Management Software

AT-S80

User's Guide

For use with the AT-FS750/16 and
AT-FS750/24 Fast Ethernet Smart
Switches

Version 2.0.0

Allied Telesis™

Contents

Figures

Tables

Tables

Preface

This guide contains instructions on how to use the AT-S80 management software to monitor and manage the AT-FS750/16 and AT-FS750/24 Fast Ethernet Smart switches.

The AT-S80 Management Software has two management interfaces: a menus interface and a web browser interface. You access the menus interface through the console port on the switch. You access the web browser interface from any management workstation on your network that has a web browser application. For background information on the management interfaces, refer to Chapter 1, "Overview" on page 17.

> **Note**
> The AT-S80 management software does not support remote management with the Telnet application protocol or an SNMP program.

> **Note**
> The interface illustrations in this book show the interface for the AT-FS750/16 Fast Ethernet Smart Switch in the menus section and the interface for the AT-FS750/24 Fast Ethernet Smart Switch in the web section of the book. The AT-S80 software features are identical in both switches with the exception of the number of ports displayed.

This preface contains the following sections:

❐ "Where to Find Web-based Guides" on page 14

❐ "Document Conventions" on page 15

❐ "Contacting Allied Telesis" on page 16

Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at **www.alliedtelesis.com**. You can view the documents online or download them onto a local workstation or server.

For information about installing the AT-FS750/16 and AT-FS750/24 switches, see the *AT-FS750/16, AT-FS750/24 Fast Ethernet Smart Switches Installation Guide* (P/N 613-000354).

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

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

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

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base:
www.alliedtelesis.com/support. 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 section of the Allied Telesis web site: **www.alliedtelesis.com**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Warranty

All Allied Telesis warranties are subject to the terms and conditions set out in the Allied Telesis Limited Warranties on our web site at **www.alliedtelesis.com/warranty**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact the Allied Telesis Technical Support group at our web site: **www.alliedtelesis.com/support/rma**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Management Software Updates

New releases of the management software for our managed products are available from the following Internet sites:

❒ Allied Telesis web site: **www.alliedtelesis.com**
❒ Allied Telesis FTP server: **ftp://ftp.alliedtelesis.com**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.

Chapter 1
Overview

This chapter provides an overview of the AT-S80 Management Software for the AT-FS750/16 and AT-FS750/24 switches. This chapter contains the following sections:

❐ "Management Overview" on page 18

❐ "Remote SNMP Management" on page 20

❐ "Management Access Level" on page 21

❐ "Ports 17 and 18 on the AT-FS750/16 Switch and Ports 25 and 26 on the AT-FS750/24 Switch" on page 22

Management Overview

The AT-S80 Management Software allows you to view and adjust the operating parameters of the AT-FS750/16 and AT-FS750/24 Fast Ethernet Switches. A few examples of the management functions are listed here:

❒ Enable and disable ports

❒ Configure a port's speed and duplex mode

❒ Create port trunks

❒ Configure a port mirror

❒ Configure Quality of Service (QoS)

❒ Create port-based and tagged virtual LANs

❒ Configure 802.1x port-based network access control

The AT-S80 management software comes preinstalled on the switch with default settings for all of the switch's operating parameters. Managing the switch is not required if the default settings are adequate for your network. Instead, you can use the device as an unmanaged switch by connecting it to your network and powering on the unit, as explained in the hardware installation guide.

> **Note**
> The default settings for the management software are listed in Appendix A, "AT-S80 Software Default Settings" on page 339.

In order to actively manage the switch and adjust its operating parameters, you must access the switch's AT-S80 management software. You can access the management software using one of the following methods:

❒ Local management using the Console port on the switch and the menus interface. See "Local Management Connection" on page 19.

❒ Remote management using a web browser and the web browser interface. See "Remote Management Connection" on page 19.

The chapters in Section I of this guide explain how to manage the switch from a local management session using the menu interface. The chapters in Section II explain how to manage the device from a remote session using the web browser interface. Both interfaces allow you to configure all of a switch's parameters.

Local Management Connection

To establish a local management connection with an AT-FS750/16 or AT-FS750/24 Fast Ethernet Switch, you must connect a terminal or a PC with a terminal emulator program to the console port on the front of the switch using the management cable which is included with the unit. This type of connection is referred to as "local" because you must be physically close to the switch, such as in the wiring closet where the device is located.

