Figure 33.

```
AT-8326GB Local Management System
Advanced Switch Configuration -> Quality of Service Configuration
Menu

 QoS Status : Disabled

 Traffic Class          Queue
 -------------       -------------
       0                   1
       1                   1
       2                   1
       3                   1
       4                   0
       5                   0
       6                   0                      0 : Highest
       7                   0                      1 : Lowest

_------------------------- <COMMAND> -------------------------

 Set [S]tatus
 Set [P]riority Queue
 [Q]uit to previous menu

 Command> _
 Enter the character in square brackets to select option
```

Figure 33 Quality of Service Configuration Menu

3. From the Quality of Service Configuration Menu, type **S** to select Set Status.

   The following prompt is displayed.

   ```
   Enable or Disable QoS (E/D) >
   E for Enable; D for Disable
   ```

4. Type **E** to select Enable QoS or **D** to disable QoS. The default setting is Disable.

5. If you activated QoS and want to change the queue assignments, type **P** to select Set Priority Queue.

   The following prompt is displayed.

   ```
   Enter Traffic Class
   Traffic class is in range of 0 to 7
   ```

6. Enter a traffic class.

   The following prompt is displayed, where X equals the traffic class specified in the last step.

   ```
   Enter queue for traffic class X>
   Queue is in range of 0 to 1
   ```

7. Enter a priority queue (0 - 1).

   Note
   The default setting for traffic classes 0 - 3 is the low priority queue. The default setting for traffic classes 4 - 7 is the high priority queue.

   All tagged frames will be directed to either the low or high priority queue as specified.

   Note
   The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered the switch.

   The priority level of tagged frames is determined by the priority level specified in the frame itself.

8. Repeat this procedure to configure priority levels for other traffic classes on the switch.

Chapter 13

IGMP Snooping

This chapter explains how to activate and configure the IGMP snooping feature on the switch. Sections in the chapter include:

❑ **IGMP Snooping Overview** on page 131

❑ **Activating IGMP Snooping** on page 132

❑ **Viewing Group Members** on page 134

IGMP Snooping Overview

The Internet Group Management Protocol (IGMP) enables routers to create lists of end nodes that want to receive multicast packets from a multicast application. The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports. An end node wanting to become a member of a particular multicast group responds to a query by sending a report. End nodes that join a multicast group are referred to as host nodes.

Once the router has received a request from a host node to join a multicast group, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

The IGMP snooping feature on the AT-8326GB switch enables the unit to monitor the flow of queries from the router and reports from the host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by further restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, the switch would flood all multicast packets out all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

Note
By default, IGMP snooping is disabled on the switch.

Note
The AT-S41 software supports both IGMP version 1 and version 2.

Activating IGMP Snooping

To enable or disable IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **I** to select the IGMP Snooping Configuration.

    The IGMP Configuration Menu is displayed in Figure 34.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option


Advanced Switch Configuration -> IGMP Configuration Menu


IGMP Snooping Status:          Disabled
IGMP Snooping Age-Out Timer : 280 seconds.


VLAN ID  Multicast group address
-------  -----------------------
  2             224.0.1.22
  7             224.0.1.25


-------------------------- <COMMAND> ----------------------------
[N]ext Page                            [E]nable/Disable IGMP Snooping
[P]revious Page                        [S]et Age Out Timer
[V]iew group members                   [Q]uit to previous menu


Command>

Enter the character in square brackets to select option
```

Figure 34 IGMP Configuration Menu

The parameters in the IGMP Configuration Menu are defined below:

[E]nable/Disable IGMP Snooping
Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature.

[S]et Age Out Timer
Specifies the time period in seconds after which the switch stops sending out multicast packets out of a port with an inactive host node. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 280 to 420 seconds. The default is 280 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

[V]iew Group Members
Allows you to display a list of the group members of each multicast group on a switch.

3. Type **E** to select enable/disable IGMP snooping option and then type **E** at the command prompt.

   IGMP is now activated on the switch.

Viewing Group Members

You can use the AT-S41 software to display a list of the members of each multicast group on a switch. To display the list, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.

2. From the Advanced Switch Configuration Menu, type **I** to select the IGMP Snooping Configuration.

3. From the IGMP Configuration Menu, type **V** to select View Group Members.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VLAN ID for the VLAN this multicast group belongs to.

   The following prompt is displayed:

   ```
   Enter IP address>
   ```

5. Enter the IP address of the of the multicast group whose members you want to see.

   The Group Members are displayed on the IGMP Configuration Menu, as shown in Figure 35.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option

IGMP Configuration Menu -> View Group Members Menu

VLAN ID:     3        Multicast group address:  224.0.1.22
Group members
----------------------------------------------------------------
3




------------------------- <COMMAND> -----------------------
[Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 35 View Group Members Menu

The information on this menu is for viewing purposes only. The columns are defined below:

Multicast Group Address
The multicast address of the group.

Group Members

The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN ID

The VLAN ID of the VLAN the multicast group belongs to.

Chapter 14

Broadcast Storm Control

This chapter contains the procedures for configuring the broadcast storm control feature of the AT-S41 management software. Sections in the chapter include:

❑ **Broadcast Storm Control Overview** on page 137

❑ **Activating Broadcast Storm Control** on page 138

Broadcast Storm Control Overview

Most frames on an Ethernet network are unicast frames. A unicast frame is sent to a single destination. That is, the node sending a unicast frame intends the frame for a particular node on the network. For example, when a node needs to send a file to a network server for storage, the node sends the file in unicast Ethernet frames containing the destination address of the server where the file is to be stored.

Broadcast frames are different. When a node sends out a broadcast frame, the frame is directed to all nodes on the network or all nodes within a particular virtual LAN. Broadcast frames can perform a variety of functions in an Ethernet network. For example, some network operating systems use broadcast frames to announce the presence of devices on the network.

The problem with broadcast frames is that too many of them traversing the network can impact network performance. Should the performance of your network has been diminished by heavy broadcast traffic, you can use the AT-S41 management software to limit the number of broadcast frames passing through the switch and so limit the number of broadcast frames on your network.

In order to use this feature, you must enable Broadcast Storm Control and set the threshold level.

Note
The AT-S41 default setting is no broadcast storm control on the switch.

Activating Broadcast Storm Control

To activate the Broadcast Storm Control feature for the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.

2. From the Basic Switch Configuration Menu, type **C** to select Storm Control Configuration.

   The Storm Configuration Menu is displayed in Figure 36.

```
AT-8326B Local Management System
Enter the character in square brackets to select option

Basic Switch Configuration -> Storm Configuration Menu

Broadcast Storm Status: Disabled

Threshold :  Low

---------------------------- <COMMAND> ----------------------------
Set [B]roadcast Status
Set [T]hreshold
[Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 36 Storm Configuration Menu

3. Type **B** to select Set Broadcast Status.

   The following prompt is displayed:

   `Enable or Disable Broadcast Storm Control (E/D)>`

4. Type **E** to enable Broadcast Storm Control or **D** to disable Broadcast Storm Control. The default setting is Disabled.

5. To configure threshold on the Broadcast Storm Control feature for the switch, type **T** to set Threshold.

   The following prompt is displayed:

   `Enter Threshold Level >`

   The values available for the threshold level are:

   L - Low (1000 64-byte packets per second)
   M - Medium (2000 64-byte packets per second)
   H - High (5000 64-byte packets per second)

   The default threshold level is Low.

6. Select a threshold level.

Chapter 15

Port Statistics

This chapter contains the procedure for displaying data traffic statistics. This chapter includes the following section:

❑ **Displaying Port Statistics** on page 140

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **S** to select Statistics.

   The Statistics Menu is displayed in Figure 37.

```
AT-8326GB Local Management System
 Main Menu -> Statistics Menu
 Stack ID: 1     Port: 1     Elapsed Time Since System Up: 000:02:37:12
 <Counter Name>       <Total>                    <Avg./s>
 Total RX Bytes       0                          0
 Total RX Pkts        0                          0
 Good Broadcast       0                          0
 Good Multicast       0                          0
 CRC/Align Errors     0                          0
 Undersize Pkts       0                          0
 Oversize Pkts        0                          0
 Fragments            0                          0
 Jabbers              0                          0
 Collisions           0                          0
 64-Byte Pkts         0                          0
 65-127 Pkts          0                          0
 128-255 Pkts         0                          0
 256-511 Pkts         0                          0
 512-1023 Pkts        0                          0
 1024-1518 Pkts       0                          0
 ------------------------------ <COMMAND> --------------------------
 [S]elect/[N]ext/[P]rev/[I]D. Port  Since [r]eset  S[t]op refresh  [Q]uit
 Command> _
 Enter the character in square brackets to select option
```

Figure 37 Statistics Menu

By default, the Statistics Menu displays the statistics for Port 1 on the master switch in a switch stack.

2. From the Statistics menu, type **S** to select a port.

   The following prompt is displayed:

   `Select port number>`

3. Enter the number of the port whose statistics you want to view. Press Return. The default Statistics Menu will be for Port 1.

4. To view the statistics for a port on another switch in a switch stack, first type **I** and then enter that switch's Stack ID. Then follow steps 2 and 3 above.

5. To clear the counters on the port and return them to 0, type **R** for Reset. To view the statistics for the port since the switch has been up, type **U** for since Up.

The Statistics Menu for a selected port is displayed in Figure 37.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option

Main Menu -> Statistics Menu
Stack ID: 1 Port: 9 Elapsed Time Since System Up: 000:01:00:30
<Counter Name>        <Total>                    <Avg./s>
Total RX Bytes        4606604                    1269
Total RX Pkts         25508                      7
Good Broadcast        19790                      5
Good Multicast        5522                       1
CRC/Align Errors      0                          0
Undersize Pkts        0                          0
Oversize Pkts         0                          0
Fragments             0                          0
Jabbers               0                          0
Collisions            0                          0
64-Byte Pkts          9150                       2
65-127 Pkts           9268                       2
128-255 Pkts          1839                       0
256-511 Pkts          5496                       1
512-1023 Pkts         14                         0
1024-1518 Pkts        0                          0
---------------------- <COMMAND> --------------------
[S]elect/[N]ext/[P]rev/[I]D. Port Since [r]eset S[t]op refresh [Q]uit

Command> _

Enter the character in square brackets to select option
```

Figure 38 Port Statistics Menu

The information in the Statistics Menu is for viewing purposes only. The statistics are defined below:

Total RX Bytes
Number of bytes received on the port.

Total RX Packets
Number of packets received on the port.

Good Broadcast
Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
The number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1023-1518 Pkts
Number of 1023- to 1518-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.

Chapter 16

Management Software Updates

This chapter explains how to obtain new versions of the AT-S41 management software and how to download the software onto an AT-8326GB switch.

You can download new management software onto a switch using either of the following methods:

❏ Local management session

❏ Trivial File Transfer Protocol

Sections in the chapter include:

❏ **Obtaining Software Updates** on page 144

❏ **Downloading New Management Software from a Local Management Session** on page 145

❏ **Downloading a New Management Software Image Using TFTP** on page 148

Obtaining Software Updates

New releases of the AT-S41 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com and from our FTP server at ftp.alliedtelesyn.com. To log on to the FTP server, enter "anonymous" for the user name and your email address for the password. Management software for the AT-8326GB switch will have "S41" as part of the filename.

Downloading New Management Software from a Local Management Session

This section contains the procedure for downloading a new version of AT-S41 management software onto a switch from a local management session. The procedure takes approximately 7 to 10 minutes to complete.

> **Note**
> You cannot perform this procedure from a Telnet or Web browser management session.

> ⚠️ **Caution**
> The switch will not forward Ethernet traffic during the software download and initialization process.

> **Note**
> The current configuration of the switch (e.g., IP address, subnet mask, and virtual LANs) is maintained when you install a new software image on the switch. To return a switch to its default configuration, refer to **Resetting the Management Software Default Values** on page 44.

This procedure assumes that you have already obtained the new version of management software and have stored it on the computer from which you will be performing this procedure.

To download a new software onto an AT-8326GB switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Local Management Session** on page 28.

2. From the Main Menu, type **T** to select Switch Tools.

3. From the Switch Tools Configuration Menu, type **U** to select Software Upgrade.

4. From the Software Upgrade Menu, type **X** for XModem Software Upgrade.

The XModem Software Upgrade Menu is displayed in Figure 39.

