Management Software

AT-S39

User's Guide

AT-8012M, AT-8012M-QS, AT-8016F/xx (MT, SC and ST), AT-8024, AT-8024GB, AT-8024M, AT-8026FC, AT-8026T, and AT-8088/xx (MT and SC)
FAST ETHERNET SWITCHES

VERSION 3.3.0

Allied Telesyn

PN 613-50245-00 Rev J

Table of Contents

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Section III
Web Browser Management 241

List of Figures

Preface

This guide contains instructions on how to configure an AT-8000 Series Fast Ethernet Switch using the AT-S39 management software.

The AT-8000 Series consists of the following Fast Ethernet switches:

- ❑ AT-8012M
- ❑ AT-8012M-QS
- ❑ AT-8016F/xx (MT, SC and ST)
- ❑ AT-8024
- ❑ AT-8024GB
- ❑ AT-8024M
- ❑ AT-8026FC
- ❑ AT-8026T
- ❑ AT-8088/xx (MT and SC)

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section contains just one chapter. It reviews the different ways that you can access the AT-S39 management software on a 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, from a workstation on your network.

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 installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at www.alliedtelesyn.com. You can view the documents on-line or download them onto a local workstation or server.

Contacting Allied Telesyn

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.

Email and Telephone Support

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

Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain a RMA number, contact Allied Telesyn's Technical Support at our 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 -> Worldwide Contacts.

Management Software Updates

You can download new releases of management software for our managed products from either of the following Internet sites:

- Allied Telesyn web site: **http://www.alliedtelesyn.com**
- Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

To download new software from the Allied Telesyn FTP server using your workstation's command prompt, you need FTP client software and you must log in to the server. Enter "anonymous" as the user name and your email address for the password.

Section I

Overview

The chapter in this section provides a brief overview of the AT-S39 management software. It explains some of the functions that you can perform with the management software and reviews different methods for accessing the AT-S39 software on an AT-8000 Series Fast Ethernet Switch.

Chapter 1
Overview

The AT-S39 management software is intended for the AT-8000 Series Fast Ethernet Switches. The software is used to monitor and adjust a switch's operating parameters. Some of the functions 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 mirrors
- ❑ Assign an Internet Protocol (IP) address and subnet mask
- ❑ Activate and configure a spanning tree protocol
- ❑ Activate enhanced stacking functions
- ❑ Configure Class of Service (COS)
- ❑ Enable and configure IGMP snooping
- ❑ Enable and configure broadcast storm control
- ❑ Download and upload image and configuration files
- ❑ Configure port security
- ❑ Enable port access control

The AT-S39 management software comes pre-installed on the switch with default settings for all operating parameters. If the default settings are adequate for your network, you can use the switch as an unmanaged switch simply by connecting the unit to your network, as explained in the hardware installation guide, and powering ON the device.

Note
The default settings for the management software can be found in Appendix A**,** AT-S39 Default Settings on page 331.

To actively manage a switch, such as to change or adjust the operating parameters, you must access the switch's AT-S39 management software. The AT-S39 software features a menu interface and a command line interface that make it very easy to use, and a special interface for managing a switch with a web browser.

There are four different ways to access the management software on an AT-8000 Series switch. In this guide, these methods are referred to as management sessions. They are:

- ❑ Local Management Session
- ❑ Telnet Management Session
- ❑ Web Browser Management Session
- ❑ SNMP Management Session

The following sections in this chapter briefly describe each type of management session.

Local Management Session

You establish a local management session with an AT-8000 Series switch by connecting a terminal or a PC with a terminal emulator program to the RS232 Terminal port on the front panel of the switch, using a straight-through RS-232 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, a menu is displayed and you can make selections to configure and monitor the switch. You can configure all of a 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 31.

A switch does not need an Internet Protocol (IP) address for you to manage it locally. You can start a local management session on a switch at any time. It will not affect the forwarding of frames by the device.

If you assign an AT-8000 Series switch an IP address and designate it as a master switch of an enhanced stack, you can will be able to manage all of the switches in the enhanced stack, all from the same local management session.

Note
For further information on enhanced stacking, refer to Enhanced Stacking Overview on page 58.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8000 Series switch. This type of management session is referred to in this guide as a remote management session because you do not have to be in the wiring closet where the switch you want to manage is located. You can manage the switch from any workstation on the network that has the application protocol.

To establish a Telnet management session with a switch, there must be at least one AT-8000 Series switch in the subnet that has been assigned an Internet Protocol (IP) address. Only one switch in a subnet needs to have an IP address. Once you have established a Telnet management session with the switch that has an IP address, you can use the enhanced stacking feature of the AT-S39 software to access all the other enhanced stacking switches in the same subnet.

Note
For further information on enhanced stacking, refer to Enhanced Stacking Overview on page 58.

Note
For instructions on how to start a Telnet management session, refer to Starting a Telnet Management Session on page 35.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage a switch. This too is referred to as remote management, just like a Telnet management session. You can manage a switch from any workstation on your network that has a web browser.

Note
For instructions on starting this type of management session, refer to Starting a Web Browser Management Session on page 242.

In order to start a web browser management session, there must be at least one enhanced stacking switch in the subnet with an IP address and whose stacking status has been set to master. Once you have started a management session on the master switch, you can manage all of the switches in the enhanced stack.

Note
For further information on enhanced stacking, refer to Enhanced Stacking Overview on page 58.

SNMP Management Session

Another way to remotely manage the switch is with an SNMP management program. A familiarity with Management Information Base (MIB) objects is necessary for this type of management.

The AT-S39 software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Interface Group MIB (RFC 1573)
- Ethernet MIB (RFC 1643)
- Remote Network MIB (RFC 1757)
- Allied Telesyn managed switch MIB

You must download the Allied Telesyn managed switch MIB (atistackinfo.mib and atiswitch.mib) file from the Allied Telesyn web site and compile the file with your SNMP program. For instructions, refer to your SNMP management documentation.

Note
SNMP management does not utilize the enhanced stacking feature. Consequently, you must assign an IP address to each switch to be managed with an SNMP program.

Management Access Levels

There are two levels of management access on an AT-8000 Series switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate password when you start an AT-S39 management session. To log in as a manager, type "manager" as the login and "friend" as the password. The default user name for operator is "operator" and the password is also "operator". The login names and passwords are case-sensitive.

Section II

Local and Telnet Management

The chapters in this section explain how to manage an AT-8000 Series switch from a local or Telnet management session. The chapters include:

Chapter 2

Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-8000 Series switch. The sections in the chapter are:

Local Management Session

On the front panel of the switch is a port labelled RS232 Terminal Port. You can use this port to establish a local (out-of-band) management session with the switch's AT-S39 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 to be managed from a local management session. You can start a local management session at any time on any AT-8000 Series switch in your network. A local management session does not interfere with the flow of Ethernet traffic through the unit.

Starting a local management session on a switch that has been configured as a Master switch allows you to manage all the switches in the enhanced stack from the same local management session. You do not have to start a separate local management session for each switch. This can simplify network management.

Starting a local management session on a switch that is not part of an enhanced stack or that is a slave switch allows you to manage just that switch.

Note
For information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Starting a Local Management Session

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

1. Connect one end of the straight-through RS232 management cable with a DB-9 connector to the RS232 Terminal Port on the switch. (The management cable is included with the switch.)

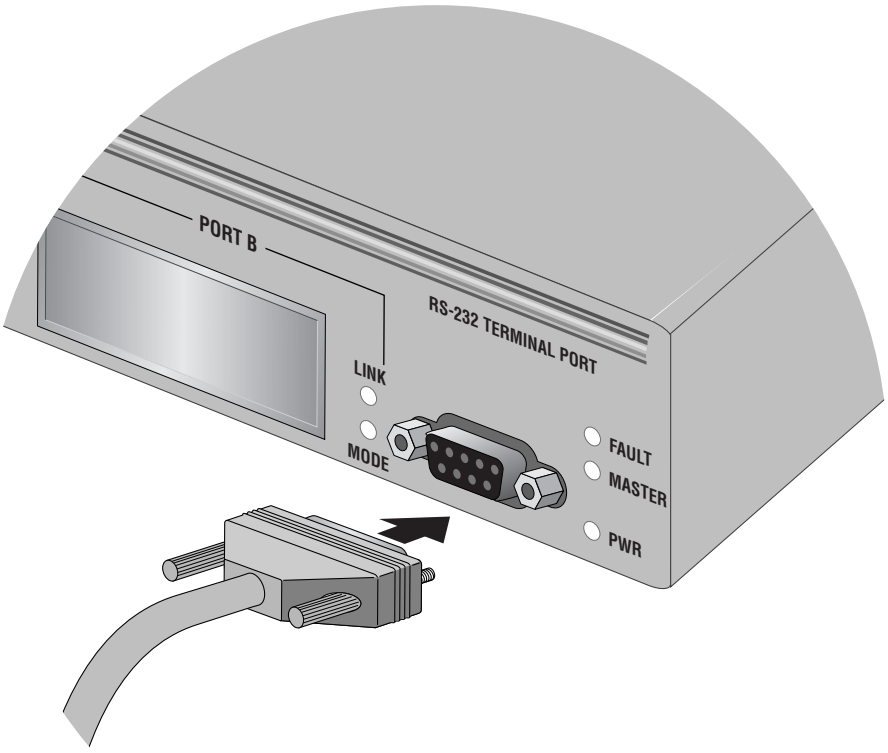

Figure 1 Connecting a Terminal or PC to the RS232 Terminal Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
   - ❑ Baud rate: 1200 bps to 115200 bps (default 9600; see Note below)
   - ❑ Data bits: 8
   - ❑ Parity: None
   - ❑ Stop bits: 1
   - ❑ Flow control: None

Note
The switch has an auto-detect feature on the serial port that automatically determines the speed of the local terminal. You activate this feature by pressing the Return or Enter key twice on your keyboard when you initially start the local interface or within five seconds after powering on or resetting the switch. The switch determines the speed of the terminal and automatically configures the speed of the RS232 Terminal Port accordingly. Otherwise, the switch uses a default baud rate of 9600 bits per second (bps). The switch maintains the terminal port speed until the system is again powered on or reset. The range of the port's baud rate is 1200 to 115200 bps.

Note
The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

Note
During boot up, the switch displays the following prompt: `Press <CTRL>B to go to Boot prompt`. This message is intended for manufacturing purposes only. (If you inadvertently display the boot prompt (=>), type **boot** and press Return to start the switch.)

4. Press the Return key twice.

   Prompts are displayed for a login name and password.

5. To view and change the switch's configuration, log in as a Manger. The login name is "manager" and the default password "friend". To just view the configuration, log in as an operator. The login name is "operator" and the default password is also "operator". Login names and passwords are case-sensitive. For information on the two access levels, refer to **Management Access Levels** on page 26. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51.

The Main Menu is shown in Figure 2.

```
Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
                  Sales Switch

Login Privilege: Manager
                     Main Menu

1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Config Menu
6 - MAC Address Tables
7 - Ethernet Statistics
8 - Diagnostics
9 - Enhanced Stacking
C - Command Line Interface

Q - Quit

Enter your selection?
```

Figure 2 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the Esc key or typing the letter **R** in a submenu or menu, returns you to the previous menu.

Please note the following:

- The Command Line Interface selection in the Main Menu is described in the **AT-S39 Command Line Interface User's Guide**.
- If the prompt "Manager$" or "Operator$" is displayed instead of the Main Menu, the management software has been configured to initially display the command line prompt instead of the Main Menu. To display the menu, type **menu** and press Return.

Enhanced Stacking

Starting a local management session on the master switch of an enhanced stack enables you to manage all the switches in the same enhanced stack from the same management session. This can save you the time and trouble of having to start a separate local management session each time you want to manage a switch in your network. It can also save you from having to go to the different wiring closets where the switches are located.

Starting a local management session on a slave switch or a switch that is not part of an enhanced switch allows you to manage just that switch.

For information on enhanced stacking and how to manage different switches from the same management session, refer to **Chapter 4, Enhanced Stacking** on page 57.

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 switch 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-8000 Series switch. This type of management is referred to as remote management because, unlike a local management session, you do not have to be in the wiring closet where the switch is located. You can use any workstation on your network with the application protocol to manage the switch.

In terms of functionally, there are almost no differences between managing a switch locally through the RS232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have nearly the same management capabilities.

Starting a Telnet management session requires that there be at least one enhanced stacking switch in your network that has an IP address and whose enhanced stacking status has been set to master. That switch is referred to as the master switch. Once you have started a Telnet management session on the master switch, you have management access to all enhanced stacking switches, including the AT-8000 Series switch, that reside in the same enhanced stack.

Note
For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Starting a Telnet Management Session

To start a Telnet management session, specify the IP address of the master switch of the enhanced stack in the Telnet application protocol and enter the management software password when prompted. The default password for manager access is "friend". The default password for operator access is "operator". Logins and passwords are case-sensitive. For information on the two access levels, refer to **Management Access Levels** on page 26. (For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51.)

The Main Menu of a Telnet management session is the same menu seen in a local management session, as shown in Figure 2 on page 33. You can perform nearly all the same functions from a local management session as you can from a Telnet management session.

The menus also function the same. To make a selection, type its corresponding number of letter. To return to a previous menu, type **R** or press ESC twice.

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 end a Telnet management session, return to the Main Menu and type **Q** for Quit.

Saving Your Parameter Changes

When you make a change to a switch parameter, the change is, in most cases, immediately activated on the switch as soon as you enter it. However, a parameter change is initially saved only to temporary memory by the switch and will be lost the next time you reset or power cycle the unit. To permanently save a change, you must select the S - Save Configuration Changes option. You should select that menu option whenever you have made a change to a switch parameter that you want the switch to retain even when it is reset or power cycled. If you do not see the menu option, then there are no parameter changes to be saved.

Chapter 3
Basic Switch Parameters

This chapter contains a variety of information and procedures. There is a discussion on when to assign an IP address to a switch and the different ways that you can go about it. There are also procedures for resetting the switch, activating the original switch default settings, and more.

Sections in the chapter include:

When Does a Switch Need an IP Address?

One of the tasks to building or expanding a network is deciding which of the managed switches need a unique IP address. In the past the rule was that a managed switch needed an IP address if you wanted to manage it remotely, such as with the Telnet application protocol or a web browser. However, if a network contained a lot of managed switches, having to assign each one an IP address was often cumbersome and time consuming. It was also often difficult keeping track of all the IP addresses.

The enhanced stacking feature of the AT-8000 Series, AT-8400 Series, and AT-8524M switches simplifies all this. With enhanced stacking, you only need to assign an IP address to one switch in each subnet in your network. The switch with the IP address is referred to as the Master switch of the enhanced stack. All switches in the same stack share the IP address.

Starting a local or remote management session on the Master switch automatically gives you complete management access to all the other switches in the same enhanced stack.

This feature has two primary benefits. First, it reduces the number of IP addresses you have to assign to your network devices. Second, it allows you to configure multiple switches through the same local or remote management session.

> **Note**
> For additional information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

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

You must also assign the switch a gateway address if the switch and a remote management workstation are separated by a router. This gateway address is the IP address of the router through which the switch and remote management station will communicate.

If you do not plan to remotely manage any of the AT-8000 Series switches in your network, you do not need to assign any of them an IP address. The switches can operate without an IP address and you will still be able to manage them completely using local management sessions.

How Do You Assign an IP Address?

Once you have decided which, if any, switches on your network need an IP address, you have to access the AT-S39 software on the switches and assign the addresses. There are actually two ways in which a switch can obtain an IP address.

The first method is for you to assign the IP configuration information manually. This procedure is explained in **Configuring an IP Address and Switch Name** on page 41.

The second method is for you to activate the BOOTP and DHCP services on the switch and have the switch automatically download its IP configuration information from a BOOTP or DHCP server on your network. This procedure is explained in **Activating the BOOTP and DHCP Client Software** on page 44.

> **Note**
> Initially assigning an IP address to a switch or activating BOOTP and DHCP can only be done through a local management session, unless the switch is a part of an existing enhanced stack.

Configuring an IP Address and Switch Name

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch from a local or Telnet management session. (If you want the switch to obtain its IP configuration from a DHCP or BOOTP server on your network, go to the procedure **Activating the BOOTP and DHCP Client Software** on page 44.)

This procedure also 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 manually set a switch's IP address, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

   The Administration Menu is shown in Figure 3.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                   Sales Switch

Login Privilege: Manager

               Administration Menu

1 - IP Address ........ 0.0.0.0
2 - Subnet Mask ....... 0.0.0.0
3 - Default Gateway ... 0.0.0.0
4 - System Name ....... Sales Switch
5 - Administrator ..... Jane Smith
6 - Comments .......... Bldg. 12, Rm. 201
7 - Set Password ......
8 - BOOTP/DHCP ........ Disabled

9 - Reset Switch
A - Server-based Authentication
D - Downloads & Uploads
P - Ping a Remote System

R - Return to Previous Menu

Enter your selection?
```

Figure 3 Administration Menu

2. Change the parameters as desired.

   The parameters in the IP Parameters menu are described below:

   1 - IP Address
   This parameter specifies the IP address of the switch. You must assign an IP address if you want the switch to function as the Master switch of an enhanced stack. (Slave switches do not need and IP address.) You must also assign it an IP address if it will not be part of an enhanced stack and you want to be able to manage it remotely using Telnet or a web browser. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

   2 - Subnet Mask
   This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The mask address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

   3 - 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. The gateway address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

   4 - System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). This parameter is optional. The name can be up to 30 alphanumeric characters. Spaces are allowed.

   Note
   You should assign each switch a name. The names can help you identify the various switches in your network. This can help you avoid performing a configuration procedure on the wrong switch.

   5 - Administrator
   This parameter specifies the name of the network administrator responsible for managing the switch. This parameter is optional. The name can be up to 30 alphanumeric characters. Spaces are allowed.

   6 - Comments
   This parameter specifies additional information about the Fast Ethernet switch, such as its location (for example, 4th Floor, room 402B). This parameter is optional. Comments can be up to 30 alphanumeric characters. Spaces are allowed.

7 - Set Password
This parameter is used to change the Manager and Operator's login passwords. For instructions, refer to **Configuring the Management Passwords** on page 51.

8 - BOOTP/DHCP
This selection activates and deactivates the BOOTP and DHCP client software on the switch. For information on this selection, refer to **Activating the BOOTP and DHCP Client Software** on page 44.

9 - Reset Switch
This selection resets the switch, as explained in **Resetting a Switch** on page 49.

A - Server-based Authentication
This selection is used to configure the TACACS+ and RADIUS client software on the switch. For information on this feature, refer to **Chapter 17, TACACS+ and RADIUS Protocols** on page 192.

Downloads and Uploads
For information on this selection, refer to **Chapter 20**, **File Downloads and Uploads** on page 220.

R - Ping a Remote System
For information on this selection, refer to **Pinging a Remote System** on page 54.

3. After you have set the parameters, type **S** to select Save Configuration Changes.

Note
A change to any parameter in this menu, including IP address, subnet mask, and gateway address, is immediately activated on the switch.

Activating the BOOTP and DHCP Client Software

The BOOTP and DHCP application protocols were developed to simplify network management. They are used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and a default gateway address.

An AT-8000 Series switch contains the client software of these protocols and can obtain IP configuration information from a BOOTP or DHCP server on your network. If you activate this feature, the switch seeks its IP address and other IP configuration information from a BOOTP or DHCP server on your network whenever you reset or power ON the device.

For this to work there must be a BOOTP or DHCP server residing on your network and you must configure the service by entering in the switch's MAC address and other appropriate information.

BOOTP and DHCP application protocols allow you to specify how the IP address is to be assigned to the switch. Choices are static and 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. This is the preferred configuration. Since the BOOTP and DHCP services always assigns the same IP address to a switch, you will always know which IP address to use when you need to remotely manage a particular switch.

If you choose dynamic, the server will assign any unused IP address that it has not already assigned to another device. This means that a switch might have a different IP address each time you reset or power cycle the device, making it difficult for you to remotely manage the unit.

Note
The default setting for the BOOTP and DHCP client software is disabled.

To activate or deactivate the BOOTP and DHCP client software on the switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

   The Administration in Figure 3 on page 41 is displayed.

2. Type **8** to select BOOTP/DHCP.

   The following prompt is displayed:

   ```
   BOOTP/DHCP (E-Enabled, D-Disabled):
   ```

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

4. Type **S** to select Save Configuration Changes.

Note

If you activate the BOOTP and DHCP client software, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

Any static IP address, subnet mask, and gateway address assigned to the switch are deleted from the Administration menu and replaced with the values the switch receives from the BOOTP or DHCP server. If you later disable BOOTP and DHCP, these values are returned to their default setting of 0.0.0.0.

Configuring SNMP Community Strings and Trap IP Addresses

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

> **Note**
> SNMP access is disabled by default. To enable SNMP access, refer to **Configuring Management Access** on page 52.

1. From the Main Menu, type **5** to select System Config Menu.

   The System Configuration Menu is shown in Figure 4.

```
  Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
                    Sales Switch

Login Privilege: Manager

                  System Config Menu

1 - MAC Aging Time ..................... 300 seconds
2 - Switch Mode ........................ Tagged
3 - Console Disconnect Timer Interval . 10 minute(s)
4 - Web Server Status .................. Enabled
5 - SNMP Access ........................ Disabled
6 - Console Startup Mode ............... Menu
7 - Reset to Factory Defaults

A - Advanced Configuration

R - Return to Previous Menu

Enter your selection?
```

Figure 4 System Configuration Menu

2. From the System Configuration Menu, type **A** to select Advanced Configuration.

   The Advanced Configuration menu is shown in Figure 5.

```
Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
                  Sales Switch

Login Privilege: Manager

           Advanced Configuration Menu

1 - IGMP Snooping Configuration
2 - Broadcast Timers Setup
3 - SNMP Configuration

R - Return to Previous Menu

Enter your selection:
```

Figure 5 Advanced Configuration Menu

3. From the Advanced Configuration menu, type **3** to select SNMP Configuration.

   The SNMP Configuration menu is shown in Figure 6.

```
Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
                  Sales Switch

Login Privilege: Manager

                SNMP Configuration

1 - GET Community .............. public
2 - SET Community .............. private
3 - Trap Community ............. public

4 - Trap Receiver 1 ............ 0.0.0.0
5 - Trap Receiver 2 ............ 0.0.0.0
6 - Trap Receiver 3 ............ 0.0.0.0
7 - Trap Receiver 4 ............ 0.0.0.0

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection:
```

Figure 6 SNMP Configuration Menu

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

   1 - GET Community
   2 - SET Community
   3 - Trap Community
   Use these parameters to set a switch's SNMP community strings. A community string can be up to thirteen characters. Community strings are case sensitive and can contain spaces and special characters, such as an exclamation point (!).

   4 - Trap Receiver 1
   5 - Trap Receiver 2
   6 - Trap Receiver 3
   7 - Trap Receiver 4
   Use these selections to specify the IP addresses of up to four management workstations on your network to receive traps from the switch.

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

5. After making your changes, type **S** to select Save Configuration Changes.

Resetting a Switch

This procedure reboots the switch.

Note
Any configuration changes not saved will be lost once the switch reboots. To save your configuration changes, return to the Main Menu and type **S** to select Save Configuration Changes.

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

To reset a switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **9** to select Reset Switch.

   The following prompt is displayed:

   ```
   Do you want to proceed with the switch reboot?
   [Yes/No] ->
   ```

3. Type **Y** to reset the switch or **N** to cancel this procedure.

   If you are running a local management session, you will see this prompt:

   ```
   Please press <ENTER> key within 5 seconds for:
      * Terminal speed detection, and
      * To view the initialization messages
   Entering any key other than <ENTER> key does not
   guarantee the above ...
   ```

4. To view the initialization messages during the reset process, press Return.

   The switch reinitializes its operating system, a task requiring approximately 20 seconds to complete. Once complete, the switch is again ready for normal network operations.

5. To resume managing the switch, you must reestablish your management session.

Configuring the AT-S39 Management Security Features

The AT-S39 software has several security features that can help prevent unauthorized individuals from changing a switch's parameter settings. The security features are:

- ❑ Manager and Operator Passwords - The management software has two standard, management login accounts: Manager and Operator. The Manager account allows you to configure all switch parameters, while the Operator account only allows you to view the parameter settings. The default login name for Manager access is "manager" and the password is "friend". The login name and password for Operator access are both "operator". Login names and passwords are case-sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 51. (You can create additional management login accounts for the switch if your network contains a TACACS+ or RADIUS authentication protocol server. For instructions, refer to **Chapter 17, TACACS+ and RADIUS Protocols** on page 192.)

- ❑ Console Timeout - This parameter causes the management software to automatically end a management session if it does not detect any activity from the local or 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 console timeout value is 10 minutes. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

- ❑ Web Access - You can disable the web browser management feature on the switch, and so prevent individuals from managing the switch remotely using a web browser. The default setting for web browser management access is enabled. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

- ❑ SNMP Access - You can also disable the SNMP management feature on the switch, and so prevent individuals from managing the switch remotely using a SNMP management program. The default setting for SNMP access is disabled. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 52.

Configuring the Management Passwords

There are two levels of management access on an AT-8000 Series switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

The default password for Manager access is "friend". The default password for Operator access is "operator". A password can be from 0 to 20 alphanumeric characters. Passwords are case-sensitive.

> **Caution**
> You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

To change the Manager or Operator password, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **7** to select Set Password.

   The Passwords Menu is shown in Figure 7.

```
Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
Login Privilege: Manager
                  Passwords Menu
1 - Set Manager Password
2 - Set Operator Password

R - Return to Previous Menu

Enter your selection?
```

Figure 7 Passwords Menu

3. Type **1** to change the Manager password or type **2** to change the Operator password.
4. Follow the prompts. You are asked to enter the new password twice.

   The new password is automatically saved by the management software. You do not need to use the Save Configuration Changes menu selection to permanently save the new password.

Configuring Management Access

To configure the console timer, web access, and SNMP access security features of the AT-S39 management software, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.

   The System Config Menu is shown in Figure 4 on page 46.

2. To configure the console timer, type **3** to select Console Disconnect Timer Interval and, when prompted, enter a value of from 1 to 60 minutes. The default value is ten minutes.

   For example, if you specify 2 minutes, the AT-S39 management software automatically ends a local or remote management session if it does not detect any activity from the management station after 2 minutes.

   A new console timer value takes affect the next time you start a local or remote management session.

3. To configure web browser access, type **4** to select Web Server Status and, when prompted, type **E** to enable the web server or **D** to disable it. The default value is enabled.

   For example, if you disable the web server, no one can manage the switch remotely using a web browser.

4. To configure SNMP management access of the switch, type **5** to select SNMP Access and, when prompted, type **E** to enable SNMP management access or **D** to disable it. The default value is disabled.

   When SNMP access is disabled, no one can manage the switch remotely using an SNMP management program.

   Your changes are immediately activated on the switch.

5. After you have made the desired changes, type **S** to select Save Configuration Changes.

Viewing the AT-S39 Version Number and Switch MAC Address

The procedure in this section displays the following switch information:

- ❑ AT-S39 version number
- ❑ Bootloader version number
- ❑ Serial number
- ❑ MAC Address

To display the information, type **8** to select Diagnostics from the Main Menu. The Diagnostics menu is shown in Figure 8.

```
      Allied Telesyn Ethernet Switch AT-8024 - AT-S39
Login Privilege: Manager
                         Diagnostics
1 - Application Software Version .... AT-S39 v3.3.0
2 - Application Software Build Date . May 12 2004 19:32:40
3 - Bootloader Version ............. ATS39_LOADER v2.1.0
4 - Bootloader Build Date ........... Jul 21 2002 16:37:14
5 - Serial Number ................... S05248014600028
6 - MAC Address ..................... 00:30:84:52:03:80
7 - System Up Time .................. 20D:15H:24M:51S
8 - Uplink Information

R - Return to Previous Menu

Enter your selection?
```

Figure 8 Diagnostics Menu

The information displayed in selections 1 through 7 in this menu is for viewing purposes only. For information on option 8, refer to **Displaying Uplink Information** on page 74.

Pinging a Remote System

You can instruct the switch to ping a remote device on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

> **Note**
> The switch must have an IP address in order for you to perform this procedure. This means that in most cases you must perform this procedure from the master switch of an enhanced switch.

To instruct the switch to ping a network device, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
2. From the Administration Menu, type **P** to select Ping a Remote System.

   The following prompt is displayed:

   ```
   Please enter an IP address ->
   ```

3. Enter the IP address of the end node you want the switch to ping and press Return.

   The results of the ping command are displayed on the screen. To stop the ping, press any key.

Returning the AT-S39 Software to the Factory Default Values

The procedure in this section returns all AT-S39 software parameters to their default values. This procedure also deletes any VLANs you created on the switch. The AT-S39 software default values can be found in **Appendix A, AT-S39 Default Settings** on page 331.

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

To return the AT-S39 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **7** to select Reset to Factory Defaults.

   The following prompt is displayed:

   ```
   Are you sure you want to reset to Factory Defaults?
   [Yes/No] ->
   ```

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

   The following prompt is displayed:

   ```
   Do you want to reset IP, Subnet and Gateway as well?
   [Yes/No] ->
   ```

4. If you type **Y** for yes, all switch parameters including the IP address, subnet mask, and gateway address are changed to their default values. If you type **N** for no, all switch parameters excluding those settings are changed to their default values.

   The following prompt is displayed:

   ```
   The Factory Defaults take effect only after the
   Switch reboots.
   Do you want to proceed with switch reboot? [Yes/No]
   ->
   ```

5. Type **Y** to reset the switch.

   The operating parameters are returned to their default values and the switch is reset.

Configuring the Console Startup Mode

You can configure the AT-S39 software to display either the Main Menu or the command line interface prompt ($) whenever you start a local or remote management session. The default is the Main Menu.

To change the console startup mode, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **6** to select Console Startup Mode.

   The following prompt is displayed:

   ```
   Enter Console Mode (M-Menu, C-CLI):
   ```

3. Type **M** if you want a management session to always start with the Main Menu, or **C** if you want it to display the command line interface prompt. The default is the Main Menu.

   A change to the console startup mode takes effect the next time you start a local or remote management session.

Chapter 4
Enhanced Stacking

This chapter explains the enhanced stacking feature. The sections in this chapter include:

Enhanced Stacking Overview

The enhanced stacking feature can make it easier for you to manage the AT-8000 Series switches in your network. It offers the following benefits:

- ❑ You can manage up to 24 switches from one local or remote management session. This eliminates the need of having to start separate management sessions for the different switches in your network.
- ❑ The switches can share the same IP address. This reduces the number of IP addresses you need to assign to your network devices for remote management.
- ❑ Remotely managing a new switch in your network is simplified. You simply connect it to your network. Once connected, you can begin to manage it immediately from any workstation in your network.

Guidelines

Here are a few guidelines to implementing enhanced stacking in your network:

- ❑ A enhanced stack can consist of any Allied Telesyn switches that feature enhanced stacking, including the AT-8000 Series switches, the AT-8400 Series switches, and the AT-8524M switch.
- ❑ An enhanced stack cannot span subnets.
- ❑ All of the switches in an enhanced stack must use the same management VLAN. This is the VLAN on which the switch expects to receive remote management packets. You can create more than one enhanced stack in a subnet by assigning switches to different Management VLANs. For information about Management VLANs, refer to **Designating a Management VLAN** on page 151.
- ❑ An enhanced stack must have at least one master switch. The master switch can be any Allied Telesyn switch that supports enhanced stacking.
- ❑ You must assign the master switch an IP address and subnet mask.
- ❑ You must set the master switch's stacking status to Master.
- ❑ The enhanced stacking feature uses the IP address 176.16.16.16. Do not assign this address to any device on your subnet if you intend to use the enhanced stacking feature.

There are three basic steps to implementing this feature on your network:

1. You must select a switch in your network to function as the master switch of the stack.

   The master switch can be any switch that supports enhanced stacking, such as an AT-8000 Series switch, an AT-8400 Series switch, or an AT-8524M switch. For networks that consist of more than one subnet, there must be at least one master switch in each subnet.

   It is recommended that each enhanced stack have two master switches, each assigned a unique IP address. That way, should you remove one of the master switches from the network, such as for maintenance, you all still be able to remotely manage the other switches in the stack using the second master switch.

2. You must assign the master switch an IP address and subnet mask.

   A master switch must have an IP address and subnet mask. The other switches in an enhanced stack, referred to as slave switches, do not.

   If an enhanced stack will have more than one master switch, you must assign each master switch a unique IP address.

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

   For instructions on how to set the IP address manually, refer to **Configuring an IP Address and Switch Name** on page 41. For instructions on activating the BOOTP and DHCP services, refer to **Activating the BOOTP and DHCP Client Software** on page 44.

3. Change the enhanced stacking status of the master switch to Master.

   This is explained in the procedure **Setting a Switch's Enhanced Stacking Status** on page 61.

Figure 9 is an example of the enhanced stacking feature.

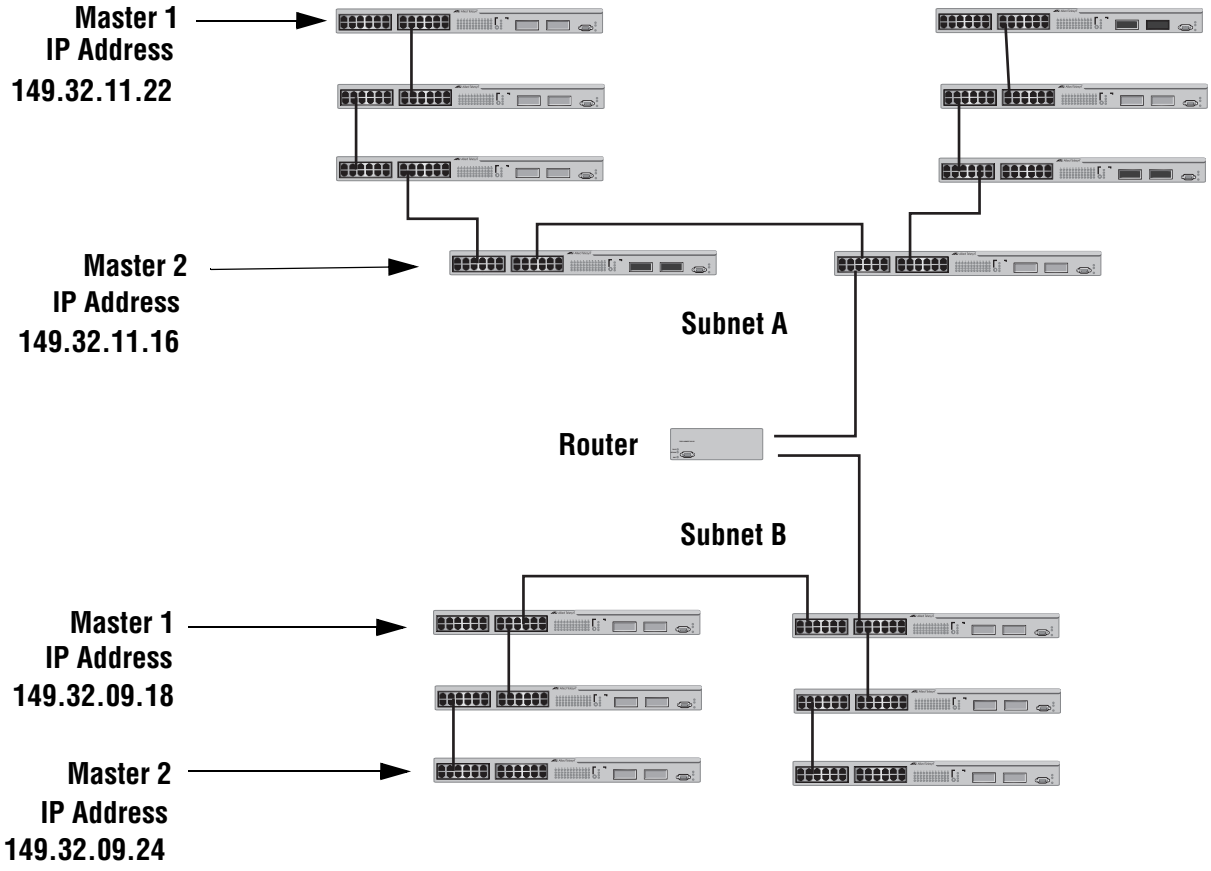

Figure 9 Enhanced Stacking Example

The example consists of a network of two subnets interconnected with a router. Each subnet consists of one enhanced stack. Two switches in each subnet have been selected as master switches of the enhanced stacks, and each has been assigned a unique IP address.

To manage the switches of an enhanced stack, you could start a local or a remote management session with one of the master switches in the enhanced stack. You would then have management access to all the enhanced stacking switches in the same stack.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master switch, slave switch, or unavailable. Each status is described below:

- Master switch - A master switch of a stack can be used to manage all the other switches in the stack. Once you establish a local or remote management session with the Master switch, you can access and manage all the switches in the stack. A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.
- Slave switch - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask. This is the default setting for a switch.
- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through enhanced stacking. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note
You cannot change the stacking status of a switch accessed through enhanced stacking. To change the stacking status of a switch that does not have an IP address or subnet mask, such as a slave switch, you must use a local management session. If the switch has an IP address and subnet mask, you can use either a local or a Telnet management session.

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Main Menu, type **9** to select Enhanced Stacking. The Enhanced Stacking menu is shown in Figure 10.

```
      Allied Telesyn Ethernet Switch AT-8024 - AT-S39
Login Privilege: Manager
                     Enhanced Stacking
1 - Switch State-(M)aster/(S)lave/(U)navailable.... Master
2 - Stacking Services

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 10 Enhanced Stacking Menu

The menu displays the current status of the switch at the end of selection "1 - Switch State." For example, the switch's current status in the figure above is Master.

Note
The "2 - Stacking Services" selection is included in the menu only for master switches.

2. To change a switch's stacking status, type **1** to select Switch State.

   The following prompt is displayed.

   ```
   Enter new setup (M/S/U) ->
   ```

3. Type **M** to change the switch to a master switch, **S** to make it a slave switch, or **U** to make the switch unavailable. Press Return.

   A change to the status is immediately activated on the switch.

4. Type **S** to select Save Configuration Changes.

Selecting a Switch in an Enhanced Stack

The first thing you should do before performing a procedure on a switch in an enhanced stack is check to be sure you are performing it on the correct switch. If you assigned system names to your switches, then this is easy. The name of the switch being managed is always displayed at the top of every management menu.

When you start a management session on the Master switch of an enhanced stack, you are by default addressing that particular switch. The management tasks that you perform affect only the master switch.

To manage a slave switch or another Master switch in the stack, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the Main Menu, type **9** to select Enhanced Stacking.
2. From the Enhanced Stacking menu, type **2** to select Stacking Services.

   The Stacking Services menu is shown in Figure 11.

```
       Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
                          Sales Switch

Login Privilege: Manager

                       Stacking Services

                                Switch     Software     Switch
Num  MAC Address    Name        Mode       Version      Model
-------------------------------------------------------------


G - Get/Refresh List of Switches
S - Sort Switches in New Order
A - Access Switch
I - Image Download to Remote Switches
C - Configuration Download to Remote Switches
B - Boot Loader Download to Remote Switches
R - Return to Previous Menu

Enter your selection?
```

Figure 11 Stacking Services Menu

3. Type **G** to select Get/Refresh List of Switches.

   The Master switch polls the network for all slave and other Master switches in the enhanced stack and displays a list of the switches in the Stacking Services menu.

   Note
   The Master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

   Note
   The menu selections I, C, and B for downloading image and bootloader files are explained in **Chapter 20**, **File Downloads and Uploads** on page 220.

   By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well by selecting the option S - Sort Switches in New Order.

4. To manage a different switch in an enhanced stack, type **A** to select Access Switch.

   A prompt similar to the following is displayed:

   ```
   Enter the switch number -> [1 to 24}
   ```

5. Type the number of the switch in the list you want to manage.

6. Enter a user name and password for the switch and press Return.

   The default user name and password for manager access is “manager” and “friend”, respectively. The default user name and password for operator access is “operator” and “operator”. User names and passwords are case-sensitive.

   The Main Menu of the selected switch is displayed. You now can manage the switch. Any management tasks you perform affect only the selected switch.

Returning to the Master Switch

When you have finished managing a slave switch and want to manage another switch in the subnet, return to the Main Menu of the slave switch and type **Q** for Quit. This returns you to the Stacking Services menu. Once you see that menu, you are again addressing the Master switch from which you started the management session.

You can either select another switch in the list to manage or, if you want to manage the Master switch, return to the master switch’s Main Menu by typing **R** twice.

Chapter 5
Port Parameters

The chapter contains procedures for viewing and changing the parameter settings for the individual ports on a switch.

This chapter contains the following procedures:

Displaying Port Status

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

   The Port Menu is shown in Figure 12

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                    Sales Switch

Login Privilege: Manager

                      Port Menu

1 - Port Configuration
2 - Port Mirroring
3 - Port Trunking
4 - Port Status
5 - Port Security
6 - Port Access Control

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 12 Port Menu

2. From the Port Menu, type **4** to select Port Status.

   The Port Status window is displayed (see Figure 13).

```
           Allied Telesyn Ethernet Switch AT-8024 - AT-S39
Login Privilege: Manager

                            Port Status

Prt  Link  Neg    MDIO Spd  Dplx  PVID   VlanID  Flow      State
-------------------------------------------------------------------
001  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding
002  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
003  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
004  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
005  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding
006  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
007  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
008  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 13 Port Status Window

The information in this window is for viewing purposes only. The columns in the window are described below:

Prt

The port number.

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.

Neg
The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode have been set manually.

MDIO
The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The status Auto indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Spd
The operating speed of the port. Possible values are:

10 - 10 Mbps

100 - 100 Mbps

1000 - 1000 Mbps (optional Gigabit Ethernet ports only)

Dplx
The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID
The port VLAN identifier currently assigned to the port. This number corresponds to the VLAN identifier (VID) where the port is an untagged member.

VlanID
The VLAN identifier of the VLAN in which the port is an untagged member. This column will not include the VIDs of the VLANs where the port is a tagged member.

Flow
The flow control setting for the port. Possible values are:

None - No flow control on the port.

Transmit - Flow control only as packets are being transmitted out the port.

Receive - Flow control only on as packets are being received on the port.

Both - Flow control for both packets entering and leaving the port.

State
The current operating status of the port. Possible values are:

Forwarding - The port is sending and receiving Ethernet frames.

Disabled - The port has been manually disabled.

Configuring Port Parameters

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

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **1** to select Port Configuration.

   The following prompt is displayed:

   ```
   Enter Ports List ->
   ```

3. Enter the port you want to configure. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

   The Port Configuration menu is shown in Figure 14.