Note
For instructions on how to start a local management session, refer to "Starting a Local Management Session" on page 26.

A switch does not need an Internet Protocol (IP) address for local management. You can start a local management session on a switch at any time. It does not interfere with the forwarding of network packets by the device.

Remote Management Connection

The AT-S80 management software has a web browser interface for managing the AT-FS750/16 and AT-FS750/24 switches remotely from any management station on your network that has a web browser application.

The switch must have an IP address in order for you to manage it remotely with a web browser. You can assign the IP address manually or activate the DHCP client so the switch automatically obtains its IP configuration from a DHCP server on the network. The initial assignment of an IP address or the activation of the DHCP client software must be performed through a local management session of the switch.

For instructions on how to start a remote management session, refer to "Establishing a Remote Connection to Use the Web Browser Interface" on page 214.

Note
A remote management station must be a member of the switch's Default VLAN for you to use it to manage the unit. The switch processes remote management packets only when they are received on an untagged port of the Default VLAN.

Note
The AT-S80 Management Software does not support remote management with the Telnet application protocol.

Remote SNMP Management

You can also remotely configure the switch using a Simple Network Management (SNMP) application such as AT-View. This management method requires an understanding of Management Information Base (MIB) objects.

Note
You must assign an IP address to the switch for remote SNMP management. For background information, see "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32.

Management Access Level

The AT-S80 Management Software has one management access level: manager. When you log in as a manager, you can view and configure all of the switch's operating parameters. You log in as a manager by entering the appropriate username and password when you start an AT-S80 management session. The default username is "manager" and the default password is "friend."

Ports 17 and 18 on the AT-FS750/16 Switch and Ports 25 and 26 on the AT-FS750/24 Switch

Ports 17 and 18 on the AT-FS750/16 switch and ports 25 and 26 on the AT-FS750/24 switch are dual ports. Each has one 10/100/1000Base-T twisted pair port and one transceiver slot for an optional SFP transceiver. Note the following when configuring these dual ports:

❒ By default, the twisted pair port of a dual port is the active port.

❒ An optional SFP port is activated when it establishes a link with an end node, at which point the affiliated twisted pair port changes to the redundant state.

❒ A twisted pair port and its affiliated optional SFP port share the same configuration settings, including port settings and VLAN assignments. When an SFP port establishes a link with an end node, it operates with the same settings as the twisted pair port.

Section I
Using the Menus Interface

The chapters in this section explain how to manage the switch using the menus interface of the AT-S80 management software. The chapters include:

❒   Chapter 2, "Getting Started with the Menus Interface" on page 25

❒   Chapter 3, "Basic Switch Parameters" on page 31

❒   Chapter 4, "Port Configuration" on page 53

❒   Chapter 5, "Port Trunking" on page 61

❒   Chapter 6, "IGMP Snooping" on page 71

❒   Chapter 7, "Static Multicast Address" on page 79

❒   Chapter 8, "Port Mirroring" on page 85

❒   Chapter 9, "Dial-in User Configuration" on page 91

❒   Chapter 10, "Virtual LANs" on page 97

❒   Chapter 11, "Simple Network Management Protocol (SNMP)" on page 119

❒   Chapter 12, "Quality of Service (QoS)" on page 139

❒   Chapter 13, "Rapid Spanning Tree Protocol (RSTP)" on page 149

❒   Chapter 14, "Bandwidth Control" on page 171

❒   Chapter 15, "IP Access List" on page 177

❒   Chapter 16, "Destination MAC Filter" on page 181

❒   Chapter 17, "802.1x Port-based Network Access Control" on page 185

❒   Chapter 18, "RADIUS Authentication Protocol" on page 201

❒   Chapter 19, "Management Software Updates" on page 207

Chapter 2

Getting Started with the Menus Interface

This chapter contains instructions on how to access the menus interface of the AT-S80 Management Software by starting a local management session. This chapter contains the following sections:

❒ "Starting a Local Management Session" on page 26

❒ "Using the Menus Interface" on page 28

❒ "Quitting from a Local Management Session" on page 29

Starting a Local Management Session

You establish a local management session with the switch by connecting a terminal or personal computer with a terminal emulation program to the the Console port on the front panel of the switch.

Note
The switch does not need an IP address when managed from a local management session.