```
AT-8326GB Local Management System
Enter the character in square brackets to select option

Software Upgrade -> XModem Software Upgrade Menu

Image Version/Date:    1.00E/Jan 15 2002 19:48:12

Baud Rate :            9600bps
Image File Name:
Image File Type:       Binary

----------------------- <COMMAND> -----------------------

[U]pgrade Image and Reboot
[Q]uit to previous menu



Command> _

Enter the character in square brackets to select option
```

Figure 39 XModem Software Upgrade Menu

5. Type **U** to select Upgrade Image and Reboot.

   The following prompt is displayed:

   ```
   Download file (Y/N)>
   ```

6. To continue with the procedure, type **Y** for Yes. To cancel the procedure, type **N** for No.

   If you select to continue, go to the next step to complete the procedure.

7. Begin the file transfer.

   Note
   The following steps show how you would transfer the file using the Hilgraeve HyperTerminal program.

   ---

8. From the local management window, select Transfer from the menu. Then select Send File from the pull-down menu.
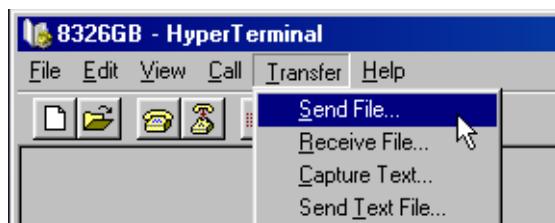
Figure 40 Local Management Window

The Send File pop-up window is displayed in Figure 41.
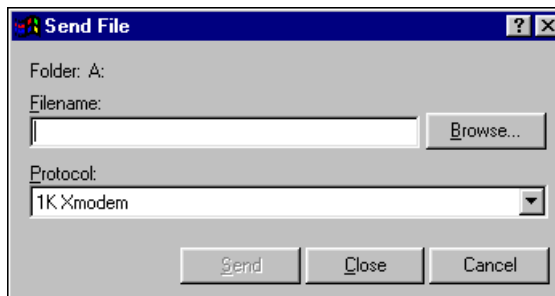
Figure 41 Send File Window

9. Click the Browse button on the Send File window to specify the location of the software.

10. Click on the Protocol field and set to 1K Xmodem transfer protocol.

11. Click Send.

The software immediately begins to download onto the switch's CPU. As this process begins, the Xmodem File Send window displays current status of the software download. This process will take minutes to complete.

The XModem File Send window is displayed in Figure 42.
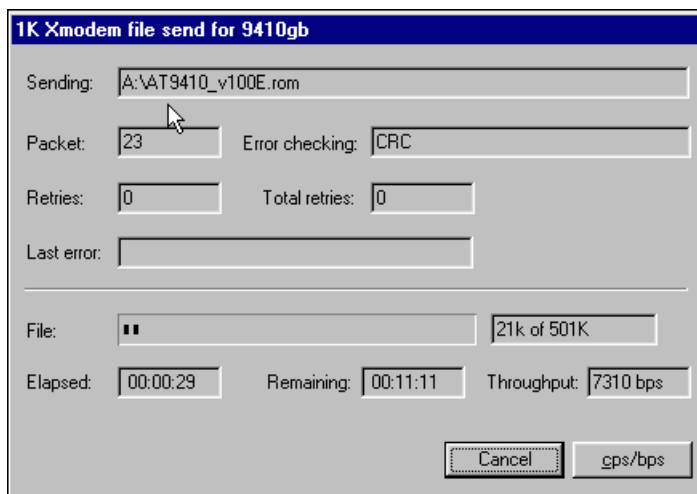
Figure 42 XModem File Send Window

Once the new software download process has completed, the switch begins to initialize the software. This process takes a few minutes. Once the initialization process is complete, the switch will automatically reboot.

Note
Do not interrupt the initialization process.

Downloading a New Management Software Image Using TFTP

TFTP software is available from various sources and is included in SNMP which can be purchased through Allied Telesyn. A command line version is included in most UNIX variants and in Windows NT. Please consult the documentation or the manufacturer of the software used on the proper use of the software.

You will need to provide the following information when using TFTP client software to download the AT-S41 software image:

❑ Set TFTP Server IP Address

❑ Set Image File Name

❑ Upgrade Image and Reboot

❑ Set Retry Count

This procedure assumes that you have already obtained a copy of TFTP software and have stored it on the computer from which you will be performing this procedure.

To download the new AT-S41 software image onto your AT-8326GB switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Local Management Session** on page 28.

2. From the Main Menu, type **T** to select Switch Tools.

3. From the Switch Tools Configuration Menu, type **U** to select Software Upgrade.

4. From the Software Upgrade Menu, type **T** for TFTP Software Upgrade.

The TFTP Software Upgrade Menu is displayed in Figure 43.

```
AT-8326GB Local Management System
Main Menu -> Software Upgrade Menu

Image Version/Date:    1.00F/Jan 15 2002 19:40:11

TFTP Server IP:        0.0.0.0
Image File Name:
Retry Count:           5

------------------------------ <COMMAND> ----------------

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image and Reboot
Set [R]etry Count
[Q]uit to previous menu



Command> _
Enter the character in square brackets to select option
```

Figure 43 TFTP Software Upgrade Menu

You will need to provide the following information when using the TFTP client software to download the AT-S41 software image. The options in the window are defined below.

Set TFTP [S]erver IP Address
This is the IP address of the server from which you are downloading the new software.

Set Image [F]ile Name
The path and filename of the software that is to be downloaded onto the switch. The filename of the software should be "ATS41.img". If necessary, change the filename of the image.

[U]pgrade Image and Reboot
Upgrades the new image to your switch and reboots the switch.

Set [R]etry Count
The amount of times your system will try to download the image using FTP. The Set Retry Count range is 1 - 20. The default setting is 5.

5. Open the TFTP client software and select the current directory where the software image is located.

6. Return to the local management software upgrade menu as displayed in Figure 43.

7. Type **U** to select Upgrade Image and Reboot.

The following prompt is displayed:

```
Download file (Y/N)>
```

8. Type **Y** to select Yes.

   The software immediately begins to download onto the switch's CPU. This process will take seconds to complete.

   Once the new software download process has completed, the switch begins to initialize the software. This process takes a few minutes. Once the initialization process is complete, the switch will automatically reboot.

Section III

Web Browser Management

The chapters in this section explain how to manage an AT-8326GB Fast Ethernet switch using a Web browser. The chapters include:

Chapter 17
Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-8326GB stack using a Web browser such as Microsoft Internet Explorer or Netscape Navigator.

Starting a Web Browser Management Session

This section explains how to start a Web browser management session.

Note
In order for you to manage an AT-8326GB stack using a Web browser, the switch must have an IP address. Initially assigning an IP address to a switch can only be done through a local management session. For instructions, refer to **Configuring an IP Address** on page 34.

To start a Web browser management session, perform the following procedure:

1. Start your Web browser.

2. Enter the IP address of the switch you want to manage in the URL field of the Web browser, as shown in Figure 44. To manage an AT-8326GB switch stack, enter the IP address of the master switch of the stack.

Switch's IP Address
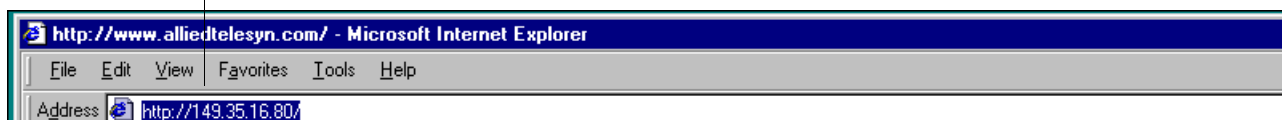
Figure 44 Entering a Switch's IP Address in the URL Field

3. When prompted, enter the login name and password. The default user name and the default password are both "manager". (The login name and password are case-sensitive.)

    To change the login name or password, refer to **Setting the User Interface Configuration** on page 38.

The management software home page will appear, as displayed in Figure 45.
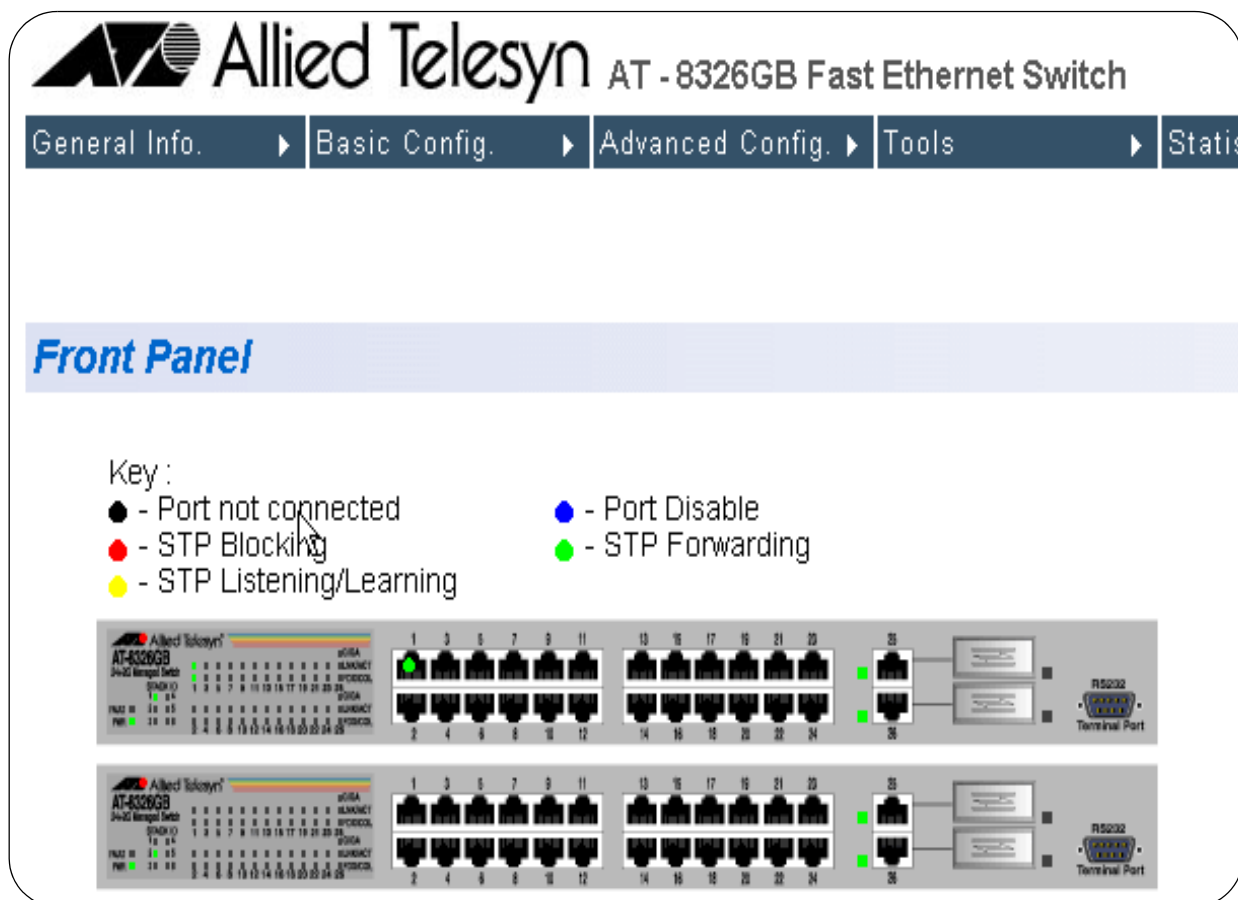
Figure 45 Management Software Home Page

This is the home page of the management software. The menu tabs are visible at the top of the home page:

❑   General Info

❑   Basic Config

❑   Advanced Config

❑   Tools

❑   Statistics

Note
A Web browser management session remains active even if you link to other sites. You can return to the management Web pages at any time as long as you do not close the browser window.

Browser Tools   You can use your browser's **bookmark** feature to remember frequently-used menu pages.

Quitting from a Web Browser Management Session   To exit from a Web browser management session, close the Web browser.

Chapter 18

Basic Switch Parameters

The procedures in this chapter explain how to set the following switch parameters:

Configuring an IP Address

> **Note**
> For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8326GB switch, refer to **When Does an AT-8326GB Switch Need an IP Address?** on page 33.

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch, as well as how to enable DHCP. If you want the switch to obtain its IP configuration from a DHCP server on your network, go to the procedure **Activating DHCP** on page 163.

To manually change a switch's IP configuration, perform the following procedure:

1. Click on the Basic Config menu tab and select IP Config from the sub-menu.

   The IP Configuration page is displayed, as shown in Figure 46.

Figure 46 IP Configuration Page

2. Change the IP configuration parameters by entering the new information in the data entry fields and clicking the Apply button.

   The parameters on the IP Configuration page are described below:

   System MAC Address
   This parameter specifies the MAC address of the switch. This parameter cannot be changed.

System IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a Web browser, a Telnet utility, or an SNMP management program.

System Subnet Mask

This parameter specifies the subnet mask for the switch.

System Default Gateway

This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

Enable/Disable DHCP Mode

This parameter allows you to enable and disable DHCP mode. DHCP is disabled by default. To learn more about DHCP mode, see **Activating DHCP** on page 163.

Configuring System Administration Information

The procedure in this section explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the switch.

To set a switch's administration information, perform the following procedure:

1. Click on the Basic Config menu tab and select Admin Config from the sub-menu.

   The Administration Configuration page is displayed, as shown in Figure 47.

Figure 47 Administration Configuration Menu

2. Change the parameters as desired, by entering the new information in the data entry fields and clicking the Apply button.

   The parameters on the Administration Configuration page are described below:

   System Description
   This parameter specifies the model name of the switch. This parameter cannot be changed.

   System Object ID
   This parameter specifies the numeric ID of the switch. This parameter cannot be changed.

System Name

This parameter specifies a name for the switch (for example, Sales). This parameter is optional and may contain up to 50 characters.

Note

It is advised that you assign each switch a name. The names can help you identify the various switches when you manage them and can help you avoid performing configuration procedures on the wrong switch.

System Location

This parameter specifies the location of the switch. This parameter is optional and may contain up to 50 characters.

System Contact

This parameter allows you to specify the name of the network administrator responsible for managing the switch. This parameter is optional and may contain up to 50 characters.

Setting the User Interface Configuration

The procedure in this section explains how to set the user interface or security features of the switch, including idle timeouts and how to enable and disable the different management session options.

To set a switch's user interface configuration, perform the following procedure:

1. Click on the Basic Config menu tab and select User Interface from the sub-menu.

   The User Interface page is displayed, as shown in Figure 48.

Figure 48 User Interface Configuration Page

2. Change the parameters as desired and click the Apply button.

   The parameters on the User Interface page are described below:

   Console UI Idle Timeout
   This parameter causes the management software to automatically end a management session if it does not detect any activity from the local management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console timeout value is 5 minutes. You can set the timeout for between 0 and 60 minutes.

Telnet UI Idle Timeout
This parameter causes the management software to automatically end a management session if it does not detect any activity from the remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the Telnet timeout value is 5 minutes. You can set the timeout for between 0 and 60 minutes.

Enable/Disable Telnet Server
You can disable the Telnet management feature on the switch, and so prevent individuals from managing the switch remotely using a Telnet session.

Enable/Disable Web Server
You can disable the Web browser management feature on the switch, and so prevent individuals from managing the switch remotely using a Web browser.

Enable/Disable SNMP Agent
You can disable the SNMP management feature on the switch, and so prevent individuals from managing the switch remotely using an SNMP agent.

Note
You cannot change the user name and password in a Web management session. For instructions on how to change the user name and password in a local management session, refer to **Setting the User Interface Configuration** on page 38.

Activating DHCP

This application protocol was developed to simplify network management. It is used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and, in some instances, a default gateway address.

The AT-8326GB Fast Ethernet switch supports this protocol and can obtain its IP configuration information from a DHCP server on your network. If you activate this feature, the switch will seek its IP address, subnet mask, and default gateway from a DHCP server residing on your network.

Most DHCP services allow you to specify whether the IP address assignment from the server is to be static or dynamic. If you choose static, the server will always assign the same IP address to the switch when the switch is reset or powered on. If you choose dynamic, the server will assign an unused IP address from its list of potential IP addresses each time the switch is reset or powered on.

> **Note**
> The DHCP option is disabled by default on the switch.

To activate or deactivate the DHCP protocols on the switch, perform the following procedure:

1. Click on the Basic Config menu tab and select IP Config from the sub-menu.

2. The IP Configuration page is displayed, as shown in Figure 46 on page 157.

3. Select Enable from the DHCP pull-down menu. DHCP is disabled by default on the switch.

4. Click the Apply button.

5. Reboot the switch using either the management software or by powering ON the switch.

Configuring SNMP Community Strings and Trap IP Addresses

To configure the SNMP community strings for the switch and to assign up to four IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. Click on the Basic Config menu tab and select SNMP Config from the sub-menu.

    The SNMP Configuration page is displayed, as shown in Figure 49.

Figure 49 SNMP Configuration Page

2. Adjust the parameters as desired. To change a value, change the information in the data entry fields or pull-down menus and click the Apply button. The parameters are described below.

    SNMP Read Community
    This parameter specifies the SNMP read community name. The maximum length for a read community name is 20 characters. This parameter is public.

    SNMP Write Community
    This command specifies the SNMP write community name. The maximum length for a read community name is 20 characters. This parameter is private.

    Enable/Disable Authentication Trap
    This command specifies a community's trap authentication.

SNMP Trap Receivers: IP Address
Allows you to add up to four SNMP trap receivers.

SNMP Trap Receivers: Community
Allows you to add a community name for each SNMP trap receiver.

Enable/Disable/Delete SNMP Trap Receiver
Allows you to specify the status of a trap receiver or to delete the trap receiver.

Changes to the SNMP parameters are immediately activated on the switch.

3. To restore the switch's default SNMP settings, click the Restore button.

Resetting the Management Software Default Values