```
  Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                    Sales Switch

Login Privilege: Manager

                 Port Configuration

Configuring Ports 4

0 - Description .......
1 - Status ............. Forwarding
2 - Negotiation ....... Auto
5 - Flow Control ...... None
6 - Advertise 10FDX ... Yes
7 - Advertise 10HDX ... Yes
8 - Advertise 100FDX .. Yes
9 - Advertise 100HDX .. Yes
M - MDI/MDIX Mode ..... Auto
C - Broadcast Control . No Broadcast Control

S - Save Configuration changes
F - Force Renegotiation
X - Reset Port
R - Return to Previous Menu

Enter your selection?
```

Figure 14 Port Configuration Menu

Note
The Port Configuration menu in the figure above is for a 10/100 Mbps twisted pair port. The menu for a fiber optic port, a GBIC module, or a stacking module will contain a subset of the parameters.

If you are configuring multiple ports and the ports have different settings, the Port Configuration menu displays the settings of the lowest numbered port. Once you have configured the settings of the port, all of its settings are copied to the other selected ports.

4. Adjust the port parameters as desired. You adjust a parameter by typing its number. This toggles the parameter through its possible settings. The parameters are described below.

0 - Port Description
You use this selection to assign a name to a port. The name can be from one to fifteen alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points.

1 - Status
You use this selection to enable or disable a port. When disabled, a port will not forward frames.

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

Possible settings are:

Forwarding - The port will forward packets. This is the default setting.

Disabled - The port will not forward packets.

2 - Negotiation
You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

If you select Auto for Auto-Negotiation, which is the default setting, the switch will set both speed and duplex mode for the port automatically. The switch determines the highest possible common speed between the port and its end node and sets the port to that speed. This helps to ensure that the port and the end node are operating at the highest possible common speed.

You should note the following concerning the operation of Auto-Negotiation on a switch port:

- ❑ In order for a switch port to successfully Auto-Negotiate its duplex mode with an end node, the end node should also be using Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation will default to half-duplex if it detects that the end node is not using Auto-Negotiation. This will result in a duplex mismatch if the end node is operating at a fixed duplex mode of full-duplex.

To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

- The auto-MDI/MDI-X setting is available only when a port's speed and duplex mode are set by Auto-Negotiation. If a port's speed or duplex mode is set manually, the port's wiring configuration defaults to MDI-X. Disabling Auto-Negotiation and setting a port's speed and duplex mode manually might require setting the port's MDI/MDI-X setting as well.

If you select Manual, two additional selections are displayed in the menu:

```
3 - Speed ............... 0100
4 - Duplex .............. Full-Duplex
```

Figure 15 Manual Speed and Duplex Mode Settings

You use these two selections to set the port's speed and duplex mode. The possible settings for the 2 - Speed selection are:

0010 - 10 Mbps

0100 - 100 Mbps

1000 - 1000 Mbps (optional Gigabit Ethernet ports only)

The possible settings for 3 - Duplex are Full-duplex and Half-duplex.

5 - Flow Control
Flow control applies only to ports operating in full-duplex mode. A port 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 settings are:

None - No flow control on the port.

Transmit - Flow control only as packets are being transmitted out the port.

Receive - Flow control only on as packets are being received on the port.

Both - Flow control for both packets entering and leaving the port.

6 - Advertise 10FDX
7 - Advertise 10HDX
8 - Advertise 100FDX
9 - Advertise 100HDX
These selections appear in the menu only when a port is configured for Auto-Negotiation. During Auto-Negotiation, a switch port determines the appropriate speed and duplex mode by advertising its capabilities to the end node connected to it.

By default, a switch port will advertise its full capabilities, which in the case of a port on an AT-8000 Series switch are 10 or 100 Mbps speed and half- or full-duplex mode.

You can use these four selections to limit the capabilities a switch port will advertise during Auto-Negotiation. For example, if you set the selection 8 - Advertise 100HDX to No, the switch port will not advertise that it is capable of 100 Mbps, half-duplex operation.

Note
In most network environments you should leave all Auto-Negotiation advertisements activated, which is the default setting.

M - MDI/MDIX Mode
Use this selection to set the wiring configuration of the port. The configuration can be Auto, MDI, or MDI-X.

The twisted pair ports on the switch feature auto-MDI/MDI-X. They configured themselves automatically as MDI or MDI-X when connected to an end node. This allows you to use either a straight-through twisted pair cable when connecting any type of network device to a port on the switch.

If you disable Auto-Negotiation on a port and set a port's speed and duplex mode manually, the auto-MDI/MDI-X feature is also disabled. A port where Auto-Negotiation has been disabled defaults to MDI-X. Disabling Auto-Negotiation may require that you manually configure a port's MDI/MDI-X setting using this option or use a crossover cable.

C - Broadcast Control
For background information on this selection and instructions on how to set the option, refer to **Broadcast Storm Control Overview** on page 188 and **Configuring the Maximum Broadcast Frame Count** on page 191.

P - Back Pressure
This menu option only appears for ports configured for half-duplex.

Backpressure performs much the same function as flow control. Both are used by a port to control the flow of ingress packets.

Where they differ is that while flow control applies to ports operating in full-duplex, backpressure applies to ports operating in half-duplex mode.

When a twisted pair port on the switch operating in half-duplex mode needs to stop an end node from transmitting data, it forces a collision. A collision on an Ethernet network occurs when two end nodes attempt to transmit data using the same data link at the same time. A collision causes the end nodes to stop sending data. This is called backpressure.

When a switch port needs to stop a half-duplex end node from transmitting data, it forces a collision on the data link, which stops the end node. Once the port is ready to receive data again, it stops forcing collisions.

The default setting for backpressure on a switch port is disabled.

5. Once you have set the port parameters, type **S** to select Save Configuration Changes.

   Configuration changes are immediately activated on a port.

The Port Configuration menu also features these selections:

F - Force Renegotiation
This selection appears in the menu only when a port is set to Auto-Negotiation. You can use the option to prompt the port to re-Auto-Negotiate with the end node. This can be helpful if you believe that a port and end node are not operating at the same speed and duplex mode.

X - Reset Port
You can use this option to reset the selected port. This can prove useful in situations where a port is experiencing a problem establishing a valid connection to the end node. The reset takes less than a second to complete. The port's current parameter settings are not changed by this option.

Displaying Uplink Information

The AT-S39 management software can display basic manufacturer information about an optional GBIC module in an AT-8024GB switch or the fiber optic ports in an AT-8026FC switch.

To display uplink information, perform the following procedure:

1. From the Main Menu, type **8** to select Diagnostics.
2. From the Diagnostics menu, type **8** to select Uplink Information.

   The GBIC Information menu is shown in Figure 16.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager
             Uplink Information Menu
1 - Uplink Information
R - Return to Previous Menu
Enter your selection?
```

Figure 16 Uplink Information Menu

3. Type **1** to select Uplink Information.

   The following prompt is displayed:

   ```
   Enter Uplink Port number -> [25 to 26]
   ```

4. Enter the port number you want to view. This will be either **25** or **26**. Press Return.

The management software displays a menu containing basic information about the GBIC module or fiber optic port. Figure 17 is an example of the menu.

```
    Allied Telesyn Ethernet Switch AT-8024GB - AT-S39
Login Privilege: Manager

                Uplink Information Menu

Port Number ..................... 25
Type of Serial Transceiver .... Unknown
Extended Serial Transceiver ... Module Not Defined
Connector Type ................. Unknown
Elect/Opt Transceiver .........
Serial Encoding ................ Unspecified
Nominal bit rate(100Mbits/s) .. 0
Length 9/125 mm Fib. (k) ...... 0
Length 9/125 um Fib. (100m) ... 0
Length 50/125 um Fib. (10m) ... 0
Length 62.5/125 um Fib. (10m) . 0


N - Next Page
R - Return to Previous Menu

Enter your selection?
```

Figure 17 GBIC Information Menu

The information in the menu cannot be changed and is for viewing purposes only.

Chapter 6
Port Security

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

Note
To change a switch's port security level, you must use a local management session. You cannot set port security from a Telnet or web browser management session, or through enhanced stacking.

Port Security Overview

This feature can enhance the security of your network. You can use it to control which end nodes can forward frames through the switch, and so prevent unauthorized individuals from accessing your network or particular parts of the network.

This type of network security uses a frame's source MAC address to determine whether the switch should forward a frame or discard it. The source address is the MAC address of the end node that sent the frame.

There are four levels of port security. Only one security level can be active on a switch at a time. The levels of port security are:

- Automatic
- Limited
- Secured
- Locked

Automatic

This operating mode disables port security. The switch learns and adds addresses to its dynamic MAC address table as it receives frames on the ports.

> **Note**
> The Automatic security mode is the default security level for the switch.

Limited

You can use this security level to manually specify the maximum number of dynamic MAC addresses each port on the switch can learn. Once a port has learned its maximum limit, it discards ingress frames with source MAC addresses not already stored in the MAC address table.

When you activate this mode, the switch deletes all MAC addresses in the dynamic MAC address table and immediately begins learning new addresses as frames are received on the ports, up to the allowed limit for each port.

The MAC aging time is disabled under this security level. Once a dynamic MAC address has been learned on a port and added to the MAC address table, it remains in the table and is never purged, even when the end node is inactive.

Static MAC addresses are retained by the switch and are not included in the count of maximum addresses that can be learned by a port. You can continue to add static MAC addresses to a port even after a port has learned its maximum number of dynamic MAC addresses.

Secure

This security level instructs the switch to forward frames based solely on static MAC addresses. When this security level is activated, the switch deletes all dynamic MAC addresses and disables the MAC address table so that no new addresses can be learned.

The switch also deletes any addresses in the static MAC address table. Once you have activated this security level, you must enter the static MAC addresses of the nodes whose frames the switch should forward. The switch will forward frames only from those nodes whose MAC addresses you enter in the static MAC address table. Any node whose MAC address is not in the static MAC address table will not be able to send frames through the switch.

Lock All Ports

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

The MAC aging time is disabled in this security level; no dynamic MAC addresses are deleted from the MAC address table, even those belonging to inactive end nodes.

Note
For background information on MAC addresses and aging time, refer to **MAC Address Overview** on page 162.

Guidelines

Here are a few general guidelines to keep in mind when using this type of port security:

- ❑ The filtering of a packet occurs on the ingress port, not on the egress port.
- ❑ You cannot use MAC address security and 802.1x port-based access control on a switch port at the same time.
- ❑ Port security is set at the switch level. You cannot set this on a per-port basis.
- ❑ Only one security level can be active on a switch at a time.

Configuring Port Security

Note
Port security can only be set through a local management session. You cannot set this feature from a Telnet or web browser management session, or through enhanced stacking.

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

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **5** to select Port Security.

   The Port Security menu is shown in Figure 18.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                    Port Security

1 - Configure Port Security Mode ....... AUTOMATIC
2 - Configure Limited Mode Parameters

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 18 Port Security Menu

3. Type **1** to select Configure Port Security Mode.

   The following prompt is displayed:

```
Enter new mode (A-Automatic, L-Limited, S-Secured, K-
locKed):
```

4. Select the desired security level. You can select only one security level. For an explanation of the levels, refer to **Port Security Overview** on page 77.

   A change to the security level is immediately activated on the switch.

5. Type **S** to select Save Configuration Changes.
6. If you selected the Limited security level, go to the next procedure to set the MAC address limits for the individual ports.

Configuring the Limited Security Mode

The Limited security mode lets you set the maximum number of dynamic MAC addresses each port on a switch can learn. When you activate this security level, the switch deletes all MAC addresses in the dynamic MAC address table and immediately begins to learn new addresses as frames are received on the ports. Once the maximum number of MAC addresses have been learned by a port, ingress frames with new source MAC addresses received on the port are discarded and are not forwarded.

You can assign the same limit to all ports or different limits to different ports.

Static MAC addresses are not deleted from the static MAC address table. 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, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **5** to select Port Security.

   The Port Security menu is shown in Figure 18 on page 79.
3. From the Port Security menu, type **2** to select Configure Limited Mode Parameters.

   The Limited Security Mode menu is shown in Figure 19.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager
         Port Security Limited Mode Menu
1 - Display MAC Limits
2 - Configure Limited Mode Parameters

R - Return to Previous Menu

Enter your selection?
```

Figure 19 Limited Security Mode Menu

4. Type **2** to select Configure Limited Mode Parameters.

   The following prompt is displayed:

   ```
   Enter ports list:
   ```

5. Enter the port(s) where you want to specify a new MAC address limit. You can specify the ports individually (e.g., 1,4), as a range (e.g., 4-7), or both (e.g., 2-7,11,15).

   The following prompt is displayed:

   ```
   Enter new MAC limit ->  [1 to 150] ->
   ```

6. Enter the maximum number of dynamic MAC addresses you want the port to be able to learn and press Return. The range is 1 to 150 addresses. The default is 100.
7. Repeat this procedure starting with Step 4 to specify MAC address limits on other ports.
8. Type **S** to select Save Configuration Changes.
9. Type **1** to select Display MAC Limits.

   The current MAC address limits for all ports are displayed.

10. Examine the MAC limits. Check to be sure that they are correct. If you assigned different values to different ports, be sure that the different values apply to the correct ports. If necessary, repeat this procedure to change any MAC address limits.

Chapter 7
Port Trunking

This chapter contains the procedures for creating and deleting port trunks. Sections in the chapter include:

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. A port trunk is 2, 3, or 4 ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A 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.

The example in Figure 20 consists of a port trunk of four data links between two AT-8024 switches.

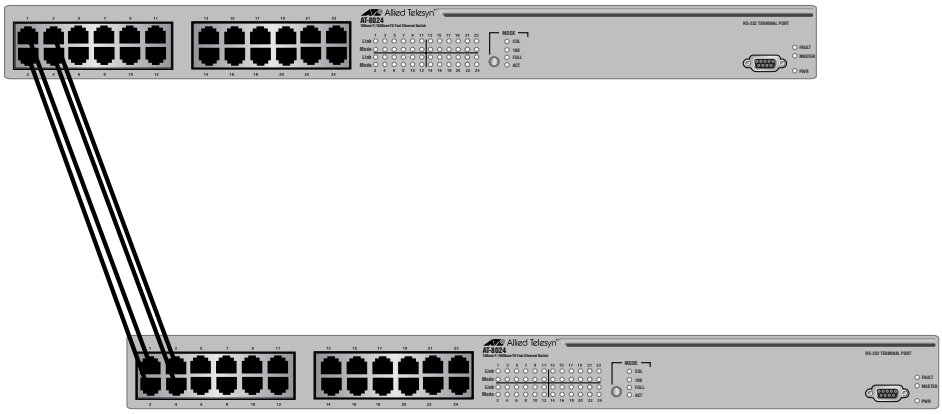

Figure 20 Port Trunk Example

Observe the following guidelines when creating a port trunk:

- ❑ An AT-8000 Series switch can support only one port trunk at a time.
- ❑ A port trunk can consist of 2, 3, or 4 ports.
- ❑ The ports of a port trunk must be of the same medium type. For example, they can be all twisted pair ports or all fiber optic ports.
- ❑ The speed, duplex mode, and flow control settings must be the same for all the ports in a trunk.
- ❑ The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.

- 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-8024 switches. On the first AT-8024 switch you had chosen ports 12, 13, 14, 15 for the trunk. On the second AT-8024 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-8024 switch to port 21 on the second AT-8024, port 13 to port 22, and so on.

- You can create a port trunk of optional GBIC modules installed in Port 25 and Port 26 of an AT-8024GB switch.

- You can create a port trunk of the fiber optic ports in an AT-8026FC switch.

- You can create a port trunk of the ports in two expansion modules in an AT-8016F switch, providing that the ports are of the same medium type and have the same operating specifications.

Port Operating Specifications

The speed, duplex mode, and flow control settings must be the same for all the ports of a port trunk. When you create a port trunk, the management software copies the current settings of the lowest numbered port in the trunk to the other ports. For example, if you create a port trunk consisting of ports 5 to 8, the speed, duplex mode, and flow control settings for port 5 are copied to ports 6, 7, and 8 so that all the ports of the trunk have the same settings. For this reason it is recommended that before creating a port trunk you first examine the settings of the lowest number port that will be in the trunk and verify that it has the correct settings.

Once you have created a port trunk, do not change the speed, duplex mode or flow control of any port in the trunk without making the same change to the other ports.

Load Distribution Methods

There are two steps to creating a port trunk. The first is to identify the ports on the switch that are to function as the port trunk. The second is to select a load distribution method. This second step is important because unless you select the correct distribution method for your configuration, the switch might not evenly distribute the load across all the links of a trunk. Naturally, this could greatly diminish the value and purpose of the port trunk.

The AT-S39 management software offers two load distribution methods. They are:

- ❑ Source Address (SA) Trunking
- ❑ Source Address / Destination Address (SA/DA) Trunking

Let's first take a look at the SA method. When a switch receives a packet from a network node, it examines the destination address to determine on which switch port, if any, the packet should be transmitted. If the packet is destined for a port trunk, the switch then examines the source address of the packet. If this is the first packet from the source node to be transmitted over a port trunk, the switch assigns the source address to one of the trunk links. All subsequent packets from the source node are sent out the assigned data link of the trunk.

The switch assigns source addresses so as to evenly distribute the addresses, or at least as much as possible, across all the ports of the trunk. The intent is to try and ensure that all links in the trunk are utilized.

Here is an example. Figure 21 on page 86 shows two AT-8000 Series Switches, an AT-8024 (Switch #1) and an AT-8024GB (Switch #2) interconnected with a port trunk of three data links. The trunk on Switch #1 consists of Ports 13 to 15 and on Switch #2 of Ports 1 to 3. The 10Base and 100Base workstations are directing traffic to a server connected to Switch #2. The server is connected to Switch #2 with a fiber optic Gigabit Ethernet data link provided by a 1000Base fiber optic GBIC module in the AT-8024GB switch.

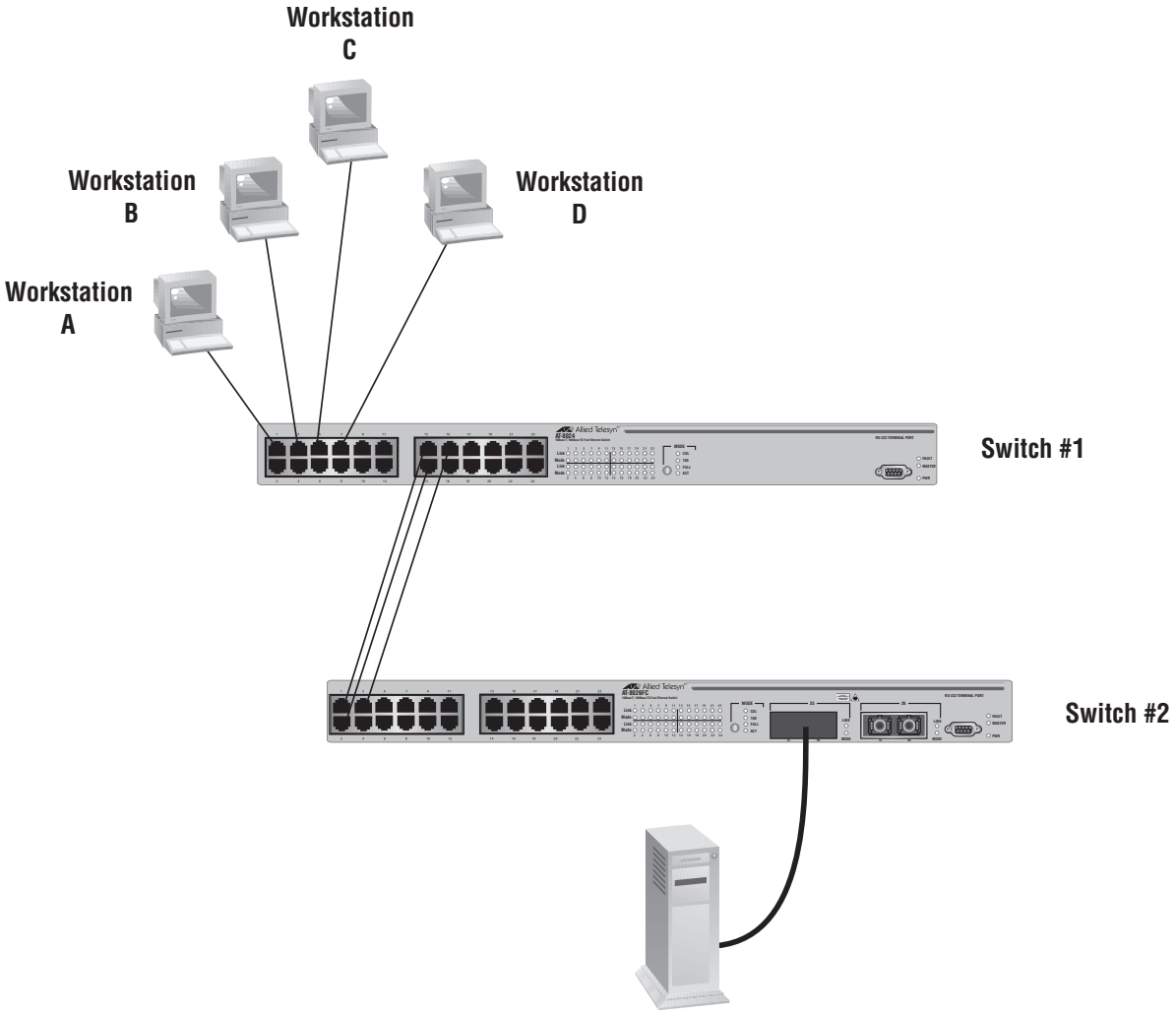

Figure 21 Load Distribution Method

Now assume that you configured the port trunk on Switch #1 for SA load distribution. The switch might distribute the load as follow:

Table 1 Switch #1 Load Distribution

Source Workstation	Source MAC Address	Trunk Port
A	00A0EE 2313A3	13
B	00A134 1A9032	14
C	00A301 9083B2	15
D	001B21 87C6D6	14

For example, when Workstation B sends a packet to the server, Switch #1 will use Port 14 of the trunk to transmit it to Switch #2.

An assignment of a source MAC address to a port trunk remains active as long as the source node remains active. If the MAC address times out, the assignment is dropped. Should the source node become active again and need to transmit a packet over the trunk, a new assignment is made, either to the same port or to a different port in the trunk.

It should be noted that packets sent back from the destination node to the original source node may travel the same or a different data link in the trunk.

As a general rule, the SA load distribution method is useful in situations where the number of source nodes equals or is greater than the number of data links in the trunk.

So when would the SA method be inappropriate? Returning to the example in Figure 21, assume you configured Switch #2 also for SA load distribution. The result would be that the switch would use only one data link in the trunk to send packets back to Switch #1, because there is only one source, a Gigabit Ethernet server, connected to Switch #2. Since there is only one source, only one data link is used. So obviously the SA method is not appropriate when there are fewer source nodes than data links.

So now let's look at the SA/DA method. A switch using the SA/DA method creates a matrix of the source and destination MAC addresses and then uses the matrix to determine which port in the trunk a frame is to be transmitted. With this method, packets from a particular source node might be sent over different data links in a trunk when sent to different destination addresses.

So let's take a look at how this might look in practice. Assume that you configured Switch #2 in our example for SA/DA. The result might be something similar to that shown in Table 2.

Table 2 Trunk Port Assignments in an SA/DA Matrix

	Destinations MAC Addresses			
Source MAC Address	Workstation A 00A0EE 2313A3	Workstation B 00A134 1A9032	Workstation C 00A301 9083B2	Workstation D 001B21 87C6D6
Server 00B012 DA0231	2	1	3	1

Even though there is only one source, all the data links in the trunk are used. For instance, if the server needed to send a packet to Workstation C, by referring to the matrix Switch #2 would use Port 3 of the trunk to transmit the packet from that particular source MAC address to Switch #1.

As you can see, the SA/DA method is useful when a port trunk needs to send packets from one source node to many destination nodes, something that the SA method is not suited for. Additionally, the SA/DA method is also valid when sending from many source nodes to one destination node, or from many sources to many destinations.

The table below shows a possible matrix for a port trunk of three data links using the SA/DA method, handling traffic from four sources to four destinations.

Table 3 Trunk Port Assignments in an SA/DA Matrix

	Destinations Addresses			
Source Addresses	**00A0EE 2313A3**	**00A134 1A9032**	**00A301 9083B2**	**001B21 87C6D6**
00B012 DA0231	1	2	3	1
001230 DA2943	2	3	1	2
0042AA D45A21	3	1	2	3
00456A C23521	1	2	3	1

The bottom line is that the SA/DA method is more flexible than the SA method. A general rule to follow is if you are not sure which load distribution to choose, you should probably go with SA/DA.

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. Be sure to review the guidelines in **Port Trunking Overview** on page 83 before performing the procedure.

Caution

Do not connect the cables to the trunk ports on the switches 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 creating a port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S62 management software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **3** to select Port Trunking.

   The Port Trunking menu is shown in Figure 22.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                   Port Trunking

1 - Trunk Ports ..... None

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 22 Port Trunking Menu

3. Type **1** to select Trunk Ports.

   The following prompt is displayed.

   ```
   Enter Trunk Port(s) ->
   ```

4. Enter the ports that will constitute the port trunk and press Return.

   You can specify the ports individually (e.g., 1,2,3,4) or as a range (e.g., 7-10).

   Once you have specified the ports of the trunk, the following menu selection appears:

   ```
   2 - Trunk Method ....... SA/DA trunking
   ```

   You use this selection to specify the load distribution method. The default is SA/DA.

5. To change the load distribution method, type **2** to toggle the selection through its possible settings of SA/DA and SA only trunking. The change in Port Trunking configuration is immediately activated on the switch.

6. Type **S** to select Save Configuration Changes.

7. Configure the ports on the remote switch for port trunking.

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

   The port trunk is ready for network operation.

Deleting a Port Trunk

> **Caution**
> Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting 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 from the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **3** to select Port Trunking.

   The Port Trunking menu is shown in Figure 22 on page 89.
3. Type **D** to select Delete trunk.

   A confirmation prompt is displayed.
4. Type **Y** for yes to delete the port trunk or **N** for no to cancel this procedure.

   The port trunk is immediately deleted from the switch.
5. Type **S** to select Save Configuration Changes.

Chapter 8
Port Mirroring

This chapter contains the procedures for creating and deleting a port mirror. Sections in the chapter include:

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the traffic being received and transmitted on one or more ports on a switch by having the traffic copied to another switch port. You can connect a network analyzer to the port where the traffic is being copied and monitor the traffic on the other ports without impacting network performance or speed.

Observe the following guidelines when creating a port mirror:

- ❑ You can mirror from one to 23 ports on a switch at a time. However, the more ports you mirror, the less likely the mirroring port will be able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the mirror port is likely to drop packets, meaning that it will not provide an accurate mirror of the traffic of the other six ports.
- ❑ The ports to be mirrored and the mirroring port must be located on the same switch.
- ❑ The ports to be mirrored and the mirroring port must be operating at the same speed. For example, you cannot use a 10/100 Mbps port to mirror traffic on a 1000 Mbps GBIC port.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **2** to select Port Mirroring.

   The Port Mirroring menu is shown in Figure 23.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                  Port Mirroring

1 - Mirror (Destination) Port ....... None
2 - Mirroring (Source) Port(s) ...... None

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 23 Port Mirroring Menu

3. Type **1** to select Mirror (Destination) Port.

   The following prompt is displayed.

   ```
   Enter Mirror port (0=None) [0 to 24] ->
   ```

4. Enter the number of the port to function as the mirror port (that is, the port to where the traffic will be copied). Press Return.

   You can specify only one mirror port.

5. Type **2** to select Mirroring (Source) Port.

   The following prompt is displayed.

   ```
   Enter Mirroring Ports (0=None):
   ```

6. Enter the number of the port whose traffic is to be mirrored. To mirror the traffic of more than one port, enter the ports individually (e.g., 1,4,6), as a range (e.g., 11-14), or both. Press Return.

   The port mirror is active on the switch. You can now connect a network analyzer to the mirror (destination) port to monitor the traffic on the other ports.

7. Type **S** to select Save Configuration Changes.

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **2** to select Port Mirroring.

   The Port Mirroring menu is shown in Figure 23 on page 94.
3. Type **1** to select Mirror (Destination) Port.

   The following prompt is displayed.

   ```
   Enter mirror port (0=None) [0 to 24] ->
   ```
4. Enter **0** and press Return.

   The port mirror on the switch is deleted. The port that was functioning as the port mirror is now available for normal network operations.
5. Type **S** to select Save Configuration Changes.

Chapter 9
STP and RSTP

This chapter provides background information on the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). The chapter also contains procedures on how to adjust the STP and RSTP bridge and port parameters. The sections in this chapter include:

Note
For detailed information on the Spanning Tree Protocol, refer to IEEE Std 802.1d. For detailed information on the Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

STP and RSTP Overview

A significant danger to Ethernet network performance is the existence of a data loop in a network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data link. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and significantly reduce network performance.

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

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

Where the two protocols differ is in the time each takes to complete the process commonly referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain intercommunications between the various network segments. This process is referred to as convergence.

With STP, convergence for a large network can take up to a minute to complete. This can result in lost data packets and the loss of intercommunication between various parts of the network during the convergence process.

RSTP is much faster. RSTP can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network.

Note
RSTP is activated by default on the switch.

The STP implementation on the AT-8000 Series Switch complies with the IEEE 802.1d standard. The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how STP and RSTP operate and define the different parameters that you can adjust.

Bridge Priority and the Root Bridge

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

A root bridge is selected by a combination of a *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's 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 can be changed on an AT-8000 Series switch. You can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

With STP, the bridge priority has a range of from 0 to 65535. You can select any value within that range.

With RSTP, the range is slightly less, from 0 to 61440. Furthermore, you can only select a value that is a multiple of 4096. To make this easier for you, the management software divides the range into increments. You specify the increment that represents the desired bridge priority value. The range is divided into sixteen increments, as shown in the following table.

Table 4 RSTP Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Path Costs and Port Costs

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 the 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 *root 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 determination of *path 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.

Path cost is determined through an evaluation of *port costs*. 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.

Path cost is simply the cumulation of the port costs between a bridge and the root bridge.

The port costs of the ports on an AT-8000 Series switch are adjustable through the management software, but the range is different depending on whether you are using STP or RSTP.

For STP, the range is 1 to 65535. You can assign a port a port cost of any value within the range. Below are the default values.

Table 5 STP Default Port Costs

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

In RSTP, the range is much greater: 0 to 20 000 000. This greater range allows you to have more control over path costs.

RSTP port cost also features an Auto-Detect feature. This features allows RSTP to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting on the ports when the switch is operating in RSTP. Table 6 lists the ports cost with Auto-Detect.

Table 6 RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2 000 000
100 Mbps	200 000
1000 Mbps	20 000

You can override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter can be used as a tie-breaker when two paths have the same cost.

In STP, the range for port priority is 0 to 255.

In RSTP, the range is 0 to 240. As with RSTP Bridge Priority, this range is broken into increments, in this case multiples of 16. When you specify a port priority for a port, you enter the increment of the desired value.

Table 7 RSTP Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Forwarding Delay and 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 temporarily 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-8000 Series 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.

Note
The forwarding delay parameter applies only to STP.

Hello Time and Bridge Packet Data Units (BPDU)

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 or RSTP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought on-line, 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-8000 Series switch. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8000 Series switch is selected as the Root Bridge of a spanning tree domain, it will transmit a BPDU every two seconds.

Point-to-Point Ports and Edge Ports

> **Note**
> This section applies only to RSTP.

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With port type defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- ❑ Point-to-point
- ❑ Edge port

If a bridge port is operating in full-duplex mode, than the port is functioning as point-to-point. Figure 24 illustrates two AT-8024 switches that have been interconnected with one data link. With the link operating in full-duplex, the ports are said to be point-to-point ports.

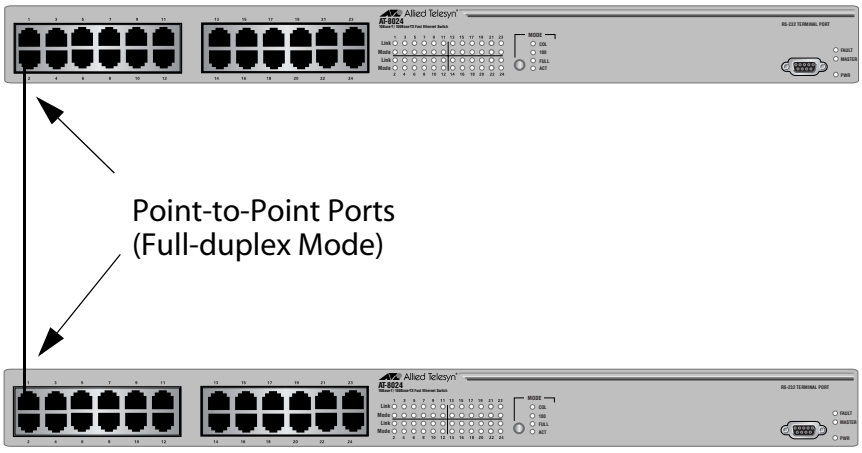

Figure 24 Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Figure 25 illustrates an edge port on an AT-8024 switch. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

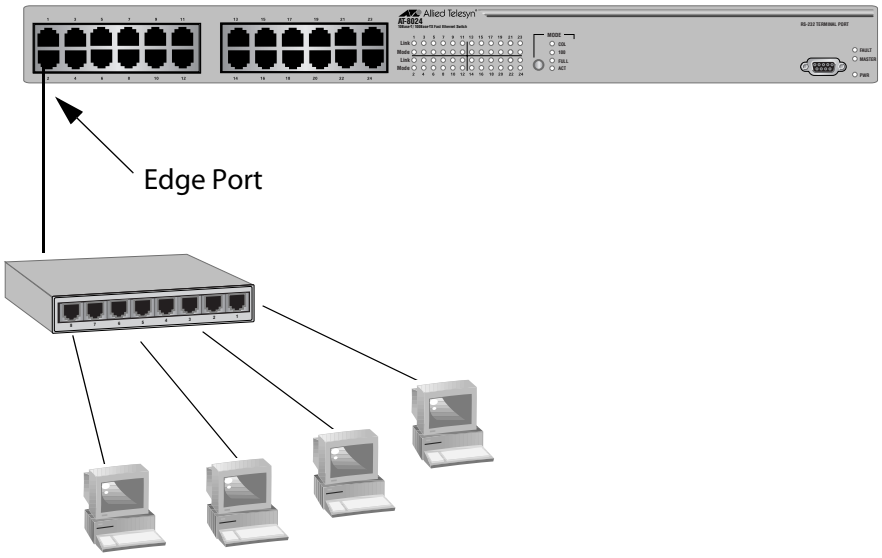

Figure 25 Edge Port

A port can be both point-to-point and edge at the same time. It would operate in full-duplex and have no STP or RSTP devices connected to it. Figure 26 illustrates a port functioning both as point-to-point and edge.

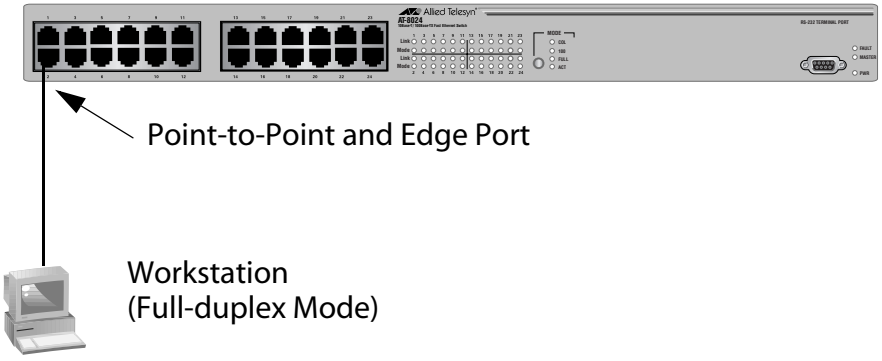

Figure 26 Point-to-Point and Edge Point

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason it might be best not to change the default values for this RSTP feature unless in have a good grasp of the concept. In most cases, the default values will work fine.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network should be able to operate together to create a single spanning tree domain.

There is no reason not to activate RSTP on an AT-8000 Series switch even when all other switches are running STP. The AT-8000 Series switch can combine its RSTP with the STP of the other switches. An AT-8000 Series switch will monitor the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets will operate in RSTP while ports receiving STP BPDU packets will operate in STP.

Spanning Tree and VLANs

The spanning tree implementation on an AT-8000 Series switch is a single-instance spanning tree. The switch supports just one spanning tree. You cannot define multiple spanning trees.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This point can pose a problem in networks containing multiple VLANs that span different switches and are connected with untagged ports. What can happen is that STP will block a data link because it detects a data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 27. Two VLANs, Sales and Production, span two AT-8024GB switches. Two links consisting of untagged ports interconnect the separate parts of each VLAN. If STP is activated on the switches, one of the links would be disabled. This problem can be avoided by not activating spanning tree or by connecting VLANs using tagged instead of untagged ports. (For information on tagged and untagged ports, refer to **Chapter 10, Virtual LANs Overview** on page 118.

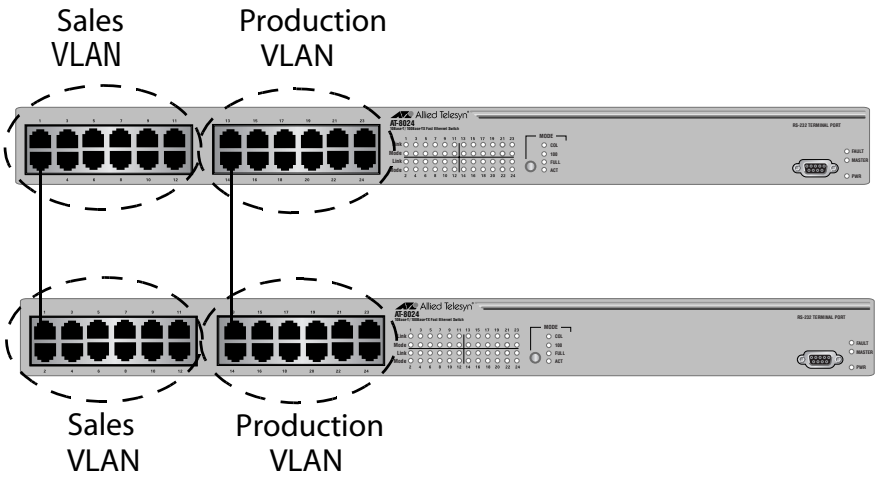

Figure 27 VLAN Fragmentation

Enabling or Disabling STP or RSTP

The AT-S39 software supports STP and RSTP. Only one spanning tree protocol can be active on the switch at a time. Before you can enable a spanning tree protocol or configure its settings, you must first select it as the active spanning tree protocol on the switch. The default active spanning tree is RSTP.

Note
Changing the active spanning tree protocol resets the switch. Some network traffic may be lost during the reset process.

To select and enable the active spanning tree protocol, or to disable spanning tree, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.

   The Spanning Tree Menu is shown in Figure 28.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                Spanning Tree Menu

1 - Spanning Tree Status ...... Disabled
2 - Active Protocol Version ... RSTP
3 - STP Configuration
4 - RSTP Configuration

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 28 Spanning Tree Menu

Note
To select a new active spanning tree, perform step 2. To enable or disable spanning tree on the switch, perform step 3.

2. To select a new active spanning tree protocol, do the following:

   a. Type **2** to select Active Protocol Version.

      The following prompt is displayed:

```
The switch will be rebooted for changing the
protocol version.
Do you want to continue? [Yes/No]
```

b. Type **Y** for yes to change the currently active spanning tree protocol, or **N** to cancel this procedure.

   The following prompt is displayed:

   ```
   Enter new active protocol version: S-STP, R-RSTP:
   ```

c. Type **S** to select STP or **R** to select RSTP.

   The following prompt is displayed:

   ```
   Enter Spanning Tree Status: E-Enable, D-Disable:
   ```

d. If you want the switch to enable the new active spanning tree protocol after resetting, type **E**. If you want spanning tree to remain disabled after the switch resets, type **D**. You might select the latter if you want to configure STP or RSTP parameters before enabling spanning tree.

   The switch resets and changes the active spanning tree protocol.

Note
Your management session with the switch is ended. To continue managing the unit, you must reestablish your session.

To configure STP settings, go to **Configuring STP** on page 107. To configure RSTP settings, go to **Configuring RSTP** on page 112.

3. To enable or disable spanning tree protocol on the switch, do the following:

   a. From the Spanning Tree Menu, type **1** to select Spanning Tree Status.

      The following prompt is displayed:

      ```
      Enter Spanning Tree Status: E-Enable, D-Disable:
      ```

   b. Enter **E** to enable spanning tree or **D** to disable it.

      A change to spanning tree status is automatically saved to permanent memory in the switch. You do not have to use the Save Configuration Changes option.

Configuring STP

This section contains the following procedures:

Configuring STP Bridge Settings

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

> ⚠ **Caution**
> The default STP parameters 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 Spanning Tree Menu, type **3** to select STP Configuration.

   The STP Menu is shown in Figure 29.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                     STP Menu

The current protocol version is STP.

1 - Bridge Priority ..... 32768
2 - Bridge Hello Time ... 2
3 - Bridge Forwarding ... 15
4 - Bridge Max Age ..... 20
5 - Bridge Identifier ... 00:30:84:11:11:11

6 - Config STP Port Settings
7 - Display STP Port Settings
8 - Reset STP to Defaults

R - Return to Previous Menu

Enter your selection?
```

Figure 29 STP Menu

2. Adjust the bridge STP settings as needed. The parameters are described below.

1 - 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. The range is 0 (zero) to 65,535, with 0 being the highest priority.

2 - Bridge Hello Time
The time interval in seconds between generating and sending configuration messages by the bridge. The range is 1 to 10 seconds. The default is 2 seconds.

3 - Bridge Forwarding
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 range is 4 to 30 seconds. The default is 15 seconds.

4 - Bridge Max 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. The range is 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1)).

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

5 - Bridge Identifier
The MAC address of the switch. This parameter cannot be changed.

6 - Config STP Port Settings
Configures the STP port parameters. For instructions, refer to **Configuring STP Port Settings** on page 109.

8 - Reset STP to Defaults
Resets all STP bridge and port settings to their default values. This option is available only when spanning tree is disabled on the switch. For instructions on disabling spanning tree, refer to **Enabling or Disabling STP or RSTP** on page 105.

3. After you have made the desired changes, type **S** to select Save Configuration Changes.
4. To change STP port settings, go to the next procedure.

Configuring STP Port Settings

To adjust a port's STP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **3** to select STP Configuration.
2. From the STP Configuration menu, type **6** to select Config STP port settings.

   The following prompt is displayed:

   ```
   Starting Port to Configure [1 to 24] ->
   ```
3. Enter the number of the port you want to configure. To configure a range of ports, enter the first port of the range.

   The following prompt is displayed:

   ```
   Ending Port to Configure [1 to 24] ->
   ```
4. To configure just one port, enter the same port number here as you entered in the previous step. To configure a range of ports, enter the last port of the range.

The STP Port Configuration menu is shown in Figure 30.

```
 Allied Telesyn AT-8024 Ethernet Switch - AT-S39
                  Sales Switch

Login Privilege: Manager

              Config STP Port Settings

Configuring Ports 4 to 4

1 - Participate ....... Yes
2 - Fast Mode ......... No
3 - Port Cost ......... Automatic Update
4 - Port Priority ..... 128
5 - Port State ........ Forwarding
6 - Root Bridge ....... 00:30:84:11:11:11

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 30 Config STP Port Settings Menu

5. Adjust the settings as desired. The parameters are described below.

Note
A change to the port priority parameter takes effect immediately. A change to the port cost value requires resetting the switch. A new port cost value is not implemented until the unit is reset.

1 - Participating
This selection activates and deactivates STP on the port. If set to Yes, which is the default, the port will participate in the spanning tree. If you select No, the port will continue to receive and transmit Ethernet frames, but it will not participate in spanning tree.

Note
A port on which STP is disabled is immediately placed in the forwarding state. It should be noted that a port where STP has been disabled cannot be placed in the blocking state by STP should there be a loop in the network topology. Consequently, it is incumbent on the network administrator to insure that no loop will develop should STP be disabled on a port.

2 - Fast Mode
The port will skip the Listening and Learning stages of STP. This setting is appropriate for ports connected to edge nodes that are not running STP. The default setting is disabled.

3 - Port 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 value for this parameter for all ports and speeds is 100. The range is 1 to 65535. To automatically set a port's STP port cost based on port speed, set the value to a "0".

4 - 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 default value for priority is 128. The range is 0 to 255.

5 - Port State
The current STP status of the port. The status can be Forwarding, Listening, Learning, or Blocking. This value cannot be changed.

6 - Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed. If STP has not been enabled on the switch, this parameter will not show a value.

6. After adjusting the parameters, type **S** to select Save Configuration Changes.

Configuring RSTP

This section contains the following procedures:

Configuring RSTP Bridge Settings

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

Caution
The default RSTP parameters are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Spanning Tree Menu, type **4** to select RSTP Configuration.

   The RSTP Menu is shown in Figure 31.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                   Sales Switch
Login Privilege: Manager
                      RSTP Menu

The current protocol version is RSTP

1 - Force Version .......... RSTP
2 - Bridge Priority ........ 32768
3 - Bridge Hello Time ...... 2
4 - Bridge Forwarding ...... 15
5 - Bridge Max Age ......... 20
6 - Bridge Identifier ...... 00:30:84:52:03:80
7 - Root Bridge ............ 00:30:84:52:03:80
8 - Root Priority .......... 32768

P - RSTP Port Parameters
D - Reset RSTP to Defaults

S - Save Configuration changes
R - Return to Previous Menu


Enter your selection?
```

Figure 31 RSTP Menu

2. Adjust the parameters as needed. The parameters are defined below.

   1 - Force Version
   This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. If you select RSPT, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge will operate in RSTP, using the RSTP parameter settings, but it will send only STP BPDU packets out the ports.

   2 - 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 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to **Table 4**, **RSTP Bridge Priority Value Increments** on page 98

   3 - 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.

   4 - Bridge Forwarding
   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, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

   5 - Bridge Max 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.

   In selecting a value for maximum age, the following must be observed:

   MaxAge must be greater than (2 x (HelloTime + 1)).

   MaxAge must be less than (2 x (ForwardingDelay - 1))

6 - Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

7 - Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed.

8 - Root Priority
The bridge priority on the root bridge. This value is for display purposes only and cannot be changed.