The procedure in this section returns all management parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

> **Note**
> The management software default values can be found in **Appendix A** on on page 235.

To return the management software to its default settings, perform the following procedure:

1. Click on the Tools menu tab and select System Reboot from the submenu.

   The System Reboot Configuration page will be displayed, as shown in Figure 50.

Figure 50 System Reboot Configuration

2. Select a Reboot Status of Start from the pull-down menu. The Reboot Status default setting is Stop.

3. Select a Reboot type of Reset to Factory Default from the pull-down menu.

4. Click the Apply button. The switch resets and reboots immediately.

Rebooting a Switch

To reboot a switch, perform the following procedure:

1. Click on the Tools menu tab and select System Reboot from the sub-menu.

   The System Reboot Configuration page will be displayed, as shown in Figure 51.
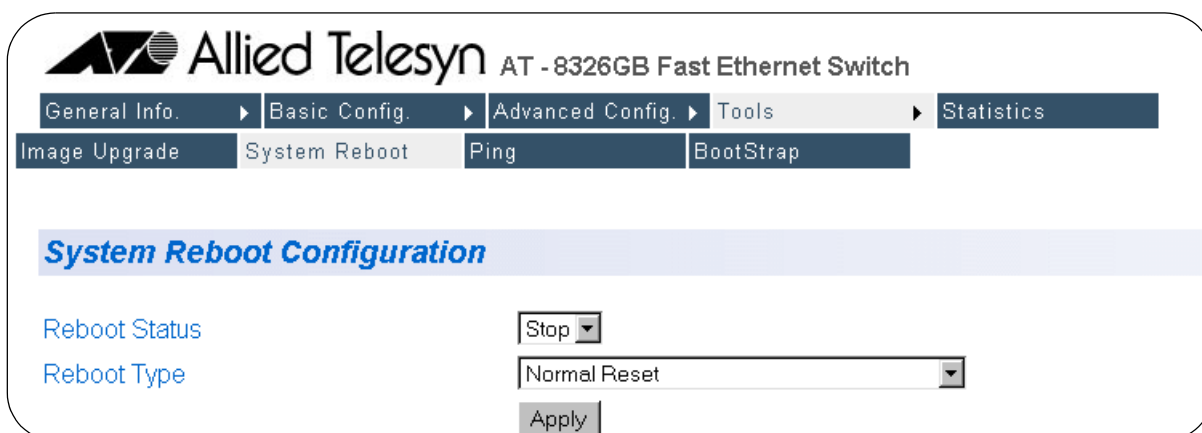
Figure 51 System Reboot Configuration

2. Select a Reboot Status of Start from the pull-down menu. The Reboot Status default setting is Stop.

3. Select a Reboot type from the pull-down menu. There are three Reboot Type options:

   Normal Reset
   Resets the switch and saves your configuration changes.

   Reset to Factory Default
   Resets the switch to its factory default settings. If you select this option, all of your configuration changes will be erased.

   Reset to Factory Default Except IP Address
   Resets the switch to its factory default settings except for the IP address you assigned to the switch.

4. Click the Apply button.

   The switch immediately reloads its operating system. This process will take a few minutes.

⚠ **Caution**
The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Viewing the AT-S41 Switch Information

The procedure in this section explains how to display general information about the switch.

To display the switch information, perform the following procedure:

1. Click on the General Info menu tab and select Switch Info from the sub-menu.

   The Switch Information page will be displayed, as shown in Figure 52.

Figure 52 Switch Information Page

There are not any configuration options on this page; it is for informational purposes only.

Ping Execution

To configure the ping execution settings on the switch, perform the following procedure:

1. Click on the Tools menu tab and select Ping from the sub-menu.

   The Ping Test Configuration page is displayed, as shown in Figure 53.

Figure 53 Ping Test Configuration Page

2. Adjust the parameters as desired. To change a value, enter the new information in the data entry field. The parameters are described below.

   Destination IP Address
   This command specifies the IP address of the end node you are pinging.

   Timeout Value
   The length of time for which the switch will continue to send pings if it does not receive a response. The default timeout setting is 3 seconds.

   Number of Ping Requests
   Number of ping attempts the switch should make before it stops pinging if it does not receive a response. The default number of ping requests is 10.

3. Click the Start button.

4. To view the ping results, click the Show Ping Results button.

    The Ping Test Result page is displayed, as shown in Figure 54.
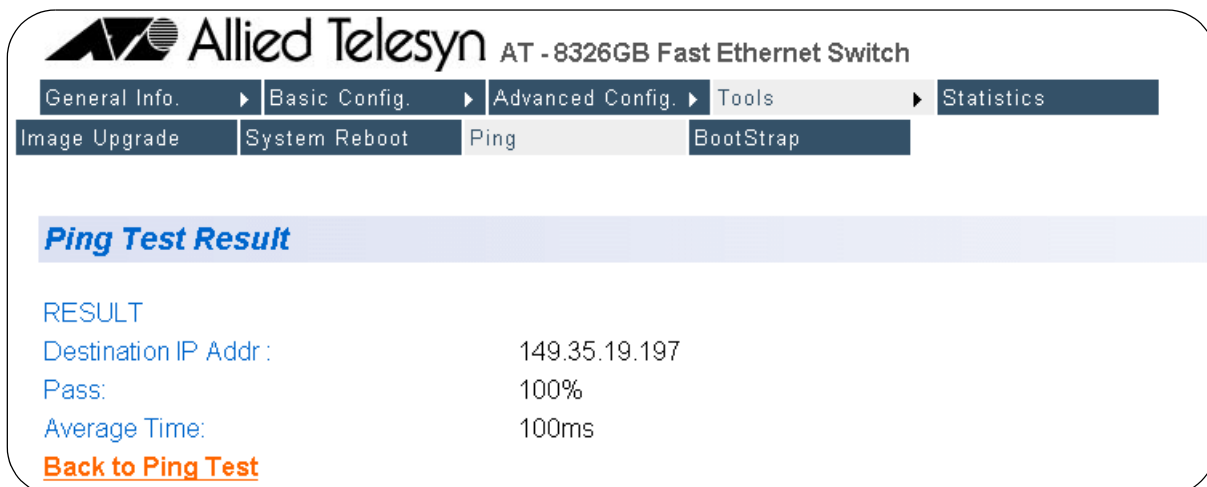
Figure 54 Ping Test Result Page

The parameters cannot be modified on this page. They are for informational purposes only. The parameters are described below.

Destination IP Address
This is the IP address you entered on the Ping Test Configuration page.

Pass
Number of successful pings.

Average Time
Average length of time for each ping request.

5. Use the Back to Ping Test link to return to the Ping Test Configuration page.

Bootstrap Configuration

The bootstrap feature allows you to download new software and configuration settings when you boot up the switch.

To configure the bootstrap settings on the switch, perform the following procedure:

1. Click on the Tools menu tab and select Bootstrap from the sub-menu.

    The Bootstrap Configuration page is displayed, as shown in Figure 55.
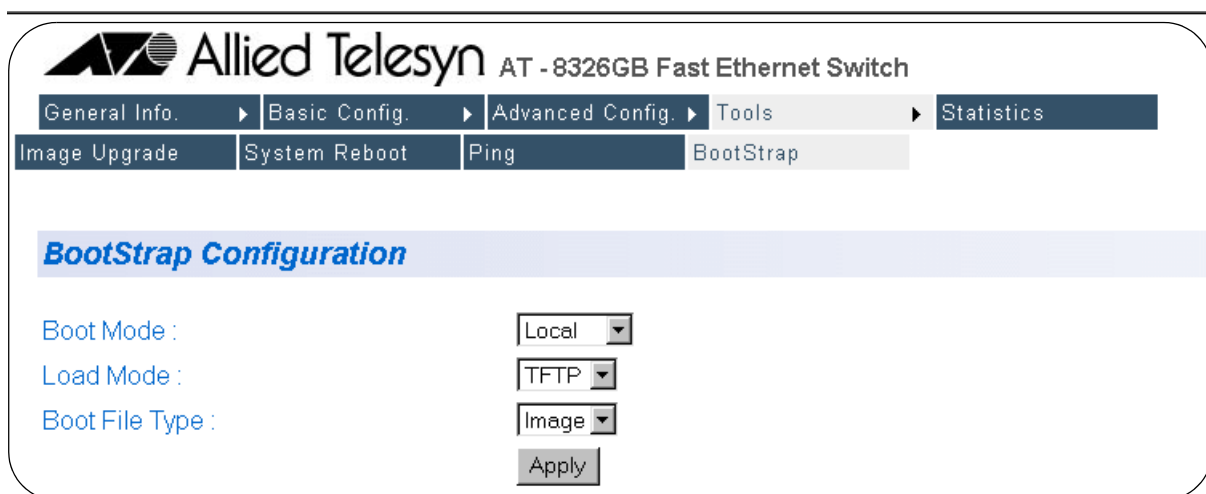
Figure 55 Bootstrap Configuration Page

2. Adjust the parameters as desired. To change a parameter setting, select the option from the pull-down menu and click the Apply button. The parameters are described below.

    Boot Mode
    Allows the user to determine how the switch should boot up. There are two boot load options: local and remote.

    > **Local**
    > If you choose the local boot load mode, the switch boots using the management software that is saved in the switch memory. This is the default boot load mode. If you are going to use the local boot load mode, you do not need to configure any of the other parameters on the Bootstrap Configuration Menu and the switch will not download any files when it boots up.

Remote
If you choose the remote boot load mode, the switch downloads software from a TFTP server and boots using the newly downloaded management software.

Load Mode
If you are using the remote boot load mode, you need to specify how the switch should download the new management software. There are two boot mode options: DHCP and TFTP.

DHCP
If you choose the DHCP boot mode, the switch will use DHCP to determine the switch IP address, the TFTP server address, and the image or configuration file name. The switch will use this information to download the management software from the TFTP server.

TFTP
If you choose the TFTP boot mode, the switch will use the IP address that you assigned to the switch on the System IP Configuration Menu as well as the TFTP server address and the image or configuration file name that you entered in the TFTP section of the Software Upgrade Menu.

Boot File Type
If you selected the remote boot load mode, you can choose what kind of files the switch will download while it is booting up. There are three file type options:

Image
An image file is the management software for the switch.

Configuration
A configuration file is a file that contains all of the existing configurations and settings for a switch. You can upload the configuration file and modify the switch settings and then download the configuration file back to the switch or onto multiple switches that you want to have the same configurations. The switch(es) will then update their configuration(s) based on the settings in the configuration file.

Image and Configuration
This option allows you to download both the management software and the configuration file.

Chapter 19

Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch. Examples of port parameters that you can adjust include duplex mode and port speed.

This chapter contains the following procedures:

❑ **Configuring Port Parameters** on page 174

❑ **Displaying Port Status** on page 178

❑ **Displaying Port Statistics** on page 181

Configuring Port Parameters

To configure the parameter settings for a port on a switch, perform the following procedure:

1. Click on the Basic Config menu tab and select Port Config from the sub-menu. Choose Port Config again in the next sub-menu.

   The Port Configuration page will appear, as displayed in Figure 56.

Figure 56 Port Configuration Page

2. Adjust the port parameter(s) that you want to configure. You can configure the parameters for only one port at a time.

   The parameters are described below:

   Port Index
   The port number.

   Trunk
   The trunk group number. A number in this column indicates that the port has been activated in a trunk. For instructions on how to create a port trunk, refer to **Port Trunks** on page 187.

Type

The port types. Ports 1-24 are 10/100Base-TX and can operate at 10/100 Mbps. Ports 25-26 are 1000Base-TX and can operate at 10/100/1000 Mbps.

Link Status

The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Admin. Status

The current operating status of the port.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. Possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for all of the ports on the switch.

Disabled - The port has been manually disabled.

Mode

The current operating settings of the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode. This is the default setting for all of the ports.

10-HDx - 10 Mbps in half-duplex mode

100-HDx - 100 Mbps in half-duplex mode

10-FDx - 10 Mbps in full-duplex mode

100-FDX - 100 Mbps in full-duplex mode

1000-FDx - 1000 Mbps in full-duplex mode

1000-HDx - 1000 Mbps in half-duplex mode

The 1000 Mbps settings can only be applied on Ports 25-26.

Flow Control

The current flow control setting on the port. The switch uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Possible values are:

Enabled - The port is allowed to use flow control. This is the default setting for all of the ports on the switch.

Disabled - The port is not configured to use flow control.

3. Once you have made the desired changes, click the Apply button.The switch immediately activates the parameter changes on the port.

Configuring Gigabit Port Type

Ports 25 and 26 can operate as either GBIC ports or 10/100/1000 Mbps twisted pair ports. The default port type setting is twisted pair. In order to change the use of these ports from one type to the other, the port type must be changed in the AT-S41 management software.

To configure a gigabit port type, perform the following procedure:

1. Click on the Basic Config menu tab and select Port Config from the sub-menu. Choose Giga Port Config in the next sub-menu.

   The Select Giga Port Type page will appear, as displayed in Figure 57.

Figure 57 Select Giga Port Type

2. Select the Stack ID of the switch on which you would like to change the gigabit port type configurations and click the Apply button to the right of the Stack ID pull-down menu.

3. Select TP (twisted pair) or GBIC from the Port Type pull-down menu for Port 25 or Port 26.

4. Click the Apply button to the right of the Port Type pull-down menu.

   The port type is changed immediately.

   Note
   When Port 25 or 26 has been set to operate as a GBIC port instead of a twisted pair port, the port mode cannot be changed in the Port Configuration Menu. The GBIC port is in a forced 1000 Mbps full-duplex mode.

Displaying Port Status

The procedure in this section displays the operating status of the ports on a switch. To display the status of a switch port, perform the following procedure:

1. Click on the General Info menu tab and select Front Panel from the sub-menu.

   The Front Panel page will appear, as displayed in Figure 58.
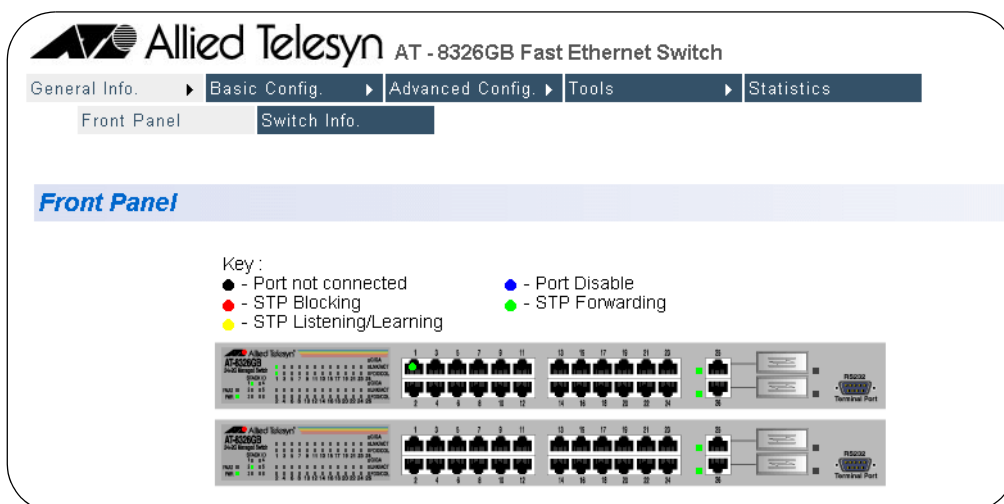
Figure 58 Front Panel Page

This page displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

2. Click on a port. You can select only one port at a time.

If you select a port, the Configuration of Port page is displayed, as shown in Figure 59.

Figure 59 Configuration of a Port

This page displays the port's configuration and operating status.

Set the port parameters as desired and click the Apply button. The parameters are described below.

Port Type
The port type. Ports 1-24 are 10/100Base-TX and can operate at 10/100 Mbps. Ports 25-26 are 1000Base-TX and can operate at 10/100/1000 Mbps.

Operation Status
The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Admin. Status
The current operating status of the port.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the

port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. Possible values are:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for all of the ports on the switch.

Disabled - The port has been manually disabled.

Speed Mode
The current operating settings of the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode. This is the default setting for all of the ports.

10-HDx - 10 Mbps in half-duplex mode

100-HDx - 100 Mbps in half-duplex mode

10-FDx - 10 Mbps in full-duplex mode

100-FDX - 100 Mbps in full-duplex mode

1000-FDx - 1000 Mbps in full-duplex mode

1000-HDx - 1000 Mbps in half-duplex mode

The 1000 Mbps settings can only be applied on Ports 25-26.

Flow Control
The current flow control setting on the port. The switch uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Possible values are:

Enabled - The port is allowed to use flow control. This is the default setting for all of the ports on the switch.

Disabled - The port is not configured to use flow control.

MAC Address
This specifies the MAC address of the port.

Priority
This parameter applies only when the switch is using STP. Priority is used as a tie-breaker when two or more ports have equal costs to the root bridge. The range is 0 - 255.
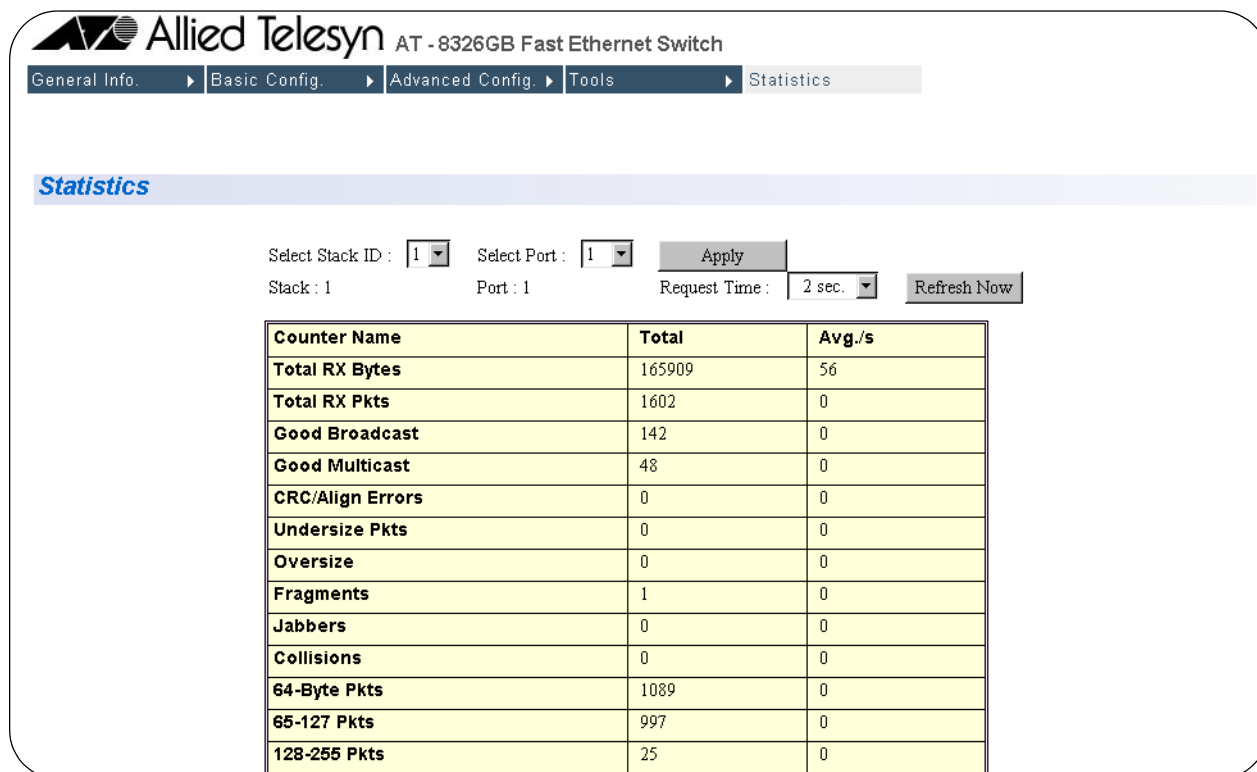
Path Cost
This parameter applies only when the switch is using STP. Path cost is used to decide which port has the lowest cost to the root bridge.

Displaying Port Statistics

The procedure in this section displays the statistics of a port on a switch. To display the statistics of a port, perform the following procedure:

1. Click on the Statistics menu tab.

   The Statistics page will appear, as displayed in Figure 60.

Figure 60 Statistics Window

2. To view the statistics for a port, select a port in the Select Port pull-down menu.

3. Click the Apply button.

   The information in the Statistics Menu is for viewing purposes only. The statistics are defined below:

   Total RX Bytes
   Number of bytes received on the port.

   Total RX Packets
   Number of packets received on the port.

   Good Broadcast
   Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
The number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1023-1518 Pkts
Number of 1023- to 1518-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.

Chapter 20

Port Security

This chapter explains how to configure port security.

Note
For background information on port security, refer to the **Port Security Overview** on page 59.

Configuring Port Security

To configure the switch's port security, perform the following procedure:

1. Click on the Advanced Config menu tab and select Port Security from the sub-menu. Choose Security Config from the next sub-menu.

    The Port Security page will appear, as displayed in Figure 61.

Figure 61 Port Security Page

2. Select the Stack ID for the switch whose port security you want to configure from the Stack ID pull-down menu. Then select the port on that switch whose security you would like to configure from the Port pull-down menu.

3. Then select a security mode for the port by checking one of the radio buttons below the Security Mode options: Normal, Limit, or Secure. For a description of these security levels, see the **Port Security Overview** on page 59.

    Note
    The default Security Mode is Normal.

4. If you selected the Limit security mode, you can set a threshold or specific limit on the maximum number of dynamic MAC addresses the port can learn. The threshold is automatically set to 1 until you change it in the Threshold data entry field. Enter the number of dynamic MAC addresses (between 1 and 170) you want the port to be able to learn.

Note
A threshold cannot be set for the port if the Security Mode is set to Normal or Secure. If a port has Normal or Secure security set, it is unable to learn dynamic MAC addresses and has a threshold of 0.

---

5. To control what happens on the port once the threshold has been met, check one of the radio buttons next to the intrusion detection notification options.

   The notification options are:

   No action

   Disable the port only

   Notify with trap only

   Notify with trap and disable the port

6. To configure the security for another port, select the Stack ID and port number from the pull-down menus at the top of the Port Security page and repeat this process.

7. To verify the new port security configurations and to see the security settings for all of the ports at once, continue to the next section: **Displaying Port Security Settings** on page 186.

Displaying Port Security Settings

To view the switch's port security settings, perform the following procedure:

1. Click on the Advanced Config menu tab and select Port Security from the sub-menu. Choose Security Overview from the next sub-menu.

2. The Port Security Overview page will appear, as displayed in Figure 62, allowing you to see the security settings for all of the ports on a switch.

Figure 62 Port Security Overview Page

3. To change any of the security settings for a port, click on the port number in the Port Index column on the left-hand side of the page. You will be taken to the Port Security page, where you can configure port security as described in the previous section.

Note
To view the port security settings for a different switch in your switch stack, use the Stack ID pull-down menu and the Apply button at the top of the page.

Chapter 21

Port Trunks

This chapter contains the procedures for creating or deleting a port trunk using a Web browser management session.

Note
For background information on port trunking, refer to the **Port Trunking Overview** on page 66.

Creating or Deleting a Port Trunk
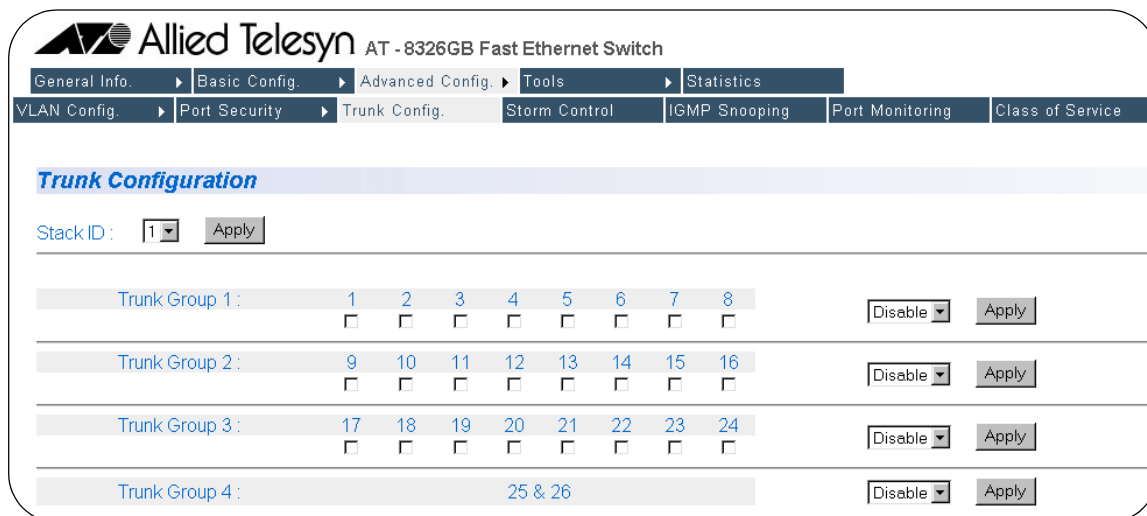
> ⚠️ **Caution**
> Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operations of your network.
>
> If you are deleting a port trunk, disconnect the cables from the ports before you delete the trunk. Deleting the trunk without first disconnecting the data cables can create a loop in your network topology, which can produce broadcast storms.

To create or delete a port trunk, perform the following procedure:

1. Click on the Advanced Config menu tab and select Trunk Config. from the sub-menu.

   The Trunk Configuration page will appear, as displayed in Figure 63.

Figure 63 Trunk Configuration Page

If the switch does not contain a port trunk, all of the ports on the switch will be un-checked. If there is a port trunk, the ports of the trunk will be checked.

2. To create a port trunk, do the following:

   a. Check the ports that will make up the port trunk. A port trunk can contain up to four ports. All of the ports in a port trunk must be in the same trunk group.

   b. Select Enable from the pull-down menu to the right of the trunk group that contains the port trunk members.

   c. Click the Apply button to the right of the port trunk group you enabled.

   The new port trunk is immediately activated on the switch.You can now connect the data cables to the ports of the trunk on the switch.

3. To delete a port trunk do the following:

   a. Deselect all port members of the trunk you want to delete.

   b. Select Disable from the pull-down menu to the right of the trunk group that contained the port trunk members.

   c. Click the Apply button to the right of the port trunk group you disabled.

Chapter 22

Port Monitoring

This chapter contains the procedure for enabling and disabling port monitoring.

Note

For background information on port monitoring, refer to **Port Monitoring Overview** on page 74.

Configuring Port Monitoring

To enable or disable port monitoring, perform the following procedure:

1. Click on the Advanced Config menu tab and select Port Monitoring from the sub-menu.

    The Port Monitoring Configuration page will appear, as displayed in Figure 64.

Figure 64 Port Monitoring Configuration Page

2. To configure port monitoring, do the following:

    a. Use the Monitoring Port pull-down menus to select the port to function as the port monitor and the stack ID for that port.

    b. Use the Port Being Monitored pull-down menus to select the port whose traffic is to be monitored and the stack ID for that port.

    c. Click the Apply button on the right-hand side of the page.

    d. Select Enable from the Monitoring Status pull-down menu and click the Apply button next to the Monitoring Status pull-down menu.

    Port monitoring is immediately activated on the switch. You can now connect a data analyzer to the monitoring port to monitor the traffic on the selected port.

3. To disable port monitoring, select Disable from the Monitoring Status pull-down menu and click the Apply button.

    The port monitor is disabled. The port that was functioning as the monitor port can now be used for normal network operations.

Chapter 23

Spanning Tree Protocol

This chapter explains how to configure the STP bridge parameters on an AT-8326GB Fast Ethernet switch from a Web browser management session.

Sections in the chapter include:

❑ **Configuring a Bridge's STP Settings** on page 193

❑ **Configuring STP Port Settings** on page 195

> **Note**
> For background information on STP, refer to the **STP Overview** on page 80.

Configuring a Bridge's STP Settings

⚠ **Caution**

STP on a bridge is disabled by default. If you enable STP, the bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure a bridge's STP parameters, perform the following procedure:

1. Click on the Basic Config menu tab and select Spanning Tree from the sub-menu. Choose STP Config from the next sub-menu.

    The Spanning Tree Bridge Configuration page will appear, as displayed in Figure 65.

Figure 65 Spanning Tree Bridge Configuration

2. Adjust the bridge STP settings as needed. The parameters are described below.