Note
Options 7 - Root Bridge and 8 - Root Priority are displayed only when RSTP is enabled on the switch.

P - RSTP Port Settings
Configures the RSTP port parameters. For instructions, refer to **Configuring RSTP Port Settings** on page 115.

D - Reset RSTP to Defaults
Resets all RSTP bridge and port settings to their default values. This option is available only when spanning tree is disabled on the switch. For instructions on disabling spanning tree, refer to **Enabling or Disabling STP or RSTP** on page 105.

3. After adjusting the parameters, type **S** to select Save Configuration Changes.

Configuring RSTP Port Settings

To adjust RSTP port parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **4** to select RSTP Configuration.
2. From the RSTP Configuration menu, type **P** to select RSTP Port Parameters. The RSTP Port Parameters menu is shown in Figure 31:

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                RSTP Port Parameters

The current protocol version is RSTP.

1 - Configure RSTP Port Settings
2 - Display RSTP Port Configuration
3 - Display RSTP Port State

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 32 RSTP Port Parameters

3. Type **1** to select Configure RSTP Port Settings.

   The following prompt is displayed:

   ```
   Starting Port to Configure [1 to 24] ->
   ```

4. Enter the number of the port you want to configure. To configure a range of ports, enter the first port of the range.

   The following prompt is displayed:

   ```
   Ending Port to Configure [1 to 24] ->
   ```

5. To configure just one port, enter the same port number here as you entered in the previous step. To configure a range of ports, enter the last port of the range.

The Configure RSTP Port Settings menu is shown in Figure 33.

```
    Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                    Sales Switch
Login Privilege: Manager
             Configure RSTP Port Settings
Configuring Ports 4 to 4
1 - Port Priority ...... 128
2 - Port Cost .......... Auto Update
3 - Point-to-Point ..... Auto Detect
4 - Edge Port .......... Yes

M - MCHECK (Check Migration to RSTP on Selected Ports)
S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 33 Configure RSTP Port Settings Menu

6. Adjust the settings as needed. The parameters are explained below.

   1 - Port 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 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to **Table 7**, **RSTP Port Priority Value Increments** on page 100.

   2 - Port 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 range is 0 to 20 000 000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2 000 000 for 10 Mbps ports, 200 000 for a 100 Mbps ports, and 20 000 for one gigabit ports.

   3 - Point-to-Point
   This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

   4 - Edge Port
   This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

M - MCHECK
This option instructs the bridge to send out RSTP BPDU packets for several seconds from the selected port. The purpose is to determine if there are any RSTP or STP bridges connected to the port. If the port receives STP BPDU packets in response, the port changes to STP compatible mode.

Note
The MCHECK option is visible and can be set only when RSTP is enabled on the switch.

All changes are immediately activated on the switch.

7. After making your changes, type **S** to select Save Configuration Changes.

Chapter 10
Virtual LANs Overview

This chapter contains overviews of tagged and port-based VLANs and the Basic VLAN Mode. It also explains how to select a VLAN mode. For the procedures for creating tagged and port-based VLANs, refer to the next chapter.

Sections in this chapter include:

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 traffic domain where the traffic generated by the nodes of a VLAN remains within the VLAN. A router or Layer 3 network device is required in order for traffic to cross a VLAN boundary.

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 a LAN segment vying for bandwidth, the greater the likelihood overall network performance will decrease.

  VLANs improve network performance because VLAN 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, because each VLAN constitutes a separate broadcast domain, broadcast traffic remains within a VLAN. This too can improve overall network performance.

- Increased security

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

- 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 LAN segment assignments through the switch's AT-S62 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

The AT-8000 Series switch supports the following VLAN modes:

- ❑ User-configured (Tagged) VLAN Mode
  - — Port-based VLANs
  - — Tagged VLANs
- ❑ Basic VLAN Mode
- ❑ 802.1Q compliant Multiple VLAN Mode
- ❑ non-802.1Q compliant Multiple VLAN Mode

The User-configured VLAN mode and the Basic VLAN Mode are explained in this chapter. The two multiple VLAN modes are described in **Chapter 12**, **Multiple VLAN Modes** on page 153.

Note
The user-configured VLAN Mode is 802.1Q compliant.

User-Configured VLAN Mode Overview

The user-configured VLANs mode lets you create your own VLANs. You can create two types of VLANs:

- ❑ Port-based VLANS (discussed in the following section)
- ❑ Tagged VLANs (see **Tagged VLAN Overview** on page 128)

Port-based VLAN Overview

Port-based VLANs are the simplest and most common form of a VLAN. In a port-based VLAN configuration, each port of the switch is assigned to a particular VLAN. Each port can belong to only one port-based VLAN at a time.

For example, you can designate ports 1, 2, and 3 as part of the Engineering VLAN and ports 5, 6, and 7 as part of the Marketing VLAN.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. Additionally, a port-based VLAN can span switches and consist of ports from multiple Ethernet switches.

> **Note**
> The AT-8000 Series switch is pre-configured with one port-based VLAN. All ports on the switch are members of this VLAN, called the Default_VLAN.

A port-based VLAN contains the following elements:

- ❑ VLAN name
- ❑ VLAN Identifier
- ❑ Untagged ports
- ❑ Port VLAN Identifier

VLAN Name

To create a port-based VLAN, you must give it a name. The name typically reflects the function of the network devices that are members of the VLAN.

VLAN Identifier

Each VLAN in a network requires a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you would assign it a VID unique from all other VLANs in your network.

If a VLAN spans multiple switches, the VID for the VLAN on the different switches should be identical. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN titled Marketing that spanned three AT-8024 switches, you would assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the management software to automatically perform this function. If you allow the management software to automatically assign the VID, the next available VID will be selected. If you are creating a VLAN on a switch that is part of a larger VLAN that spans several switches, you must manually assign the number so that the VLAN has the same VID across all switches linked in that VLAN.

Untagged Ports

You must specify which ports on the switch are members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The term *untagged* derives from the fact that the frames received on a port will not contain any information that indicates VLAN membership, and that such membership will be determined solely by the port's PVID.

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID 5. Consequently, the PVID for each port in the VLAN would need to be assigned the value 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S39 management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is an untagged member.

General Rules for Creating Port-Based VLANs

Below is a summary of the general rules to observe when creating port-based VLANs.

- ❑ Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches must be assigned the same VID.
- ❑ A port can be an untagged member of only one port-based VLAN at a time.
- ❑ Each port must be assigned a PVID. This value is assigned automatically by the AT-S39 management software. The value is the same for all ports in a port-based VLAN and is identical to the VLAN's VID.
- ❑ A port-based VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where 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 interconnect the VLANs.

Drawbacks to Port-based VLANs

Drawbacks to port-based VLANs:

- ❑ Sharing network resources, such as servers and printers, across multiple VLANs can be difficult. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs. The introduction of a router into the network can create security issues, including unauthorized access to your network.
- ❑ A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches requires one port on each switch to interconnect the various sections of that VLAN.

In network configurations with many individual VLANs that span switches, ports are often ineffectively used to interconnect the various VLANs.

Port-based Example 1

Figure 34 illustrates an example of one AT-8024 Fast Ethernet Switch with three port-based VLANs. (For purposes of the following examples, the Default_VLAN is not shown.)

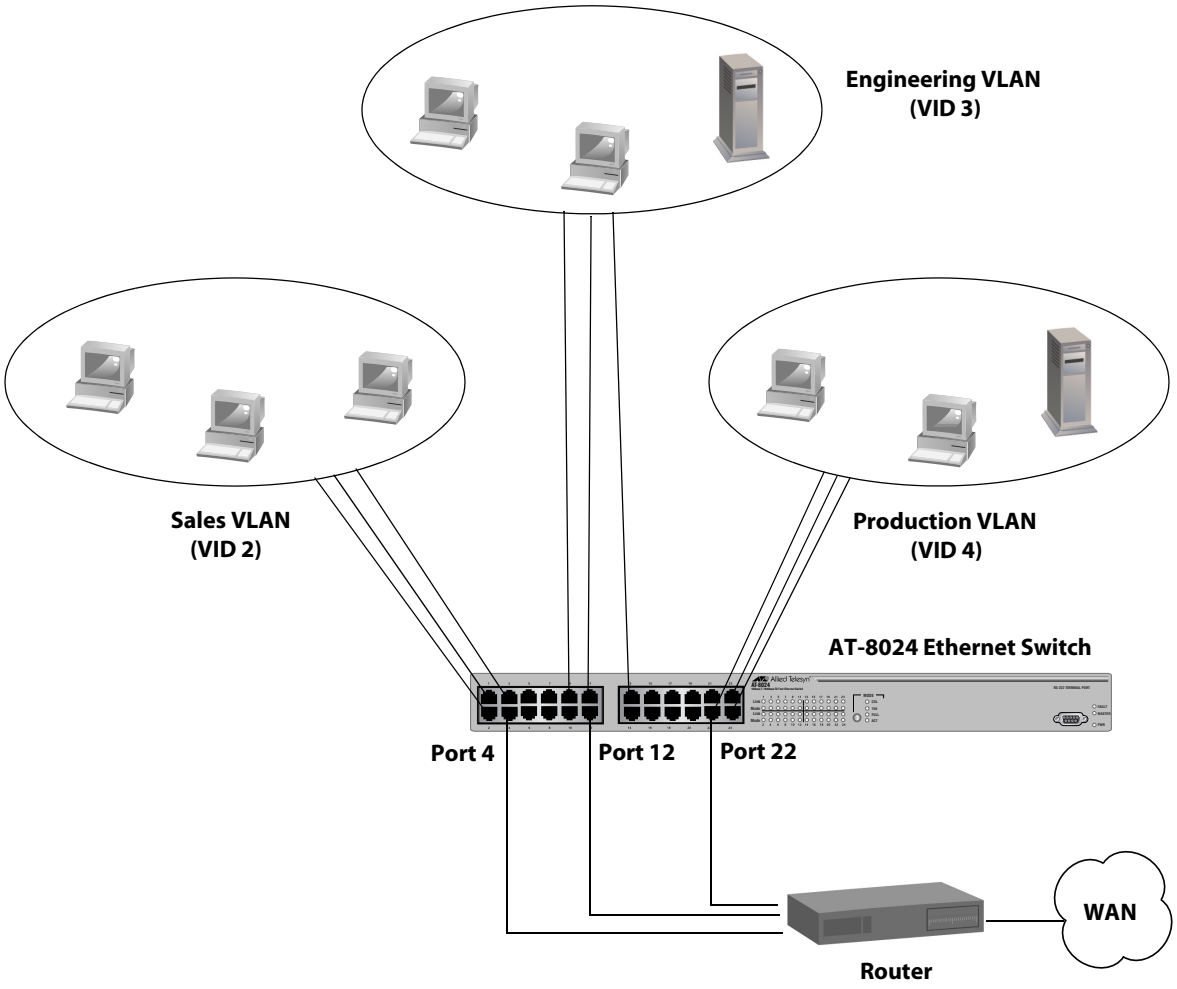

Figure 34 Port-based VLAN - Example 1

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switch.

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-8024 (top)	Ports 1 - 4 (PVID 2)	Ports 9, 11 - 13 (PVID 3)	Ports 21 - 24 (PVID 4)

Each VLAN has been assigned a unique VID. You assign this number when you create a VLAN.

The ports have been assigned PVID values. A port's PVID is assigned automatically by the management software when you create the VLAN. A PVID is the same as the VID to which the port is an untagged member.

In the example, each VLAN has one port connected to the router. The router interconnects the various VLANs and provides access to the WAN.

Port-based Example 2

Figure 35 illustrates more port-based VLANs. In this example, two VLANs span more than one Ethernet switch.

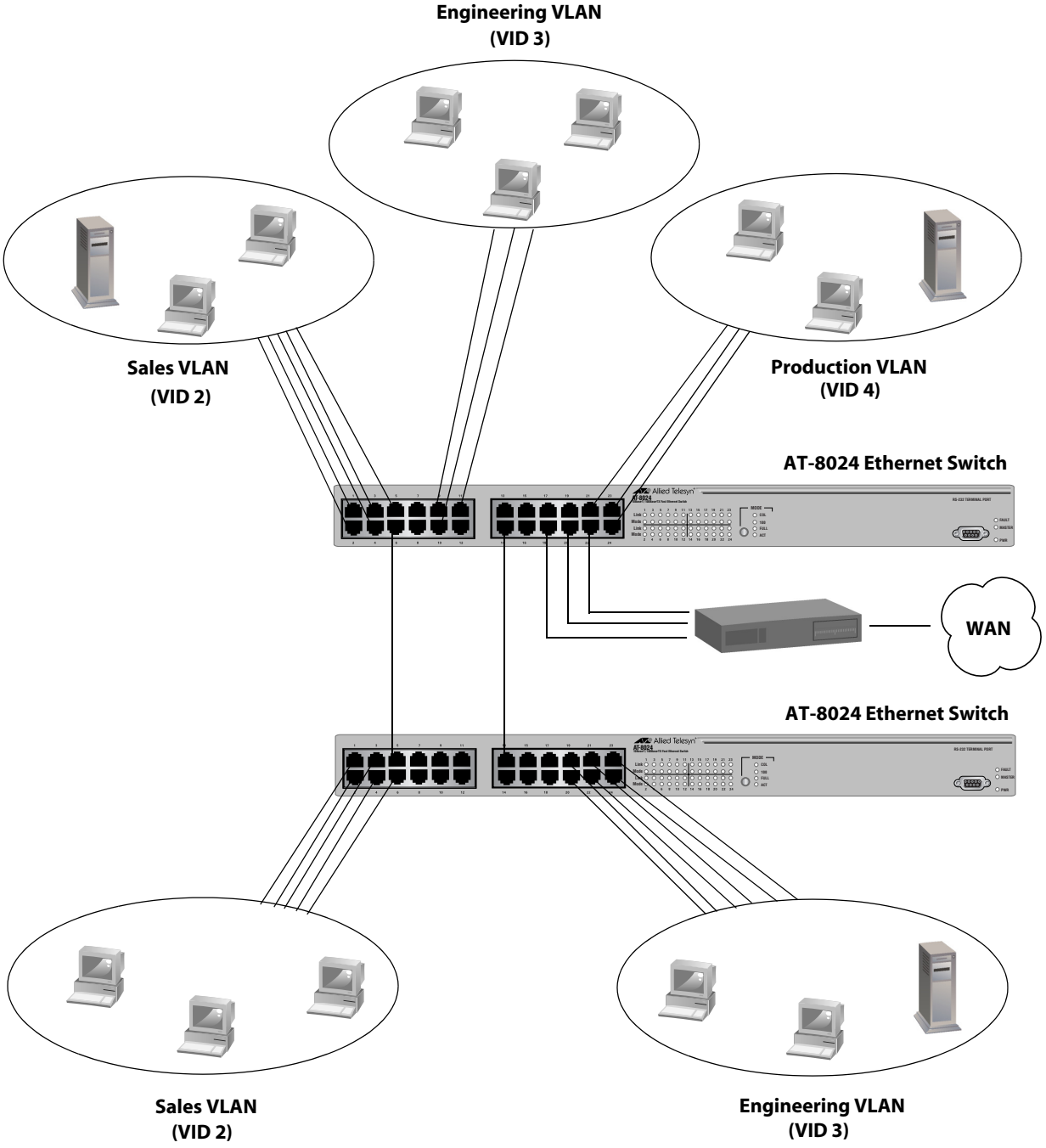

Figure 35 Port-based VLAN - Example 2

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-8024 (top)	Ports 1 - 6, 18 (PVID 2)	Ports 9 - 11, 14, 20 (PVID 3)	Ports 21 - 24 (PVID 4)
AT-8024 (bottom)	Ports 1 - 6 (PVID 2)	Ports 13, 19-24 (PVID 3)	none

- Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of seven untagged ports on the top switch and six untagged ports on the bottom switch.

  The two parts of the VLAN are interconnected by a direct link from Port 6 on the top switch to Port 5 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.

  Port 18 on the top switch connects to the router. This port allows the Sales VLAN to exchange Ethernet frames with the other VLANs and to access the WAN.

- Engineering VLAN - This port-based VLAN uses Ports 9 to 11 on the top switch and Ports 19 to 24 on the bottom switch as connections to the workstations of the VLAN.

  Since this VLAN spans multiple switches, it needs a direct connection between its various parts to provide a communications path. This is provided in the example with a direct connection from Port 14 on the top switch and Port 13 on the bottom switch.

  This VLAN uses Port 20 on the top switch as a connection to the router and the WAN.

- Production VLAN - This is the final VLAN in the example. It has the VLAN of 4 and its ports have been assigned the PVID also of 4.

  The nodes of this VLAN are connected to only the top switch. So this VLAN does not require a direct connection to the bottom VLAN. However, it uses Port 22 as a connection to the router.

Tagged VLAN Overview

The second type of user-configured VLAN supported by the AT-8000 Series switch is the *tagged VLAN*. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This contrasts to a port-based VLAN, where the PVIDs assigned to the ports 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). As explained earlier in this chapter in **VLAN Identifier** on page 121, this number uniquely identifies each VLAN in a network.

When a tagged port receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that are members of the VLAN whose VID matches the tag in the frame.

A port receiving or transmitting tagged frames is referred to as a *tagged port*. 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 a tagged VLAN is that the tagged ports 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, a 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 is accepted and forwarded to the appropriate port. If the frame's VID does not match any of the VLANs that the port is a member of, the frame is discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- ❑ VLAN Name
- ❑ VLAN Identifier
- ❑ Tagged and Untagged Ports

- ❑ Port VLAN Identifier

Note
For explanations of VLAN name and VLAN identifier, refer back to **VLAN Name** and **VLAN Identifier** on page 121.

Tagged and Untagged Ports

You must specify which ports are members of the VLAN. In the case of a tagged VLAN, VLAN members are usually a combination of both tagged and untagged ports. When you create the VLAN, you specify which ports are tagged and which ports are untagged.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the management software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID.

Because a tagged port determines VLAN membership by examining the tagged header within the frames that it receives and not by the PVID, you might conclude there is no need for a PVID. However, the PVID is used if a tagged port receives an untagged frame—a frame without any tagged information. The port forwards the frame based on the port's PVID. This is only in cases where an untagged frame arrives on a tagged port. Otherwise, the PVID of a port is ignored on a tagged port.

General Rules to Creating a Tagged VLAN

Below is a summary of the rules to observe when creating a tagged VLAN.

- ❑ Assign each tagged VLAN a unique VID. If a particular VLAN spans multiple switches or stacks, each part of that VLAN on the different switches or stacks must be assigned the same VID.
- ❑ A tagged port can be a member of multiple VLANs.
- ❑ An untagged port can be an untagged member of only one VLAN at a time.

- The AT-8000 Series switch can support up to 32 tagged and port-based VLANS.

Tagged VLAN Example

Figure 36 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

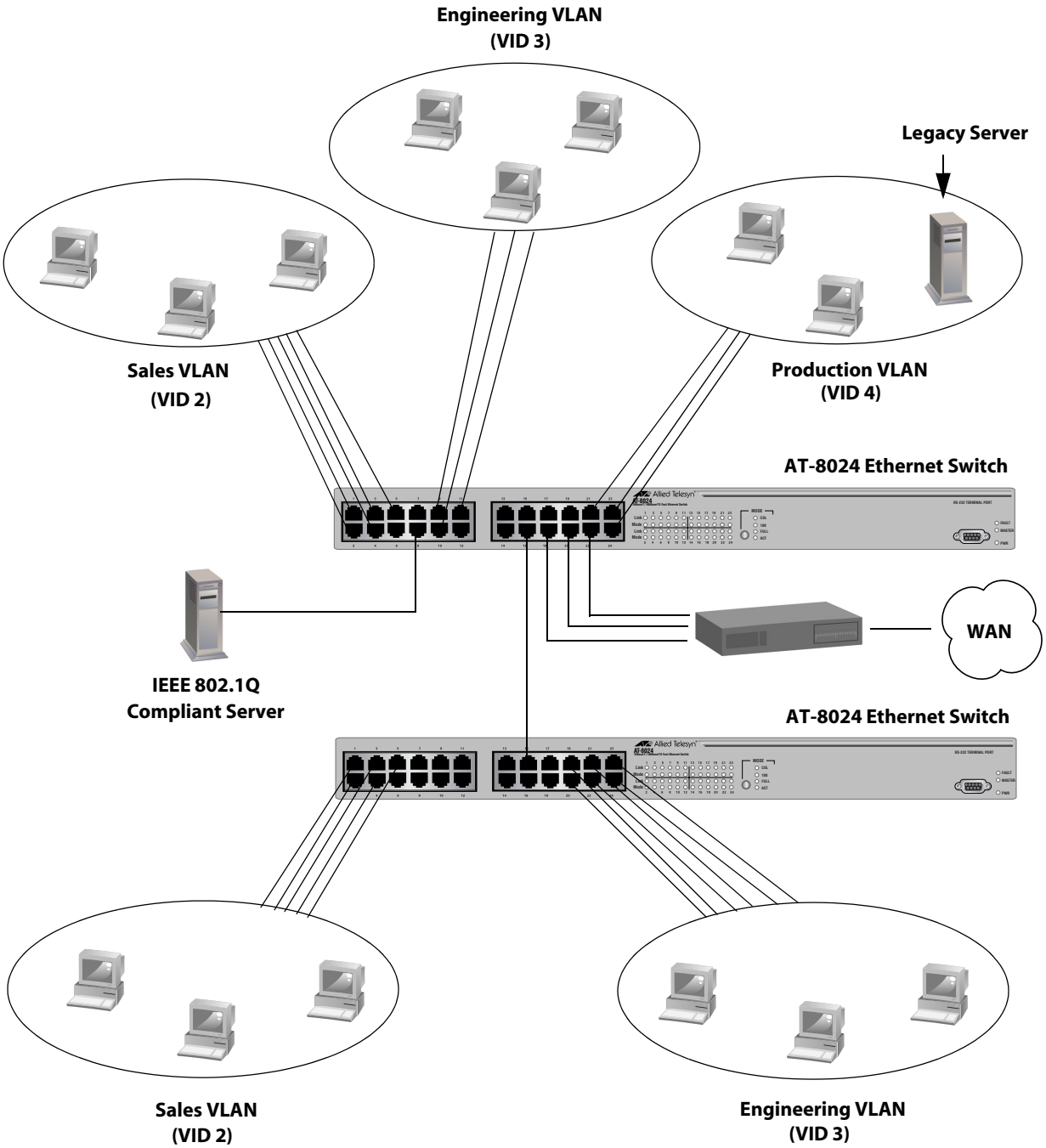

Figure 36 Example of a Tagged VLAN

The port assignments for the VLANs are as follows:

Switch	**Sales VLAN (VID 2)**		**Engineering VLAN (VID 3)**		**Production VLAN (VID 4)**	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8024 (top)	1 to 5, 18 (PVID 2)	8, 16	9 to 11, 20 (PVID 3)	8, 16	21 to 24 (PVID 4)	8
AT-8024 (bottom)	1 to 5 (PVID 2)	15	19 to 24 (PVID 3)	15	none	none

This example is similar to the **Port-based Example 2** on page 126. Tagged ports have been added to simplify network implementation and management.

Port 8 is a tagged port on the top switch. This port has been made a tagged member of the three VLANs. It is connected to an IEEE 802.1Q-compliant server, meaning the server can handle frames from multiple VLANs. Now all three VLANs can access the server without having to access a router or other interconnection device.

It is important to note that even though the server is receiving and transmitting frames between more than one VLAN, data remains separated and secure.

In the example, Port 16 on the top switch and Port 15 on the bottom switch are tagged ports used to simplify network design. These ports are tagged members of the Sales and Engineering VLANs. These ports provide a connection between the different parts of the two VLANs.

In the **Port-based Example 2** on page 126, each VLAN required its own data link between the switches to connect the different parts of the VLANs. With tagged ports, you can use one data link to carry data traffic from several VLANs, while still maintaining data separation and security. The tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the tagged frame originated.

Procedures for user-configured VLANs can be found in **Creating Port-based and Tagged VLANs** on page 134.

Basic VLAN Mode Overview

The Fast Ethernet switches support a special VLAN configuration referred to as Basic VLAN Mode. When the Basic VLAN Mode is activated, frames are forwarded based solely on MAC addresses. All VLAN information, including PVIDs assigned to ports and VLAN tags in tagged frames, is ignored. Tagged frames are analyzed only for priority level.

Packets are passed through the switch unchanged. Tagged and untagged frames exit the switch the same as they entered, either tagged or untagged.

You can continue to create and modify port-based and tagged VLANs when the Basic VLAN Mode is activated, but the VLANs are ignored.

Note
For instructions on how to activate the Basic VLAN mode, refer to **Setting the VLAN Mode** on page 133.

Setting the VLAN Mode

The procedure in this section explain how to set the switch for either the user configured (Tagged) VLAN mode, which supports tagged and port-based VLANs, or the Basic VLAN mode. The default setting for the switch is the user configured (Tagged) VLAN mode. (To configure the switch for a Multiple VLAN mode, refer to **Activating or Deactivating a Multiple VLAN Mode** on page 159.

To set the VLAN mode on the switch, do the following:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **1** to select VLANs Status (the current VLAN status is shown in this menu). The following prompt is displayed:

   ```
   Enter VLAN Status (E-Enable, D-Disable) ->
   ```

3. Type **E** to enable VLAN status if you want the switch to support port-based and tagged VLANs. This is the default. Type **D** to disable VLAN status if you want the switch to ignore all VLAN information and to operate in the Basic VLAN mode. Press Return.
4. Type **2** to select Ingress Filtering Status. The following prompt is displayed:

   ```
   Enter Ingress Filtering Status (E-Enable, D-
   Disable) ->
   ```

5. Do one of the following

   - ❑ If you enabled VLAN status in step 3, type **E** to enable filtering if you want tagged packets filtered as they enter a switch port, or **D** if you do not want tagged packets filtered as they enter a switch port. For more information on ingress filtering, refer to **Enabling or Disabling Ingress Filtering** on page 149.
   - ❑ If you disabled VLAN status for the Basic VLAN mode, type **D** to disable ingress filtering.

   A change to the VLAN status is immediately activated on the switch.

6. Type **S** to select Save Configuration Changes.

> **Note**
> The above procedure is the recommended method for setting a switch's VLAN mode. An alternative method is using Option 2 - Switch Mode in the System Configuration Menu.

Chapter 11
Creating Port-based and Tagged VLANs

This chapter contains procedures for creating, modifying, and deleting user-configured VLANs from a local or Telnet management session. To create VLANs, the switch's VLAN mode must be set to the User Configure (Tagged) VLAN mode, which is the default setting. For instructions on setting the switch mode, please refer to **Setting the VLAN Mode** on page 133.

This chapter contains the following sections:

Note
For background information on VLANs, refer to **Chapter 10**, **Virtual LANs Overview** on page 118.

Creating a New Port-based or Tagged VLAN

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

1. From the Main Menu, type **2** to select VLAN Menu.

   The VLAN Menu is shown in Figure 37.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                      VLAN Menu

1 - VLANs Status .................Enabled
2 - Ingress Filtering Status ....Enabled
3 - VLANs Mode ...................User Configured
4 - Management VLAN ..............1 (Default_VLAN)
5 - Configure VLANs
6 - Configure COS Priorities
7 - Show VLANs
8 - Show PVIDs & Priorities

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 37 VLAN Menu

2. From the VLAN Menu, type **5** to select Configure VLANs.

   The Configure VLANs menu is shown in Figure 38.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                   Configure VLANs

1 - Create VLAN
2 - Modify VLAN
3 - Delete VLAN
4 - Clear All Vlans

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 38 Configure VLANs Menu

3. From the Configure VLANs menu, type **1** to select Create VLAN.

   The Create VLAN menu is shown in Figure 39.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

                   Create VLAN

1 - VLAN Name ............
2 - VLAN ID (VID) ........ 2
3 - Tagged Ports .........
4 - Untagged Ports .......
5 - Mirror Port ....... None

C - Create VLAN
R - Return to Previous Menu

Enter your selection?
```

Figure 39 Create VLAN Menu

4. Type **1** to select VLAN Name and enter a name for the new VLAN. The VLAN name can be from one to fifteen characters in length. The name should reflect the function of the nodes that will be members 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 switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

   Note
   A VLAN must be assigned a name.

5. Type **2** to select VLAN ID (VID) and enter a VID value for the new VLAN. The permitted range of the VID value is 2 to 4094.

   The management software will use the next available VID number on the switch as the default value. If this VLAN will be unique in your network, then its VID must also be unique. If this VLAN will be part of a larger VLAN that spans multiple switches, than the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you should assign the Sales VLAN on each switch the same VID value.

   The switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-8024 switch to a network that already

has VLANs using VIDs 2 through 24, the AT-S39 software will still use VID 2 as the default value for the first VLAN you create on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Note
A VLAN must have a VID.

6. If the VLAN will contain tagged ports, type **3** to select Tagged Ports and specify the ports. If this VLAN will not contain any tagged ports, leave this field empty. 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).
7. Type **4** to select Untagged Ports and specify the ports on the switch to function as untagged ports in the VLAN. If this VLAN will not contain any untagged ports, leave this field empty. 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).
8. If you want all received traffic on the ports of the VLAN to be mirrored to another port on the switch, type **5** to select Mirroring Port and enter a port number when prompted.

   This feature is useful when troubleshooting a VLAN. By placing a packet sniffer on the mirroring port, you can analyze the VLAN traffic.

   Note
   In most cases, this parameter should be left with its default value of 0. A value of 0 means that the VLAN traffic will not be mirrored. For more information on port mirroring, refer to **Port Mirroring Overview** on page 93.

9. Type **C** to select Create VLAN.

   If the switch is successful in creating the new VLAN, you will see the following message:

   ```
   SUCCESS - Press any key to continue.
   ```

   The new VLAN is now active on the switch.

10. Press any key.

    The Configure VLANS menu in Figure 38 is displayed.

11. Type **S** to select Save Configuration Changes.

12. Press Esc or type **R** to return to the Configure VLANS menu. To verify that the VLAN was created correctly, complete steps 13 through 14. Otherwise, you can repeat this procedure to create additional VLANs.
13. Type **7** to select Show VLANs.
14. Check to see that the VLAN was created correctly and that it contains the appropriate ports. If you need to modify the VLAN, go to **Modifying a VLAN** on page 141.

Note
Ports designated as untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

Example of Creating a Port-based VLAN

The following procedure creates the Sales VLAN illustrated in Figure 34 on page 124. This VLAN will be assigned a VID of 2 and will consist of four untagged ports, Ports 1 to 4. The VLAN will not contain any tagged ports and the VLAN traffic will not be mirrored on another port.

To create the example Sales VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **1** to select Create VLAN.
4. Type **1** to select VLAN Name and enter "Sales". Press Return.
5. Type **2** to select VLAN ID (VID) and enter "2". This is the VID value for the new VLAN. Press Return.
6. Type **4** to select Untagged Ports and enter "1-4". These are the untagged ports of the VLAN. Press Return.
7. Type **C** to select Create VLAN.
8. After the switch displays the prompt notifying you that it created the VLAN, press any key.

   The new Sales VLAN has been created.

9. Type **S** to select Save Configuration Changes.

Example of Creating a Tagged VLAN

The following procedure creates the Engineering VLAN in the top switch illustrated in Figure 36 on page 130. This VLAN will be assigned a VID of 3. It will consist of four untagged ports, Ports 9, 10, 11, and 20, and two tagged ports, Ports 8 and 16. The VLAN traffic will not be mirrored on another port.

To create the example Engineering VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANs.
3. From the Configure VLANs menu, type **1** to select Create VLAN.
4. Type **1** to select VLAN Name and enter “Engineering”. Press Return.
5. Type **2** to select VLAN ID (VID) and enter “3”. This is the VID value for the new VLAN. Press Return.
6. Type **3** to select Tagged Ports and enter “8,16”. These are the tagged ports of the VLAN. Press Return.
7. Type **4** to select Untagged Ports and enter “9-11, 20”. These are the untagged ports of the VLAN. Press Return.
8. Type **C** to select Create VLAN.
9. After the switch displays the prompt notifying you that it created the VLAN, press any key.

   The new Engineering VLAN has been created.

10. Type **S** to select Save Configuration Changes.

Modifying a VLAN

Note
To modify a VLAN, you need to know its VID. To view VLAN VIDs, refer to the procedure **Displaying VLAN Information** on page 144.

To modify a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **2** to select Modify a VLAN.

   The Modify a VLAN menu is shown in Figure 40.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                   Sales Switch

Login Privilege: Manager

                    Modify VLAN

1 - VLAN ID (VID) ........

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 40 Modifying a VLAN Menu

4. Type **1** to select VLAN ID (VID).

   The following prompt is displayed:

   ```
   Enter new value -> [1 to 4096] ->
   ```

5. Enter the VID of the VLAN you want to modify. Press Return.

   The Modify a VLAN menu for the selected VLAN is displayed. This menu contains all relevant information about the VLAN.

6. Change the VLAN's information as desired.

   The menu selections are described below:

   1 - VLAN Name
   Use this selection to change a VLANs name. The name can be from one to fifteen characters in length. 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 (!).

When changing a VLAN's name, observe the following guidelines:

- ❑ A VLAN's new name cannot be the same as the name of another VLAN on the same switch. For example, if the switch already contains a VLAN called Sales, you cannot change an existing VLAN's name to Sales.
- ❑ You cannot change the name of the Default_VLAN.

Note
A VLAN must have a name.

2 - VLAN ID (VID)
This is the VLAN's VID value. You cannot change this value.

3 - Tagged Ports
Use this selection to add or remove tagged ports from 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).

When adding or removing tagged ports, observe the following guidelines:

- ❑ To add or remove tagged ports, enter the new list of tagged ports for the VLAN. The new list will overwrite the existing ports. Consequently, to retain a port, you must reenter it. For example, if the VLAN currently contains tagged port 4 and you wanted to add port 7, you would enter "4,7".
- ❑ If the VLAN will not contain any tagged ports, leave this field empty.
- ❑ If the VLAN contains tagged ports and you want to remove them all, enter a 0 (zero) for this value.

4 - Untagged Ports
Use this selection to add or remove untagged ports from 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).

When adding or removing untagged ports, observe the following guidelines:

- ❑ To add or remove untagged ports, enter the new list of untagged ports for the VLAN. The new list will overwrite the existing ports. Consequently, to retain a port, you must reenter it. For example, if the VLAN currently contains untagged ports 15 through 19 and you want to add ports 4 through 9, you would enter "4-9,15-19".

- ❑ If the VLAN does not contain untagged ports, leave this field empty.
- ❑ To remove all untagged ports from a VLAN, enter a 0 (zero) for this value.
- ❑ You cannot remove untagged ports directly from the Default_VLAN. Instead, you remove an untagged port from the Default_VLAN by assigning the port as an untagged port to another VLAN.

An untagged port removed from a VLAN is automatically returned to the Default_VLAN as an untagged port.

5 - Mirroring Port
Use this option to direct all received traffic on the ports of the VLAN to a mirror port on the switch. This feature is useful when troubleshooting a VLAN. By placing a packet sniffer on the mirroring port, you can analyze the VLAN traffic.

Note
In most cases, this parameter should be left with its default value of 0. A value of 0 means that the VLAN traffic will not be mirrored. For more information on port mirroring, refer to **Port Mirroring Overview** on page 93.

7. After making the desired changes, type **M** to select Modify VLAN.

   A confirmation prompt is displayed.

8. Press any key.

   The VLAN is modified. Changes to a VLAN are immediately activated on the switch.

9. Type **S** to select Save Configuration Changes.
10. Repeat this procedure starting with Step 4 to modify other VLANs.

Displaying VLAN Information

To view the name, VID number, and member ports of all the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **7** to select Show VLANs.

   An example of the Show VLANs menu is shown Figure 41.

```
            Allied Telesyn Ethernet Switch AT-8024
                          Show VLANs
Login Privilege: Manager
VID          VLAN Name      Mirror  Untagged (U) / Tagged (T)
-----------------------------------------------------------------


1            Default_VLAN           U: 20-24
                                    T: 7,9
2            Sales                  U: 1-7
                                    T: 9
3            Production             U: 8-19
                                    T: 7


N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 41 Show VLANs Menu - User Configured

Deleting a VLAN

This procedure deletes a port-based or tagged VLAN. All untagged ports in a deleted VLAN are returned to the Default_VLAN. You cannot delete the Default_VLAN.

Note
To delete a VLAN, you need to know its VID. To view VLAN VIDs, refer to the procedure **Displaying VLAN Information** on page 144.

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **3** to select Delete VLAN.

   The Delete a VLAN menu is shown in Figure 42.

```
Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager
                  Delete a VLAN
1 - VLAN ID (VID) ........

R - Return to Previous Menu

Enter your selection?
```

Figure 42 Delete a VLAN Menu

4. Type **1** to select VLAN ID (VID).

   The following prompt is displayed:

   ```
   Enter new value -> [2 to 4096] ->
   ```

5. Enter the VID of the VLAN you want to delete and press Return.

Note
You cannot delete the Default_VLAN, which has a VID of 1.

The specifications of the selected VLAN are displayed. Use this menu to confirm that you are deleting the correct VLAN.

6. Type **D** to delete the VLAN or **R** to cancel the procedure.

   The following confirmation prompt is displayed:

   ```
   Are you sure you want to delete this VLAN [Yes/No] ->
   ```

7. Type **Y** to delete the VLAN or **N** to cancel the procedure. Press Return.

   A confirmation message is displayed:

8. Press any key.
9. Type **S** to select Save Configuration Changes.

   The VLAN has been deleted. All untagged ports in the deleted VLAN are returned to the Default_VLAN as untagged ports.

10. Repeat this procedure starting with Step 4 to delete other VLANs.

Deleting All VLANs

This section contains the procedure for deleting all port-based and tagged VLANs, except the Default_VLAN, on a switch.

> **Note**
> To delete selected VLANs, perform the procedure **Deleting a VLAN** on page 145.

To delete all VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **4** to select Clear All VLANs.

   The following confirmation message is displayed:

   ```
   This operation deletes ALL user created VLANs!
   Do you want to continue [Yes/No] ->
   ```

4. Type **Y** to delete all VLANs or **N** to cancel the procedure. Press Return.

   A confirmation message is displayed.

5. Press any key.
6. Type **S** to select Save Configuration Changes.

   All VLANs are deleted and all ports are returned to the Default_VLAN as untagged ports.

Displaying PVIDs and Priorities

The following procedure displays a window that lists the PVIDs for all the ports on the switch. The window also contains the current priority queue settings for each port. To display the PVID settings on the switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **8** to select Show PVIDs & Priorities.

   The Show PVIDs & Priorities window is displayed. An example of the window is shown in Figure 43.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
             Show PVIDs & Priorities

Port  PVID      Priority   Override Priority
-------------------------------------------

01     1           0              No
02     1           0              No
03     1           0              No
04     1           0              No
05     1           0              No
06     1           0              No
07     1           0              No

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 43 Show PVIDs and Priorities Window

The PVID column displays the current PVID value for each switch port.

Note
The Priority and Override Priority columns relate to the switch's Class of Service feature. For information, refer to **Chapter 14**, **Class of Service** on page 174.

Enabling or Disabling Ingress Filtering

There are certain rules that a switch follows as it receives and forwards an Ethernet frame. There are rules for frames as they enter a port (called *ingress rules*) and rules for when a frame is transmitted out a port (called *egress rules*). A switch will not accept and forward a frame unless the frame passes the ingress and egress rules.

There are quite a few ingress and egress rules for Fast Ethernet switches. Fortunately, this discussion need only review the rules as they apply to tagged frames, because ingress filtering does not apply to untagged frames, nor to any frames, tagged or untagged, when the switch is operating in the Basic Mode.

First, just as a reminder, a tagged frame is an Ethernet frame that contains a tagged header. The header contains the VID of the VLAN to which the frame originated. For further information, refer to **User-Configured VLAN Mode Overview** on page 121.

Let's first examine how the ingress rules are applied to tagged frames when ingress filtering is enabled. What the switch does is it examines the tagged header of each tagged frame that enters a port and determines whether the tagged frame and the port that received the frame are members of the same VLAN. If they belong to the same VLAN, the port accepts the frame. If they belong to different VLANs, the port discards the frame.

Here is an example. Assume that a tagged frame with a VID of 4 is received on a tagged port that is a member of a VLAN also with a VID of 4. In this case, the port accepts the frame, because both the frame and the port belong to the same VLAN. If the frame and port had belonged to different VLANs, the frame is discarded.

So how do the ingress rules apply when ingress filtering is disabled? First, any tagged frame is accepted on any port on the switch. It does not matter whether the frame and the port belong to the same or different VLANs.

Once the tagged frame is received, the switch examines the tagged header and determines if the VID in the header corresponds to any VLANs on the switch. If there isn't a corresponding VLAN, the switch discards the frame. If there is, the switch transmits the frame out the port to the destination node, assuming that the destination node's MAC address is in the MAC address table, or floods the port to all ports on the VLAN if the MAC address is not in the table.

There is one other thing that should be mentioned about ingress filtering and tagged packets, and that is the priority tag. Each tagged frame has a priority tag in it that instructs the switch as to the importance of the frame. Frames with a high priority are handled ahead of frames with a low priority.

Activating or deactivating ingress filtering has no effect on the switch's handling of priority tags. A switch will always examine a priority tag in a tagged frame, regardless of the status of ingress filtering.

In most cases, you will probably want to leave ingress filtering activated on the switch, which is the default. You can enable or disable ingress filtering on a per switch basis. You cannot set this per port.

To enable or disable ingress filtering, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **2** to select Ingress Filtering Status. Current status for this functionality (enabled or disabled) is displayed next to this feature selection.The following prompt is displayed:

```
Enter Ingress Filtering Status (E-Enable, D-Disable)
->
```

3. Type **E** to activate ingress filtering or **D** to disable ingress filtering on the switch.
4. Type **S** to select Save Configuration Changes.

   A change to the status of ingress filtering is immediately activated on the switch.

Designating a Management VLAN

The management VLAN is the VLAN on which the AT-S39 management software expects to receive remote management packets. This VLAN is important if you will be managing a switch remotely using Telnet or a web browser, or through the enhanced stacking feature of the switch.

Management packets are packets generated by a management workstation when you manage a switch remotely using the Telnet application protocol or a web browser. The AT-S39 management software on a switch will act upon the management packets only if they are received on the management VLAN.

The default management VLAN on an AT-8000 Series switch is the Default_VLAN. If you do not create any additional VLANs and link the switches together using untagged ports, then there will be no need to specify a new management VLAN in order to remotely manage the devices.

However, if you create additional VLANs on your switches, it may be necessary for you to create a management communications path and then specify that path as the new management VLAN.

Below are several rules to observe when using this feature:

- ❑ The management VLAN must exist on the AT-8000 Series switches, and other enhanced stacking switches, that you want to manage remotely.
- ❑ Using the following procedure, you must specify the management VLAN in the AT-S39 software on each slave and master switch of an enhanced stack.
- ❑ The uplink and downlink ports on the switches that are functioning as the tagged or untagged data links between the switches must be either tagged or untagged members of the management VLAN.
- ❑ The port on the switch to which the management station is connected must be a member of the management VLAN. (This rule does not apply when managing the switch locally through the RS-232 terminal port.)

As an example, assume that you have an enhanced stack of seven AT-8000 Series switches with one master switch. If the uplink and downlink ports between the various switches are members of the Default_VLAN and if the management station is connected to a port of the Default_VLAN, you can remotely manage all the switches because the Default_VLAN is the default management VLAN.

Now assume that you decide to create a VLAN called NMS with a VID of 24 for the sole purpose of remote network management. For this, you need to create the NMS VLAN on each AT-8000 Series switch you want to manage remotely, being sure to assign each NMS VLAN the VID of 24. Then you need to be sure that the uplink and downlink ports connecting the switches together are either tagged or untagged members of the NMS VLAN. You also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you must be sure to connect your management station to a port on a switch that is a tagged or untagged member of the management VLAN.

Note
You cannot specify a management VLAN when the switch is operating in a multiple VLAN mode.

To specify a management VLAN, do the following:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **4** to select Management VLAN.

   The following prompt is displayed:

   ```
   Enter Management VLAN ID [1 to 4094] ->
   ```

3. Specify the VID of the VLAN that is to function as the management VLAN. This VLAN must already exist on the switch.

   The following prompt is displayed:

   ```
   SUCCESS - Press any key to continue ...
   ```

4. Press any key.
5. Type **S** to select Save Configuration Changes.

Chapter 12
Multiple VLAN Modes

This chapter describes the Multiple VLAN Modes and how to select a mode. This chapter contains the following sections:

Multiple VLAN Modes Overview

The Multiple VLAN modes simplify the task of configuring the switch in network environments that require a high degree of network segmentation. In the multiple VLAN modes, the ports on a switch are prohibited from forwarding traffic to each other and are only allowed to forward traffic to a user designated uplink port. These configurations isolate the traffic on each port from all other ports, while providing the ports with access to the uplink port.

The AT-S62 software supports two types of multiple VLAN modes:

- ❑ 802.1Q-compliant Multiple VLAN mode
- ❑ Multiple VLAN mode (also referred to as non-802.1Q compliant Multiple VLAN mode)

Note
Multiple VLAN modes are supported only in single switch (i.e. edge switch) environments. This means that cascading of switches while in a multiple VLAN mode is not allowed.

Activating a multiple VLAN mode on a cascaded switch can possibly result in disconnection of network paths between switches unless the port used to link the switch (being configured for multiple VLAN mode) is configured as the uplink port.

Activating a multiple VLAN mode on cascaded switches can also affect enhanced stacking as the master switch may not be able to detect member switches beyond the first cascaded switch.

802.1Q-Compliant Multiple VLAN Mode

802.1Q-compliant Multiple VLAN mode is appropriate when the device connected to the uplink port is 802.1Q compatible, meaning that it can handle tagged packets.

This mode places each port on the switch into a separate VLAN as an untagged port. Each VLAN also contains a user designated uplink port. This uplink port, which is a tagged port, is shared by all the VLANs on the switch. There can be only one uplink port on a switch.

The VLANs are called client VLANs. The VLAN names, the VIDs, and the PVIDs are based on port number. For example, the VLAN for Port 4 is named Client_VLAN_4 and is given the VID of 4, the VLAN for Port 5 is named Client_VLAN_5 and has a VID of 5, and so on. PVIDs are also assigned automatically. For example, the PVID for Port 4 is 4, to match the VID of 4.

When you activate the 802.1Q-compliant VLAN mode, you are asked to specify the uplink port for all the client VLANs. Once you have specified the port, the switch automatically configures the VLANs.

Table 8 is an example of this multiple VLAN mode. It shows the client VLANs on a switch that supports 26 ports. Port 15 has been selected as the uplink port.

Note
In 802.1Q Multiple VLANs mode, the device connected to the uplink port must be 802.1Q-compliant. It must be able to handle tagged packets.

Table 8 802.1Q-Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_1	1	1	15
Client_VLAN_2	2	2	15
Client_VLAN_3	3	3	15
Client_VLAN_4	4	4	15
Client_VLAN_5	5	5	15
Client_VLAN_6	6	6	15
Client_VLAN_7	7	7	15
Client_VLAN_8	8	8	15
Client_VLAN_9	9	9	15
Client_VLAN_10	10	10	15
Client_VLAN_11	11	11	15
Client_VLAN_12	12	12	15
Client_VLAN_13	13	13	15
Client_VLAN_14	14	14	15
Uplink_VLAN	**15**	**15**	
Client_VLAN_16	16	16	15
Client_VLAN_17	17	17	15

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_18	18	18	15
Client_VLAN_19	19	19	15
Client_VLAN_20	20	20	15
Client_VLAN_21	21	21	15
Client_VLAN_22	22	22	15
Client_VLAN_23	23	23	15
Client_VLAN_24	24	24	15
Client_VLAN_25	25	25	15
Client_VLAN_26	26	26	15

Note
Remote management of the switch is possible only through the uplink port.

Non-802.1Q Compliant Multiple VLAN Mode

The Non-802.1Q Compliant Multiple VLAN mode is appropriate when the device connected to the uplink port is non-802.1Q compatible, meaning that the device cannot handle tagged packets.

This mode has similarities to the 802.1Q-compliant Multiple VLAN mode. Like the latter, it places each port into a separate VLAN as an untagged port. It also uses the same mechanism in naming VLANs and assigning VIDs and PVIDs.

The main difference is in the uplink port. Rather than being tagged, it is untagged. This is why the mode is referred to as non-802.1Q compliant. To be compliant, a port cannot be an untagged member of more than one VLAN at a time. Since in this mode the uplink port is an untagged member of multiple VLANs, this mode is non-compliant.

It should also be noted that while the other ports on the switch reside in separate VLANs, they are also untagged members of the Uplink VLAN.

The advantage of this mode is that the device connected to the uplink port does not have to be 802.1Q compliant.

When you select the Non-802.1Q Multiple VLAN mode, you are asked to specify the uplink port. The switch then automatically configures the VLANs.

Table 9 is an example of this mode. The table lists the VLANs on a switch that supports 26 ports where port 15 was selected as the uplink port. Ports 1 to14 and 16 to 26 are configured as untagged Client VLANs. Port 15, the uplink port, is configured as the Uplink VLAN that contains all ports as members.

Table 9 Non-802.1Q Compliant Multiple VLANs Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_1	1	1,15	
Client_VLAN_2	2	2,15	
Client_VLAN_3	3	3,15	
Client_VLAN_4	4	4,15	
Client_VLAN_5	5	5,15	
Client_VLAN_6	6	6,15	
Client_VLAN_7	7	7,15	
Client_VLAN_8	8	8,15	
Client_VLAN_9	9	9,15	
Client_VLAN_10	10	10,15	
Client_VLAN_11	11	11,15	
Client_VLAN_12	12	12,15	
Client_VLAN_13	13	13,15	
Client_VLAN_14	14	14,15	
Uplink_VLAN	**15**	**ALL**	
Client_VLAN_16	16	16, 15	
Client_VLAN_17	17	17,15	
Client_VLAN_18	18	18,15	
Client_VLAN_19	19	19,15	
Client_VLAN_20	20	20,15	
Client_VLAN_21	21	21,15	
Client_VLAN_22	22	22,15	

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_23	23	23,15	
Client_VLAN_24	24	24,15	
Client_VLAN_25	25	25,15	
Client_VLAN_26	26	26,15	

Caution
The non-802.1Q-Compliant Multiple VLAN mode does not protect the switch from VLAN leakage. If a packet arrives on the uplink port containing a destination MAC address not in the MAC address table, the switch will broadcast the packet out all ports, except the uplink port. This means that all end nodes on the switch will receive the packet.

Preserving User-Configured VLANs

When the VLAN mode is set to either of the multiple VLAN mode, user-configured VLAN definitions cannot be created or modified. However, the software preserves user-configured VLANs that were configured before multiple VLAN mode was enabled. When the user switches back to user-configured VLANs mode, the software automatically enables the user-configured VLANs with the pre-existing configuration.

Uplink VLANs - Multiple VLANs Mode Management

Although both multiple VLAN modes support remote management of the switch via a management VLAN, the management VLAN is designated by default to the uplink port and you are not allowed to modify it. If you are in a multiple VLAN mode and you select the Management VLAN parameter in the VLAN menu, the following message is displayed:

```
Management VLAN can not be changed in Multiple VLANs
mode
```

Activating or Deactivating a Multiple VLAN Mode

The following procedure explains how to enable or disable a multiple VLANs mode on an AT-8000 Series switch.

> **Note**
> The VLAN mode on the switch must be set to User Configured (Tagged) VLAN mode, and not the Basic Mode, for the unit to operate in a multiple VLAN mode. To set a switch's VLAN mode, refer to **Setting the VLAN Mode** on page 133.

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **3** to select VLANs Mode. The following prompt is displayed:

```
Enter VLAN Mode (U-UserConfig, M-Multiple, Q-802.1Q
Multiple VLANs) ->
```

3. Type **M** to enable Non-802.1Q compliant multiple VLANs, **Q** to enable Q-802.1Q Multiple VLANs, or **U** to select user configured VLAN mode, where you can create your own port-based and tagged VLANs. The default setting is the user configured VLAN mode. If you select one of the multiple VLAN modes, the following prompt is displayed:

   ```
   Enter Uplink VLAN Port number ->  [1 to 26] ->
   ```

4. Enter the Uplink VLAN port number. The following confirmation is displayed:

   ```
   SUCCESS - VLAN Mode set to Multiple VLANs mode
   ```

   The new mode is immediately activated on the switch. If you selected the 802.1Q compliant Multiple VLANs Mode and you accessed the switch through enhanced stacking or a Telnet management session, it is possible that your remote management session will end and you will not be able to reestablish it. Remote management of a switch operating in that multiple VLAN mode is possible only through the uplink port.

Displaying VLAN Information

To view the name, VID number, and member ports of all the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **7** to select Show VLANs.

   The Show VLANs window is displayed. An example of the window is shown in Figure 44.

```
        Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                          Sales Switch

Login Privilege: Manager

                            Show VLANs

VID    VLAN Name            Untagged Port(s)   Tagged Port(s)
-------------------------------------------------------------

1      Client_VLAN_1           1, 15             ---
2      Client_VLAN_2           2, 15             ---
3      Client_VLAN_3           3, 15             ---
4      Client_VLAN_4           4, 15             ---
5      Client_VLAN_5           5, 15             ---
6      Client_VLAN_6           6, 15             ---
7      Client_VLAN_7           7, 15             ---
8      Client_VLAN_8           8, 15             ---

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 44 Show VLANs Window -Multiple VLAN

Chapter 13
MAC Address Table

The chapter contains the procedures for viewing the static and dynamic MAC address table.

This chapter contains the following sections:

MAC Address Overview

The hardware devices that you connect to your network have unique MAC addresses assigned by the device manufacturers. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The AT-8000 Series switch contains a 4 kilobyte 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 has 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 where 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 frame to the appropriate port when 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 and increases 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. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

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-8000 Series switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 173.

The MAC address table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, 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

The management software has two menu selections for displaying the MAC addresses of a switch. One selection displays the static and dynamic MAC addresses while the other displays just the static addresses.

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

1. From the Main Menu, type **6** to select MAC Address Tables.

   The MAC Address Table menu is shown in Figure 45.

```
  Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                    Sales Switch

Login Privilege: Manager

                  MAC Address Tables

1 - Show all MAC Addresses
2 - Add static MAC Address
3 - Delete MAC Address
4 - Delete all dynamic MAC Addresses
5 - Show all static MAC addresses
6 - View MAC addresses by Port
7 - View the port of MAC address
8 - View MAC addresses by VLAN ID
9 - View IP Multicast MAC Addresses
A - View MAC addresses on base ports

R - Return to Previous Menu

Enter your selection?
```

Figure 45 MAC Address Table Menu

2. Select one of the following:

   - ❑ To display all static and dynamic MAC addresses for all ports, type **1** to select Show All MAC Addresses
   - ❑ To display only static MAC addresses, type **5** to select Show All Static MAC Addresses.
   - ❑ To display static and dynamic addresses for only the base ports (excludes GBIC ports and ports on expansion modules), type **A** to select View MAC Addresses on Base Ports.

The management software displays the MAC addresses. Figure 46 is an example of the Show All MAC Addresses window, which displays both static and dynamic MAC addresses. The static MAC address window is exactly the same, except for the title and the fact that it displays only static MAC addresses.

```
              Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                              Sales Switch

Login Privilege: Manager

                            Show All MAC Addresses


MAC               Port PMAP     CPU MIR  EMP  VlanID Type
------------------------------------------------------------------------
01:80:C1:00:02:01 0    00000000 Yes Yes  Yes  0      Static (fixed, non-aging)
00:a0:d2:18:1a:c8 1    00000000 No  No   No   1      Dynamic
00:a0:c4:16:3b:80 2    00000000 No  No   No   1      Dynamic
00:a0:12:c2:10:c6 3    00000000 No  No   No   1      Dynamic
00:a0:c2:09:10:d8 4    00000000 No  No   No   1      Dynamic
00:a0:33:43:a1:87 5    00000000 No  No   No   1      Dynamic
00:a0:12:a7:14:68 6    00000000 No  No   No   1      Dynamic
00:a0:d2:22:15:10 7    00000000 No  No   No   1      Dynamic
00:a0:d4:18:a6:89 8    00000000 No  No   No   1      Dynamic


U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 46 Show All MAC Addresses Window

The information is for viewing purposes only. The columns in the window are defined below.

MAC
The unicast or multicast MAC address.

Port
The port on the switch where the MAC address was learned. This column is empty for a multicast address.

PMAP
The ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different multicast groups. (The abbreviation PMAP is derived from "port mapping.")

Each "0" is a hexadecimal value for the binary value "0000". Each binary "0" represents a port on the switch. A binary "0" means that the port is not a member of a multicast group while a "1" means that it is.

The port numbering scheme is from right to left. As an example, assume that ports 1 through 4 on the switch were members of the same multicast group. This would be represented in the column as follows: “0000000F”. Another example is “000020F. This example would indicate that ports 1 to 4 and port 10 on the switch were members of the same multicast group.

This column is empty for unicast addresses.

CPU
This feature is not supported.

MIR
Indicates whether the traffic on the port is being mirrored. Yes means the traffic is being mirrored while No indicates that it is not.

EMP
Indicates whether multicast packets are being forwarded by ports in the blocking state. This feature is not supported at this time. This column will indicate “No” for all multicast addresses, except for the switch’s MAC address. Multicast packets are forwarded only by ports in the forwarding state.

VLANID
The VID of the VLAN to which the port is an untagged member.

Type
The MAC address type. The type can be either static or dynamic.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for adding static unicast and multicast addresses to the switch. You can assign up to 255 static MAC addresses per port on an AT-8000 Series switch.

To add a static unicast or multicast address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **2** to select Add Static MAC Address.

   The following prompt is displayed:

   ```
   Please enter a MAC address ->
   ```
3. Enter the static unicast or multicast MAC address in the following format:

   ```
   XXXXXX XXXXXX
   ```

   Once you have specified the MAC address, the following prompt is displayed:

   ```
   Please enter a port number: [1 to 24] ->
   ```
4. Enter the number of the port on the switch to which you want to assign the address. If you are adding a static unicast address, you can specify only one port. If you are adding a static multicast address, you can specify multiple ports.

   The management software adds the address to the MAC address table.
5. Repeat steps 2 to 4 to enter additional static MAC addresses.

Deleting MAC Addresses

The following procedure explains how to delete a static, dynamic, or multicast MAC address from the MAC address table.

To delete an address from the MAC address table, perform the following procedure:

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **3** to select Delete MAC Address.

   The following prompt is displayed:

   ```
   Please enter a MAC address ->
   ```
3. Enter the MAC address to be deleted in the following format and press Return:

   ```
   XXXXXX XXXXXX
   ```

   The MAC address is deleted from the switch's MAC address table.

   Note
   You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

4. Repeat the procedure to delete additional MAC addresses.

Deleting All Dynamic MAC Addresses

The management software allows you to purge the MAC address table of all dynamic MAC addresses. Once the table has been purged, the switch immediately begins to relearn the MAC addresses as frames are received on the ports.

Note
This procedure does not delete static MAC addresses.

To delete all dynamic MAC addresses from the MAC address table, perform the following procedure.

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **4** to select Delete All Dynamic MAC Addresses.

   A following prompt is displayed:

   ```
   All learned MAC (non-static) addresses will be
   deleted.
   Do you want to continue? [Yes/No] ->
   ```

3. Type **Y** for yes to delete the dynamic MAC addresses or **N** for no to cancel the procedure.

   If you type **Y** for yes, the dynamic MAC addresses are deleted from the MAC address table. The switch immediately begins to relearn the addresses and to add them to the table.

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 **6** to select MAC Address Table.
2. From the MAC Address Tables menu, type **6** to select View MAC Addresses by Port Menu.

   The following prompt is displayed:

   ```
   Please enter port number -> [1 to 26] ->
   ```

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

   A window is displayed with the MAC addresses of the end nodes on the port. The columns in the window and the definitions of the columns are the same as for the Show All MAC Addresses window on page 165.

   The information in this window is for viewing purposes only.

Identifying a Port Number by MAC Address

In some situations, you might want to know which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The procedure in this section offers an easier way. You can specify the MAC address and let the management software automatically locate the port on the switch where the device is connected.

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **7** to select View the Port of MAC Address.

   The following prompt is displayed:

   ```
   Please enter MAC address:
   ```

3. Enter the MAC address of the node in the following format and press Return:

   ```
   xxxxxx xxxxxx
   ```

   The management software displays a prompt containing the port number on the switch to which the node is connected, if the address was learned dynamically, or to which the address was assigned, for a static address.

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 VID number of the VLAN whose MAC addresses you want to view. To obtain a VLAN's VID, refer to **Displaying VLAN Information** on page 144.

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

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **8** to select View MAC Addresses by VLAN ID Menu.

   The following prompt is displayed:

   ```
   Please enter a VLAN ID: [1 to 4095] ->
   ```
3. Enter the VID of the desired VLAN and press Return.

   The management software displays a window with a list of the MAC addresses of the nodes in the VLAN. For an example of the window and for definitions of the columns, refer to the Show All MAC Addresses window on page 165.

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 sent to or 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:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Config Menu, type **1** to select MAC Aging Time.

   The following prompt is displayed:

   ```
   Enter your new value -> [1 to 1048575]
   ```
3. Enter a new value in seconds.

   The value should be an increment of 5 seconds, for example 410, 415, or 420. A value that is not an increment of 5 is rounded down to the next increment of 5. For example, the value 524 is rounded down to 520.

   The new value is immediately activated on the switch.

Chapter 14
Class of Service

This chapter contains the procedures for configuring the Class of Service (CoS) feature of the AT-S39 software. Sections in the chapter include:

Class of Service Overview

When a port on an Ethernet switch becomes oversubscribed—its egress queues contain more packets than the port can handle in a timely manner—the port may be forced to delay the transmission of some packets. This can result in the delay of packets reaching their destinations.

Minor delays are often of no consequence to a network or its performance. But there are some applications, referred to as delay or time sensitive applications, that can be impacted by packet delays. Voice transmission and video conferencing are two examples. If packets carrying data for either of these are delayed from reaching their destination, the audio or video quality may suffer.

This is where CoS can be of value. It allows you to manage the flow of traffic through your switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

CoS applies primarily to tagged packets. If you read **Tagged VLAN Overview** on page 128, then you know that a tagged packet contains information within it that specifies the VLAN to which the packet belongs.

A tagged packet also contains a priority level. This priority level is used by network switches and other networking devices to know how important (delay sensitive) that packet is compared to other packets. Packets of a high priority are typically handled before packets of a low priority.

CoS, as defined in the IEEE 802.1p standard, has eight levels of priority. The priorities are 0 to 7, with 0 the lowest priority and 7 the highest.

When a tagged packet is received on a port on the switch, it is examined by the AT-S62 software for its priority. The switch software uses the priority to determine which egress priority queue the packet should be directed to on the egress port.

Each switch port has two egress queues, high and low. A packet in a high priority egress queue is typically transmitted out a port sooner than a packet in a low priority queue.

Table 10 lists the mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 10 Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0, 1, 2, 3	low
4, 5, 6, 7	high

For example, assume that a tagged packet with a priority level of 3 enters a port on the switch. The switch, after examining the packet's destination address, determines that the packet is to be sent out port 6. The switch must now determine which of port 6's egress queues the packet should be stored in. It examines the priority level in the packet, which is 3. Now the switch knows to store the packet in port 6's low egress queue.

You can change these mappings. For example, you might decide that packets with a priority level of 3 need to be handled by an egress high queue, instead of the low queue.

It needs to be noted that this determination is made when a packet is received on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port.

For example, when you configure a switch port so that all ingress tagged frames are handled by the egress priority queue Q2, all tagged frames received on the port are directed to the Q2 priority egress queue on the egress ports, regardless of the priority levels in the packets themselves.

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain a priority level. By default, all untagged packets are placed in a port's low egress queue. But you can override this and instruct a port's untagged egress frames to be stored in the high priority queue.

One last thing to note is that the AT-S39 software does not change the priority level in a tagged packet. The packet leaves the switch with the same priority it had when it entered. This is true even if you change the default priority-to-egress queue mappings.

Configuring CoS

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **6** to select Configure COS Priorities.

   The following prompt is displayed:

   ```
   Enter port number -> [1 to 24] ->
   ```

3. Enter the port where you want to configure CoS. You can configure only one port at a time. Press Return. The Configure COS Priorities menu is shown in Figure 47.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

             Configure COS Priorities

1 - Port Number ..................... 1
2 - Port VLAN ID (PVID) ............. 1
3 - Priority (0-7) 0=Low 7=High ..... 0
4 - Override Priority (Y/N) ......... N

C - Configure COS Priorities
S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 47 Configure COS Priorities

Note
Menu options 1 and 2 cannot be changed.

4. Type **3** to select Priority (0 - 7). The following prompt is displayed:

   ```
   Enter new value -> [0 to 7]
   ```

5. If you want all tagged and untagged frames received on the port to go to the low priority egress queue, enter a value from 0 to 3. (It does not matter which value you enter so long as it's from 0 to 3.) If you want all frames received on the port to go to the high priority egress queue, enter a value from 4 to 7. (Again, it does not matter which number it is so long as it is from 4 to 7.)
6. If you are configuring a tagged port and you want the switch to ignore the priority tag in the tagged frames that ingress the port, type **4** to select Override Priority and type **Y**. If you select yes, all ingress tagged frames will be directed to either the low or high priority egress queue as specified in Step 5.

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 default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.

7. Type **C** to select Configure Port VLANS & Priorities.
8. Type **S** to select Save Configuration Changes.
9. Repeat this procedure to configure CoS on other ports on the switch.

Note
To view the priority queue assignment for each port and the override priority status, refer to **Displaying PVIDs and Priorities** on page 148.

Chapter 15
IGMP Snooping

This chapter explains how to activate and configure the Internet Group Management Protocol (IGMP) snooping feature on the switch. Sections in the chapter include:

IGMP Snooping Overview

IGMP enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group 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.

A node wanting to become a member of a particular multicast group responds to a query by sending a *report*. A report indicates an end node's intention to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. Once a host node has been made a member of a multicast group, it must continue to periodically issue reports to remain a member.

Once the router has received a report from a host node, 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 AT-S39 management software supports IGMP Version 1 and Version 2. One of the differences between the two versions is how a host node indicates that it no longer wants to be a member of a multicast group. In Version 1, it simply stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames, and removes it from the membership list of the multicast group.

In Version 2, a host node exits from a multicast group by sending a *leave request*. Once a router receives a leave request from a host node, it removes the node from appropriate membership list. The router will also stop sending out multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

IGMP snooping enables the Fast Ethernet switch to monitor the flow of queries from a router and reports from 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 restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, a switch would have to flood 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.

The AT-8000 Series switch supports both IGMP Version 1 and Version 2. The switch maintains its multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note
By default, IGMP snooping is disabled on the switch.

Activating IGMP Snooping

To activate or deactivate IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Config Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu is shown in Figure 48.

```
      Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                        Sales Switch

Login Privilege: Manager

                IGMP Snooping Configuration

1 - IGMP Snooping Status ......... Disabled
2 - Multicast Host Topology ...... Single-Host/Port (Edge)
3 - Host/Router Timeout Interval . 260 seconds
4 - Maximum Multicast Groups ..... 256
5 - Multicast Router Port(s) ..... Auto Detect
6 - View Multicast Hosts List
7 - View Multicast Router List

S - Save Configuration Changes
R - Return to Previous Men

Enter your selection:
```

Figure 48 IGMP Snooping Configuration Menu

The options in the menu are defined below:

1 - IGMP Snooping Status
Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature.

2 - Multicast Host Topology
Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Host/Port (Intermediate).

The Single-Host/Port setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node

stops sending reports. The switch responds by immediately ceasing the transmission of further multicast packets out the port where the host node is connected.

The Multi-Host setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Multi-Host Port (Intermediate) selection.

3 - Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 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.

4 - Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

5 - Multicast Router Port(s)
Specifies the port on the switch to which the multicast router is detected. You can let the switch determine this automatically by selecting Auto Detect, or you can specify the port yourself by entering a port number. To select Auto Detect, enter "0" (zero) for this parameter. You can specify more than one port.

Your changes are activated immediately on the switch.

Note
Selections 6 and 7 in the menu are discussed later in this chapter.

4. After making the desired changes, type **S** to select Save Configuration Changes.

Displaying a List of Host Nodes

You can use the AT-S39 software to display a list of the multicast groups on a switch, as well as the host nodes. To display the list, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Config Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu in Figure 48 is displayed.
4. From the IGMP Snooping Configuration menu, type **6** to select View Multicast Host List.

   The View Multicast Host List is shown in Figure 49.

```
Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

           View Multicast Hosts List

=============================================
MulticastGroup  MemberPort   VLAN   Host IP
=============================================

U - Update Display
R - Return to Previous Menu


Enter your selection?
```

Figure 49 View Multicast Hosts List Window

The information in this window is for viewing purposes only. The columns are defined below:

Multicast Group
The multicast address of the group.

Membership Port
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN
The VID of the VLAN in which the port is an untagged member.

Host IP
The IP address(es) of the host node(s) connected to the port.

Displaying a List of Multicast Routers

A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. You can use the AT-S39 software to display a list of the multicast routers that are connected to the switch.

To display a list of the multicast routers, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu is shown in Figure 48.
4. From the IGMP Snooping Configuration menu, type **7** to select View Multicast Routers List.

   The View Multicast Router List is shown in Figure 49.

```
Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

          View Multicast Routers List

=============================================
Port            VLAN          Router IP
=============================================

U - Update Display
R - Return to Previous Menu


Enter your selection?
```

Figure 50 View Multicast Routers List Window

The information in this window is for viewing purposes only. The columns are defined below:

Port
The port on the switch where the multicast router is connected.

VLAN
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the multicast router.

Chapter 16
Broadcast Storm Control

This chapter contains the procedures for configuring the broadcast storm control feature of the AT-S39 management software. Sections in the chapter include:

Broadcast Storm Control Overview

Most frames on an Ethernet network are usually unicast frames. A unicast frame is a frame sent to a single destination. 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, it sends the file in a unicast Ethernet frame containing the destination address of the server where the file is to be stored.

Broadcast frames are different. Broadcast frames are directed to all nodes on the network or all nodes within a particular virtual LAN. Broadcast packets can perform a variety of functions. 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 a network can impact network performance. The more bandwidth consumed by broadcast frames, the less available for unicast frames.

Should the performance of your network be impacted by heavy broadcast traffic, you can use the AT-S39 management software to limit the number of broadcast frames forwarded by the switch and so restrict their number.

To accomplish this, you specify the maximum number of broadcast frames you want the switch to forward within a specified time interval. Broadcast frames that exceed the maximum on a port during the time interval are not forwarded and are discarded by the switch.

In order to use this feature, you must set two values: the *interval timer* and the *maximum broadcast frame limit*.

The interval timer defines the time period used in counting the number of forwarded broadcast frames on a port. There are two interval timers. One timer is for ports operating at 10 Mbps or 100 Mbps. The second timer is for 1000 Mbps ports. The timer interval for 10 and 100 Mbps ports is measured in milliseconds. The timer interval for 1000 Mbps ports is in microseconds. A time interval setting applies to all ports operating at the corresponding speed on the switch.

The maximum broadcast frame limit specifies the maximum number of broadcast frames a port will forward during the timer interval. Broadcast frames received once the maximum has been exceeded are not forwarded by a port and are discarded. You can specify a different maximum for each port on the switch.

It is important to note that the maximum number applies to the egress port of a broadcast frame, not the ingress port. That is, any port on the switch will accept any number of broadcast frames. But a port will transmit out (forward) a broadcast frame only if it has not exceeded the maximum number of broadcast frames it can transmit.

Here's an example. Let's assume you set the timer interval for 10 and 100 Mbps ports to 100 milliseconds and the maximum broadcast frame limit for a particular 100 Mbps port on the switch to 200 broadcast frames. At these settings, the port will forward (transmit out) up to 200 broadcast frames every 100 milliseconds. If the maximum is exceeded during the time interval, the port discards any additional broadcast frames and does not forward them.

Note
The AT-S39 default setting is no Broadcast Storm Control on the switch.

Configuring the Interval Timer

To set the interval timer for the Broadcast Storm Control feature, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration Menu, type **2** to select Broadcast Timers Setup. The Broadcast Storm Control menu is shown in Figure 51.

```
  Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

              Broadcast Storm Control

1 - Timer for 10/100 MB ports ..... 10 milli sec
2 - Timer for 1000 MB ports ....... 100 micro sec

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 51 Broadcast Storm Control Menu

4. Type **1** or **2** and enter a value when prompted. The interval timer for 10 Mbps and 100 Mbps ports is in milliseconds and has a range of 10 to 120 milliseconds. The value should be entered in increments of 10 milliseconds.

   The interval timer for 1000 Mbps ports is in microseconds and has a range of 100 to 120000 microseconds. The value should be entered in increments of 100 microseconds.

   A value for an interval timer applies to all ports operating at the corresponding speed.

   Note
   The 1000 Mbps speed applies only to optional Gigabit Ethernet ports.

   Your changes are immediately activated on the switch.
5. Once you have set the desired timer intervals, type **S** to select Save Configuration Changes.
6. Go to the next procedure and specify the maximum number of broadcast frames the ports on the switch can transmit.

Configuring the Maximum Broadcast Frame Count

To specify the maximum number of broadcast frames a port on the switch can transmit, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **1** to select Port Configuration.

   The following prompt is displayed:

   ```
   Enter Ports List ->
   ```

3. Enter the port(s) that you want to configure and press Return.

   The Port Configuration menu is shown in Figure 14 on page 69.

4. Type **B** to select Broadcast Control.

   The following prompt is displayed:

   ```
   Enter Max. Broadcasts (0 -> No limit):
   [0 to 1023] - >
   ```

5. Specify the maximum number of broadcast frames the port can transmit during the timer interval. Press Return.

   For example, assume that you are specifying the maximum broadcast frame count for a port operating at 100 Mbps, and you specified a 10 millisecond interval timer for 100 Mbps ports. If you entered a value of 200 at the prompt, the port would transmit a maximum of 200 broadcast frames every 10 milliseconds. Any broadcast frames over the maximum are discarded by the port and are not transmitted.

   Entering a value of "0" disables Broadcast Storm Control on the port.

   Your changes are immediately activated on the switch.

6. Type **S** to select Save Configuration Changes.

Chapter 17
TACACS+ and RADIUS Protocols

This chapter contains the procedure for configuring the two authentication protocols TACACS+ and RADIUS. Sections in the chapter include:

TACACS+ and RADIUS Overview

TACACS+ and RADIUS are authentication protocols used to enhance the security of your network. (TACACS+ is an acronym for Terminal Access Controller Access Control System. RADIUS is an acronym for Remote Authentication Dial In User Services.) The authentication protocols are used to transfer the task of authenticating network access from a network device to an authentication protocol server.

The AT-S39 software comes with TACACS+ and RADIUS client software. You can use the client software to add two security features to the switch. The first feature, described in this chapter, involves creating new manager accounts. These accounts define who can log onto a switch to change the unit's operating parameter settings. The second feature is 802.1x Port-based Access Control, explained in **Chapter 18**, **802.1x Port-Based Access Control** on page 202.

The AT-S39 software has two standard management login accounts: Manager and Operator. The Manager account lets you change a switch's parameter settings while the Operator account only lets you view the settings. Each account has its own password. The Manager account has a default password of "friend" and the Operator account has a default password "operator."

For those networks managed by just one or two network managers, the standard accounts may be all you need. However, for larger networks managed by several network managers, you might want each manager to have his or her own management login account rather than for them to share an account.

This is where TACACS+ and RADIUS can be useful. You can use them to transfer the task of validating manager access from an AT-8000 Series switch to an authentication protocol server. You can use the protocols to create a series of username and password combinations that define who can manage an AT-8000 Series switch.

To add new manager accounts, you need to do the following:

- ❑ You must install TACACS+ or RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesyn.

Note
The switch communicates with the authentication server via the switch's management VLAN. Consequently, the node functioning as the authentication server must be communicating with the switch through a switch port that is a member of that VLAN. The default management VLAN is Default_VLAN. For further information, refer to **Designating a Management VLAN** on page 151.

- ❑ The authentication protocol server can be on the same subnet or a different subnet as the AT-8000 Series switch. If the server and switch are on different subnets, be sure to specify a default gateway in the Administration Menu so that the switch and server can communicate with each other.
- ❑ You need to configure the TACACS+ or RADIUS server software. This involves the following:
  - — Specifying the username and password combinations.
  - — Assigning each combination an authorization level. This will differ depending on the server software you are using. TACACS+ controls this through the sixteen (0 to 15) different levels of the Privilege attribute. A privilege level of "0" gives the combination Operator status. Any value from 1 to 15 gives the combination Manager status.

    For RADIUS, management level is controlled by the Service Type attribute. This attribute has 11 different values, of which only two are functional with an AT-8000 Series switch. A value of Administrative for this attribute gives the username and password combination Manager access. A value of NAS Prompt assigns the combination Operator status.

Note
This manual does not explain how to configure TACACS+ or RADIUS server software. For that you need to refer to the documentation that came with the software.

- ❑ Finally, you need to configure the TACACS+ or RADIUS client software on the switch, as explained later in this chapter in **Configuring the Authentication Client Software** on page 196.

Functions of an Authentication Protocol

There are three basic functions an authentication protocol provides:

- ❑ Authentication
- ❑ Authorization
- ❑ Accounting

When a network manager logs in to a switch, the switch passes the username and password entered by the manager to the authentication protocol server. The server checks to see if the username and password are valid for that switch. This is referred to as authentication.

If the combination is valid, the authentication protocol server notifies the switch and the switch completes the login process, allowing the manager to access the switch.

If the username and password combination is invalid, the authentication protocol server notifies the switch and the switch cancels the login.

Authorization defines what a manager can do once logged in to a switch. You assign an authorization level to each username and password combination that you create on the server software. The access level will be either Manager or Operator.

The final function of the TACACS+ protocol is accounting, which keeps track of user activity on network devices. The AT-S39 management software does not support this function.

Note
The AT-S39 management software does not support the two earlier versions of the TACACS+ protocol, TACACS and XTACACS.

TACACS+ and RADIUS Configuration Guidelines

By default, the authentication client software is disabled on an AT-8000 Series switch. In order to activate it, you will need to provide the following information:

- ❑ Which authentication protocol you want to use. Only one authentication protocol can be active on a switch at a time.
- ❑ IP addresses of up to three authentication servers.
- ❑ The encryption key used by the authentication servers.

Note
For more information on TACACS+, refer to the RFC 1492 standard. For more information on RADIUS, refer to the RFC 2865 standard.

Configuring the Authentication Client Software

To configure the TACACS+ and RADIUS client software settings, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
2. From the Administration Menu, type **A** to select Server-based Authentication.

   The Authentication Menu is shown in Figure 52.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager

               Authentication Menu

1 - Server-based Authentication ..... Disabled
2 - Authentication Method ........... TACACS+
3 - TACACS+ Configuration
4 - RADIUS Configuration

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 52 Authentication Menu

> **Note**
> Option 1 - Server-based Authentication applies only to the manager account feature described in this chapter. The menu option does not apply to the 802.1x port-based access control feature. If this option is disabled, the switch uses its standard Manager and Operator accounts when you log on to manage the switch. If enabled, the switch uses the manager accounts on the TACACS+ or RADIUS server. If you want to disable the manager account feature, toggle the menu option until it displays Disabled, which is the default setting. Disabling Option 1 does not effect the 802.1x port-based access control feature.

3. To select an authentication protocol, type **2** to select Authentication Method. The following prompt is displayed:

```
Enter T-TACACS+, R-RADIUS ->
```

4. Type **T** to select TACACS+ or **R** for RADIUS. The default is TACACS+. Only one protocol can be active on the switch at a time.

   If you selected TACACS+, go to Step 5. If you selected RADIUS, go to Step 6.

5. To configure TACACS+, do the following:

   a. Type **3** to select TACACS+ Configuration.

      The following menu is displayed:

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager
               Authentication Menu
1 - TAC Server 1 .................. 0.0.0.0
2 - TAC Server 2 .................. 0.0.0.0
3 - TAC Server 3 .................. 0.0.0.0
4 - TAC Server Order ............... 1 2 3
5 - TAC Global Secret ..............
6 - TAC Timeout ................... 30 seconds

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 53 Authentication Menu (TACACS+)

   b. Configure the settings as needed. The settings are described below:

      1 - TAC Server 1
      2 - TAC Server 2
      3 - TAC Server 3
      Use these parameters to specify the IP addresses of up to three network servers containing TACACS+ server software. After you have entered an IP address, you will see the following prompt:

```
Use per-server secret [Y/N] ->
```

      If you will be specifying more than one TACACS+ server and if all of the servers use the same encryption secret, you can answer No to this prompt and enter the encryption secret using the TAC Global Secret parameter.

      However, if you are specifying only one TACACS+ server or if the servers have difference encryption secrets, then respond with Yes to this prompt. You will see:

```
Enter per-server secret [max 40 characters] ->
```

      Use this prompt to enter the encryption secret for the TACACS+ server whose IP address you are specifying.

4 - TAC Server Order
You use this selection to indicate the order in which you want the switch to query the TACACS+ servers for logon authentication. Of course, you can skip this option if you specified only one IP address. The default is 1, 2, and 3, in that order.

5 - TAC Global Secret
If all of the TACACS+ servers have the same encryption secret, rather then entering the same secret when you enter the IP addresses, you can use this option to enter the secret just once.

3 - TAC Timeout
This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

c. Once you have finished configuring the settings, type **R** to return to the Authentication Menu.

d. Type **1** to select Server-based Authentication. This menu option is used to enable and disable the manager account feature on the switch. If disabled, the switch uses its standard Manager and Operator accounts when you log on to manage the switch. If enabled, the switch uses the manager accounts on the TACACS+ or RADIUS server. The following prompt is displayed:

```
Server Based User Authentication (E-Enabled, D-
Disabled) ->
```

e. Type **E** to enable the manager account feature on the switch or **D** to disable it. The default is disabled.

f. After you have finished configuring the parameters, type **S** to select Save Configuration Changes.

6. To configure the RADIUS protocol, from the Authentication Menu in Figure 52 on page 196 do the following:

   a. Type **4** to select RADIUS Configuration. The following menu is displayed:

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

           RADIUS Client Configuration

1 - Global Encryption Key ............. 0.0.0.0
2 - Global Server Timeout period....... 0.0.0.0
3 - RADIUS Server 1 Configuration ..... 0.0.0.0
4 - RADIUS Server 2 Configuration ..... 0.0.0.0
5 - RADIUS Server 3 Configuration ..... 0.0.0.0
6 - Show Status

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 54 RADIUS Client Configuration

   b. Configure the parameters as needed. The parameters are defined below:

Global Encryption Key
This parameter specifies the encryption key for the RADIUS servers. This option is useful if you will be entering more than one RADIUS server and all the servers share the same encryption key. If the servers use different encryption keys, leave this option blank.