    Enable/Disable STP
    Enables and disables STP on the switch. The default setting is disabled.

Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Maximum Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. 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. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Forward Delay

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, resulting in network loops. The default is 15 seconds.

3. After you have made the desired changes, click the Apply button.

   Changes are immediately activated on the switch.

Configuring STP Port Settings

To display and configure the STP settings, perform the following procedure:

1. Click on the Basic Config menu tab and select Spanning Tree from the sub-menu. Choose STP Port Config from the next sub-menu.

   The Spanning Tree Port Configuration page will appear, as displayed in Figure 66.

Figure 66 Spanning Tree Port Configuration

2. Select the Stack ID of the switch on which you want to configure STP port settings and click the Apply button to the right of the Stack ID.

3. Adjust the parameter settings for a port as desired. The parameters are described below.

   The 8326GB Fast Ethernet switch has an "All" setting that allows a global setting to be set for all ports on the switch.

   Priority
   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0-255. The default value for priority is 128.

Note
Port priority cannot be set on ports that are part of a trunk group.

Path Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The default values for this parameter are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port.??? The range is 1 to 65535.

The following parameters are for display purposes only and cannot be changed from the Spanning Tree Port Configuration Menu.

Port Index
The port number. "All" indicates a setting that includes all ports on the switch.

Port Status
The current STP status of the port. Possible values are:

❑ Forwarding

❑ Listening

❑ Learning

❑ Blocking

Port Speed
This parameter indicates the operating speed of the port.

MAC Address
The MAC address of the port.

4. Click the Apply button to the right of the port settings.

Chapter 24

Virtual LANs

This chapter explains how to create, modify, and delete VLANs. This chapter also explains how to change a switch's VLAN operating mode.

> **Note**
> For background information on VLANs, refer to **Chapter 10, Virtual LANs**.

This chapter contains the following sections:

Creating a Tagged or Untagged VLAN

The procedure for creating a new VLAN is divided into the following phases:

❑ Phase 1: Assigning a VID and name and specifying the port members

❑ Phase 2: Converting tagged ports into untagged ports

Performing Phase 1 is required whenever you create a new VLAN. Every VLAN must have a name, VID, and, of course, ports. You will need to perform Phase 2 if some or all of the ports of a VLAN will be untagged ports. Ports that you want to function as untagged ports must be converted by changing their PVIDs, as explained in Phase 2.

To create a new VLAN, start by performing the procedure in Phase 1.

Note
The following procedures assume that the switch is operating in the 802.1Q VLAN mode. Only when the switch is operating in the 802.1Q mode can you create tagged and untagged VLANs. For instructions on how to change the switch's VLAN mode, refer to **Setting the VLAN Type** on page 213.

Phase 1   This phase assigns a VID and a name to your VLAN and also designates the VLAN port members.

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select Create VLAN from the next sub-menu.

   The Create/Modify VLAN page will appear, as displayed in Figure 67.
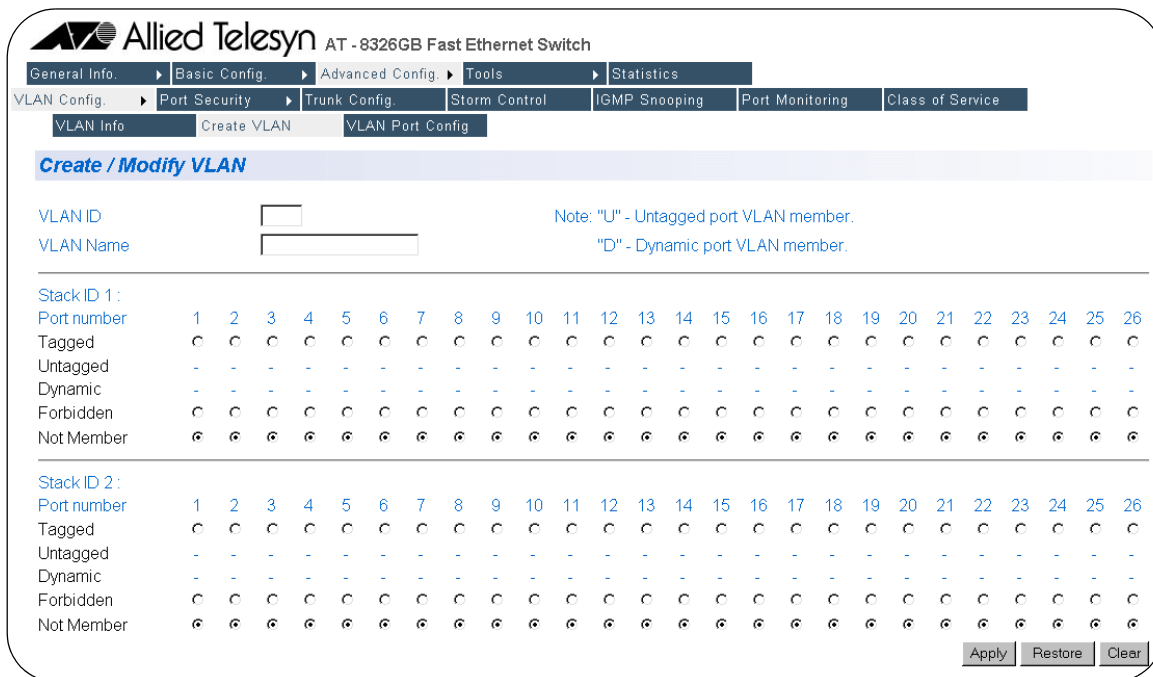
Figure 67 Create/Modify VLAN (802.1Q VLANs)

2. Enter a VLAN ID in the VLAN ID field.

   If this VLAN will be unique in your network, then its VID must also be unique from all other VIDs in the network.

   If this VLAN will be part of a larger VLAN that spans multiple stacks, than the VID value for the VLAN should be the same on each stack. For example, if you are creating a VLAN called Sales that will span three stacks, you must assign the Sales VLAN on each stack the same VID value.

   The VLAN ID must be a value between 2 and 4094.

3. Enter a name for the VLAN of up to 32 characters in the VLAN Name field.

   The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name spaces, but not special characters, such as asterisks (*) or exclamation points (!).

If the VLAN will be unique in your network, then the name should be unique as well.

If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

4. Select the Tagged port radio buttons for both the tagged and untagged ports that are to be members of the new VLAN. Do this for each switch in the stack that will contain ports for the new VLAN.

> **Note**
> The procedure in Phase 2 explains how to convert tagged ports into untagged ports by changing the PVIDs.

5. If you activated GVRP on the stack and you do not want certain tagged ports in the VLAN to participate in GVRP, click the Forbidden radio buttons of those tagged ports.

> **Note**
> The Not Member row is explained in the section **Viewing or Modifying a Tagged or Untagged VLAN** on page 203.

6. Click the Apply button.

You have now created a new VLAN. You gave it a VID and a name. You also specified which ports were to be members of the new VLAN.

However, it is important to note that, by default, all of the ports that you just added to the new VLAN are tagged ports, meaning they are shared ports. The ports are still members of their current VLANs.

If you want to convert the ports into untagged ports, you must perform the procedure in Phase 2.

> **Note**
> There are two additional buttons in the bottom right-hand corner of the page. The Restore button will cancel any changes you have made to the VLAN since using the Apply button. The Clear button removes all checks from all radio buttons, letting you select each port's configuration. If you leave any port columns blank when you click the Apply button, the management software will assign those ports to the Not Member row.

Phase 2   This phase to creating a new VLAN converts the tagged ports that you added to the new VLAN into untagged ports. This process involves changing the PVIDs of the ports so that they match the VID of the new VLAN. For example, if you assigned the new VLAN a VID of 4, you must change the PVIDs of the untagged ports to 4. The following procedure explains how this is accomplished.

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Port Config from the next sub-menu.

    The VLAN Port Configuration page will appear, as displayed in Figure 68.

Figure 68 VLAN Port Configuration

This page lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 6 all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

By default, this window initially displays the PVIDs for the ports on the master switch.

2. Use the Stack ID pull-down menu to select a switch in the stack that contains ports that you want to identify as untagged ports of the new VLAN. (You can skip this step to change to the master switch, since the master switch is selected by default.)

3. Enter a new PVID value in the PVID field for the port number whose PVID you want to change.

For example, if you wanted to make Port 5 an untagged port of a VLAN with a VID of 7, you would change the PVID for Port 5 to the value 7.

4. Click the Apply button.

    Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the new VLAN as an untagged port.

    If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

5. Repeat steps 2 and 4 to assign new PVIDs to any other ports in the stack that are to be untagged members of the new VLAN.

    This completes the procedure for creating a new VLAN. To confirm the creation of the new VLAN, go to the next procedure.

Viewing or Modifying a Tagged or Untagged VLAN

There are two phases to modifying a VLAN. You might need to perform both phases or just one, depending on what it is you want to change in the VLAN. The phases are:

❑ Phase 1: In this phase, you can view a VLAN's configuration, as well as change a VLAN's name and add or remove tagged ports.

❑ Phase 2: In this phase, you can add or remove untagged ports.

Phase 1   This phase explains how to display the Config VLAN Member Menu of a VLAN. You can use the page to view a VLAN's configuration as well as change a VLAN's name and add or remove tagged ports.

> **Note**
> If you do not want to change a VLAN's name or add or remove tagged ports, then skip this procedure and go straight to Phase 2 to add or remove untagged ports.

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Info from the next sub-menu.

   The VLAN Information will appear, as displayed in Figure 69

Figure 69 VLAN Information (802.1Q VLANs)

This page lists all of the VLANs that currently exist in the stack.

2. To view a VLAN's configuration or to make changes to a VLAN, click the Modify link in the right column for the VLAN you want to view or modify.

The VLAN Create/Modify page will appear, as displayed in Figure 70.
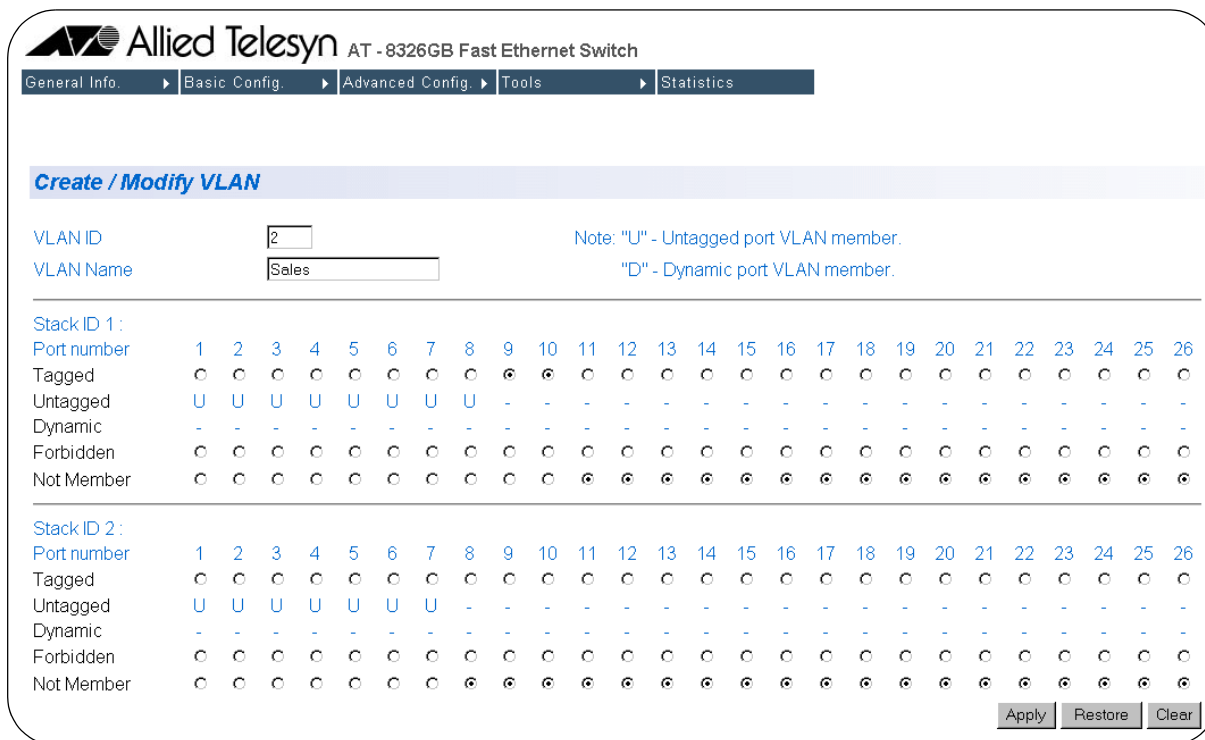
Figure 70 VLAN Create/Modify (802.1Q VLANs)

The rows on the page are defined below:

Tagged
A dot in a radio button indicates the corresponding port is a tagged member of the VLAN. For example, referring to the figure above, ports 9 and 10 on the master switch are tagged members of the VLAN.

Untagged
A 'U' for a port indicates that the port is an untagged member of the VLAN. For example, referring to the figure above, ports 1 through 8 on the master switch are untagged members of the VLAN.

Forbidden
A dot in a radio button indicates that the switch will not learn VLANs from the end node connected to the port. This applies only to tagged ports and only when GVRP has been activated on the switch.

Not Member
A selected radio button in this row indicates that the port is not a member of the VLAN.

3. To add a tagged port to the VLAN, click the Tagged radio button of the port.

> **Note**
> You cannot add untagged ports to a VLAN from this window. To add untagged ports, refer to **Phase 2**, below.

4. If you want to remove a tagged port from the VLAN, click the Not Member radio button of the appropriate port.

> **Note**
> You cannot remove untagged ports from a VLAN from this window. To remove untagged ports, refer to **Phase 2**, below.

5. If GVRP has been activated on the stack and you do not want the switch to learn new VLANs on a particular tagged port, click the Forbidden radio button of the appropriate tagged port.