Global Server Timeout period
This parameter specifies the maximum amount of time the switch will wait for a response from a RADIUS server before assuming that the server cannot respond. If the timeout expires and the server hasn't responded, the switch queries the next RADIUS server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

3 - RADIUS Server 1 Configuration
4 - RADIUS Server 1 Configuration
5 - RADIUS Server 1 Configuration
Use these parameters to specify the IP addresses of up to three network servers containing the RADIUS server software. Selecting one of the options displays the following menu:

```
Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

          RADIUS Server 1 Configuration

1 - Server IP Address ................. 0.0.0.0
2 - Server Authentication UDP Port .... 1812
3 - Server Encryption Key ........ <Not Defined>

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 55 RADIUS Server Configuration

The options are described below:

1 - Server IP Address
Use this option to specify the IP address of a RADIUS server.

2 - Server Authentication UDP Port
Use this option to specify the UDP port of the RADIUS protocol. The default is port 1812.

3 - Server Encryption Key
Use this option to specify the encryption key for the RADIUS server.

c. Once you have finished configuring the settings in the RADIUS Client Configuration menu, type **R** to return to the Authentication Menu.

Note
Steps d. and e. do not apply to the 802.1x port-based access control feature.

d. If you are configuring the RADIUS client software to use the new manager account feature, type **1** to select Server-based Authentication. This menu option is used to enable and disable the manager account feature on the switch. If disabled, the switch uses its standard Manager and Operator accounts when you log on to manage the switch. If enabled, the switch uses the manager accounts on the TACACS+ or RADIUS server. If you configured the

RADIUS client software for the 802.1x port-based access control feature, but not for the manager accounts feature, leave this option disabled.

The following prompt is displayed:

```
Server Based User Authentication (E-Enabled, D-
Disabled) ->
```

e. Type **E** to enable the manager account feature on the switch or **D** to disable it. The default is disabled.

f. After you have finished configuring the parameters, type **S** to select Save Configuration Changes.

Chapter 18
802.1x Port-Based Access Control

This chapter contains an overview and procedures for the 802.1x port-based access control feature. Sections are as follows:

Note
You must use a local management session to configure port-based access control. You cannot configure this feature through enhanced stacking or from a Telnet management session.

802.1x Port-based Access Control Overview

The AT-S39 management software has several different methods for protecting your network and its resources from unauthorized access. For instance, **Chapter 6**, **Port Security** on page 76, explains how you can restrict network access by having the switch accept or discard packets based on source MAC addresses.

This chapter explains yet another way. This method is referred to as port-based access control (IEEE 802.1x). It uses the RADIUS protocol to control who can send traffic through and receive traffic from a port. With this feature, the switch will not allow an end node to send or receive traffic through a port until the user of the node has logged on by entering a username and password that the RADIUS server must validate.

The benefit to this type of network security is obvious. This feature can prevent an unauthorized individual from connecting a computer to a port or using an unattended workstation to access your network resources. Only those users to whom you have assigned valid usernames and passwords will be able to use the switch to access the network

This port security method uses the RADIUS authentication protocol. The AT-S39 software comes with RADIUS client software. If you have already read **Chapter 17**, **TACACS+ and RADIUS Protocols** on page 192, then you know that you can also use the RADIUS client software on the switch, along with a RADIUS server on your network, to create new manager accounts that control who can manage and change the AT-S39 parameter on the switch.

Note
RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature. This feature is not supported with the TACACS+ authentication protocol. Since the switch can support only one authentication protocol at a time, you must use the RADIUS protocol if you want a switch to support both the IEEE 802.1 port access control feature, as explained in this chapter, and new manager accounts, as explained in **Chapter 17**, **TACACS+ and RADIUS Protocols** on page 192.

Here are a few terms to keep in mind when using this feature.

- Supplicant - A supplicant is an end user or end node that wants to access the network through a port. A supplicant is also referred to as a client.
- Authenticator - The authenticator is a port on the switch that prohibits network access by a supplicant until the network user has entered a valid username and password.

- ❑ Authentication server - The authentication server is the network device that has the RADIUS server software. This is the device that will do the actual authenticating of the user names and password from the supplicants.

The AT-8524M switch itself does not authenticate the username and passwords from the clients. Rather, it simply acts as an intermediary between a supplicant and the authentication server during the authentication process.

Authentication Process

Below is a brief overview of the authentication process that occurs between a supplicant, authenticator, and authentication server. For further details, refer to the IEEE 802.1x standard.

1. Either the authenticator port or the supplicant can initiate an authentication message exchange. The switch initiates an exchange when it detects a change in the status of a port (such as when the port transitions from no link to valid link), or if it receives a packet on the port with a source MAC address not in the MAC address table.

   An authenticator starts the exchange by sending an EAP-Request/Identity packet. A supplicant starts the exchange with an EAPOL-Start packet, to which the authenticator responds with a EAP-Request/Identity packet.

2. The supplicant responds with an EAP-Response/Identity packet to the authentication server via the authenticator.
3. The authentication server responds with an EAP-Request packet to the supplicant via the authenticator.
4. The supplicant responds with an EAP-Response/MDS packet containing a username and password.
5. The authentication server sends either an EAP-Success packet or EAP-Reject packet to the supplicant.
6. Upon successful authorization of the supplicant by the authentication server, the switch adds the supplicant's MAC address to the MAC address as an authorized address and begins forwarding network traffic to and from the port.
7. When the supplicant sends an EAPOL-Logoff message, the switch removes the supplicant's MAC address from the MAC address table, preventing the supplicant from sending or receiving any further traffic from the port.

Port Roles

Part of the task to implementing this feature is specifying the roles of the ports on the switch. A port can have one of two roles:

- ❑ None
- ❑ Authenticator

None Role

A port in the none role does not participate in port-based access control. Any device can connect to the port and send traffic through it and receive traffic from it without having to provide a username and password. This is the default setting for a port.

You would set a port to this role if you did not want its client to have to log on to use the network. This also happens to be the correct role for a port that's connected to an authentication server. Since an authentication server cannot authenticate itself, the port to which it is connected must be set to this role.

Authenticator Role

Placing a port in the authenticator role activates port access control on the port. A port in the role of authenticator will not forward network traffic to or from the end node until the client has entered a username and password and the authentication server has validated them.

Determining whether a port should be set to the authenticator role is straightforward. If you want the user of the end node connected to the port to log in before using the network, then you should set the port to the authenticator role.

As mentioned earlier, the switch itself does not authenticate the user names and passwords from the clients. That is the responsibility of the authentication server, which contains the RADIUS server software. Instead, a switch simply acts as an intermediary for the authentication server by denying access to the network by the client until the client has provided a valid username and password, which the authentication server validates.

General Steps

Here are the general steps to implementing 802.1x Port-based Access Control and RADIUS accounting on the switch:

1. You must install RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesyn. Funk Software Steel-Belted Radius and Free Radius have been verified as fully compatible with the AT-S39 management software.

Note
This feature is not supported with the TACACS+ authentication protocol.

2. You need to install 802.1x client software on those workstations that are to be supplicants. Microsoft WinXP client software and Meeting House Aegis client software have been verified as fully compatible with the AT-S39 management software.
3. You must configure and activate the RADIUS client software in the AT-S39 management software. The default setting for the authentication protocol is disabled. You will need to provide the following information:

   ❑ The IP addresses of up to three RADIUS servers.

   ❑ The encryption keys used by the authentication servers.

   The instructions for this step are in **Configuring the Authentication Client Software** on page 196.

4. You must configure the port access control settings on the switch. This involves the following:

   ❑ Specifying the port roles.

   ❑ Configuring 802.1x port parameters.

   ❑ Enabling 802.1x port access control.

   The instructions for this step are found in this chapter.

Port-based Access Control Guidelines

Here are the guidelines to using this feature:

- ❑ Ports operating under port-based access control do not support port trunking or dynamic MAC address learning.
- ❑ The appropriate port role for a port on an switch connected to an authentication server is None.
- ❑ The verification process between a supplicant and the authentication server does not allow for tagged packets. Consequently, each VLAN that contains clients must have a separate authentication server and the server must be connected to a port that is an untagged member of the VLAN in which the supplicants are members.
- ❑ Allied Telesyn does not recommend connecting more than one supplicant to an authenticator port on the switch.

Note
Connecting multiple supplicants to a port set to the authenticator role does not conform to the IEEE 802.1x standard, can introduce security risks, and can result in undesirable switch behavior. To avoid this, Allied Telesyn recommends not using the authenticator role on a port that is connected to more than one end node, such as a port connected to another switch or a hub.

- A username and password combination is not tied to the MAC address of an end node. This allows end users to use the same username and password when working at different workstations.
- Once a supplicant has successfully logged on, the MAC address of the end node is added to the switch's MAC address table as an authenticated address. It remains in the table until the end user logs off the network or does not respond to a reauthentication request. Only then is the address removed. The address is not timed out, even if the end node becomes inactive.

Note
End users of port-based access control should be instructed to always log off when they are finished with a work session. This will prevent unauthorized individuals from accessing the network through unattended network workstations.

- You cannot use the MAC address port security feature, described in **Chapter 6**, **Port Security** on page 76, on ports that are set to the Authenticator role.
- There can be only one port in the authenticator role between a supplicant and the authentication server.
- The Authentication Menu for configuring the RADIUS client software has the selection "1 - Server-based Authentication." This option does not apply to the 802.1x port-based access control, but only to new manager accounts, as described in **Chapter 17**, **TACACS+ and RADIUS Protocols** on page 192. It does not need to be toggled to Enabled for the switch to use the RADIUS configuration information. If you want to use 802.1x port-based access control but not create new manager accounts, you can leave the menu selection as disabled.

- Ports used to interconnect switches should be set to the none role, as illustrated in Figure 56.

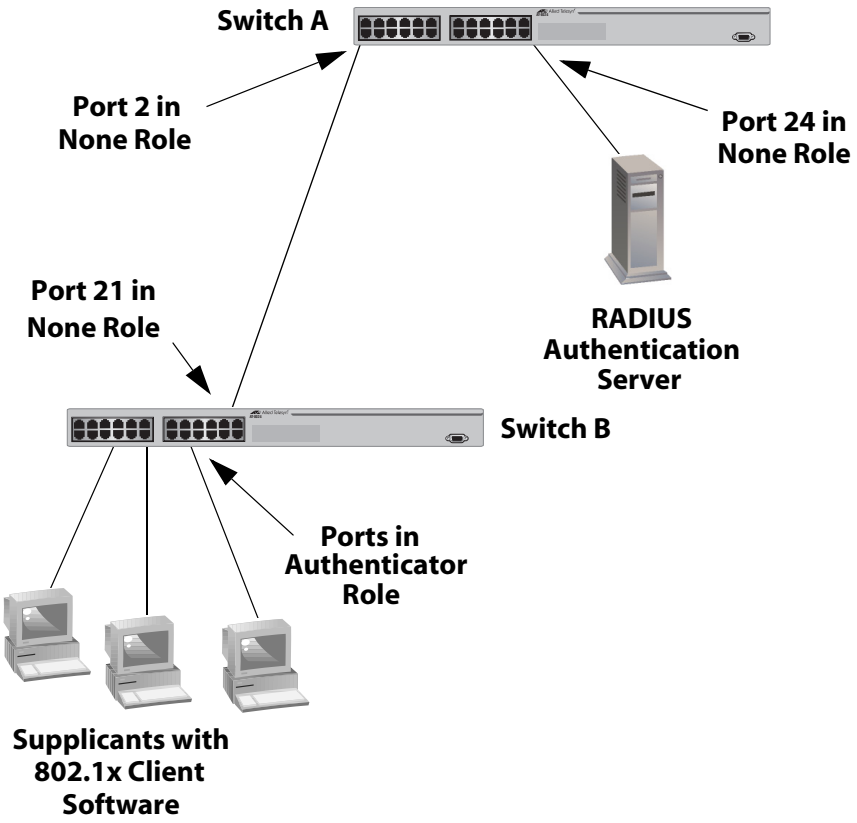

Figure 56 Port-based Authentication Across Multiple Switches

Enabling and Disabling Port Access Control

This procedure explains how to enable and disable port-based access control on the switch. If you plan to activate the feature, there are two things you need to do first. They are:

- ❑ Configure the RADIUS authentication protocol on the switch, as explained in **Configuring the Authentication Client Software** on page 196.
- ❑ Assign port roles and configure the parameter settings, as explained in **Configuring Port Access Control Parameters** on page 211.

To enable or disable 802.1x port-based access control, perform the following procedure:

> **Note**
> You must use a local management session to configure port-based access control. You cannot configure this feature through a Telnet management session or enhanced stacking.

1. From the Main Menu, type **1** to select Port Menu.

   The Port Menu is shown in Figure 12 on page 66.

2. Type **6** to select Port Access Control.

   The Port Access Control menu is shown in Figure 57.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

               Port Access Control

1 - Port Access Control ..............  Enabled
2 - Authentication Method ............  RADIUS EAP
3 - Configure Port Access Parameters
4 - Display Port Access Parameters
5 - Display Port Access Status

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 57 Port Access Control Menu

Note
Option 2 - Authentication Method cannot be changed. 802.1x port-based access control is supported only with the RADIUS authentication protocol. It is not supported with TACACS+.

3. Type **1** to select Port Access Control. The following prompt is displayed:

   ```
   Port Access Control (E-Enable, D-Disable):
   ```

4. Type **E** to enable port access control, or **D** to disable port access control. Press Return.

   The change is immediately activated on the switch.

5. Type **S** to select Save Configuration Changes.

Configuring Port Access Control Parameters

Note
You must use a local management session to configure port-based access control. You cannot configure this feature through a Telnet management session or enhanced stacking.

To configure port access control parameters, perform the following procedure:

1. From the main menu, type **1** to select the Port menu.
2. In the Port menu, type **6** to select the Port Access Control menu.
3. In the Port Access Control Menu, type **3** to select Configure Port Access Parameters. The following prompt is displayed:

   ```
   Enter ports list ->
   ```

4. Enter the port you want to configure. You can specify more than one port at a time. Press Return. The following menu is displayed.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager
        Configure Port Access Parameters
Configuring Ports 3
0 - Port Role ......... None

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 58 Configure Port Access Parameters

5. Type **0** to select Port Role. The following prompt is displayed:

   ```
   Enter new port role [N-None, A-Authenticator] ->
   ```

6. If you type **N** for None, the port will not participate in port access control. This is the default setting. If the port is connected to a supplicant, type **A** to set the port's role to Authenticator. You will see the Configure Port Access Parameters menu, shown in Figure 59. Go to the next step to configure the settings.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

        Configure Port Access Parameters

Configuring Ports 3
0 - Port Role ............. Authenticator
1 - Port Control .......... Auto
2 - Quiet Period .......... 60
3 - Tx Period ............. 30
4 - Reauth Period ......... 3600
5 - Supplicant Timeout .... 30
6 - Server Timeout ........ 30
7 - Max Requests .......... 2

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 59 Configure Port Access Parameters Menu

7. Select the parameter that you wish to modify. The parameters are described below:

   0 - Port Role
   This parameter specifies the current authentication status of the port. If Authenticator is selected, the port performs the role of authenticating the supplicants that are connected to the port. If None is selected, the port does not participate in port access control. The default for this parameter is None.

   1 - Port Control
   This parameter can take the following values:

   - **Auto**: Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address. This is the default setting.

   - **Force-authorized**: Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.

- **Force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

2 - Quiet Period
Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

3 - Tx Period
Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

4 - Reauth Period
Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

5 - Supplicant Timeout
Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

6 - Server Timeout
This is the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 30 seconds. The range is 1 to 65,535 seconds.

7 - Max Requests
This parameter specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

8. Type **S** to select Save Configuration Changes.

Viewing Port Access Status

Note
You must use a local management session to view port-based access control parameters. You cannot view the parameters through a Telnet management session or enhanced stacking.

To view port access status, perform the following procedure:

1. From the main menu, type **1** to select the Port menu.
2. In the Port menu, type **6** to select the Port Access Control menu.
3. From the Port Access Control Menu, type **5** to select Display Port Access Status. The Port Access Status is displayed (see Figure 60).

```
     Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                      Sales Switch
Login Privilege: Manager
                Display Port Access Status
Port   PortRole        Status           Supplicant
-------------------------------------------------------
001  None            ------          -----------------
002  Authenticator   ------          -----------------
003  Authenticator   ------          -----------------
004  Authenticator   ------          -----------------
005  None            ------          -----------------
006  None            ------          -----------------
007  None            ------          -----------------
008  None            ------          -----------------

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 60 Display Port Access Status Menu

Chapter 19
Ethernet Statistics

This chapter contains the procedures for displaying data traffic statistics. Sections in the chapter include:

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **7** to select Ethernet Statistics.

   The Ethernet Statistics menu is shown in Figure 61.

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch
Login Privilege: Manager

               Ethernet Statistics
1 - Display Port Statistics
2 - Display Module Statistics
3 - Clear Statistics

R - Return to Previous Menu

Enter your selection?
```

Figure 61 Ethernet Statistics Menu

2. From the Ethernet Statistics menu, type **1** to select Display Port Statistics.

   A window is displayed containing the statistics for each port. The information in this window is for viewing purposes only. The statistics are defined below:

   Total Count (TOTAL_COUNT)
   Number of bytes received and transmitted on the port.

   Transmit Packets (TX_COUNT)
   Number of bytes transmitted out the port.

   Received Packets (RX_COUNT)
   Number of bytes received on the port.

   Received Broadcast (RX_BRDCAST)
   Number of broadcast packets received on the port.

   Received Multicast (RX_MLTCAST)
   Number of multicast packets received on the port.

   Received Unicast (RX_UNICAST)
   Number of unicast packets received on the port.

   Received Overflow (RX_OVERFLOW)
   Number of times the capacity of the port's buffer has been exceeded.

CRC Error (CRC_ERROR)
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets (UNDERSIZE)
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Fragmented Packets (FRAGMENT)
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Port Discards (PRT_DISCARD)
Number of frames successfully received and buffered by the port, but discarded and not forwarded.

To clear all port and switch counters and return them to "0", select option "3 - Clear Statistics" from the Ethernet Statistics menu.

Displaying Switch Statistics

To display Ethernet statistics for the entire switch, perform the following procedure:

1. From the Main Menu, type **7** to select Ethernet Statistics.
2. From the Ethernet Statistics menu, type **2** to select Display Module Statistics.

   The statistics for the entire switch are displayed in the Display Module Statistics window, shown in Figure 62.

```
Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

            Display Module Statistics

Ethernet statistics for this module

TOTAL_COUNT ................. 0
TX_COUNT .................... 0
RX_COUNT .................... 0
RX_BRDCAST .................. 0
RX_MLTCAST .................. 0
RX_UNICAST .................. 0
RX_OVERFLOW ................. 0
CRC_ERROR ................... 0
UNDERSIZE ................... 0
FRAGMENT .................... 0
PORT_IN_DISCARDS ............ 0

U - Update Display
C - Clear Module Statistics
R - Return to Previous Menu

Enter your selection?
```

Figure 62 Display Module Statistics Window

The information in this window is for viewing purposes only. The statistics are defined below:

Total Count
Number of valid packets received and transmitted by the switch.

Transmit Packets
Number of packets transmitted from the switch.

Received Packets
Number of packets received by the switch.

Received Overflow
Number of times the capacity of the port buffers have been exceeded.

Received Broadcast
Number of broadcast packets received on the switch.

Received Multicast
Number of multicast packets received on the switch.

CRC Error
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the switch.

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 switch.

Fragmented Packets
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the switch.

Port in Discards
Number of frames successful received and buffered by the switch, but discarded and not forwarded.

To clear the counters on the switch and return them to "0", select option "C - Clear Module Statistics" from the Display Module Statistics window or option "3 - Clear Statistics" from the Ethernet Statistics Menu.

Chapter 20
File Downloads and Uploads

This chapter contains the following sections:

Note
For instructions on how to obtain the latest version of the AT-S39 management software, refer to **Management Software Updates** on page 18.

File Uploads and Downloads Overview

The firmware on an AT-8000 Series switch consists of the following three parts:

- ❑ AT-S39 management software

  This is the operating software for the switch.

- ❑ AT-S39 bootloader

  This code initially controls the switch whenever you power on or reset the unit.

- ❑ Switch configuration

  This contains the settings for the different switch parameters, such as VLANs, STP settings, and so forth.

> **Note**
> In versions previous to AT-S39 Version 2.0.1, the management software and bootloader were offered as separate files. In all later versions, the files are combined into one image file.

You can use the AT-S39 management software to download a new version of the management software and bootloader onto a switch so that a switch always has the latest software.

You can also download a configuration file from a master switch to other switches in an enhanced stack, or to a management workstation. This is useful in network environments where there are AT-8000 Series switches that need to be configured the same, or nearly the same. You can configure the master switch of an enhanced stack network and download its configuration file to the other switches, saving you the trouble of having to configure each switch individually. The download of a configuration file includes all switch information, including IP address, subnet mask, gateway address, enhanced stacking status, and BOOTP/DHCP status.

> **Note**
> A configuration file for an AT-8000 Series switch cannot be edited with a text editor.

There are a several methods for downloading and uploading files from a switch. They are:

- Local management session

  This method uses a local management session to upload or download a file onto a switch. This method supports Xmodem and TFTP. You can use this method on any type of AT-8000 switch, regardless of its enhanced stacking status (i.e., master, slave or unavailable.) The procedures for this are explained in **Downloading Files from a Local Management Session** on page 223 and **Uploading Files from a Local Management Session** on page 235.

- Remote management session

  Another method is from a remote management session of a switch. This can be a switch you accessed through enhanced stacking or directly through a Telnet management session. This method uses TFTP. The procedures for this method are in **Downloading Files from a Remote Management Session** on page 229 and **Uploading Files from a Remote Management Session** on page 239.

- Switch to switch

  This method downloads files from the master switch of an enhanced stack to the slave switches. This method is useful if you have a large number of AT-8000 Series switches in your network. It simplifies the task of updating the management software on the switches. You can upgrade the AT-S39 software on the master switch, and then instruct the switch to download its software to the other switches in the enhanced stack. You can also use this to download a configuration file from a master switch to slave switches. You cannot use this method to upload files. This procedure is explained in **Downloading Files Switch to Switch** on page 232.

Note
You cannot upload or download files from a web browser management session.

Downloading Files from a Local Management Session

This section contains the procedure for downloading a new AT-S39 software image file or configuration file onto a switch from a local management session.

Note
To download a file through enhanced stacking or a Telnet management session, go to **Downloading Files from a Remote Management Session** on page 229.

Here are guidelines that apply to download files from a local management session:

- All switch models in the AT-8000 Series use the same management software image.
- You can use Xmodem or TFTP.
- If you are downloading a new AT-S39 software image, the switch's current configuration settings (for instance, IP address, port security, and virtual LANs) are not changed.
- If you are downloading a configuration file, the switch's current configuration settings are overwritten by the configuration settings contained in the file. This includes the IP address, subnet mask, enhanced stacking status, and BOOTP/DHCP status.
- A configuration file should only be downloaded onto a switch of the same model from which the configuration file originated (for example, AT-8024M to AT-8024M). It is not recommended that you download a configuration file onto a switch of a different model (for example, AT-8012M to AT-8024GB). Undesired switch behavior may result.
- A switch running AT-S39 Version 1.4 or earlier must first be ungraded to Version 1.4.1 or 1.4.2 before you can install a new AT-S39 image.

Caution
Downloading a new AT-S39 image file or configuration file will cause a switch reset. Some network traffic may be lost.

Here are guidelines that apply to an Xmodem download:

- Xmodem can only download a file onto the switch on which you started the local management session. Xmodem cannot download files through enhanced stacking.

- ❑ The file to be downloaded must be stored on the computer or terminal connected to the RS232 Terminal Port on the switch.

Here are guidelines that apply to a TFTP download:

- ❑ There must be a node on your network that contains the TFTP server software. The AT-S39 image file or configuration file to download must be stored on the server.
- ❑ You should start the TFTP server software before you begin the download procedure.
- ❑ The switch where you are downloading the file must have an IP address and subnet mask. Consequently, you cannot use TFTP on a slave switch of an enhanced stack unless the switch has an IP address. Rather, you would need to perform the download using Xmodem or, alternatively, switch-to-switch, as explained in **Downloading Files Switch to Switch** on page 232.

To download a new software image or configuration file onto a switch from a local management session, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software or configuration file.

   For instructions, refer to **Starting a Local Management Session** on page 31.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

   The Downloads and Uploads menu is shown in Figure 63:

```
 Allied Telesyn Ethernet Switch AT-8024 - AT-S39
                  Sales Switch

Login Privilege: Manager

               Downloads & Uploads

1 - Download Application Image/Bootloader
2 - Download Configuration Data

3 - Upload Application Image
4 - Upload Configuration Data

R - Return to Previous Menu

Enter your selection?
```

Figure 63 Downloads & Uploads Menu

Note
Options 3 and 4 in the menu are described in **Uploading Files from a Local Management Session** on page 235.

4. To download a new software image onto the switch, type **1**. To download a configuration file, type **2**.

   The following prompt is displayed:

   ```
   Download Method/Protocol [X-Xmodem, T-TFTP]:
   ```

5. To download a file using Xmodem, go to Step 6. To download a file using TFTP, do the following:

   a. Type **T**.

      The following prompt is displayed:

      ```
      TFTP Server IP address:
      ```

   b. Enter the IP address of the TFTP server.

      The following prompt is displayed:

      ```
      Remote File Name:
      ```

   c. Enter the file name of the image file or configuration file you want to download.

      The download begins. If you are downloading a configuration file, the switch automatically resets once the download is complete. Some network traffic may be lost during the system reset.

Caution
When downloading a switch image file, the switch must initialize it by decompressing it and writing it to flash. This requires one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file.

   If you are downloading a new AT-S39 image file, the conclusion of the download and software initialization process is signalled with this message:

   ```
   Please press <ENTER> key TWICE to proceed with
   Switch Reboot...
   ```

   d. Press the Return key twice to reset the switch. Some network traffic may be lost during the system reset.

      The download process is complete once the switch has completed its reset. The new AT-S39 image file or configuration file is now active on the switch.

   e. To continue managing the switch, you must reestablish your management session.

6. To download an AT-S39 image file or configuration using Xmodem, do the following:

   a. Type **X** at the prompt displayed in Step 4.

      The following prompt is displayed:

      ```
      You are going to invoke the Xmodem download
      utility.
      Do you wish to continue? [Yes/No]
      ```

   b. Type **Y** for Yes.

      The following prompt is displayed:

      ```
      Use Hyper Terminal's 'Transfer/Send File' option
      to select Filename & Protocol

      Note: Please select '1K Xmodem' protocol for
      faster download...
      ```

   c. Begin the file transfer of the new management software image or configuration file.

   Note
   The transfer protocol must be Xmodem or 1K Xmodem.

   Steps d. through h. illustrate the download procedure using the Hilgraeve HyperTerminal program.

   d. From the HyperTerminal main window, select the **Transfer** menu. Then select **Send File** from the pull-down menu, as shown in Figure 64.

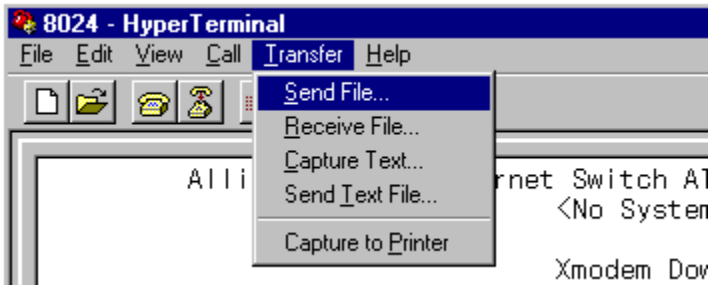

Figure 64 Local Management Window

The Send File window in Figure 65 is displayed.

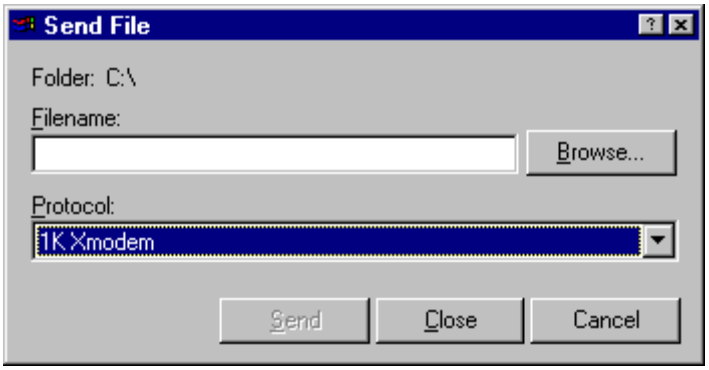

Figure 65 Send File Window

e. Click the Browse button and specify the location and file to be downloaded onto the switch.

f. Click on the Protocol field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.

g. Click **Send**.

   The software immediately begins to download onto the switch. The Xmodem File Send window in Figure 66 displays current status of the software download. The download process takes a couple minutes to complete.

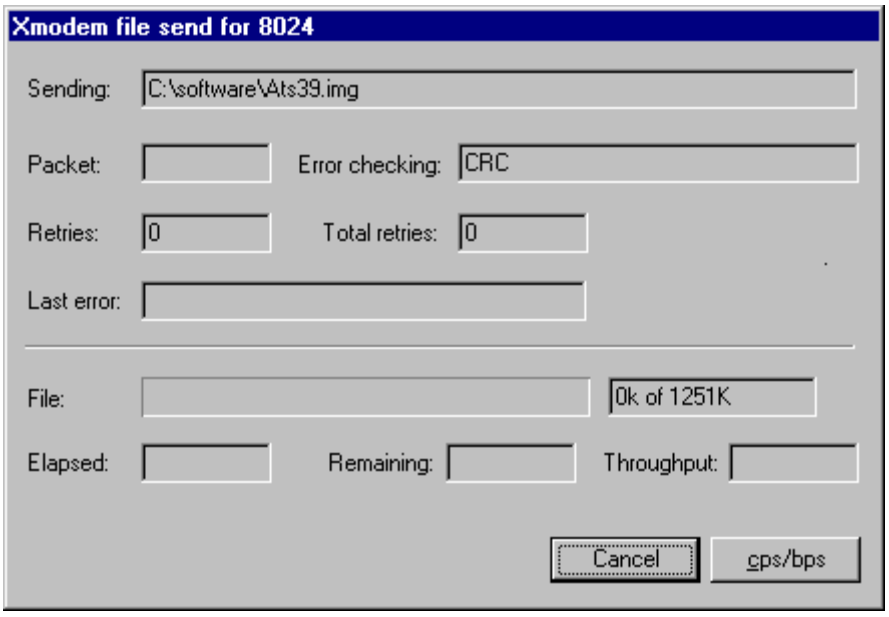

Figure 66 XModem File Send Window

The download begins. If you are downloading a configuration file, the switch automatically resets once the download is complete. Some network traffic may be lost during the system reset.

Caution

When downloading a switch image file, the switch must initialize it by decompressing it and writing it to flash. This requires one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file.

The completion of the download and initialization process of an AT-S39 image file is signalled with this message:

```
Please press <ENTER> key TWICE to proceed with
Switch Reboot...
```

h. Press the Return key twice to reset the switch. Some network traffic may be lost during the system reset.

   The download process is complete once the switch has completed its reset. The new AT-S39 image file or configuration file is now active on the switch.

i. To continue managing the switch, you must reestablish your management session.

Downloading Files from a Remote Management Session

This section contains the procedure for downloading a new AT-S39 software image or configuration file onto a switch from a remote session. The remote switch can be a switch accessed through enhanced stacking (such as a slave switch) or a switch where you started a Telnet management session.

Please note the following before you begin the procedure:

- ❑ You must use TFTP to remotely download a file.
- ❑ There must be a node on your network that contains the TFTP server software. The AT-S39 image file or configuration file to download must be stored on the server.
- ❑ You should start the TFTP server before you begin the download procedure.
- ❑ The switch where you are downloading the file must have an IP address and subnet mask. Consequently, you cannot use TFTP on a slave switch of an enhanced stack unless the switch has an IP address. Rather, you would need to perform the download from a local management session using Xmodem or, alternatively, switch-to-switch, as explained in **Downloading Files Switch to Switch** on page 232.
- ❑ If you are downloading a new AT-S39 software image, the switch's current configuration settings (for instance, IP address, port security, and virtual LANs) are not changed.
- ❑ If you are downloading a configuration file, the switch's current configuration settings are overwritten by the configuration settings contained in the file.
- ❑ A configuration file should only be downloaded onto a switch of the same model from which the configuration file originated (for example, AT-8024M to AT-8024M). It is not recommended that you download a configuration file onto a switch of a different model (for example, AT-8012M to AT-8024GB). Undesired switch behavior may result.
- ❑ A switch running AT-S39 Version 1.4 or earlier must first be ungraded to Version 1.4.1 or 1.4.2 before you can install a new AT-S39 image.

Caution
Downloading a new AT-S39 image file or configuration file will cause a switch reset. Some network traffic may be lost.

To remotely download a new software image or configuration file onto a switch, perform the following procedure:

1. From the Main Menu of the switch where you want to remotely download the file, type **4** to select Administration Menu.
2. From the Administration Menu, type **D** to select Downloads & Uploads.

   The Downloads and Uploads menu is shown in Figure 63 on page 224.
3. To download a new software image onto the switch, type **1**. To download a configuration file, type **2**.

   The following prompts are displayed:

   ```
   Switch will reboot after download. Remote access
   will be terminated!

   Only TFTP downloads are available for a remote
   access

   TFTP Server IP Address:
   ```
4. Enter the IP address of the TFTP server.

   The following prompt is displayed:

   ```
   Remote File Name:
   ```
5. Enter the filename of the image file or configuration file stored on the TFTP server to be downloaded onto the switch.

   Once the filename has been specified, the download begins. File download takes only a few moments.

   If you are downloading a configuration file, the switch automatically resets once the download is complete. Some network traffic may be lost during the system reset.

⚠ Caution

When downloading a switch image file, the switch must initialize it by decompressing it and writing it to flash. This requires one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file.

   The completion of the download and initialization process of an AT-S39 image file is signalled with this message:

   ```
   Please press <ENTER> key TWICE to proceed with
   Switch Reboot...
   ```
6. Press the Return key twice to reset the switch. Some network traffic may be lost during the system reset.

The download process is complete once the switch finishes the reset process. The new AT-S39 image file or configuration file is now active on the switch.

7. To continue managing the switch, you must reestablish your management session.

Downloading Files Switch to Switch

This procedure explains how to download an AT-S39 software image from a master AT-8000 Series switch to another switch. This procedure is useful in networks that contain a large number of AT-8000 Series switches. Once you have updated the software on the master switch of an enhanced stack, you can instruct the master switch to automatically upgrade the other slave and master AT-8000 Series switches in the same enhanced stack.

This procedure can also be used to download a master switch's configuration file to another switch in an enhanced stack. This provides an easy way to quickly configure multiple switches that are to have similar configurations. You can configure the master switch and then download its configuration to other switches in the enhanced stack that are to have the same configuration. The download of a configuration file includes all switch information, including IP address, subnet mask, gateway address, enhanced stacking status, and BOOTP/DHCP status.

Caution
Installing a new AT-S39 image file or configuration file on a switch involves a switch reset. Some network traffic may be lost.

A configuration file should only be downloaded onto a switch of the same model from which the file originated (for example, AT-8024M to AT-8024M). It is not recommended that you download a configuration file onto a switch of a different model (for example, AT-8012M to AT-8024GB). This can result in undesired switch behavior.

To download a management software image or configuration file from a master switch to other switches in the same enhanced stack, perform the following procedure:

1. Start a local or Telnet management session on the master switch of the enhanced stack.
2. From the Main Menu, type **9** to select Enhanced Stacking. The Enhanced Stacking window is shown in Figure 10 on page 61.
3. From the Enhanced Stacking window, type **2** to select Stacking Services. The Stacking Services menu is shown in Figure 11 on page 63.

Note
The "2 - Stacking Services" selection is available only on master switches.

4. Type **G** to select Get/Refresh List of Switches.

   The master switch polls the enhanced stack for all slave and other master switches and displays a list of the switches in the Stacking Services menu.

   Note
   The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of unavailable.

   By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well. This is accomplished with the selection S - Sort Switches in New Order.

5. Do one of the following:

   - ❑ To download both the AT-S39 software image and bootloader on the master switch to another AT-8000 Series switch, type **I** to select Image Download to Remote Switches.
   - ❑ To download the configuration file on the master switch to another AT-8000 Series switch, type **C** to select Config Download to Remote Switches.
   - ❑ To download just the bootloader on the master switch to another switch, type **B** to select Bootloader Download to Remote Switches.

   The following prompts are displayed:

   ```
   Remote switches will reboot after download is
   complete
   Enter the starting remote switch number -> [1 to 12]
   ```

6. Enter the number of the switch whose software or configuration file you want to update. To update a range of switches, enter the number of the first switch.

   The following prompt is displayed:

   ```
   Enter the ending remote switch number -> [1 to 12]
   ```

7. Enter the last switch in the range you want to update. To update just one switch, enter the same number here as you entered in the previous step.

   The following prompt is displayed:

   ```
   Do you want to show remote switch burning flash ->
   [Yes/No]
   ```

8. You can respond with Yes or No to this prompt. It does not affect the download.

The following prompt is displayed:

```
Do you want confirmation before downloading each
switch -> [Yes/No]
```

9. Answering Yes to this prompt means that the management software will prompt you with a confirmation message before it begins to upgrade each switch. Answering No means the management software will not display a confirmation prompt before downloading.

   The management software begins the download.

   If you are downloading a configuration file, the switch automatically resets once the download is complete. Some network traffic may be lost during the system reset.

⚠ Caution

When downloading a switch image file, the switch must initialize it by decompressing it and writing it to flash. This requires one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file.

The completion of the download and initialization process of an AT-S39 image file is signalled with this message:

```
Please press <ENTER> key TWICE to proceed with
Switch Reboot...
```

10. Press the Return key twice to reset the switch. Some network traffic may be lost during the system reset.

    The download process is now complete. The new AT-S39 image file or configuration file is now active on the switch.

Uploading Files from a Local Management Session

This section contains the procedure for uploading a switch's AT-S39 software image or configuration file from a local management session.

Note
To upload a file through enhanced stacking or a Telnet management session, go to **Uploading Files from a Remote Management Session** on page 239.

Please note the following before you begin the procedure:

- ❑ You can use Xmodem or TFTP to upload a file from a local management session.
- ❑ Xmodem can upload a file only from the switch where you started the local management session. Xmodem cannot upload files through enhanced stacking.
- ❑ To use TFTP, note the following:
  - — There must be a node on your network that contains the TFTP server software.
  - — You should start the TFTP server before you begin the upload procedure.
  - — The switch where you are uploading the file must have an IP address. Consequently, you cannot use TFTP to upload a file from a slave switch unless it has an IP address.

Note
It is not recommended that you upload an AT-S39 software image onto a management workstation for download onto another switch. New AT-S39 software images for download onto a switch should be obtained from the Allied Telesyn web site.

To upload a software image or configuration file from a switch using a local management session, perform the following procedure:

1. Start a local management session on the switch from where you intend to upload the management software image or configuration file.

   For instructions, refer to **Starting a Local Management Session** on page 31.
2. From the Main Menu, type **4** to select Administration Menu.

3. From the Administration Menu, type **D** to select Downloads & Uploads.

   The Downloads and Uploads menu in Figure 63 on page 224 is displayed.

4. To upload the AT-S39 software image and bootloader from the switch, type **3**. To upload a configuration file, type **4**.

   The following prompt is displayed:

   ```
   Upload Method/Protocol [X-Xmodem, T-TFTP]:
   ```

5. To upload a file using Xmodem, go to Step 6. Upload a file using TFTP, do the following:

   a. Type **T**.

      The following prompt is displayed:

      ```
      TFTP Server IP address:
      ```

   b. Enter the IP address of the TFTP server.

      The following prompt is displayed:

      ```
      Remote File Name:
      ```

   c. Enter the file name that the file is to be stored as on the TFTP server.

      Once the filename has been specified, the upload begins. Uploading a configuration file takes only a few moments. Uploading an AT-S39 image file can take several minutes.

6. To upload a file using Xmodem, do the following:

   a. At the prompt is step 4, type **X**.

      The following prompt is displayed:

      ```
      You are going to invoke Xmodem upload utility:
      Do you wish to continue? [Yes/No] ->
      ```

   b. Type **Y** for Yes.

      The following messages are displayed:

      ```
      Use Hyper Terminal's 'Transfer/Receive File'
      option to select Protocol

      Note: Please select '1K Xmodem' protocol for
      faster upload...
      ```

   c. Begin the file transfer.

   Note
   The transfer protocol must be Xmodem or 1K Xmodem.

Steps d. through h. illustrate how you would upload a file using the Hilgraeve HyperTerminal program.

d. From the HyperTerminal main window, select the **Transfer** menu. Then select **Receive File** from the pull-down menu, as shown in Figure 67.

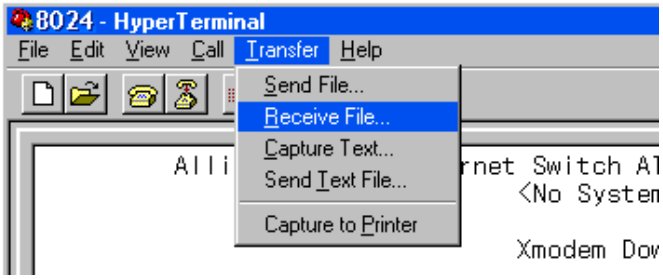

Figure 67 Local Management Window

The Receive File window is shown in Figure 68.

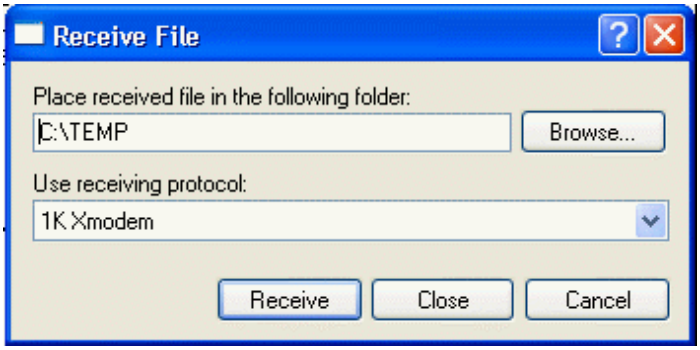

Figure 68 Receive File Window

e. Click the **Browse** button and specify the location on your computer where you want the system file stored.

f. Click on the **Use Receiving Protocol** field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.

g. Click **Receive**. The Receive Filename window is shown in Figure 69.

Figure 69 Receive Filename Window

The extension for an image file should be ".img" and the extension for a configuration file should be ".cfg."

The switch uploads the file from the switch to your computer.

Uploading Files from a Remote Management Session

This section contains the procedure for uploading a switch file from a remote management session. The remote switch can be a switch that you accessed through enhanced stacking or a switch where you started a Telnet management session.

> **Note**
> To upload a file through enhanced stacking or a Telnet management session, go to **Uploading Files from a Remote Management Session** on page 239.

Please note the following before you begin the procedure:

- ❑ You must use TFTP when uploading a file through enhanced stacking or a Telnet management session.
- ❑ The switch where you are uploading the file must have an IP address and subnet mask. Consequently, you cannot use TFTP on a slave switch of an enhanced stack unless the slave switch has an IP address.
- ❑ There must be a node on your network that contains the TFTP server software.
- ❑ You should start the TFTP server software before you begin the upload procedure.

To remotely upload a switch file, perform the following procedure:

1. From the Main Menu of the switch from where you want to upload the file, type **4** to select Administration Menu.
2. From the Administration Menu, type **D** to select Downloads & Uploads.

   The Downloads and Uploads menu is shown in Figure 63 on page 224.
3. To upload the AT-S39 image, type **3**. To upload the configuration file, type **4**.

   The following prompts are displayed:

   ```
   Only TFTP uploads are available for a remote access
   TFTP Server IP Address:
   ```
4. Enter the IP address of the TFTP server.

   The following prompt is displayed:

   ```
   Remote File Name:
   ```

5. Enter a filename for the image file or configuration file. This is the name by which the file will be stored on the TFTP server.

   Once the filename has been specified, the upload begins. File upload takes only a few moments.

   The upload is completed when the Download and Upload menu is displayed again.

Section III

Web Browser Management

The chapters in this section explain how to manage an AT-8024 or AT-8024GB Fast Ethernet switch using a web browser. The chapters include:

Chapter 21
Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-8000 Series switch 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.

There must be at least one Allied Telesyn enhanced stacking switch on your network that has an IP address. The switch with the IP address is referred to as the master switch. Once you have started a web browser management session on the master switch, you will have management access to all other enhanced stacking switches that reside in the same stack.

> **Note**
> For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

> **Note**
> If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. Enter the IP address of the master switch of the enhanced stack in the URL field of the browser, as shown in Figure 70.

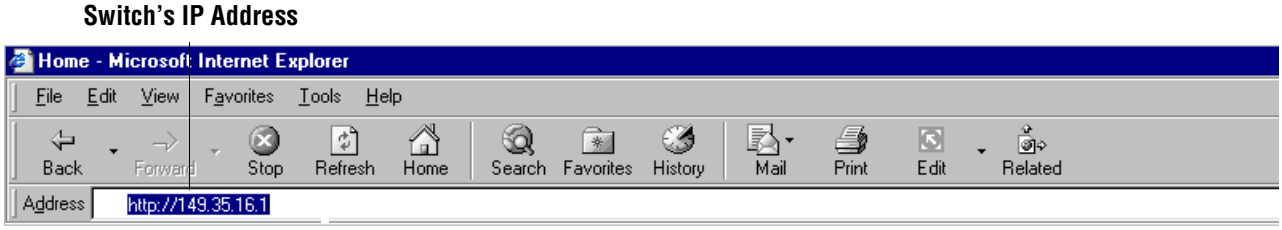

Figure 70 Entering a Switch's IP Address in the URL Field

3. When prompted, enter a user name and password. For manager access, enter "manager" as the user name. The default password is "friend". For operator access, enter "operator" as the user name. The default password is "operator". Logins and passwords are case-sensitive. (For information on the two access levels, refer to **Management Access Levels** on page 26.)

The user names cannot be changed. To change a password, refer to **Configuring an IP Address and Switch Name** on page 41.

The window shown in Figure 71 is displayed.

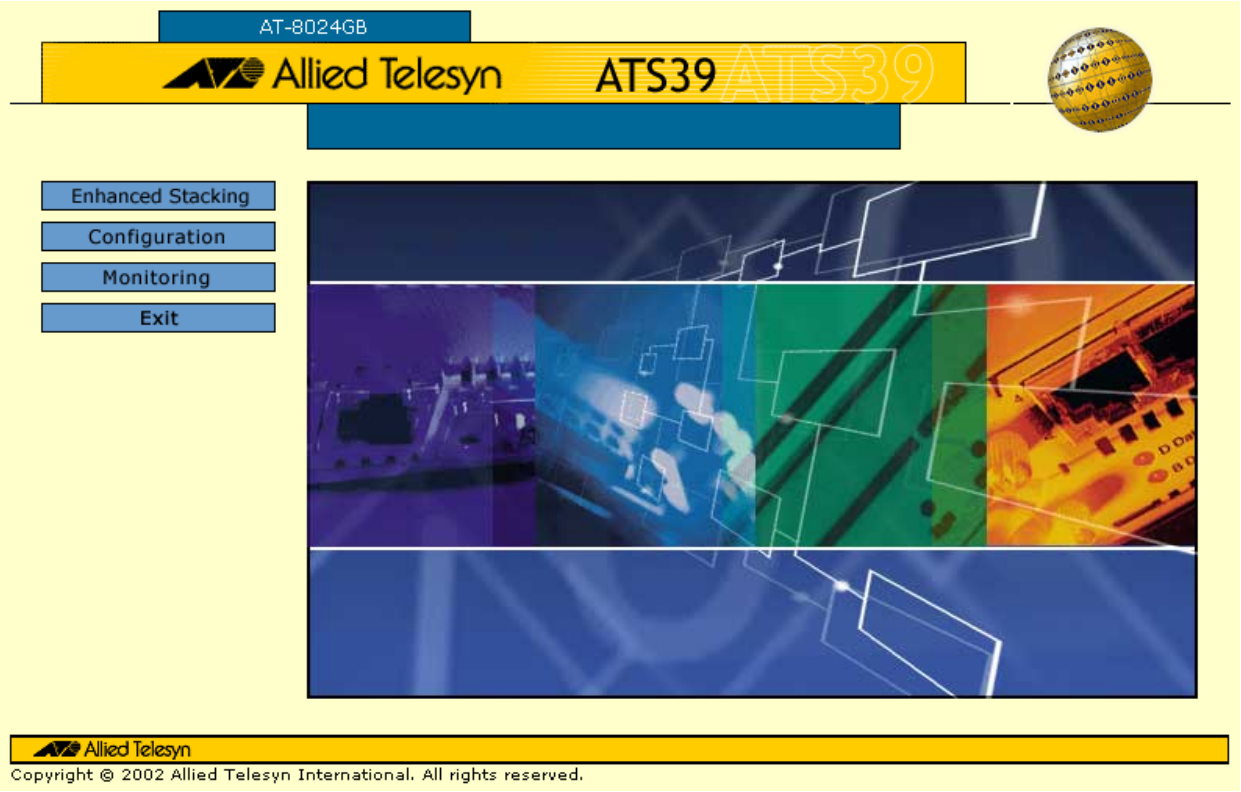

Figure 71 Home Page

This is the Home page of the management software. In the left portion of the Home page is the main menu:

- Enhanced Stacking (master switches only)
- Configuration
- Monitoring
- Exit (or Disconnect for slave switches)

Note
A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Browser Tools

You can use the browser tools to move around the AT-S39 menus. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature on frequently-used AT-S39 menus and windows.

Quitting a Web Browser Management Session

To exit from a web browser management session, select Exit from the main menu.

Chapter 22
Basic Switch Parameters

This chapter contains the following sections:

Configuring an IP Address and Switch Name

Note
For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8000 Series switch, refer to **When Does a Switch Need an IP Address?** on page 39.

To set the IP address, subnet mask, and other basic information for an AT-8000 Series switch, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

The General tab in Figure 72 is displayed.

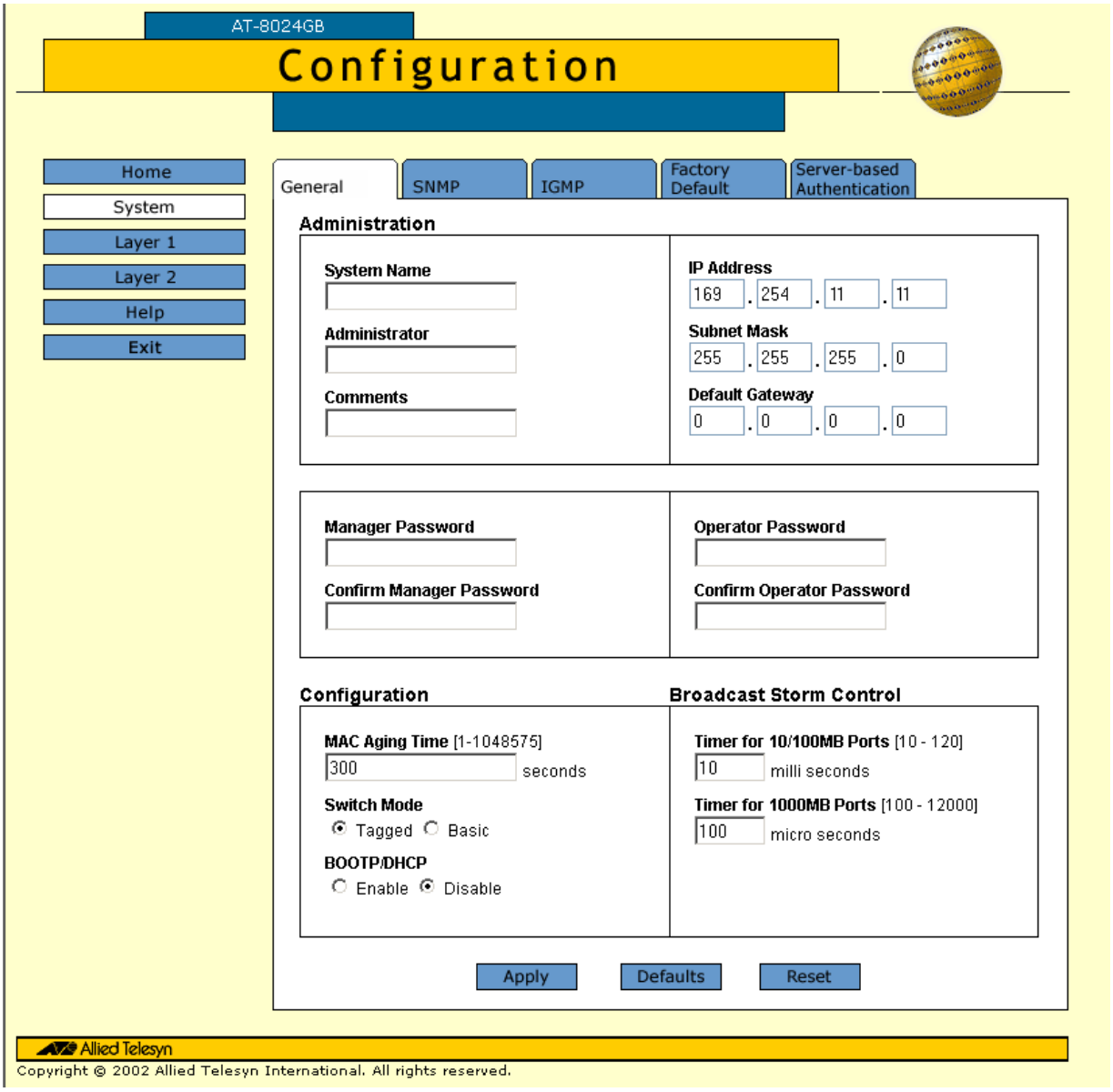

Figure 72 General Tab Menu - Configuration

This procedure describes the parameters in the Administration section of the menu. The parameters in the Configuration and Broadcast Storm Control sections are discussed later in this guide.

The Reset button at the bottom of the tab resets the switch. For instructions, refer to **Resetting a Switch** on page 256.

The Defaults button returns the parameter settings in the Configuration section and Broadcast Storm Control section in the tab to the default values.

3. Change the parameters as desired.

   The parameters are described below:

   System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). Entering a value for this parameter is optional. The name can be up to 30 alphanumeric characters. Spaces are allowed.

   Note
   You should assign each switch a name. The names can help you identify the various switches in your network. This can help you avoid performing a configuration procedure on the wrong switch.

   Administrator
   This parameter specifies the name of the network administrator responsible for managing the switch. Entering a value for this parameter is optional. The administrator's name can be up to 30 alphanumeric characters. Spaces are allowed.

   Comments
   This parameter specifies additional information about the Fast Ethernet switch, such as its location (e.g., Floor 4, Wiring closet 402B). Entering a value for this parameter is optional. Comments can be up to 30 alphanumeric characters. Spaces are allowed.

   Manager Password
   Manager Confirm Password
   These parameters are used to change the administrator's login password for the switch. To create a new password, enter the new password into both fields.

   The default password for Manager access is "friend". A password can be from 0 to 20 alphanumeric characters. Passwords are case-sensitive.

   Caution
   You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

   Operator Password
   Operator Confirm Password
   These parameters are used to change the operator's login password for the switch. To create a new password, enter the new password into both fields.

The default password for Operator access is “operator”. A password can be from 0 to 20 alphanumeric characters. Passwords are case-sensitive.

⚠ Caution
You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

IP address
This parameter specifies the IP address of the switch. You must assign an IP address if you want the switch to function as the Master switch of an enhanced stack. (Slave switches do not need and IP address.) You must also assign it an IP address if it will not be part of an enhanced stack and you want to be able to manage it remotely using Telnet or a web browser. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Subnet mask
This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The mask address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Gateway address
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. The gateway address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

4. After you have set the parameters, click **Apply**. Your changes are not stored by the switch until you click Apply.

Note
A change to any of the above parameters, including the IP address and subnet mask, is immediately activated on the switch.

A change to the IP address of the switch will result in the loss of the remote management session. You can restart the management session using the switch’s new IP address.

Activating the BOOTP and DHCP Client Software

For background information on BOOTP and DHCP, refer to the section **Activating the BOOTP and DHCP Client Software** on page 44.

Note
The default setting for the BOOTP and DHCP client software is disabled.

To activate or deactivate the BOOTP and DHCP client software on the switch from a web browser management session, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

   The General Tab menu is displayed, as shown in Figure 72 on page 248.

3. In the BOOTP/DHCP options in the General tab menu, click either **Enable** or **Disable**.

   Note
   If you activate the BOOTP and DHCP client software, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

   Any static IP address, subnet mask, and gateway address assigned to the switch are deleted from the System Configuration menu and replaced with the values the switch receives from the BOOTP or DHCP server. If you later disable BOOTP and DHCP, these values are returned to their default setting of 0.0.0.0.

Viewing System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **System**.
3. Select the **General** tab.

   The General tab window is shown in Figure 73s.

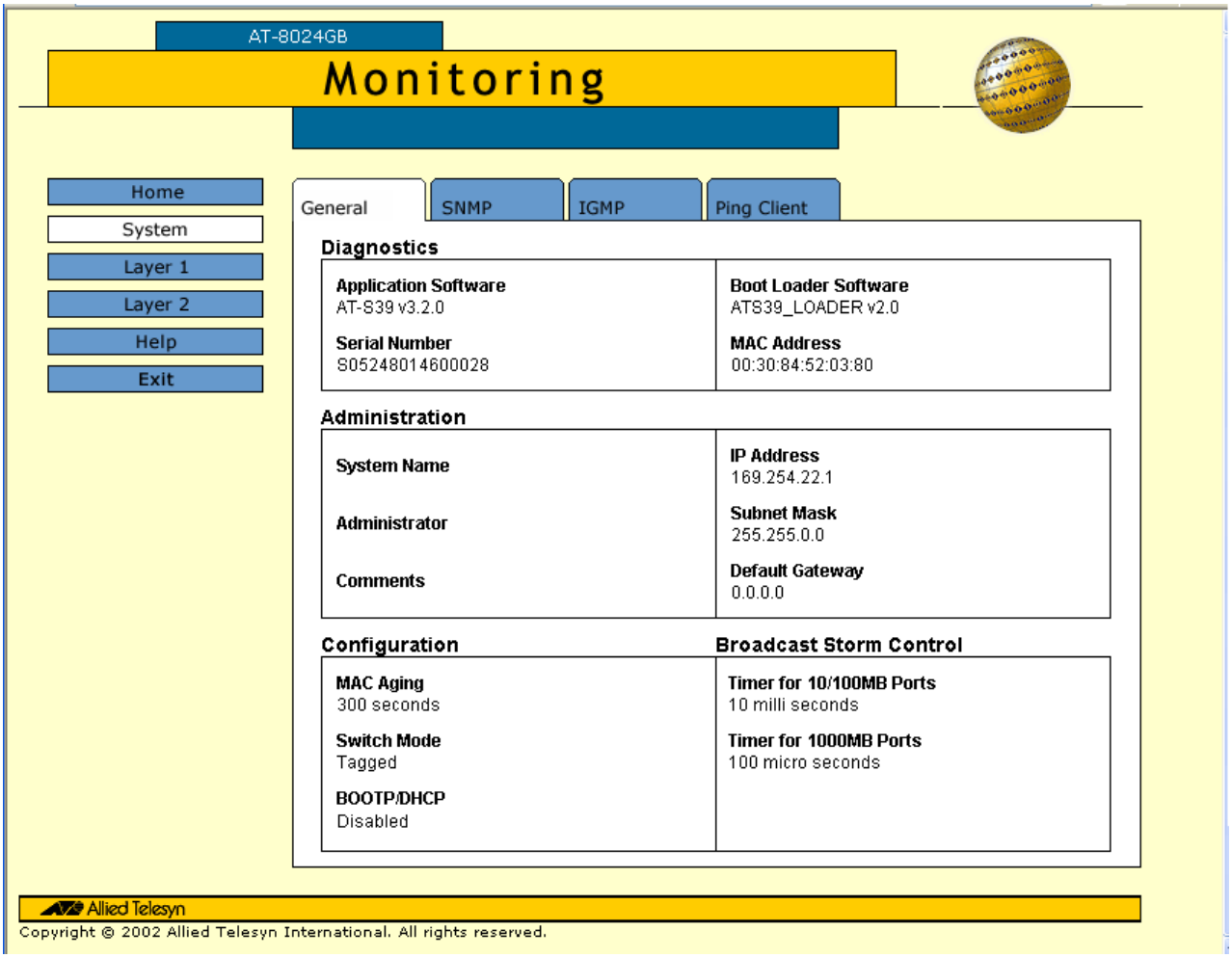

Figure 73 General Tab Window - Monitoring

This window is for viewing purposes only. You cannot change any of the values from this window. The sections in the window are defined below.

Diagnostics
This section displays the switch's serial number and the switch's MAC address. These values cannot be changed.

Administration
This section contains a variety of information, including the IP address of the switch and the system name. These parameters are defined in the procedure **Configuring an IP Address and Switch Name** on page 247, which also explains how to change the parameters.

Configuration
This section contains the following items:

- MAC Aging - Specifies how long an inactive dynamic MAC address can remain in the MAC address table before it is deleted. The default is 300 seconds (5 minutes). For background information about MAC addresses, refer to **MAC Address Overview** on page 162.

- Switch Mode - Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic Mode. For information about VLANs, refer to the overview sections in **Chapter 10, Virtual LANs Overview** on page 118.

- BOOTP/DHCP - Defines whether the switch obtains its IP address from a BOOTP or DHCP server on your network. If this parameter is enabled, the switch obtains its IP address from a BOOTP or DHCP server.

Broadcast Storm Control
For an explanation of these parameters, refer to **Broadcast Storm Control Overview** on page 188.

Configuring the SNMP Parameters and Trap IP Addresses

To change the switch's SNMP community strings or to specify the IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **System**.
3. Select the **SNMP** tab.

   The SNMP menu in Figure 74 is displayed.

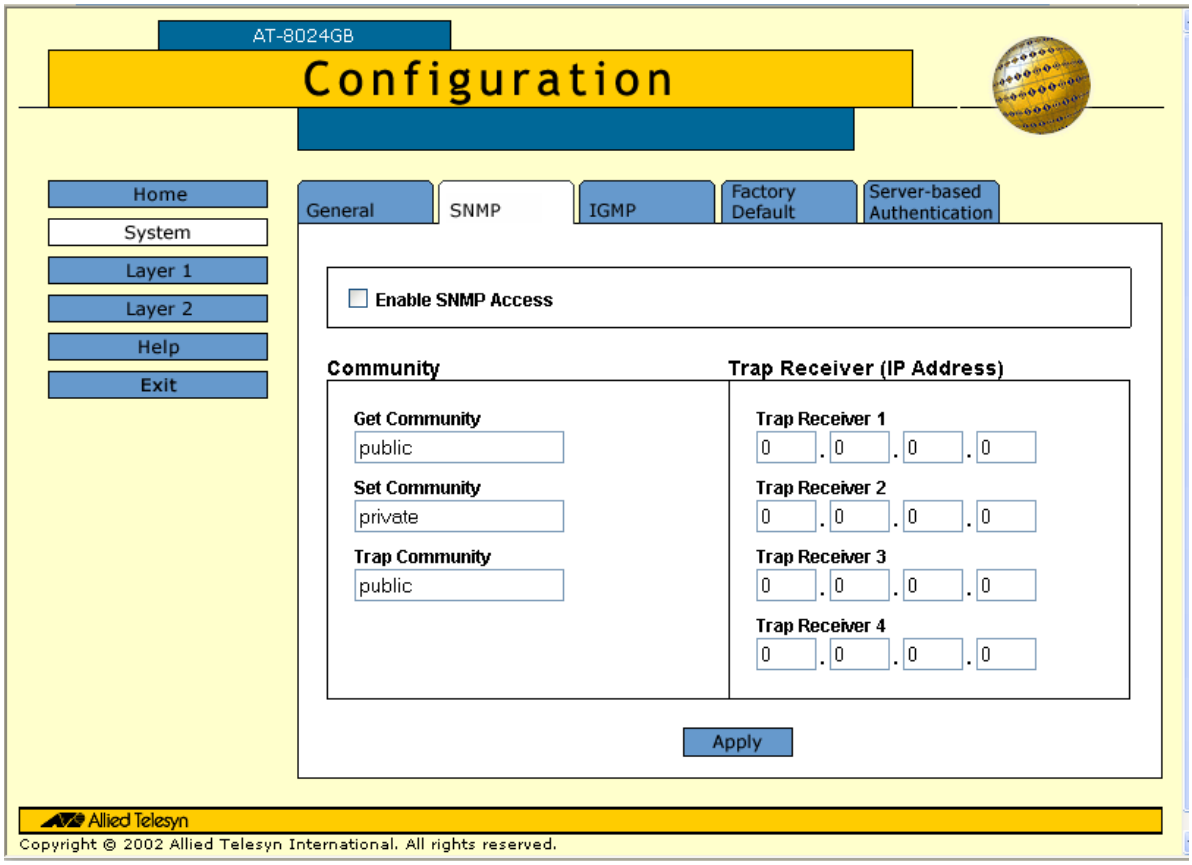

Figure 74 SNMP Tab

4. Adjust the parameters as desired. The parameters are described below.

GET Community
SET Community
Trap Community
Use these parameters to set a switch's SNMP community strings. A community string can be up to thirteen characters. Community strings are case sensitive and can contain spaces and special characters, such as an exclamation point (!).

Trap Receiver 1
Trap Receiver 2
Trap Receiver 3
Trap Receiver 4
Use these selections to specify the IP addresses of up to four management workstations on your network to receive traps from the switch.

5. To configure SNMP management access of the switch, click the Enable SNMP Access check box in the menu. If the check box is empty, the switch cannot be managed through SNMP. This is the default. When SNMP access is disabled, no one can manage the switch remotely using an SNMP management program.

6. Click **Apply** to save your changes to the switch.

   Changes are immediately activated on the switch.

Resetting a Switch

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

To reset a switch, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

3. Click the **Reset** button at the bottom of the menu.

   A confirmation prompt is displayed.

4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

   Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

> **Note**
> The switch must have an IP address in order for you to perform this procedure. This means that in most cases you must perform this procedure from the master switch of an enhanced switch.

To instruct the switch to ping a network device, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select the **System** menu option.
3. Select the **Ping Client** tab.

   The Ping Client Menu is shown in Figure 75.

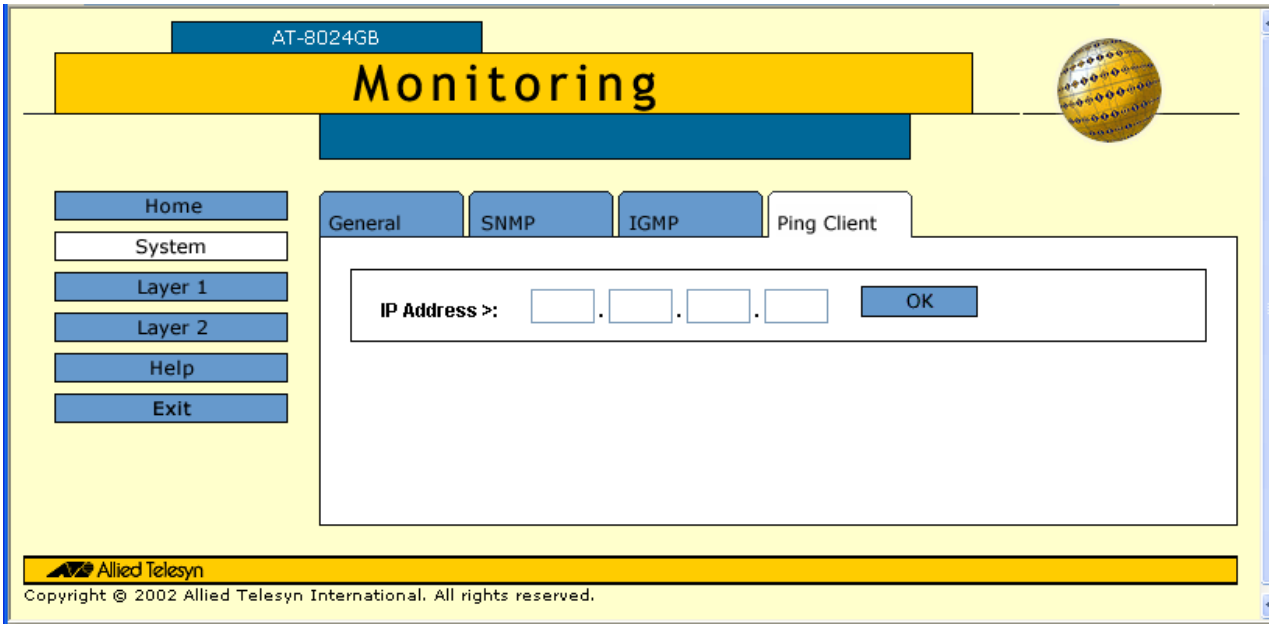

Figure 75 Ping Client Menu

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

   The results of the ping are displayed in a new window.
6. To stop the pinging, click **OK**.

Returning the AT-S39 Software to the Factory Default Values

The procedure in this section returns all AT-S39 software parameters, except the IP address, subnet mask, and gateway address, to their default values. This procedure also deletes any VLANs that you have created on the switch. The AT-S39 software default values can be found in **Appendix A, AT-S39 Default Settings** on page 331.

Caution
Performing this procedure resets the switch. The switch will not forward traffic during the brief period required to reload its operating software. Some network traffic may be lost.

To return the AT-S39 management software to its default settings, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Factory Default** tab. The Factory Default tab is shown in Figure 76.

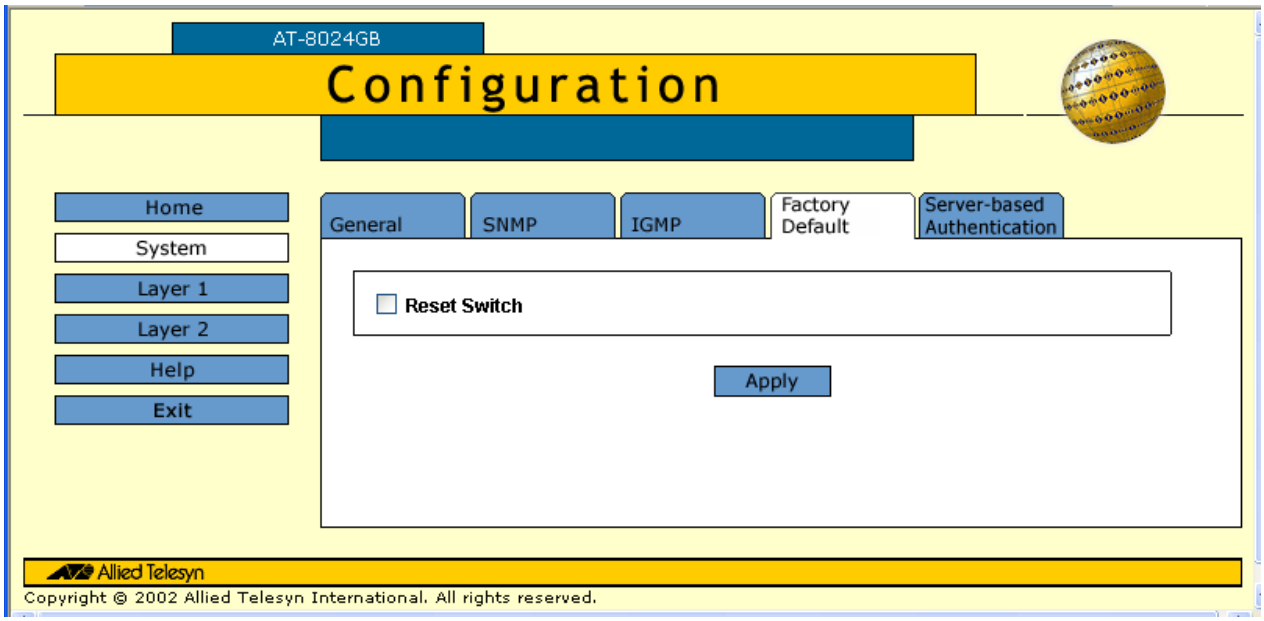

Figure 76 Factory Default Tab

4. Click the **Reset Switch** check box.
5. Click **Apply**.

   A confirmation prompt is displayed.

6. Click **OK**.

   The parameter settings are reset to their default values and the switch is reset.

7. To resume managing the switch, you must reestablish your management session.

Chapter 23
Enhanced Stacking

This chapter contains the following procedures:

Note
For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- Master - A master switch of a stack can be used to manage all other AT-8000 Series switches in a subnet. Once you have established a local or remote management session with the master switch, you can access and manage all the switches in the subnet.

  A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.

- Slave - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask. This is the default setting for a switch.

- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note
The only switch whose stacking status you can change through a web browser management session is the switch on which you started the management session, typically a master switch. You cannot change the stacking status of a switch accessed through enhanced stacking. To change the stacking status of a switch that does not have an IP address and subnet mask, you must use a local management session.

To adjust a switch's enhanced stacking status from a web browser management session, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. Select the **Enhanced Stacking** tab.

Note
If the window does not have an Enhanced Stacking tab, you are attempting to change the stacking status of a switch accessed through enhanced stacking. This is not allowed. The only stacking status you can change remotely from a web browser management session is the switch on which you started the session.

The Enhanced Stacking tab is shown in Figure 77.

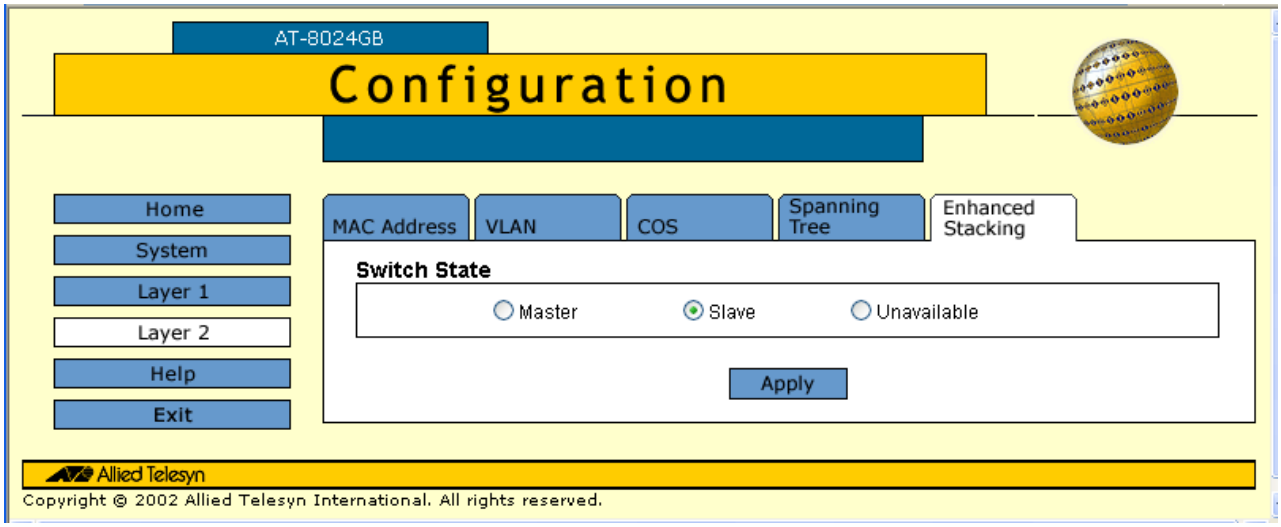

Figure 77 Enhanced Stacking Tab

4. Click the desired enhanced stacking status for the switch.
5. Click **Apply**.

   The new enhanced stacking status is immediately activated on the switch.

Selecting a Switch in an Enhanced Stack

The first thing to do before you perform any procedure on a switch in an enhanced stack is check to be sure you are performing it on the correct switch. This is easy if you assigned system names to your switches. The name of the switch being managed is displayed at the top of every management menu.

When you start a web browser management session on the master switch of a subnet, you are by default addressing that particular switch. The management tasks that you perform effect only the master switch.

To manage a slave switch or another master switch in the same enhanced stack, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the Home page of the master switch, select **Enhanced Stacking**.

   Note
   If the Home page does not have an Enhanced Stacking menu selection, you are not addressing the master switch of the stack. Either you accessed the switch through enhanced stacking or the switch's enhanced stacking status is slave or unavailable.

   The master switch polls the network for all slave and master switches in the enhanced stack and displays a list of the switches in the Stacking Switches menu, shown in Figure 78.

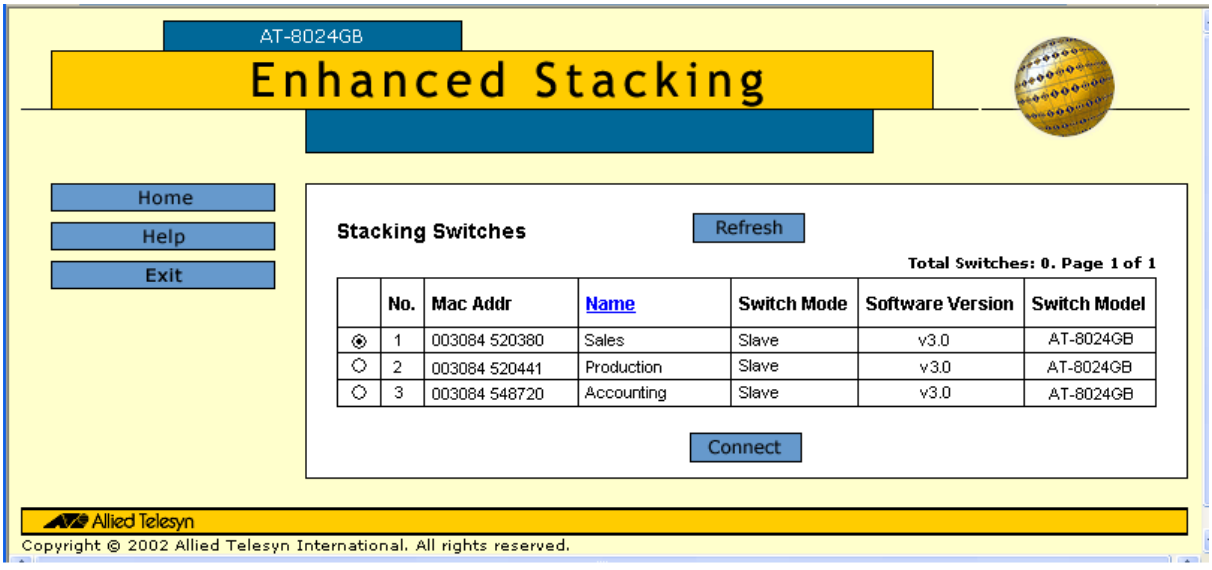

Figure 78 Stacking Switches Menu

Note
The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

You can refresh the list by clicking **Refresh**. This instructs the master switch to again poll the subnet for all AT-8000 Series switches.

2. To manage another switch in an enhanced stack, click the dialog circle to the left of the appropriate switch in the list.
3. Click **Connect**.

   The Home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you have finished managing a slave switch and want to manage another switch in the subnet, select **Disconnect** from the menu. This returns you to the Stacking Switches window in Figure 78 on page 263. Once you see that window, you are again addressing the master switch from which you started the management session.

You can either select another switch in the list to manage or, if you want to manage the master switch, return to the master switch's Home page by selecting **Home**.

To end a management session, select **Exit** from the master switch's menu.

Chapter 24
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

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

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Setting** tab.

   The Port Setting tab is shown in Figure 79.

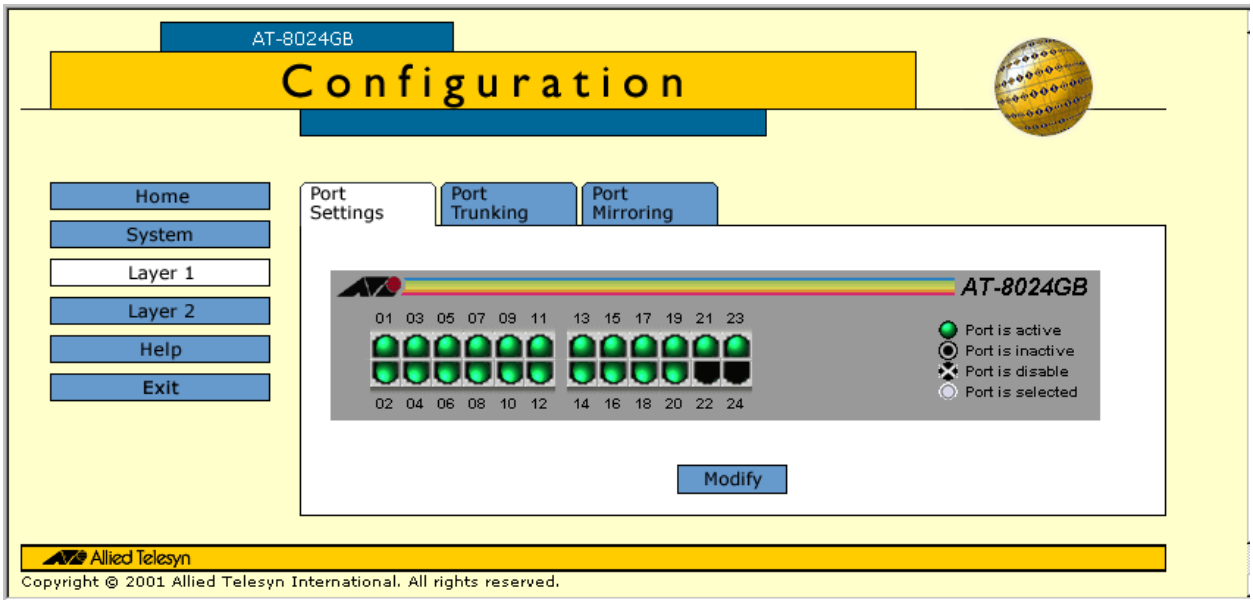

Figure 79 Port Setting Configuration Tab

4. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)
5. Click **Modify**.

The Settings for Port menu is displayed. An example of the menu is shown in Figure 80.

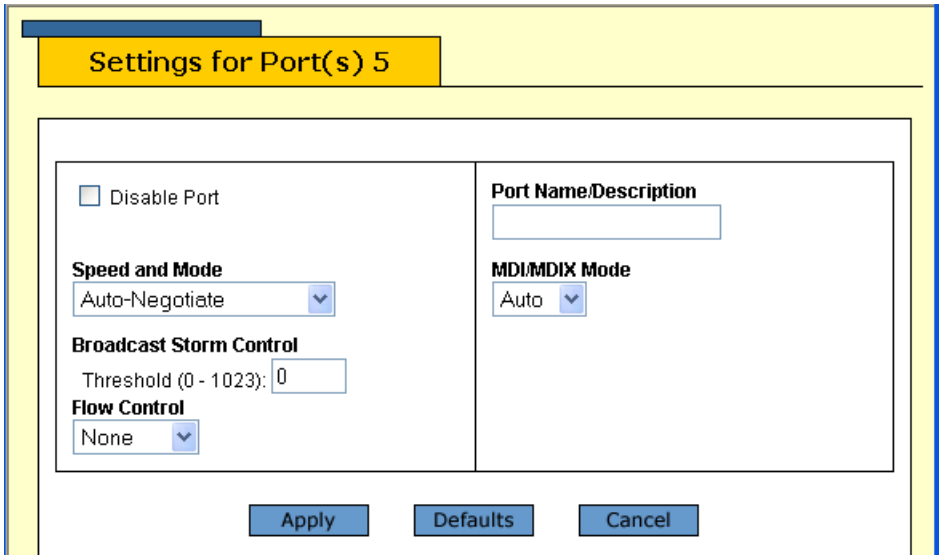

Figure 80 Settings for Port Menu

Note
The **Default** button returns the port settings to the default values. Default values are listed in **Appendix A, AT-S39 Default Settings** on page 331.

If you are configuring multiple ports and the ports have different settings, the Settings for Port menu displays the settings of the lowest numbered port. Once you have configured the settings of the port, all of its settings are copied to the other selected ports.

6. Adjust the port parameters as desired.

   The parameters are described below.

   Disable Port
   You use this selection to enable or disable a port. When disabled, a port will not forward frames. The default for this port parameter is enabled.

   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 again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

   A check in the box indicates the port is disabled. No check indicates the port is enabled.

Speed and Mode
The operating speed and duplex mode of the port. Possible settings for this parameter are:

- ❑ Auto-Negotiate: The port will Auto-Negotiate both speed and duplex mode. This is the default.
- ❑ 10Mbps - Half Duplex
- ❑ 10Mbps - Full Duplex
- ❑ 100Mbps - Half Duplex
- ❑ 100Mbps - Full Duplex

If you select Auto-Negotiation, which is the default setting, the switch will set both speed and duplex mode for the port automatically. The switch determines the highest possible common speed between the port and its end node and sets the port to that speed. This helps to ensure that the port and the end node are operating at the highest possible common speed.

You should note the following concerning the operation of Auto-Negotiation on a switch port:

- ❑ In order for a switch port to successfully Auto-Negotiate its duplex mode with an end node, the end node should also be using Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation will default to half-duplex if it detects that the end node is not using Auto-Negotiation. This will result in a duplex mismatch if the end node is operating at a fixed duplex mode of full-duplex.

  To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

- ❑ When Auto-Negotiation is disabled on a port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. Consequently, if you disable Auto-Negotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Broadcast Storm Control
The maximum number of broadcast packets the port can receive within a specified period of time. If the threshold is reach, any additional broadcast packets received on the port are discarded by the switch. For background information on this feature, refer to

Broadcast Storm Control Overview on page 188. For instructions on how to set this value, refer to **Setting the Maximum Number of Broadcast Frames** on page 325.

Flow Control
Flow control applies only to ports operating in full-duplex mode. 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 settings are:

None - No flow control on the port.

Transmit - Flow control only as packets are being transmitted out the port.

Receive - Flow control only on as packets are being received on the port.

Both - Flow control for both packets entering and leaving the port.

Port Name/Description
This selection assigns a name to a port. The name can be from one to fifteen alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points.

MDI/MDIX
This selection sets the wiring configuration of the port. The configuration can be Auto, MDI, or MDI-X.

The twisted pair ports on the switch feature auto-MDI/MDI-X. They configured themselves automatically as MDI or MDI-X when connected to an end node. This allows you to use either a straight-through twisted pair cable when connecting any type of network device to a port on the switch.

If you disable Auto-Negotiation on a port and set a port's speed and duplex mode manually, the auto-MDI/MDI-X feature is also disabled. A port where Auto-Negotiation has been disabled defaults to MDI-X. Disabling Auto-Negotiation may require that you manually configure a port's MDI/MDI-X setting using this option or use a crossover cable.

Back Pressure
This menu option only appears for ports configured for half-duplex mode.

Backpressure performs much the same function as flow control. Both are used by a port to control the flow of ingress packets.

Where they differ is that while flow control applies to ports operating in full-duplex, backpressure applies to ports operating in half-duplex mode.

When a twisted pair port on the switch operating in half-duplex mode needs to stop an end node from transmitting data, it forces a collision. A collision on an Ethernet network occurs when two end nodes attempt to transmit data using the same data link at the same time. A collision causes the end nodes to stop sending data. This is called backpressure.

When a switch port needs to stop a half-duplex end node from transmitting data, it forces a collision on the data link, which stops the end node. Once the port is ready to receive data again, it stops forcing collisions.

The default setting for backpressure on a switch port is disabled.

7. Once you have made the desired changes, click **Apply**.

   The switch immediately activates the parameter changes on the port.

Displaying Port Status and Statistics

The procedure in this section displays the operating status of the ports on a switch and port statistics. You can view a port's operating speed, duplex mode, MDI/MDI-X configuration, and more. You can also view the operating status of any GBIC modules installed in an AT-8024GB.

To display the status or statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 1**.
3. Select the **Port Settings** tab. The tab is shown in Figure 81.

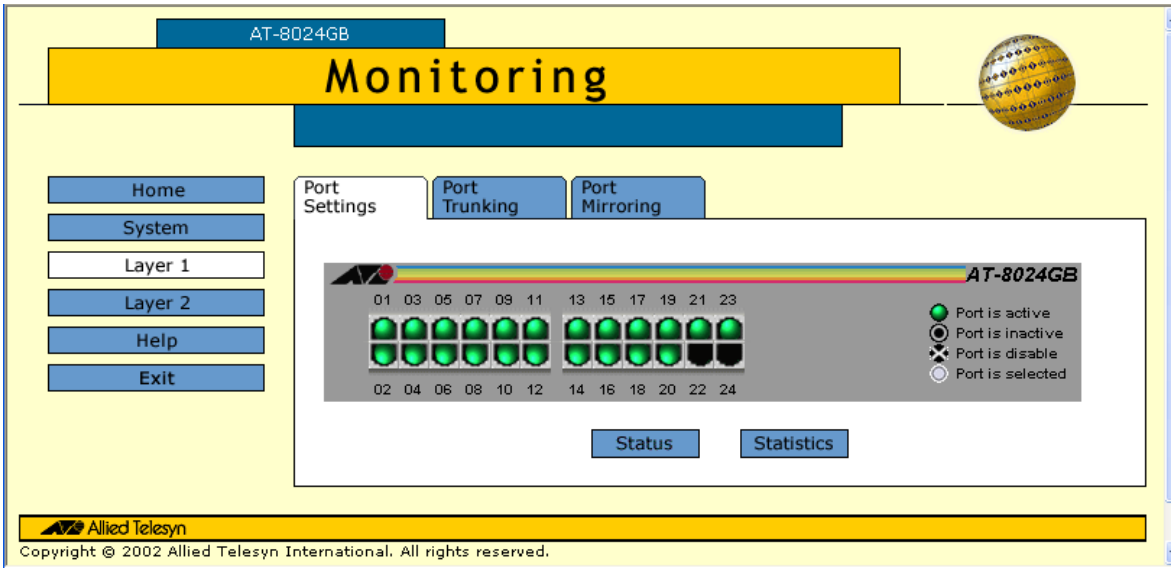

Figure 81 Port Monitoring Page

This page displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

4. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
5. Click **Status** to display the port's operating status or **Statistics** to display port statistics.

If you select port status, the Port Status window in Figure 82 is displayed.

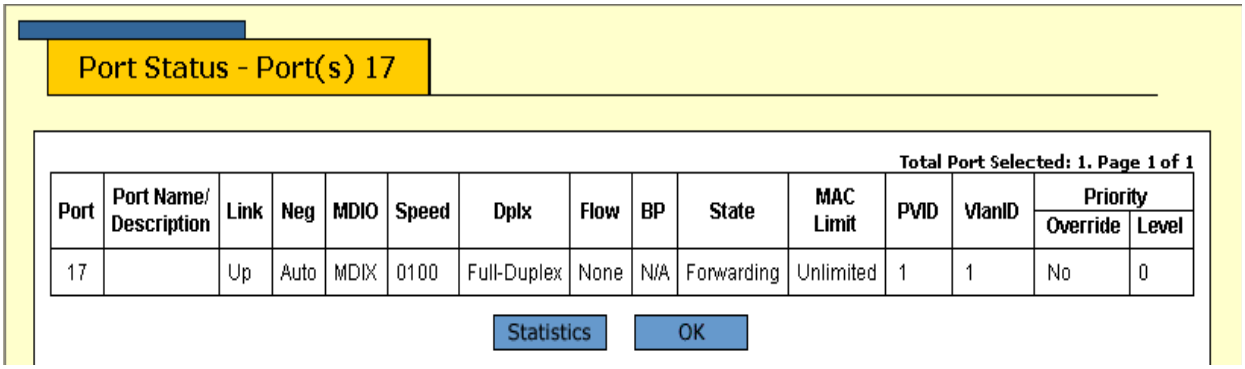

Figure 82 Port Status Window

The information in this window is for viewing purposes only. To adjust port parameters, refer to **Configuring Port Parameters** on page 266.

The columns in the window are described below:

Port
The port number.

Port Name/Description
Port's name or description.

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.

Neg
The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode are set manually.

MDIO
The operating configuration of the port. Possible values are Auto, MDI and MDI-X.

Speed
The operating speed of the port. Possible values are:

0010 - 10 Mbps

0100 - 100 Mbps

1000 - 1000 Mbps

Dplx
The duplex mode of the port. Possible values are half-duplex and full-duplex.

Flow
The port's flow control setting. Possible values are:

None - No flow control on the port.

Transmit - Flow control only on packets being transmitted out the port.

Receive - Flow control only on packets being received on the port.

Both - Flow control for both packets entering and leaving the port.

BP

The port's back pressure setting.

State
The operating status of the port. Possible values are Forwarding and Disabled.

MAC Limit
The maximum number of MAC addresses the port can learn when operating in the Limited security mode. This value is only operational when the port is operating in the Limited security mode.

PVID
The port VLAN identifier assigned to the port.

VlanID
The VID of the VLAN in which the port is an untagged member.

Priority Override
The status of the override priority feature. If the status is Yes, tagged and untagged packets entering the port are directed to either the low or high priority queue as specified in CoS. If the status is No, tagged frames entering the port are directed to the low or high queue according to the priority levels specified in the tagged packets. For further information on this feature, refer to **Class of Service Overview on page 175**.

Priority Level
The priority queue to which untagged packets are directed when received on the port. A value of 1 to 3 directs untagged packets to the low priority queue while a value of 4 to 7 directs packets to the high priority queue. If the override priority feature has been activated on the port, tagged packets will be directed to the priority queue reflected by this status parameter. For further information on this feature, refer to **Class of Service Overview** on page 175.

If you select Statistics, the Statistics window in Figure 83 is displayed.

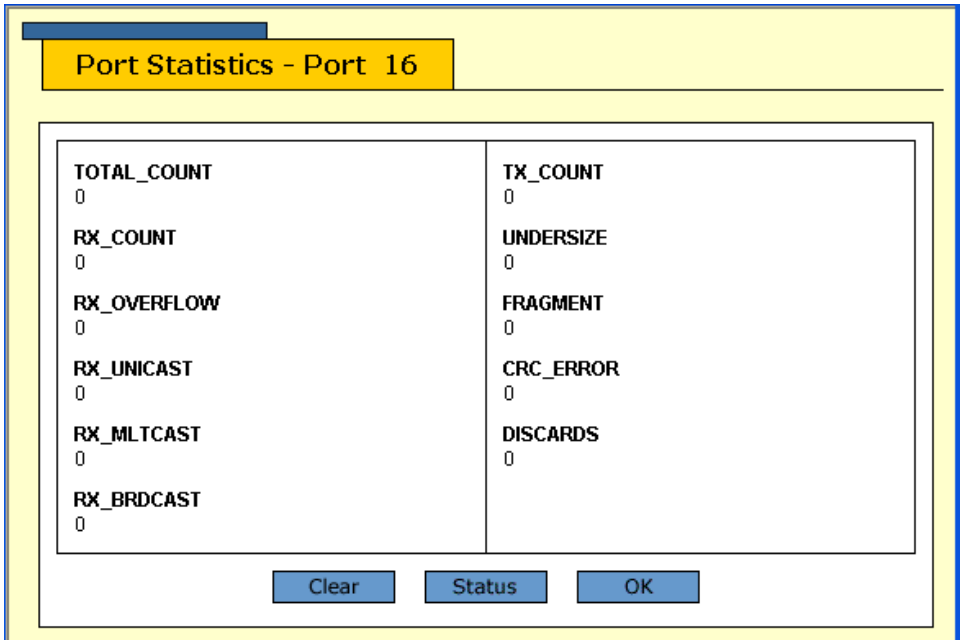

Figure 83 Port Statistics Window

The information in this window is for viewing purposes only. The statistics are defined below:

TOTAL_COUNT
Total number of packets transmitted and received on the port.

RX_COUNT
Number of packets received on the port.

RX_OVERFLOW
Number of times frames entering the port have exceeded the capacity of the port's buffer.

RX_UNICAST
Number of unicast received on the port.

Rx_MLTCAST
Number of multicast packets received on the port.

RX_BRDCAST
Number of broadcast packets received on the port.

TX_COUNT
Number of packets transmitted by the port.

UNDERSIZE
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

FRAGMENT
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

CRC_ERROR
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port

DISCARDS
Number of frames successfully received and buffered by the port, but discarded and not forwarded.

Chapter 25
Port Security

This chapter explains how to display the current port security level on the switch from a web browser management session.

Note
For background information on port security, refer to **Port Security Overview** on page 77.

Note
You must use a local management session to change a switch's port security level. You cannot set port security from a Telnet or web browser management session, or through enhanced stacking.

Displaying the Port Security Level

To display the switch's port security level, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Port Security** tab.

   The current security level is displayed.

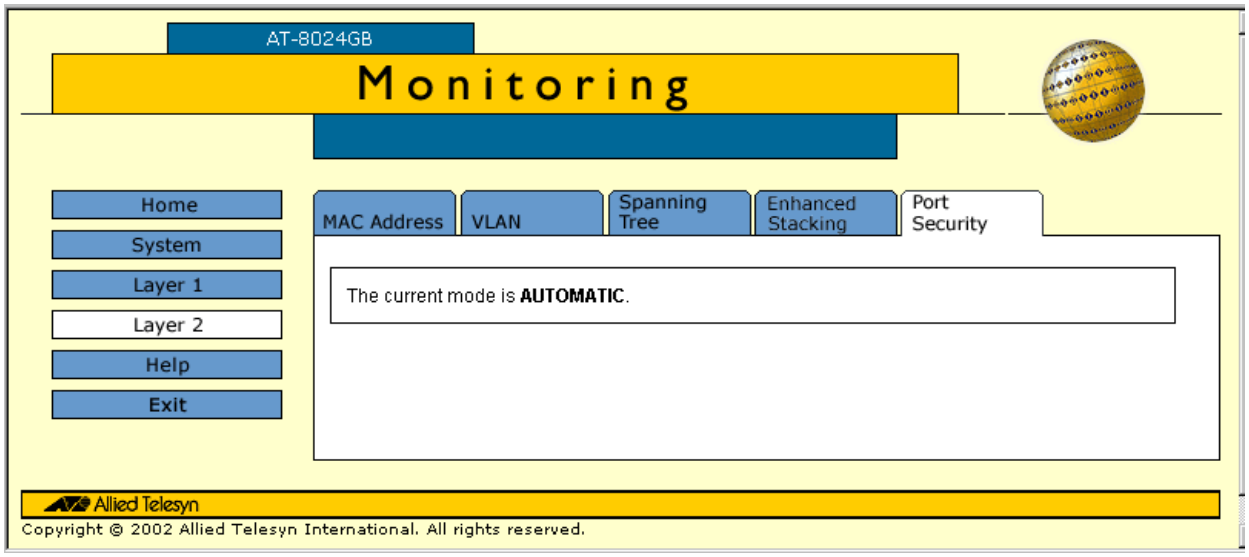

Figure 84 Port Security Menu

Chapter 26
Port Trunks

This chapter contains the procedure for creating or deleting a port trunk from a web browser management session.

Note
For background information and guidelines on port trunking, refer to **Port Trunking Overview** on page 83.

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 port trunk on both the switch and end node. Connecting the cables prior to configuring the port trunk will create a loop 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 result in broadcast storms.

To create or delete a port trunk, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Trunking** tab.

   The management software displays the Port Trunking menu in Figure 85.

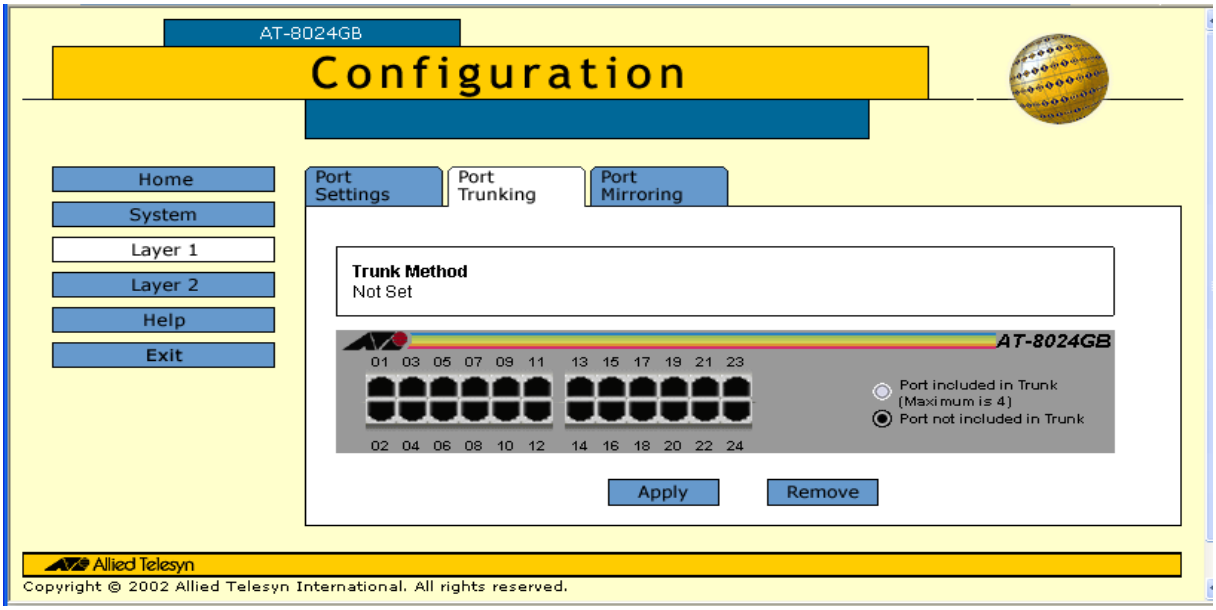

Figure 85 Port Trunking Menu

If the switch does not contain a port trunk, all ports in the switch image will be black. If there is a port trunk, the ports of the trunk will be white.

To create a port trunk, go to step 4. To delete a port trunk, go to step 5.

4. To create a port trunk, do the following:

   a. Click the ports that will make up the port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain 2, 3, or 4 ports.

      Once you have selected the ports of the trunk, the following appears under Trunk Method.

      

   b. Click the desired load distribution method. The default is SA/DA.

   c. Click **Apply**.

   d. Configure the ports on the remote switch for port trunking.

   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.

5. To delete a port trunk, click **Remove**. The port trunk is immediately deleted from the switch.

Chapter 27
Port Mirroring

This chapter contains the following procedure:

- ❑ **Creating or Deleting a Port Mirror** on page 282

Note
For background information on port mirroring, refer to **Port Mirroring Overview** on page 93.

Creating or Deleting a Port Mirror

To create or delete a port mirror, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Mirroring** tab.

   The management software displays the Port Mirroring menu in Figure 86.

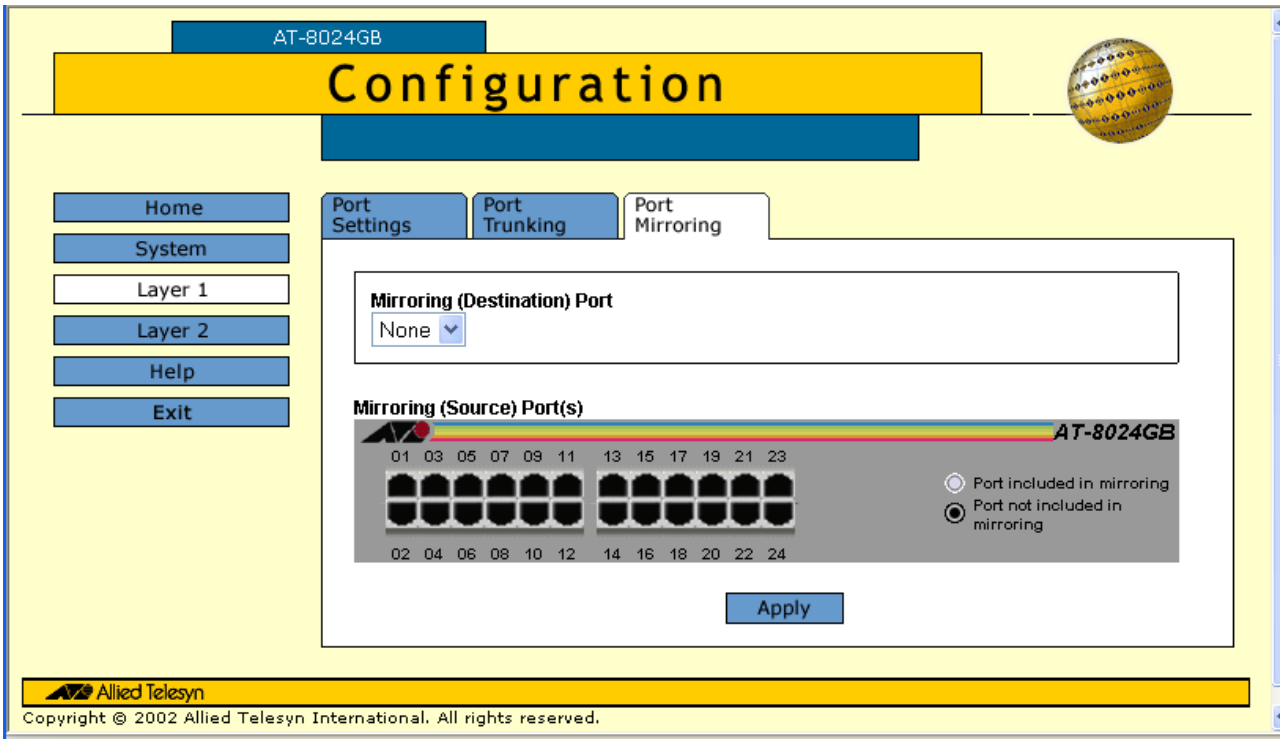

Figure 86 Port Mirroring Menu

To create a port mirror, go to step 4. To delete a port mirror, go to step 5.

4. To create a port mirror, do the following:

   a. Use the pull-down menu from Mirroring Port to select the port to function as the port mirror. This is the port will the traffic from the source ports will be copied to. You can select only one mirroring port.

   b. Click the port(s) in the graphical switch image whose traffic is to be copied to the mirror port. These are the source ports.

   c. Click **Apply**.

The port mirror is immediately activated on the switch. You can now connect a data analyzer to the mirror port to monitor the traffic on the selected ports.

5. To disable port mirroring, select "None" from the Mirroring Port pull-down menu and click **Apply**.

   The port mirror is deleted. The port that was functioning as the mirror port can now be used for normal network operations.

Chapter 28
STP and RSTP

This chapter explains how to configure the STP and RSTP parameters on an AT-8000 Series switch from a web browser management session.

Sections in the chapter include:

Note
For background information on spanning tree, refer to **STP and RSTP Overview** on page 97.

Enabling or Disabling STP or RSTP

The AT-S39 software supports STP and RSTP. Only one spanning tree protocol can be active on the switch at a time. Before you can enable a spanning tree protocol or configure its settings, you must first select it as the active spanning tree protocol on the switch. The default active spanning tree is RSTP.

Note
Changing the active spanning tree protocol resets the switch.

To select and enable a spanning tree protocol, or to disable spanning tree, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 87.

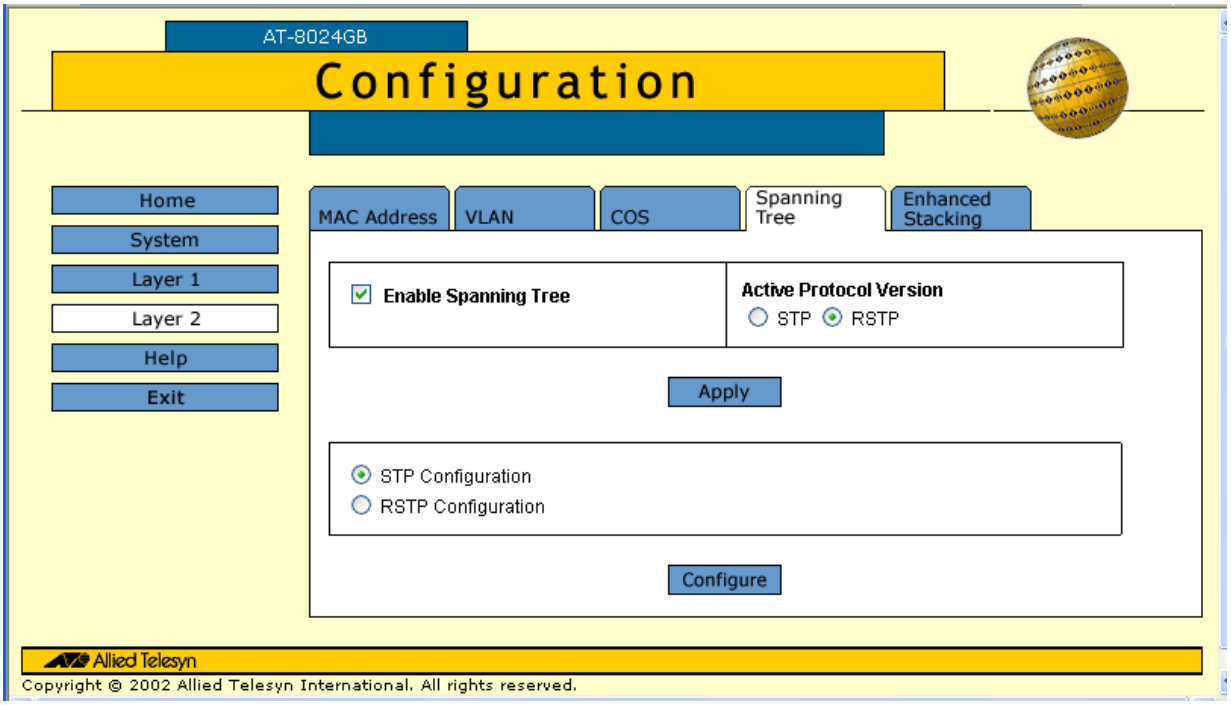

Figure 87 Spanning Tree Tab

Note
To select a new active spanning tree protocol, perform step 4. To enable or disable spanning tree on the switch, perform step 5.

4. To select an active spanning tree protocol, do the following:
   a. Click **STP** or **RSTP** in the Active Protocol Version section of the menu. The default is RSTP. Only one spanning tree protocol can be active on the switch at a time.

      The switch resets and changes the active spanning tree protocol.

   b. To continue managing the switch, you must reestablish your management session. To configure STP settings, go to **Configuring STP** on page 287. To configure RSTP settings, go to **Configuring RSTP** on page 291.
5. To enable or disable the spanning tree protocol, do the following:
   a. Click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.
   b. Click **Apply**.

Configuring STP

This section contains the following procedures:

Configuring STP Bridge Settings

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

> **Caution**
> The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Spanning Tree tab menu, click **STP Configuration** and click **Configure**.

   The Spanning Tree menu is shown in Figure 88.

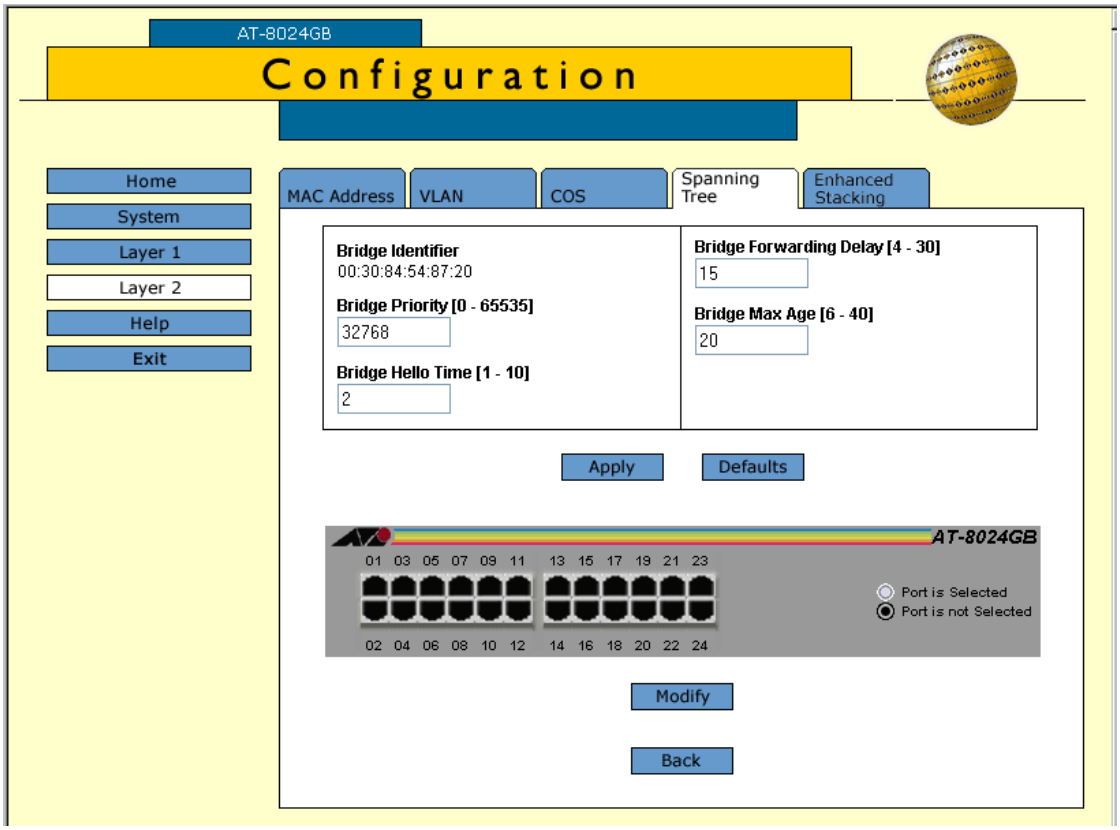

Figure 88 STP Bridge Configuration Menu

2. Adjust the bridge STP settings as needed. The parameters are described below.

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

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 lowest 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 Forwarding 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, possibly resulting in a network loop. The default is 15 seconds.

Bridge Max 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.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1)).

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

3. After you have made the desired changes, click **Apply**.

Configuring STP Port Settings

To configure STP port settings, do the following:

1. From the Spanning Tree tab menu, click **STP Configuration** and click **Configure**.
2. To adjust a port's RSTP settings, click on a port in the switch image and click **Modify**. You can select more than one port at a time.

   The Port Spanning Tree Protocol menu is shown in Figure 89.

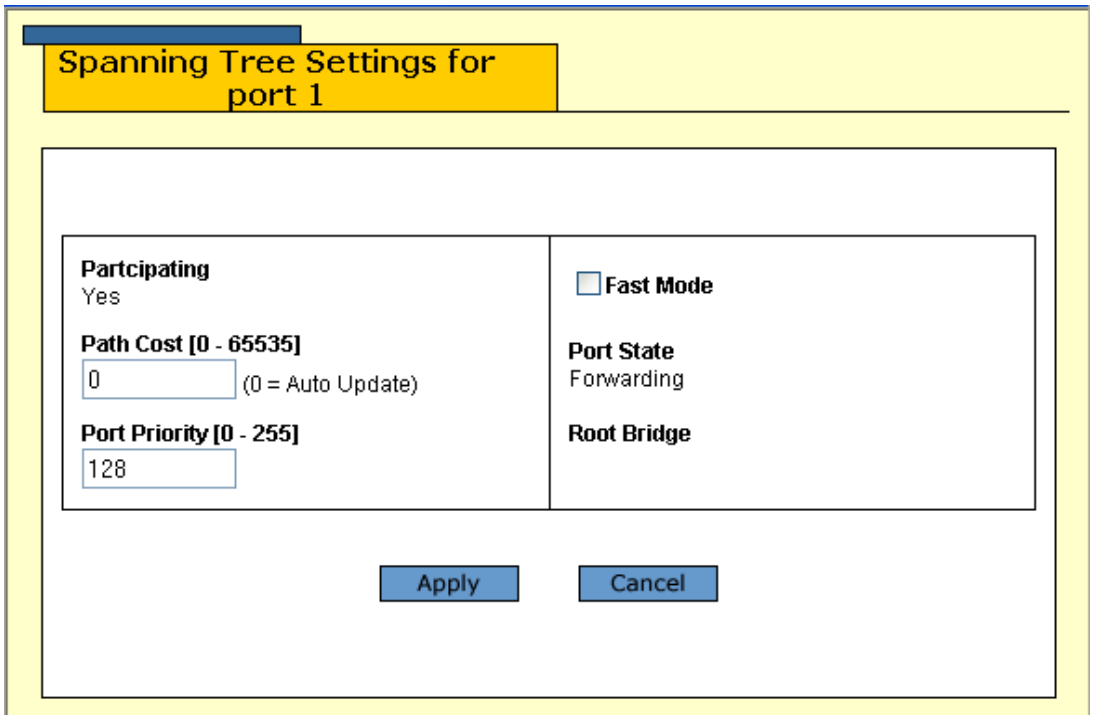

Figure 89 STP Port Configuration Menu

3. Adjust the settings as desired. The parameters are described below.

   Participating
   This parameter indicates whether the port is participating in the spanning tree domain. You cannot change this value from a web browser management session. It can be changed from a local or Telnet management session, as explained in **Configuring STP Port Settings** on page 109.

Path Cost
Though it says path cost, this is actually the port cost of the port. The spanning tree algorithm uses port cost 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.

Port 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 default value for priority is 128. The range is 0-255.

Fast Mode
When you check this check box, the port will skip the Listening and Learning stages of STP. This setting is appropriate for ports connected to edge nodes that are not running STP.

Port State
This field indicates the STP state of the port, which can be listening, learning, forwarding, or blocked. This value is for display purposes only and cannot be changed.

Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed. If STP has not been enabled, this parameter will not show a value.

4. Once you have configured the parameters, click **Apply**.

   All changes are immediately activated on the switch.

Configuring RSTP

This section contains the following procedures:

- ❑ **Configuring RSTP Bridge Settings** on page 291
- ❑ **Configuring RSTP Port Settings** on page 293

Configuring RSTP Bridge Settings

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

Caution
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Spanning Tree tab menu, click **RSTP Configuration** and click **Configure**.

   The RSTP Bridge Configuration menu in Figure 90 is displayed.

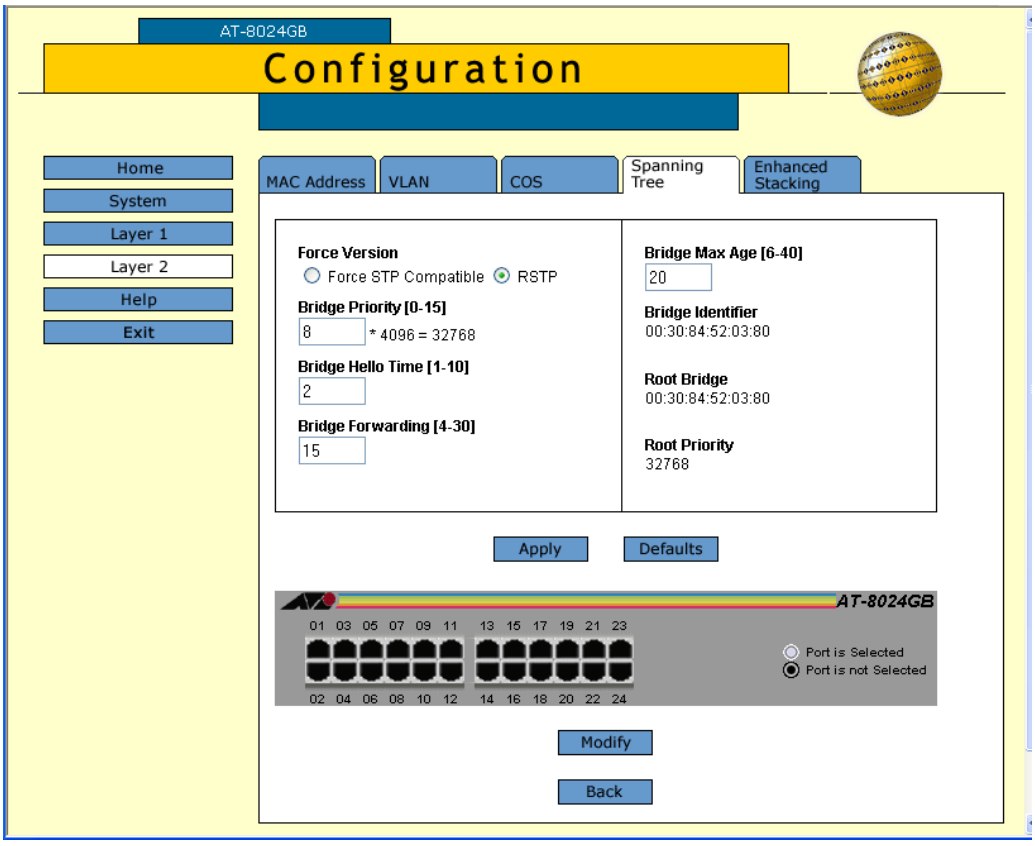

Figure 90 RSTP Bridge Configuration Menu

2. Adjust the parameters are needed. The parameters are defined below.

Force Version
This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. If you select RSPT, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge will operate all ports in STP. The default is RSTP.

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 lowest priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to **Table 4**, **RSTP Bridge Priority Value Increments** on page 98

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 Forwarding
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, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max 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.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1)).

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed. This value only appears when RSTP has been enabled on the switch.

Root Priority
The priority number of the root bridge. This value only appears when RSTP has been enabled on the switch.

3. After you have made your changes, click **Apply**.

Configuring RSTP Port Settings

To configure RSTP port settings, do the following:

1. From the Spanning Tree tab menu, click **RSTP Configuration** and click **Configure**.

   The RSTP Bridge Configuration menu is shown in Figure 90 on page 291.

2. To adjust a port's RSTP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The Port Rapid Spanning Tree Protocol menu is shown in Figure 91.

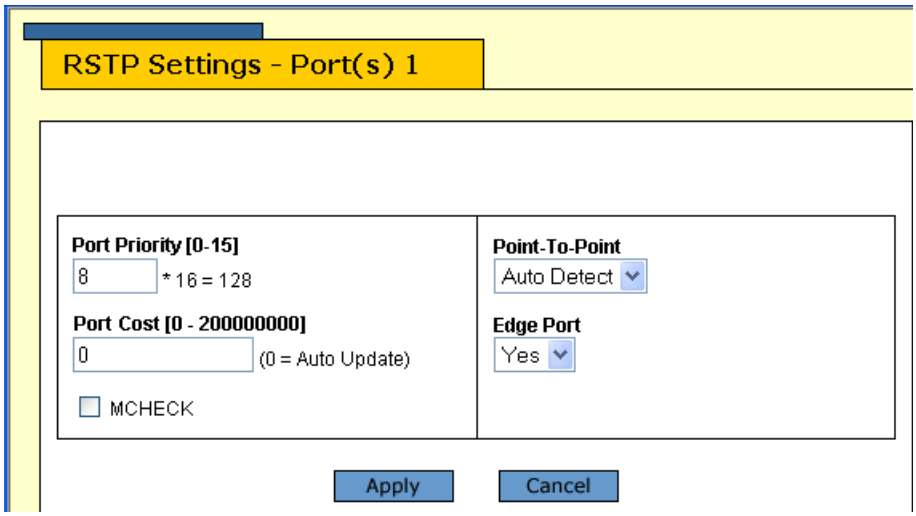

Figure 91 RSTP Port Configuration Menu

3. Adjust the settings as desired. The parameters are described below.

   Port 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 to 240 in increments of 16. The default value is 8 (priority value of 128). For a list of the increments, refer to **Table 7**, **RSTP Port Priority Value Increments** on page 100.

   Path Cost
   Though it says path cost, this is actually the port cost of the port. The spanning tree algorithm uses port cost to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20 000 000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port.

   MCHECK
   This option instructs the bridge to send out RSTP BPDU packets for several seconds from the selected port. The purpose is to determine if there are any RSTP or STP bridges connected to the port. If the port receives STP BPDU packets in response, the port changes to STP compatible mode.

   Note
   The MCHECK option is displayed in the window only when RSTP is enabled on the switch.

   Point-to-Point
   This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

   Edge Port
   This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

4. Once you have configured the parameters, click **Apply**.

   All changes are immediately activated on the switch.

Displaying STP or RSTP Settings

To display STP or RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

   The Spanning Tree menu in Figure 93 is displayed. This menu displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.

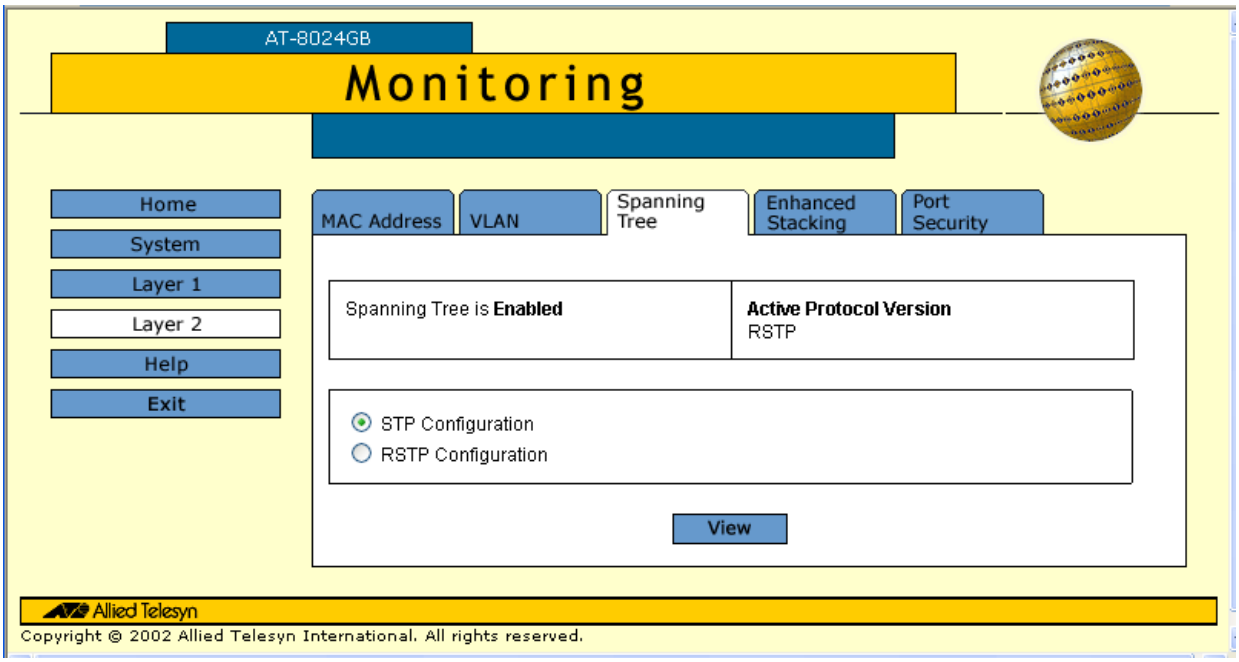

Figure 92 Spanning Tree Tab - Monitoring

4. To view STP or RSTP parameter settings, click either **STP Configuration** or **RSTP Configuration** and click **View**.

The example in Figure 93 is for RSTP. The information in this window is for viewing purposes only.

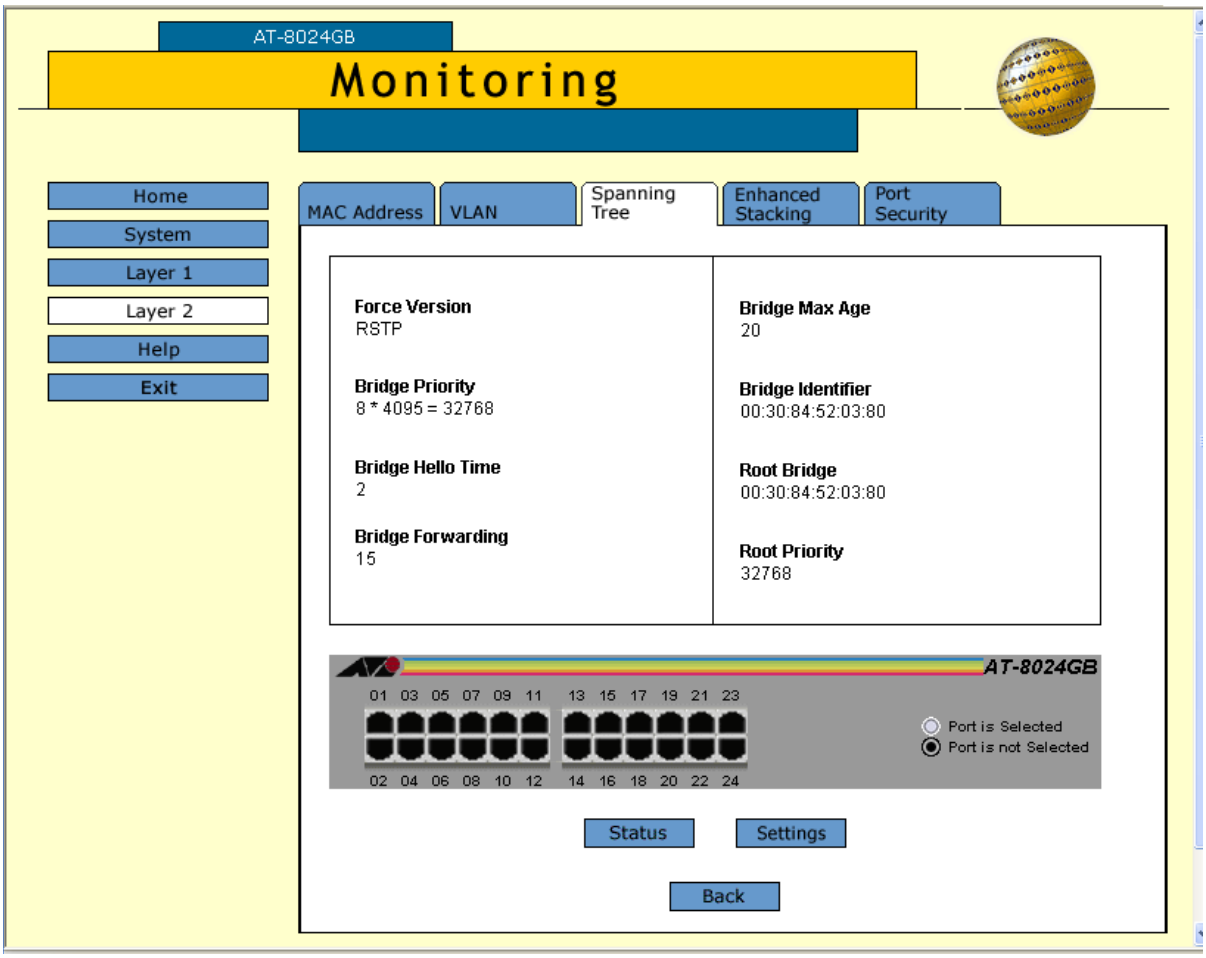

Figure 93 Rapid Spanning Tree Window - Monitoring

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

Chapter 29
Virtual LANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs from a web browser management session. This chapter also explains how to select a multiple VLAN mode.

Note
For background information on VLANs, refer to **Chapter 10, Virtual LANs**.

This chapter contains the following sections:

Creating A New Port-based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the procedure below:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu is shown in Figure 94.

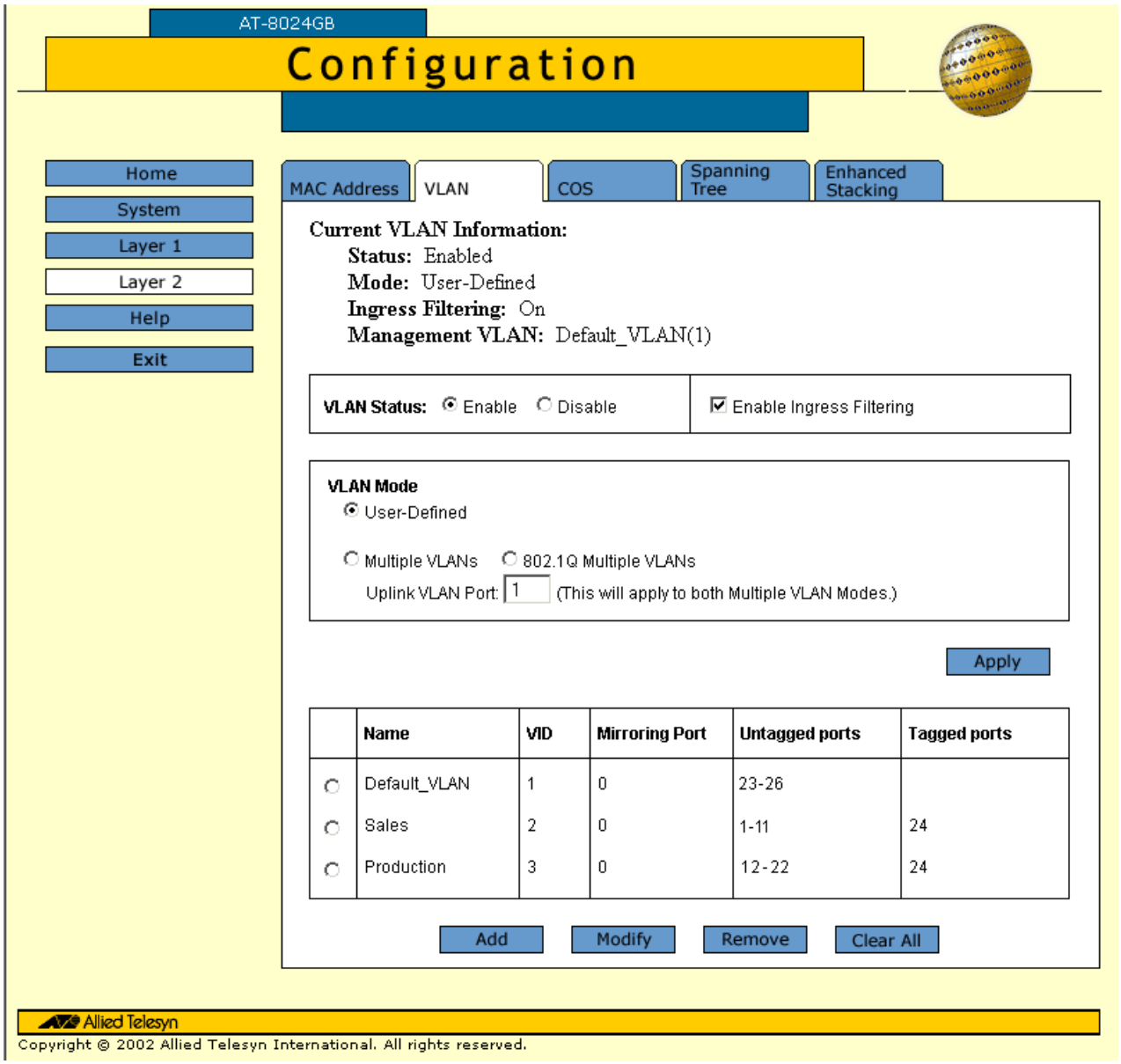

Figure 94 VLAN Menu

4. Click **Add**. The Add VLAN menu is shown in Figure 95.

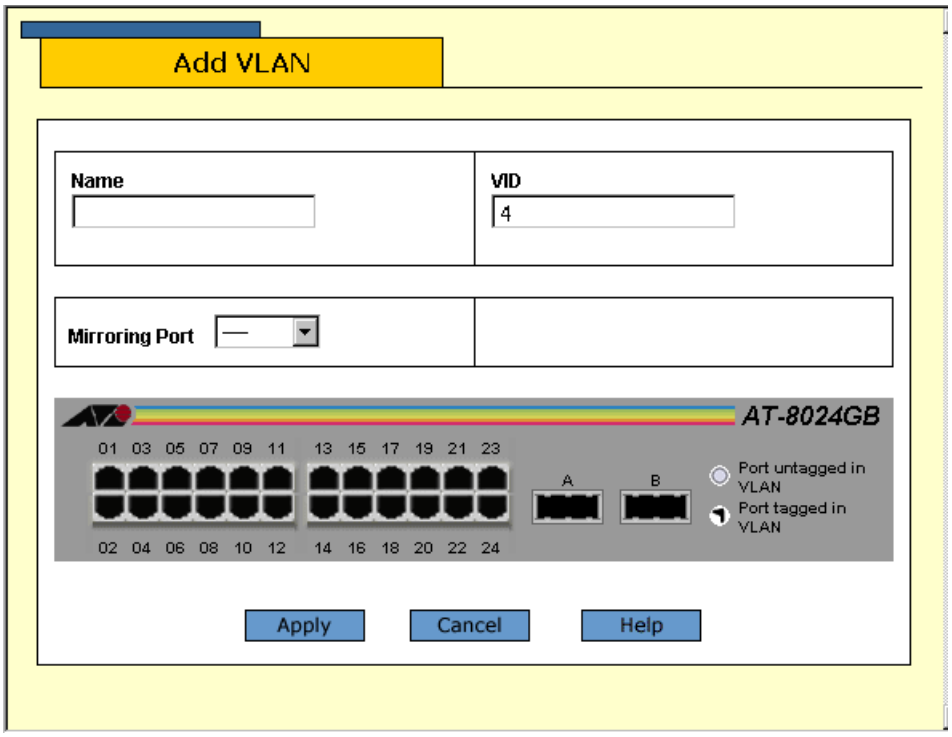

Figure 95 Add VLAN Menu

5. Select the **Name** field and enter a name for the new VLAN. The VLAN name can be from one to fifteen characters in length. The name should reflect the function of the nodes that will be members 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 switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

   Note
   A VLAN must be assigned a name.

6. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4096.

   The management software will use the next available VID number on the switch as the default value. If this VLAN will be unique in your network, then its VID must also be unique. If this VLAN will be part of a larger VLAN that spans multiple switches, than the VID value for the

VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you should assign the Sales VLAN on each switch the same VID value.

The switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-8024 switch to a network that already has VLANs using VIDs 2 through 24, the AT-S39 software will still use VID 2 as the default value for the first VLAN you create on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Note
A VLAN must have a VID.

7. If you want all received traffic on the ports of the VLAN to be mirrored to another port on the switch, select the mirroring port from the **Mirroring Port** pull-down menu.

   This feature is useful when troubleshooting a VLAN. You can analyze the VLAN traffic by placing a network analyzer on the mirroring port.

   Note
   In most cases, this parameter should be left at its default value of "—". This value means that the VLAN traffic will not be mirrored. For more information on port mirroring, refer to **Port Mirroring Overview** on page 93.

8. To select ports for the VLAN, click on the appropriate ports in the switch image.

   Clicking repeatedly on a port toggles the port through the following possible settings:

    Untagged port

    Tagged port

    Port not a member of the VLAN

9. Once you have selected the ports for the VLAN, click **Apply**.

Note

Ports designated as untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

The new VLAN is now ready for network operations.

Modifying a Port-based or Tagged VLAN

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

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 94 on page 298 is displayed.
4. Click the circle next to the name of the VLAN you want to modify. You can select only one VLAN.
5. Click **Modify**.

   The configuration menu for the VLAN is displayed.
6. Modify the VLAN parameters by referring to Step 5 to Step 8 in the previous procedure, **Creating A New Port-based or Tagged VLAN** on page 298.

   When modifying a VLAN, observe the following guidelines:

   - ❑ You cannot change the VID of a VLAN.
   - ❑ You cannot change the name of the Default_VLAN.
   - ❑ When changing a VLAN's name, be sure that the new name is unique on the switch.
7. After making the desired changes, click **Apply**.

Note
Untagged ports that are added to a VLAN are automatically removed from their current VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN leaves the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

Deleting a Port-based or Tagged VLAN

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 94 on page 298 is displayed.
4. Click the circle next to the name of the VLAN you want to delete. You can select only one VLAN.
5. Click **Remove**.

   A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

Note
You cannot delete the Default_VLAN.

To delete all VLANs from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 94 on page 298 is displayed.
4. Click **Clear All**.

   A confirmation prompt is displayed.
5. Click **OK** to delete all the VLANs or **Cancel** to cancel the procedure.

   If you click OK, all VLANs except for the Default_VLAN are deleted from the switch. The ports in the VLANs are returned to the Default_VLAN as untagged ports.

Displaying VLANs

To display the VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 2**.
3. From the Layer 2 page, select the **VLAN** tab.

   The management software displays the window shown in Figure 96. The information in this window is for viewing purposes only.

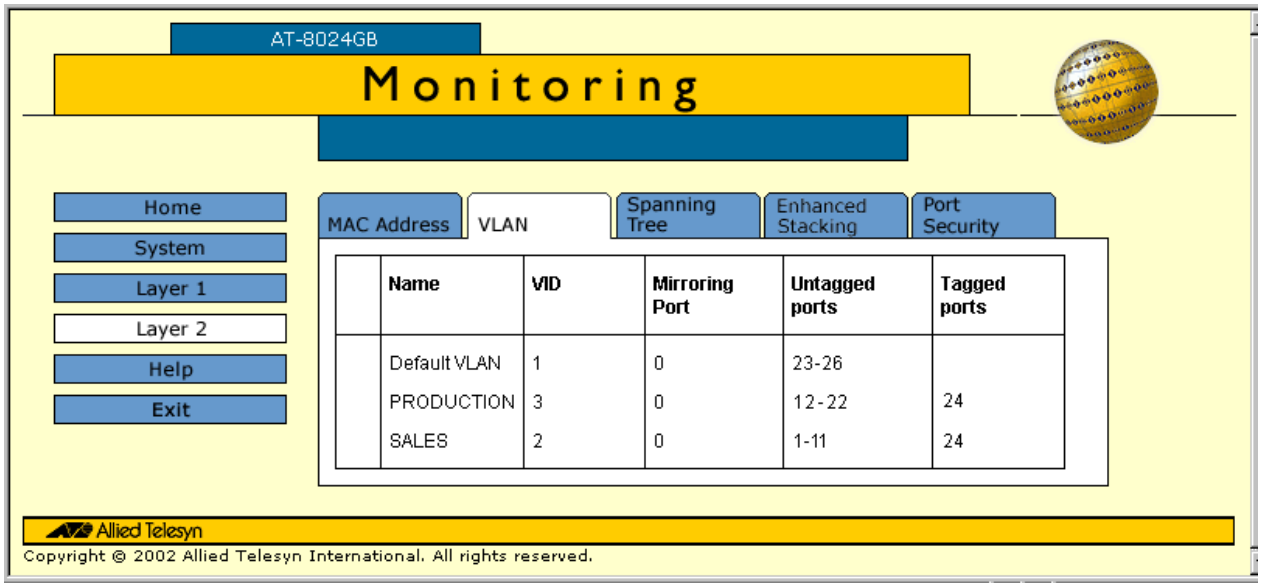

Figure 96 VLAN Monitoring Window

Setting the VLAN Mode

The procedures in this section explain how to set the switch for either the user configured (Tagged) VLAN mode, which supports port-based and tagged VLANs, or the Basic VLAN mode. The default setting for the switch is the user configured (Tagged) VLAN mode. There are two ways that you can do this. Both methods are described below. (If you want to set the switch to one of the Multiple VLAN modes, refer to **Selecting a Multiple VLANs Mode** on page 306.

Note
For descriptions of switch modes and VLAN modes, refer to **Virtual LANs Overview** on page 118.

Procedure 1