6. After you have made the desired changes to the VLAN, click the Apply button.

Phase 2   You must perform this phase whenever you need to add or remove an untagged port from a VLAN. This phase explains how to change the PVIDs of the ports so that they match the VID of a different VLAN. For example, if you want to assign Port 2 as an untagged member of a VLAN with a VID of 4, you must change the PVID of the port to 4.

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Port Config from the next sub-menu.

    The VLAN Port Configuration page will appear, as displayed in Figure 68.

Figure 71 VLAN Port Configuration

This page lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 6 all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

By default, this page initially displays the PVIDs for the ports on the master switch.

2. Use the Stack ID pull-down menu to select a switch in the stack that contains ports that you want to identify as untagged ports of the new VLAN. (You can skip this step to change to the master switch, since the master switch is selected by default.)

3. Enter a new PVID value in the PVID field for the port number whose PVID you want to change.

For example, if you wanted to make Port 5 an untagged port of a VLAN with a VID of 7, you would change the PVID for Port 5 to the value 7.

4. Click the Apply button.

   Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the other VLAN as an untagged port.

   If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

5. Repeat steps 2 and 4 to assign new PVIDs to any other ports in the stack that are to be untagged members of the VLAN.

This completes the procedure for modifying a VLAN.

Deleting a Tagged or Untagged VLAN

To delete a VLAN, perform the following procedure:

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Info from the next sub-menu.

   The VLAN Configuration - Members page is displayed. This window lists all the VLANs that currently exist in the stack. An example of the window is shown in Figure 69 on page 203.

2. Click the Delete link in the right column for the VLAN you want to delete.

   A confirmation prompt is display.

3. Click OK to delete the VLAN or Cancel to cancel the procedure.

   If you click OK, the VLAN is deleted from the stack. All untagged ports in the VLAN are returned to the Default VLAN.

Creating a Port-based VLAN

To create a port-based VLAN, perform the following procedure:

> **Note**
> This procedure assumes that the switch is set to the Port-based VLAN Type. For instructions on how to change the VLAN mode on the switch, refer to **Setting the VLAN Type** on page 213.

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select Create VLAN from the sub-menu.

    The Create/Modify VLAN page will appear, as displayed in Figure 72.

Figure 72 Create/Modify VLAN (Port-based VLAN)

2. Enter a unique VLAN ID in the Index data entry field. The VLAN ID must be a value between 2 and 4094.

    Since the stack does not examine the VID in tagged headers of tagged frames when operating in the Port-based VLAN mode, this VID value does not need to be unique from all other VLANs in your network. It only needs to be unique from the other VLANs in the stack on which you are creating the VLAN.

3. Enter a VLAN name in the VLAN name text entry field. The name can be from 1 to 32 characters. The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

4. Select the check boxes for the ports you would like to include in the VLAN.

5. Click the Apply button in the bottom right-hand corner of the page.

Note

The ports that you just added to the new VLAN are not removed from their current VLAN assignments. You must remove the ports manually from the other VLANs if you do not want them to be shared. For instructions, refer to **Viewing or Modifying a Port-based VLAN** on page 211.

Note
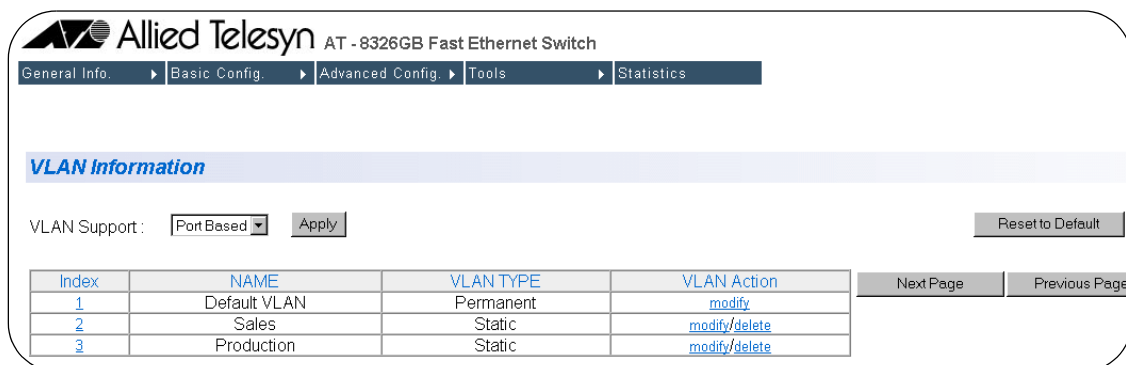
There are two additional buttons in the bottom right-hand corner of the page. The Restore button will cancel any changes you have made to the VLAN since using the Apply button. The Clear button removes all check marks from all check boxes, letting you re-start the port selection process.

Viewing or Modifying a Port-based VLAN

To view the configuration of a port-based VLAN or to modify a VLAN, such as to add or remove ports or to change the VLAN name, perform the following procedure:

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Info from the next sub-menu.

    The VLAN Information page will appear, as displayed in Figure 73
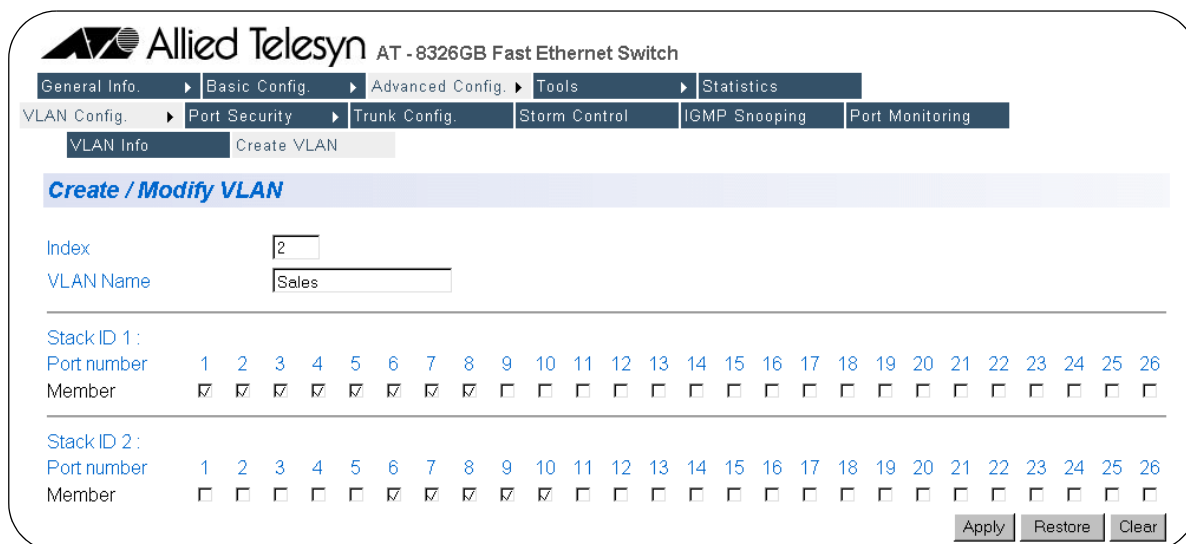
Figure 73 VLAN Information (Port-based)

This page lists the port-based VLANs in the stack.

2. Click the Modify link in the right column for the VLAN you want to view or modify.

    The Create/Modify VLAN page will appear, as displayed in Figure 74.

Figure 74 Create/Modify VLAN (Port-based VLANs)

The page indicates which ports in the stack are members of the VLAN. A check in a check box indicates that the port is a VLAN member. An empty box indicates that the port is not a VLAN member.

3. To change the VLAN's name, enter a new name in the VLAN Name text entry field. The name can be from 1 to 32 characters. The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). This menu item is optional; the management software does not require you to provide VLAN names.

4. To add or remove a port, click on the appropriate check box.

Note
You cannot remove ports from the Default VLAN unless they already belong to another VLAN. Additionally, port removed from other VLANs are returned to the Default VLAN.

Setting the VLAN Type

An AT-8326GB stack can operate in either the 802.1Q VLAN mode for creating tagged and untagged VLANs or the port-based VLAN mode.

Note
The VLAN Type default is 802.1Q.

To change a stack's VLAN Type, perform the following procedure:

1. Click on the Advanced Config menu tab and select VLAN Config from the sub-menu. Select VLAN Info from the next sub-menu.

   The VLAN Information page will appear, as displayed in Figure 69 on page 203.

2. Using the VLAN Support pull-down menu, select either 802.1Q to create tagged and untagged ports or Port Based to create port-based VLANs.

   Note
   The default is 802.1Q.

3. Click the Apply button.

   Note
   Changing the VLAN Type setting deletes all VLANs except the Default VLAN.

Chapter 25

MAC Address Table

This chapter contains instructions on how to view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

❑ **Viewing the MAC Address by Port** on page 215

❑ **Viewing the MAC Addresses by MAC** on page 216

❑ **Viewing the MAC Addresses of a VLAN** on page 218

❑ **Adding Static MAC Addresses** on page 220

❑ **Deleting Static MAC Addresses** on page 221

Note
For background information on the MAC address table, refer to the **MAC Address Overview** on page 116.

Viewing the MAC Address by Port

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You can also use this procedure to view any static MAC addresses that have been assigned to a port.

1. Click on the Basic Config menu tab and select Forwarding DB from the sub-menu. Choose Sort by Port from the next sub-menu.

    The Sort by Port page will appear, as displayed in Figure 75.

Figure 75 Sort by Port Window

2. Select the Stack ID for the switch whose MAC addresses you want to view.

3. Select the port whose static and dynamic MAC addresses you want to view from the Port Number pull-down menu.

4. Click the Apply button next to the Port Number.

    A page is displayed with the MAC addresses of the nodes on the port. The columns in the window and the definitions of the columns are the same as for the **Display MAC Address by MAC Menu** on page 119.

Viewing the MAC Addresses by MAC

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on all ports of a switch. This procedure will also let you view all static MAC addresses that have been assigned to the ports on the switch.

To view the MAC addresses by MAC on the switch, perform the following procedure.

1. Click on the Basic Config menu tab and select Forwarding DB from the sub-menu. Choose Sort by MAC from the next sub-menu.

1. The Sort by MAC page will appear, as displayed in Figure 76.

Figure 76 Sort by MAC

The management software displays a page with a list of all static and dynamic MAC addresses of the nodes of all ports. For definitions of the columns, refer to **Display MAC Address by MAC Menu** on page 119.

2. To search by MAC address, enter a MAC address into the Search MAC Address field and click the Apply button.

The page displays the corresponding port number for the entered MAC address.

3. To modify the aging time, enter a value in seconds in the Aging Time field and click the Apply button. The Aging Time setting is in the range of 10 to 1048 seconds. The default setting is 300 seconds.

    The management software immediately activates the new aging time value on all ports of the switch.

    For more information on setting the Aging Time, please refer to **Changing the Aging Time** on page 125.

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the end nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

Note
Viewing MAC addresses by VLAN is not supported in port-based VLAN mode.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. Click on the Basic Config menu tab and select Forwarding DB from the sub-menu. Choose Sort by VLAN from the next sub-menu.

   The Sort by VLAN page will appear, as displayed in Figure 77.

Figure 77 Sort by VLAN

Note
To perform this procedure, you need to know the VLAN ID number of the VLAN whose MAC addresses you want to view.

2. Enter the VLAN ID whose static and dynamic MAC addresses you want to view into the VLAN ID field.

3. Click the Apply button next to the VLAN ID field.

   The management software displays the MAC addresses of the nodes of all ports in the VLAN.

4. To modify the aging time, enter a value in seconds in the Aging Time field and click the Apply button. The Aging setting is in range of 10 to 1048 seconds. The default setting is 300 seconds.

   The management software immediately activates the new aging time value on all ports of the switch.

Adding Static MAC Addresses

The management software allows you to assign up to 256 static MAC addresses on an AT-8326GB switch.

To add a static address to the MAC address table, perform the following procedure:

1. Click on the Basic Config menu tab and select Forwarding DB from the sub-menu. Choose Static FDB from the next sub-menu.

   The Static MAC Address Configuration page will appear, as displayed in Figure 78.

Figure 78 Static MAC Address Configuration

2. Enter a MAC Address you want to configure in the MAC Address field.