The first method for setting the switch to the user configured (Tagged) VLAN mode or the Basic VLAN mode is provided here:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, choose **System**.
3. Select the **General** tab.
4. In the Switch Mode section of the menu, click either **Tagged** or **Basic**.

   If you select Tagged, which is the default, the switch will support both port-based VLANs and tagged VLANs. If you select Basic, the switch will operate in the Basic mode.
5. Click **Apply**. A change to the VLAN status is immediately activated on the switch.

Procedure 2

Here is the second method for setting the VLAN mode on the switch:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 94 on page 298 is displayed.
4. In the **VLAN Status** section of the menu, click either **Enable** or **Disable**. If you select Enable, which is the default, the switch will support port-based VLANs and tagged VLANs. If you select Disable, the switch will operate in the Basic mode.
5. Click **Apply**. A change to the VLAN status is immediately activated on the switch.

Selecting a Multiple VLANs Mode

To select a multiple VLAN mode, perform the procedure below:

> **Note**
> The VLAN mode on the switch must be set to User Configured (Tagged) VLAN mode, and not to Basic Mode, in order for the unit to operate in a multiple VLANs mode. To set a switch's VLAN mode, refer to **Setting the VLAN Mode** on page 305.

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab. T

   The VLAN menu in Figure 94 on page 298 is displayed.
4. In the VLAN Mode section of the menu, select one of the following:

   - ❑ User-Defined: Supports tagged and port-based VLANs and the Basic VLAN mode
   - ❑ Multiple VLAN: Supports the non-802.1Q compliant Multiple VLANs Mode
   - ❑ 802.1Q Multiple VLANs: Supports the 802.1Q compliant Multiple VLANs Mode
5. If you selected a multiple VLAN mode, in the Uplink VLAN Port field enter the port on the switch to function as the uplink port for the VLANs.
6. Click **Apply**.

   The new mode is immediately activated on the switch. If you selected the 802.1Q compliant Multiple VLANs Mode, it is possible that your remote management session will end and you will not be able to reestablish it. Remote management of a switch operating in that multiple VLAN mode is possible only through the uplink port.

Chapter 30
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:

Note
For background information on MAC addresses, refer to **MAC Address Overview** on page 162.

Viewing the MAC Address Table

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

1. From the Home page, select either **Configuration** or **Monitoring**.
2. Select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu is displayed. Figure 97 shows how this menu appears when you display it through the Configuration main menu selection. If displayed through the Monitoring main menu selection, the Add button is not included. This button is used to add static unicast and multicast address to the switch. For instructions, refer **Adding Static Unicast and Multicast MAC Addresses** on page 311.)

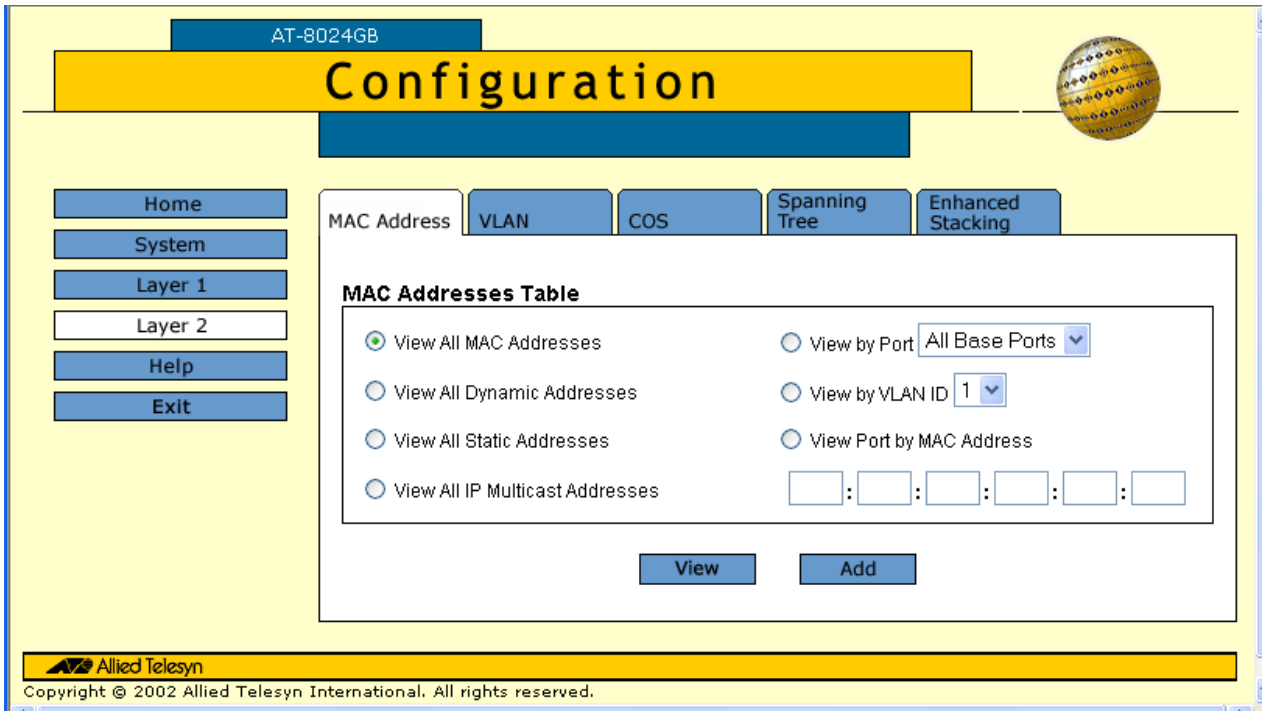

Figure 97 Forwarding Database Tab

4. Select an option to display MAC addresses. The options are described below.

   View All MAC Addresses
   This option displays both static and dynamic MAC addresses.

   View All Dynamic Addresses
   This option displays only dynamic MAC address. Dynamic MAC addresses are addresses that the switch has learned by examining the source addresses of frames received on the ports.

View All Static Addresses
This option displays only the static MAC addresses. Static MAC addresses are addresses that you entered manually into the MAC address table.

View All IP Multicast Addresses
This option displays the multicast MAC addresses.

View By Port
The pull-down menu with this option is used to display the MAC addresses learned on a particular port.

View By VLAN ID
This option displays the MAC addresses learned by a particular VLAN on the switch. You specify the VLAN by its VID.

View Port by MAC Address
This option is used to determine the port on the switch to which an end node is communicating with the switch. To use this option, enter the MAC address of the node in the field.

5. Once you have selected one of the options, click **View**.

   The MAC addresses are displayed in a window. The columns in the window are defined below:

   MAC Address
   The MAC address of the node connected to the switch.

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

   PMAP
   The ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different multicast groups. (The abbreviation PMAP is derived from "port mapping.")

   Each "0" is a hexadecimal value, representing fours ports on the switch. The hexadecimal value is arrived at from the binary value "0000", where each binary "0" represents a switch port. A binary "0" means that the port is not a member of a multicast group while a "1" means that it is.

   The port numbering scheme is from right to left. As an example, assume that ports 1 through 4 on the switch were members of the same multicast group. The PMAP column for the address would represent this as follows: "0000000F". Another example is "000020F. This example would indicate that ports 1 to 4 and port 10 on the switch were members of the same multicast group.

CPU
Indicates whether the traffic received on the port is sent to the switch's CPU. Yes indicates that the traffic is being sent to the CPU while No indicates it is not.

MIR
Indicates whether the traffic on the port is being mirrored. Yes means the traffic is being mirrored while No indicates that it is not.

EMP
Indicates whether multicast packets are being forwarded by ports in the blocking state. This feature is not supported at this time. This column will indicate "No" for all multicast addresses, except for the switch's MAC address. Multicast packets are forwarded only by ports in the forwarding state.

VLAN ID
The VID of the VLAN where the port is an untagged member.

Type
The MAC address type. The type can be either static or dynamic.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning static unicast and multicast address to ports on the switch. You can assign up to 255 static MAC addresses per port.

To add a static unicast or multicast address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu is shown in Figure 97 on page 308.
4. Click **Add**.

   The Add Static MAC Address menu is shown in Figure 98.

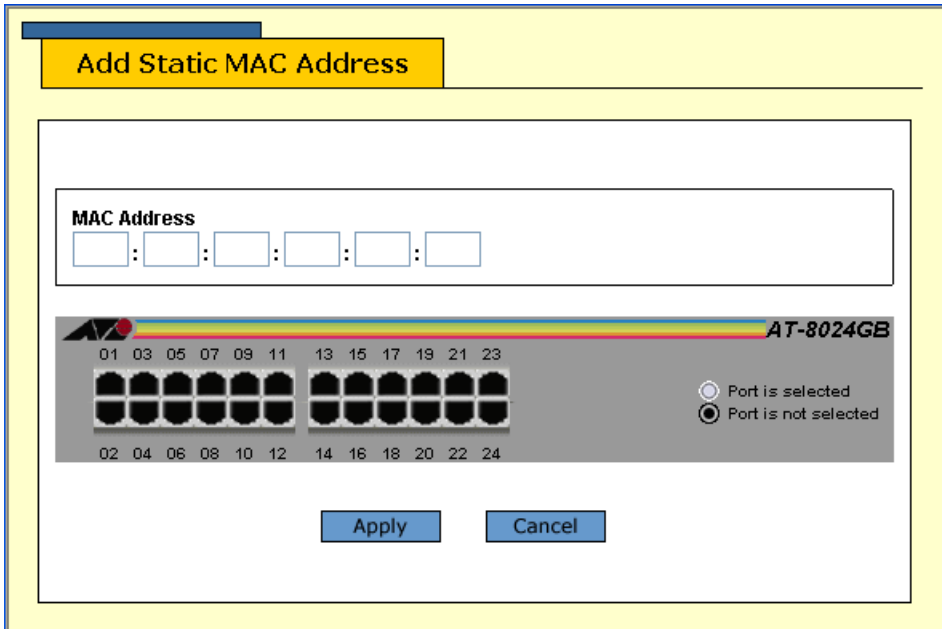

Figure 98 Add Static MAC Address Menu

5. In the MAC Address section of the menu, enter the new static MAC address. If you are adding a static unicast address, you can specify only one port. If you are adding a static multicast address, you can specify multiple ports.
6. In the graphical image of the switch click the port to which you want to assign the address. A selected port turns white. You can select only one port.
7. Click **Apply**.
8. Repeat this procedure to add other static addresses to the switch.

Deleting MAC Addresses

To delete a static, dynamic, or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu is shown in Figure 97 on page 308.
4. Display the MAC addresses on the switch by selecting one of the options. For instructions, refer to **Viewing the MAC Address Table** on page 308.
5. Click the dialog circle next to the MAC address you want to delete from the switch. (If the MAC address does not have a dialog circle, it is a system MAC address that cannot be deleted.)
6. Click **Remove**.

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 sent to or 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:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **System**.
3. From the System page, select the **General** tab.

   The General tab is shown in Figure 72 on page 248.
4. Enter a new value in seconds in the MAC Aging Time field of the menu. This field is located in the Configuration section of the menu.

   The value should be an increment of 5 seconds, for example 410, 415, or 420. A value that is not an increment of 5 is rounded down to the next increment of 5. For example, the value 524 is rounded down to 520. The default is 300 seconds (5 minutes).
5. Click **Apply**.

Chapter 31
Class of Service

This chapter contains instructions on how to configure CoS. This chapter contains the following procedure:

- ❑ **Configuring CoS** on page 315

Note
For background information on CoS, refer to **Class of Service Overview** on page 175.

Configuring CoS

To configure CoS, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **CoS** tab.

   The CoS tab is shown in Figure 99.

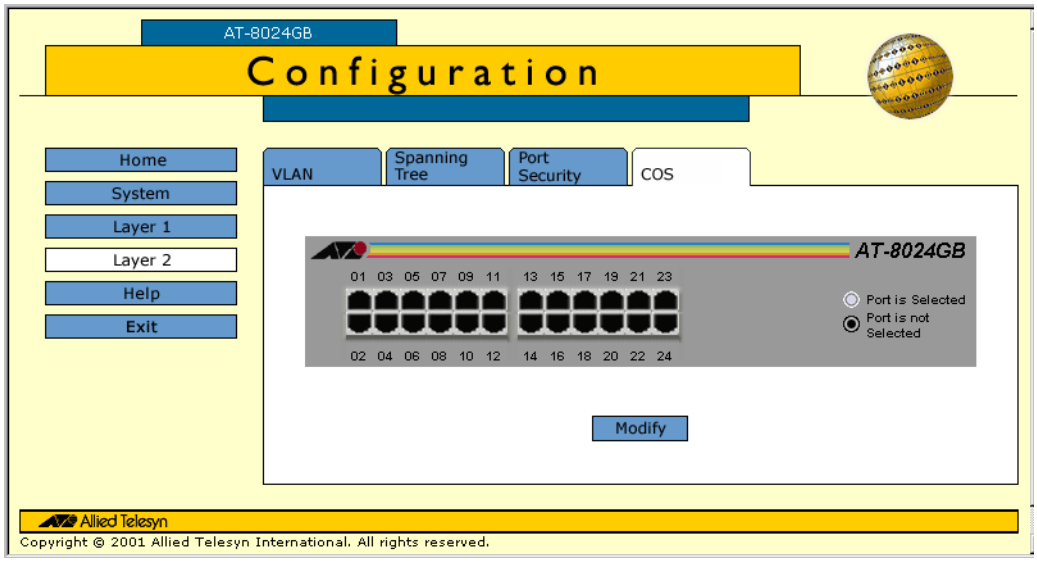

Figure 99 CoS Tab

4. Click the port where you want to configure CoS. You can select only one port at a time. A selected port turns white. (To deselect a port, click it again.)
5. Click **Modify**.

The CoS Settings for Port menu is shown in Figure 100.

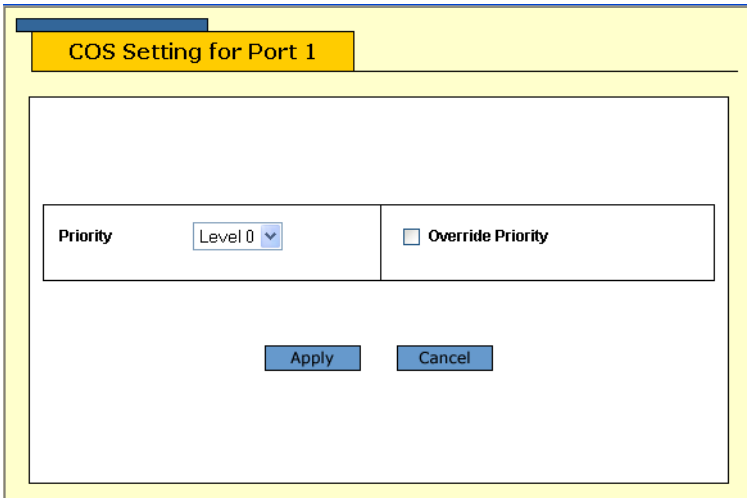

Figure 100 CoS Setting for Port Menu

6. If you want all tagged and untagged frames received on the port to go to the low priority queue, select any level from Level 0 to Level 3 from the Priority pull-down menu. (It does not matter which of these levels you select.) If you want all frames received on the port to go to the high priority queue, select any level from Level 4 to Level 7. (Again, it does not matter which level you select.)
7. If you are configuring a tagged port and you want the switch to ignore the priority tag in the tagged frames entering the port, click the Override Priority option. If you activate this feature, all tagged frames will be directed to either the low or high priority queue specified in Step 6.

Note
The tagged information in a frame is not changed as the switch forwards a frame. A tagged frame exits the switch with the same priority level it had when it entered.

The default for this parameter is No, meaning that the priority level of a tagged frame is determined by the priority level specified in the frame itself.

8. Click **Apply**.

   Configuration changes are immediately activated on the switch.

Chapter 32
IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. Sections in the chapter include:

Note
For background information on this feature, refer to **IGMP Snooping Overview** on page 180.

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management session, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **System**.
3. Select the **IGMP** tab.

   The IGMP tab in Figure 101 is displayed.

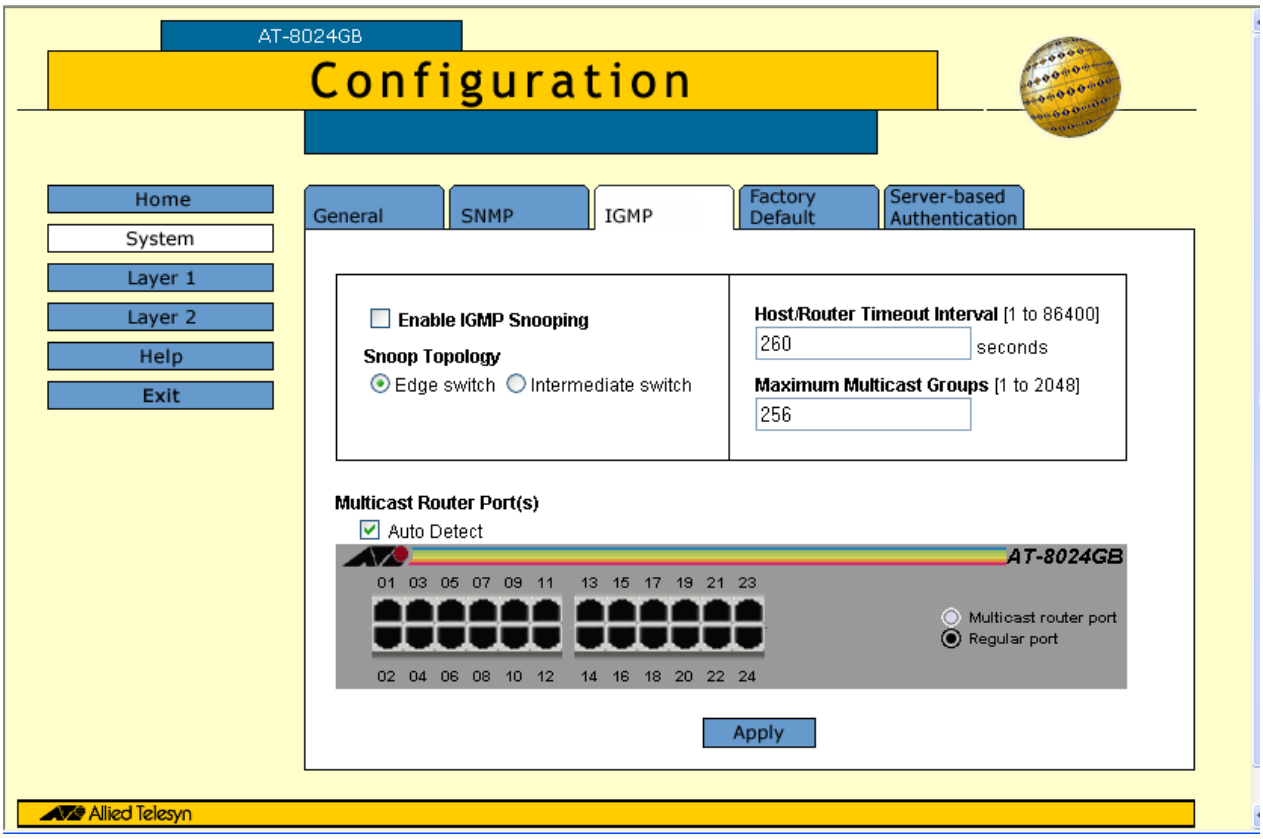

Figure 101 IGMP Menu - Configuration

4. Adjust the IGMP parameters as necessary.

   The parameters are explained below:

   Enable IGMP Snooping Status
   Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

Snoop Topology
Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times-out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 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.

Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

Multicast Router Port(s)
Specifies the port on the switch to which the multicast router is detected. You can let the switch determine this automatically by selecting Auto Detect, or you can specify the port yourself by clicking on the ports in the graphical image. A white port indicates a multicast router port.

By default, the switch automatically detects the presence of multicast routers by watching for queries on its ports. Once it has received a query, it notes the port on which the query was received and identifies the port as a multicast port.

If desired, you can deactivate the auto-detection of multicast routers and indicate the multicast router ports yourself. To deactivate the auto-detection, click on the **Auto Detect** check box. If the check box is empty, auto-detect is deactivated.

To indicate the multicast router ports manually, use the graphical image of the switch. Clicking a port toggles it to white, indicating that the port is connected to a multicast router.

5. After setting the IGMP parameters, click **Apply**.

Displaying a List of Host Nodes and Multicast Routers

You can use the AT-S39 software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. To view host nodes and multicast routers, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring window, select the **System** menu option.
3. Select the **IGMP** tab.

   The window in Figure 102 is displayed.

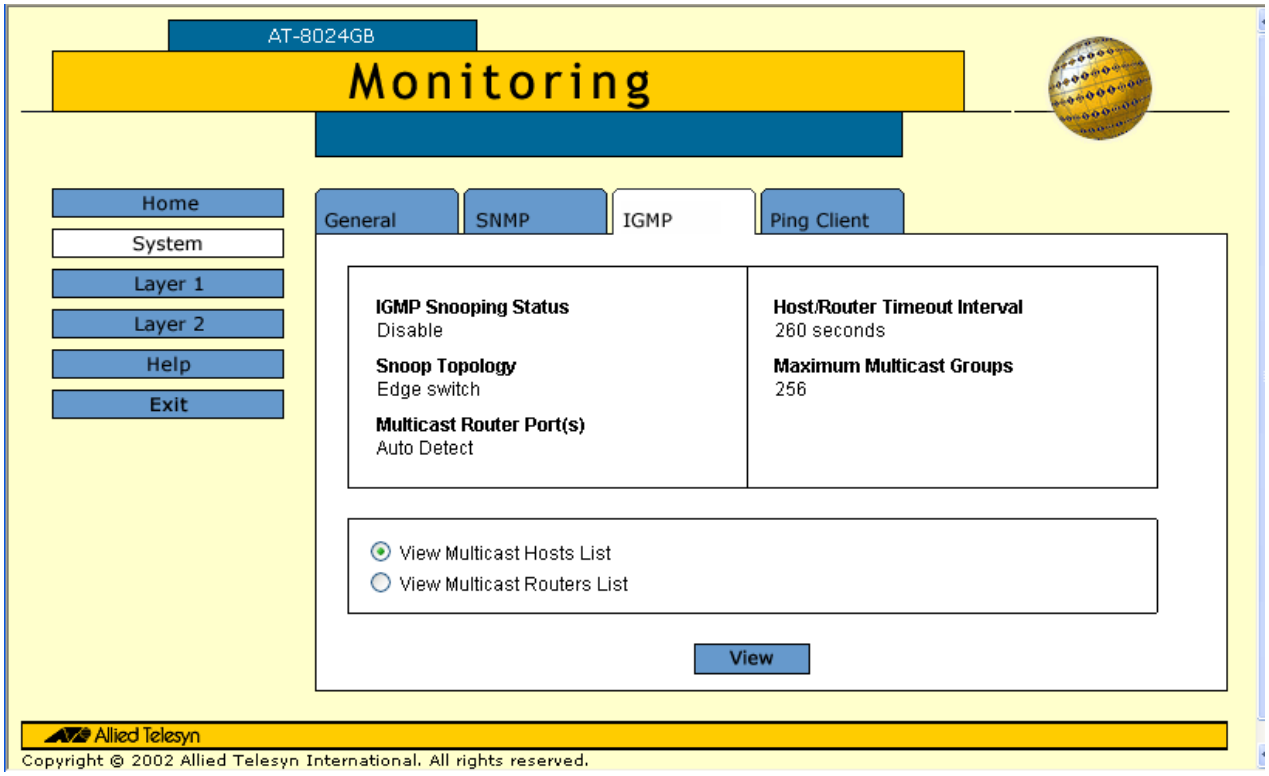

Figure 102 IGMP Window - Monitoring

4. To view the multicast addresses and the host nodes, click **View Multicast Host List** and then click **View**. To view the multicast routers, click **View Multicast Router List** and then click **View**.

Viewing a list of host nodes displays a window containing the following information. The information in the window is for viewing purposes only.

Multicast Group
The multicast address of the group.

Member Port
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Host IP
The IP address(es) of the host node(s) connected to the port.

Viewing a list of multicast routers displays a window containing the following information. The information in the window is for viewing purposes only.

Port
The port on the switch where the multicast router is connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the port on the router.

Chapter 33
Broadcast Storm Control

This chapter contains instructions on how to configure the Broadcast Storm Control feature on the switch. Sections in the chapter include:

Note
For background information on this feature, refer to **Broadcast Storm Control Overview** on page 188.

Configuring the Interval Timer

The interval timer defines the time period used in counting the number of broadcast packets transmitted by a port. A port will not transmit more than its maximum number of broadcast frames during the specified timer interval. If a port reaches its maximum number, it will discard and not forward any additional broadcast frames. You can specify a different interval timer for 10 and 100 Mbps ports and 1000 Mbps ports.

To specify an interval timer, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System menu option is selected by default along with the General tab when you open the Configuration page. If they are not already selected, select them now.

2. In the Broadcast Storm Control section, enter values for the two interval timers.

   The interval timer for 10 Mbps and 100 Mbps ports is in milliseconds and has a range of 10 to 120 milliseconds. The value should be entered in increments of 10.

   The interval timer for 1000 Mbps ports is in microseconds and has a range of 100 to 120000 microseconds. The value should be entered in increments of 100.

   A value for an interval timer applies to all ports operating at the corresponding speed.

3. After you have entered your values, click **Apply**.

4. Go to the next procedure to set values for the maximum number of broadcast frames the ports on the switch will transmit.

Setting the Maximum Number of Broadcast Frames

To set the maximum number of broadcast frames you want the ports on the switch to transmit, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.

   When you open the Layer 1 page, the Port Settings tab is selected by default. If it is not selected, select it now.
3. In the graphical switch image, click a port where you want to specify the maximum number of broadcast frames.

   The selected port turns white. To deselect a port, click it again. You can select more than one port at a time.
4. Click **Modify**.

   The current settings for the port are displayed in the Port Configuration menu.
5. In the Broadcast Storm Control section of the menu, enter the maximum number of broadcast packets you want the port to be able to transmit.

   The range is 0 to 1023 broadcast frames. Specifying a value of "0" disables Broadcast Storm Control on the port. The port will forward all broadcast frames. This is the default

   As an example, assume that you enter a value of 300 as the maximum number of broadcast frames for a port. Also assume that the port is operating at 100 Mbps and that you specified an interval timer of 100 milliseconds for 100 Mbps ports. The result would be that the port could transmit up to 300 broadcast frames every 100 milliseconds. If it received more than 300 broadcast frames for transmission during a 100 millisecond period, the extra broadcast frames would be discarded by the port and would not forwarded.
6. Click **Apply**.
7. Repeat this procedure to set the maximum number of broadcast frames for other ports on the switch.

Chapter 34
TACACS+ and RADIUS Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedure:

Note
For background information on the authentication protocols, refer to **TACACS+ and RADIUS Overview** on page 193.

Configuring TACACS+ and RADIUS

To configure the authentication protocols, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **System**.
3. From the System page, select the **Server-based Authentication** tab. The tab is shown in Figure 103.

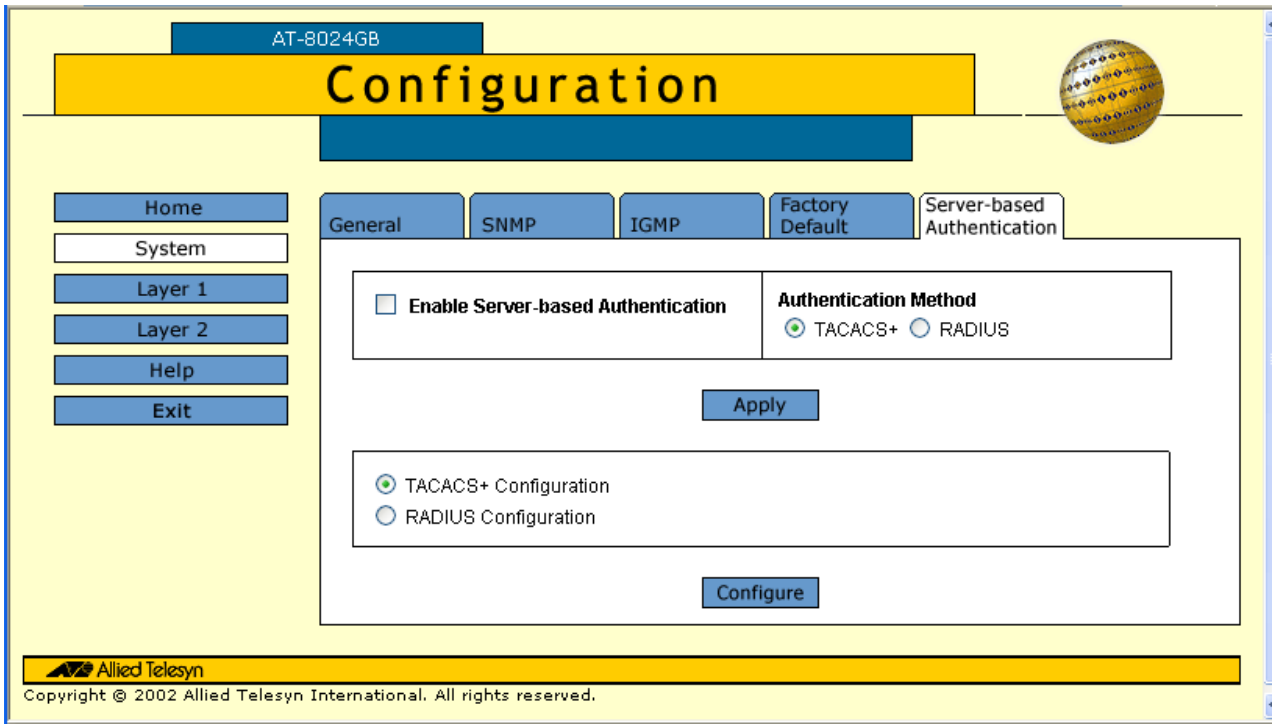

Figure 103 Server-based Authentication Tab

Note
The Enable Server-based Authentication check box applies only to the manager account feature. It does not apply to the 802.1x port-based access control feature. If this option is disabled (no check in box), which is the default setting, the switch uses its standard Manager and Operator accounts when you log on to manage the switch. If enabled, the switch uses the manager accounts on the TACACS+ or RADIUS server.

4. To enable or disable the authentication feature on the switch, click the Disable Server-based Authentication check box. A check in the box indicates that this feature is disabled. No check indicate the feature is enabled. The default is disabled.

5. To select an authentication protocol, click either TACACS+ or RADIUS in the Authentication Method section of the menu. The default is TACACS+. Only one authentication protocol can be active on the switch at a time.

6. Click **Apply**.

Note
If you activated the authentication feature, go to Step 6 to configure TACACS+ or Step 7 to configure RADIUS.

7. If you selected RADIUS, go to Step 8. To configure TACACS+, do the following:

   a. From the Server-based Authentication tab, click the check circle next to TACACS+ Configuration and click **Configure**.

      The TACACS+ Configuration menu in Figure 104 is displayed.

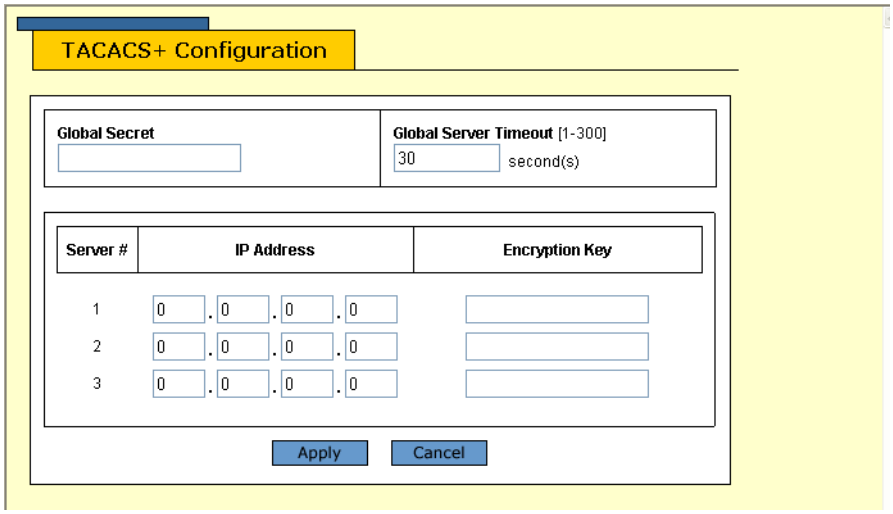

Figure 104 TACACS+ Configuration Menu

   b. Configure the parameters as needed. They are described below.

      Global Secret
      If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

      Global Server Timeout
      This parameter specifies the maximum amount of time the switch will wait for a response from a TACACS+ server before assuming the server cannot respond. If the timeout

expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and **Encryption Secret**
Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server's secret in the Global Secret field.

c. After you have finished configuring the parameters, click **Apply**. This closes the TACACS+ Configuration window.

d. In the Server-Based Authentication tab, click the option Enable Server-based Authentication. A check should appear in the box. This activates the manager accounts feature on the switch. The switch now uses the manager accounts configured on the TACACS+ server whenever you log on to manage the switch.

8. To configure RADIUS client software, do the following:

   a. From the Server-based Authentication tab, click the check circle next to RADIUS Configuration and click **Configure**.

      The RADIUS Configuration menu is shown in Figure 104.

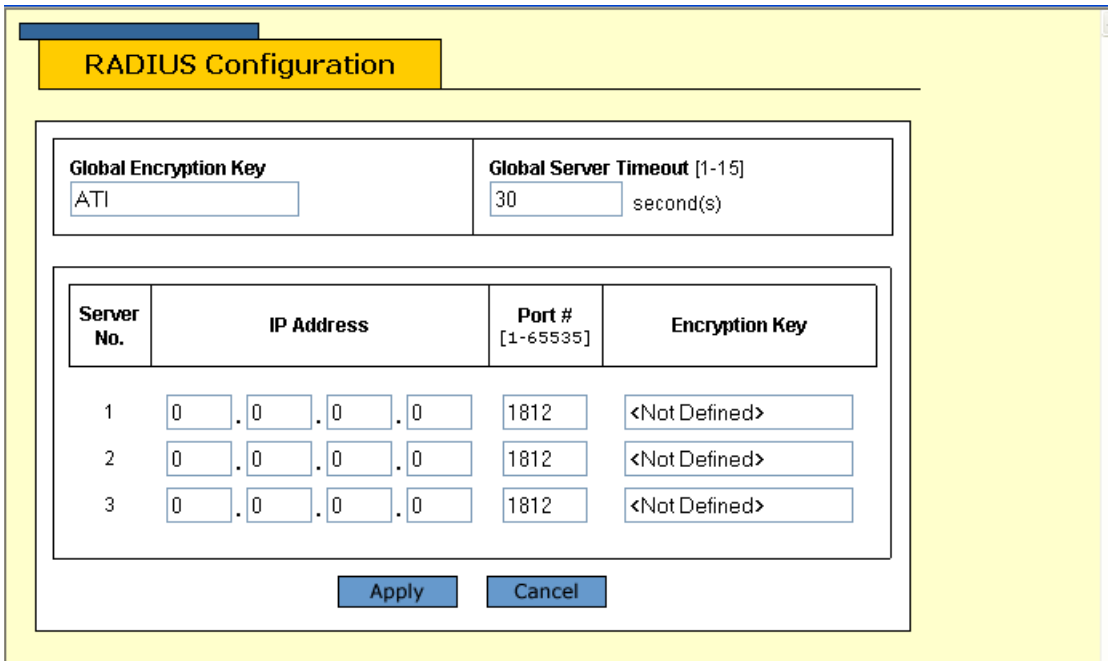

Figure 105 RADIUS Configuration Menu

b. Configure the parameters as needed. They are described below.

Global Encryption Key
If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout
This parameter specifies the maximum amount of time the switch will wait for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and **Encryption Key**
Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

c. After you have finished configuring the parameters, click **Apply**. This closes the RADIUS Configuration menu.

Note
Step d. does not apply to the 802.1x port-based access control feature.

---

d. In the Server-Based Authentication tab, click the option Enable Server-based Authentication. A check should appear in the box. This activates the manager accounts feature on the switch. The switch now uses the manager accounts configured on the RADIUS server whenever you log on to manage the switch. If you configured the RADIUS client software for the 802.1x port-based access control feature, and not for the manager accounts feature, leave this option disabled.

Appendix A
AT-S39 Default Settings

This appendix lists the AT-S39 factory default settings.

Management Interface Default Settings

The following table lists the management interface default settings.

Management Interface Setting	Default
Manager Login Name	manager
Manager Password	friend
Operator Login Name	operator
Operator Password	operator
Console Disconnect Timer Interval	10 minutes

Note
Login names and passwords are case-sensitive.

Switch Administration Default Settings

The following table describes the switch administration default settings.

Administration Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
System Name	None
Administrator	None
Comments	None
BOOTP/DHCP	Disabled
MAC Address Aging Time	300 seconds

System Software Default Settings

The following table lists the system software default settings.

System Software Setting	Default
Console Startup Mode	Menu

Enhanced Stacking Default Setting

The following table lists the enhanced stacking default setting.

Enhanced Stacking Setting	Default
Switch State	Slave

SNMP Default Settings

The following table describes the SNMP default settings.

SNMP Communities Setting	Default
SNMP Status	Disabled
Get Community	public (Read Only)
Set Community	private (Read|Write)
Trap Community	public
Trap Receivers 1, 2, 3, 4	0.0.0.0

Port Configuration Default Settings

The following table lists the port configuration default settings.

Port Configuration Setting	Default
Status	Enabled
Back Pressure	Disabled
Flow Control	None
Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation
MDI/MDI-X	Auto-MDI/MDIX

Class of Service

The following table lists the default mappings of IEEE 802.1p priority levels to egress port priority queues.

IEEE 802.1p Priority Level	Port Priority Queue
0, 1, 2, 3	low
4, 5, 6, 7	high

IGMP Snooping Default Settings

The following table lists the IGMP Snooping default settings.

IGMP Snooping Setting	Default
IGMP Snooping Status	Disabled
Multicast Host Topology	Single Host/ Port (Edge)
Host/Router Timeout Interval	260 seconds
Maximum Multicast Groups	64
Multicast Router Ports Mode	Auto Detect

Spanning Tree Switch Settings

The following table describes the Spanning Tree Protocol default settings for the switch.

STP Switch Setting	Default
Spanning Tree Status	Disabled
Active Protocol Version	RSTP

STP Default Settings

The following table describes the STP default settings.

STP Setting	Default
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Port Cost	Automatic -Update
Port Priority	128

RSTP Default Settings

The following table describes the RSTP default settings.

RSTP Setting	Default
Force Version	RSTP
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Edge Port	Yes
Point-to-Point	Auto Detect
Port Cost	Automatic Update
Port Priority	128

VLAN Default Settings

This section provides VLAN default settings.

VLAN Setting	Default
Default VLAN Name	Default_VLAN (all ports)
Management VLAN ID	1 (Default_VLAN)
VLAN Mode	User Configured
Basic VLAN Mode	Disabled
Multiple VLANs Modes	Disabled

Port Security Default Settings

The following table lists the port security default settings.

Port Security Setting	Default
Security Mode	Automatic (no security)
MAC Limit	No Limit

802.1x Port-Based Network Access Control Default Settings

The following table describes the 802.1x Port Access Control default settings.

802.1x Port Access Control Setting	Default
Port Access Control	Disabled
Authentication Method	RADIUS EAP
Port Role	None

Server-Based Authentication Default Settings

This section describes the server-based authentication, RADIUS, and TACACS+ client default settings.

Server-Based Authentication Default Settings

The following table describes the server-based authentication default settings.

Server-based Authentication Setting	Default
Server-based Authentication	Disabled
Active Authentication Method	TACACS+

RADIUS Default Settings

The following table lists the RADIUS configuration default settings.

RADIUS Configuration Setting	Default
Global Encryption Key	ATI
Global Server Timeout Period	30 seconds
RADIUS Server 1 Configuration	0.0.0.0
RADIUS Server 2 Configuration	0.0.0.0
RADIUS Server 3 Configuration	0.0.0.0
Auth Port	1812
Encryption Key	Not Defined

TACACS+ Client Default Settings

The following table lists the TACACS+ client configuration default settings.

TACACS+ Client Configuration Setting	Default
TAC Server 1	0.0.0.0
TAC Server 2	0.0.0.0
TAC Server 3	0.0.0.0
TAC Server Order	1 2 3
TAC Global Secret	None
TAC Timeout	30 seconds

Index