3. Use the Stack ID pull-down menu to select the switch whose ports you want to configure.

4. Use the Port Number pull-down menu to select the port number you want to configure.

5. Enter a VLAN ID value in the VLAN ID field.

6. Click the Apply button.

   The management software adds the static address to the MAC address table for the specified port and VLAN.

7. Repeat steps 2, 3, and 5 to enter additional static MAC addresses.

Deleting Static MAC Addresses

To delete a static MAC address, perform the following procedure:

1. Click on the Basic Config menu tab and select Forwarding DB from the sub-menu. Choose Static FDB from the next sub-menu.

    The Static MAC Address Configuration window will appear, as displayed in Figure 79.

Figure 79 Static MAC Address Configuration

The management software displays all static addresses from the MAC address table.

2. Select the Delete option on the right side of the page for the MAC Address you want to delete.

    The management software deletes the static address you have selected from the MAC address table.

3. Repeat step 2 to delete additional static MAC addresses.

Chapter 26
Quality of Service

This chapter contains instructions on how to configure QoS. This chapter contains the following procedure:

❏ **Configuring QoS** on page 223

> **Note**
> For background information on QoS, refer to **Quality of Service Overview** on page 127.

Configuring QoS

> **Note**
> Quality of Service is not supported in port-based VLAN mode.

To configure QoS, perform the following procedure:

1. Click on the Advanced Config menu tab and select Quality of Service from the sub-menu.

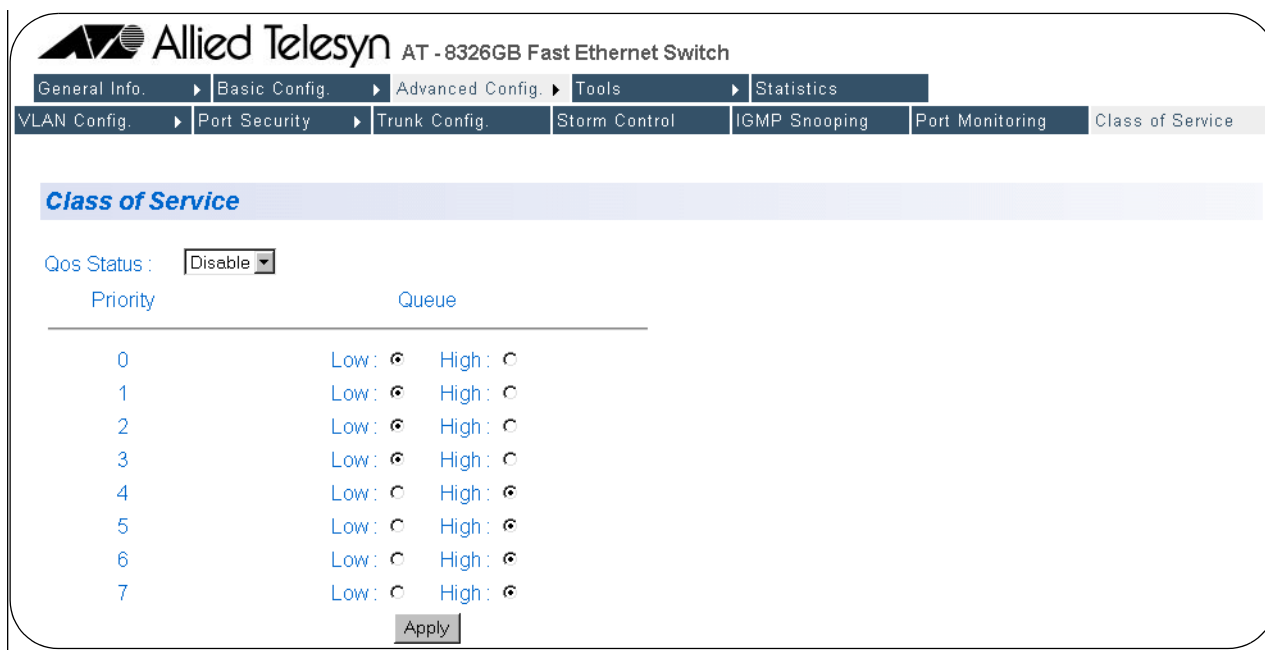   The Quality of Service page will appear, as displayed in Figure 80.

Figure 80 Quality of Service

2. Select a Low or High priority queue for the traffic classes whose priority you wish to change.

> **Note**
> The default setting for traffic classes 0 - 3 is the low priority queue. The default setting for traffic classes 4 - 7 is the high priority queue.

3. Select Enable from the QoS Status pull-down menu.

4. Click the Apply button.

    All tagged frames will be directed to either the low or high priority queue specified in Step 2.

Note
The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame exits the switch with the same priority level that it had when it entered.

Chapter 27

IGMP Snooping

This chapter explains how to activate and configure the IGMP snooping feature on the switch. Sections in the chapter include:

❏ **Activating IGMP Snooping** on page 226

❏ **Viewing Group Members** on page 228

> **Note**
> For background information on this feature, refer to **IGMP Snooping** on page 130.

Activating IGMP Snooping

To enable or disable IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. Click on the Advanced Config menu tab and select IGMP Snooping from the sub-menu.

   The IGMP Snooping page will appear, as displayed in Figure 81.

Figure 81 IGMP Snooping

The parameters on the IGMP Snooping page are defined below:

IGMP Snooping Status
Enables and disables IGMP snooping on the switch.

After selecting Enable or Disable, click the Apply button below the pull-down menus.

Age Out Timer
Specifies the time period in seconds after which the switch stops sending out multicast packets out of a port with an inactive host node. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 280 to 420 seconds. The default is 280 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

After entering a new time, click the Apply button below the pull-down menus.

VID

The VLAN ID of the VLAN the multicast group belongs to. This parameter will only be visible if you have created a VLAN.

Multicast Group Address

The multicast address of the group.

To view the members of the multicast group, click on the multicast address.
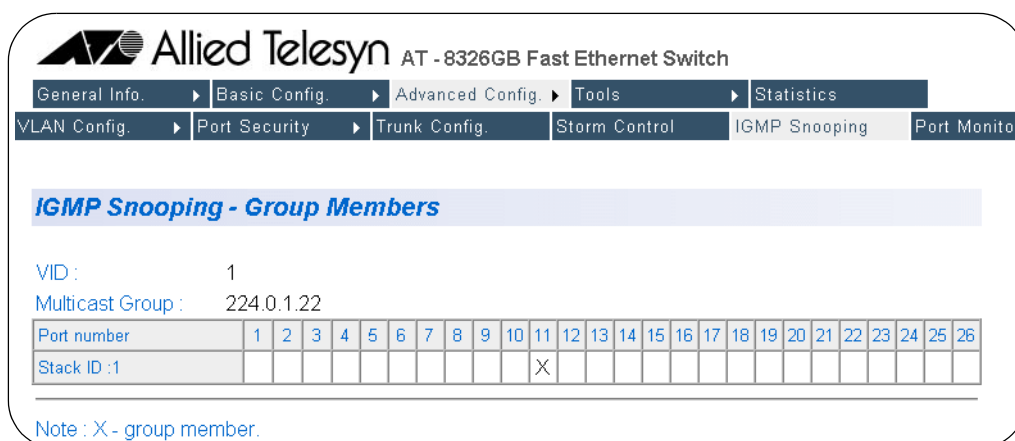
Viewing Group Members

You can use the AT-S41 software to display a list of the members of each multicast group on a switch. To display the list, perform the following procedure:

1. Click on the Advanced Config menu tab and select IGMP Snooping from the sub-menu.

   The IGMP Snooping page will appear, as displayed in Figure 81 on page 226.

2. Click on a multicast group address. The group members will appear on the IGMP Snooping Group Members page, as displayed in Figure 82.

Figure 82 IGMP Snooping Group Members

The information on this page is for viewing purposes only. The parameters are defined below:

VID
The VLAN ID of the VLAN the multicast group belongs to. This parameter will only be visible if you have created a VLAN.

Multicast Group Address
The multicast address of the group.

Port Number
The ports on the switch.

Stack ID
The stack ID of the switch. An X in this row indicates that the port in the corresponding column is a member of this multicast group.

Chapter 28

Broadcast Storm Control

This chapter contains instructions on how to configure the broadcast storm control feature on the switch.

Note
For background information on this feature, refer to **Broadcast Storm Control** on page 136.

Activating Broadcast Storm Control and Setting a Threshold

To activate broadcast storm control and set a threshold, perform the following procedure:

1. Click on the Advanced Config menu tab and select Storm Control from the sub-menu.

    The Broadcast Storm Control page will appear, as displayed in Figure 83.

Figure 83 Broadcast Storm Control Page

2. Select Enable from the Storm Control Status pull-down menu.

3. To set the threshold, select an option from the Threshold value pull-down menu.

    The values available for the threshold level are:

    Low (1000 64-byte packets per second)
    Medium (2000 64-byte packets per second)
    High (5000 64-byte packets per second)

    The default threshold level is Low.

4. Click the Apply button located below the pull-down menus to save your configuration choices.

Chapter 29

Management Software Updates

This chapter explains how to obtain new versions of the AT-S41 management software and how to download the software onto an AT-8326GB switch from a Web browser management session.

You can download new management software onto a switch using the Trivial File Transfer Protocol

Sections in the chapter include:

❑ **Obtaining Software Updates** on page 232

❑ **Downloading a New Management Software Image Using TFTP** on page 233

Obtaining Software Updates

New releases of the AT-S41 management software are available from the Allied Telesyn Web site at www.alliedtelesyn.com and from our FTP server at ftp.alliedtelesyn.com. To log on to the FTP server, enter "anonymous" for the user name and your e-mail address for the password. Management software for the AT-8326GB switch will have "S41" as part of the filename.

Downloading a New Management Software Image Using TFTP

TFTP software is available from various sources and is included in SNMP which can be purchased through Allied Telesyn. A command line version is included in most UNIX variants and in Windows NT. Please consult the documentation or the manufacturer of the software used on the proper use of the software.

You will need to provide the following information when using the TFTP client software to download the AT-S41 software image:

❑ Download Server IP

❑ Download File Name

This procedure assumes that you have already obtained a copy of TFTP software and have stored it on the computer from which you will be performing this procedure.

To download the new AT-S41 software image onto your AT-8326GB switch, perform the following procedure:

1. Establish a Web management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Web Browser Management Session** on page 153.

2. Click on the Tools menu tab and choose Image Upgrade from the sub-menu.

   The Image Upgrade page will appear, as displayed in Figure 84.

Figure 84 Image Upgrade Page

The parameters on the Image Upgrade page are defined below:

Image Version/Date
The software version and date currently on the switch.

File Type

❑ **Image**
An image file is the management software for the switch.

❑ **Configuration**
A configuration file is a file that contains all of the existing configurations and settings for a switch. You can upload the configuration file and modify the switch settings and then download the configuration file back to the switch or onto multiple switches that you want to have the same configurations. The switch(es) will then update their configuration(s) based on the settings in the configuration file.

❑ **Image and Configuration**
This option allows you to download both the management software and the configuration file.

Download Server IP
This is the IP address of the server from which you are downloading the new software.

Download File Name
The filename of the software that is to be downloaded onto the switch. The filename of the software should be "ATS41.img". If necessary, change the filename of the image.

3. Select a File Type form the pull-down menu.

4. Type the IP address into the Download Server IP field.

5. Type the software image name into the Download File Name field.

6. Open the TFTP client software and select the current directory where the software image is located.

7. Return to the Web management Image Upgrade page as displayed in Figure 84.

8. Click the Apply button to upgrade the image.

   The software immediately begins to download onto the switch's CPU. This process will take a few minutes.

   Once the new software download process has completed, the switch begins to initialize the software. The initialization process will take a few minutes. Once the initialization process is complete, the switch will automatically reboot.

Appendix A

AT-S41 Default Settings

This appendix lists the AT-S41 factory default settings.

Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
DHCP	Disabled
IGMP Snooping	Disabled
System Name	None
MAC Aging Time	300 seconds
Spanning Tree Protocol	
Status	Disabled
Bridge Priority	32768
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15
Twisted Pair Ports	
Status	Enabled
Duplex Mode	Auto-Negotiate
Speed	Auto-Negotiate
Flow Control	Enabled
Broadcast Control	Disabled
MDI/MDI-X	Auto
Security	Normal
Port Mirroring	Disabled

Setting	Default
Port Trunking	Disabled
Ports 25 and 26	
Port Type (GBIC or Twisted Pair)	Twisted Pair
VLANs	
Port-based and Tagged VLANs	Enabled
Default VLAN Name	Default VLAN (all ports)
VID	1
RS-232 Terminal Port	
Emulation Mode	VT100
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Data Rate	9600 bps
Key Mode	Terminal
Software Management Access	
Login Name	manager
Login Password	manager