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

1. Connect one end of the management cable included with the switch to the Console port on the switch, as shown in Figure 1.
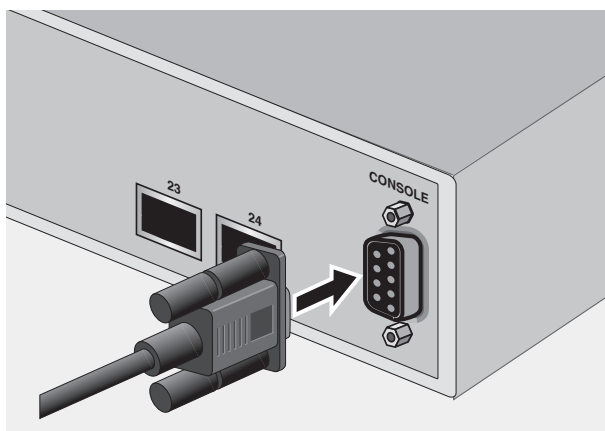
Figure 1. Connecting the Management Cable to the Console Port

2. Connect the other end of the cable to the RS-232 port on a terminal or PC with a terminal emulator program.

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

    ❒ Baud per second: 9600

    ❒ Data bits: 8

    ❒ Stop bits: 1

    ❒ Flow control: None

Note
These settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulation program. They cannot be changed.

The Login Menu is shown in Figure 2.

```
=========================================================
AT-FS750/16 Management System
Local - Console
Allied Telesis International Corp.
Copyright 2008
=========================================================
Login Menu

Login:
```

Figure 2. Login Menu

4. Enter the manager login name and press Return. The default name is "manager."

    You are prompted for a password.

5. Enter the manager password. The default password is "friend."

    Note
    The login name and password are case sensitive. To change the login name or password, refer to "Setting the User Interface Configuration" on page 38.

The Main Menu is shown in Figure 3.

```
Main Menu

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




Command>
```

Figure 3. Main Menu

Using the Menus Interface

If you are using a DEC VT00 or ANSI (the default) terminal configuration, refer to Table 1 for instructions on how to move through the menus and select menu options.

Table 1. Menus Interface Operations

When directed to	You must
Enter your selection	Type the menu option letter.
Enter information (for example, entering a port number)	Type the information and press Enter.
Return to previous menu	Type Q for Quit to Previous Menu.

When you press Enter to select a field in which you can enter a value, the ">" symbol is displayed. For example:

```
Enter new password>
```

The ">" symbol indicates that you can enter a new value for the parameter or change the existing value. After you have entered a value, press Enter. Changes are immediately activated on the switch.

Quitting from a Local Management Session

To quit from a local management session, return to the Main Menu and type **Q** for Quit. Always be sure to exit from a management session when you are finished. This can protect the switch from unauthorized changes to its configuration should you leave your workstation unattended.

Note
A local management session automatically times out if there is no management activity during a timeout period. The timeout feature is intended to protect the parameter settings on the switch from unauthorized changes should you leave your management station unattended during a management session. The default timeout value is 10 minutes. To change the timeout default value, refer to "Setting the User Interface Configuration" on page 38.

Chapter 3

Basic Switch Parameters

This chapter contains the following sections:

❐ "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32

❐ "Enabling and Disabling the DHCP Client" on page 35

❐ "Configuring System Administration Information" on page 36

❐ "Setting the User Interface Configuration" on page 38

❐ "Viewing Switch Information" on page 43

❐ "Rebooting the Switch" on page 46

❐ "Pinging a Remote System" on page 48

❐ "Returning the AT-S80 Management Software to the Factory Default Values" on page 51

Configuring the IP Address, Subnet Mask, and Gateway Address

This procedure explains how to manually assign an IP address, subnet mask, and gateway address to the switch. Note the following before performing the procedure:

❑ The switch does not need an IP address, subnet mask, or default gateway for normal network operations. These parameters must be assigned values only if you plan to remotely manage the device with a web browser from a management workstation on your network.

❑ A gateway address is only required if your remote management station is separated from the switch by a router.

❑ To configure the switch to obtain its IP configuration from a DHCP server on the network, go to "Enabling and Disabling the DHCP Client" on page 35.

To manually configure the switch's IP settings, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4.

```
Main Menu -> Basic Switch Configuration Menu

System [A]dministration Configuration
System [I]P Configuration
S[N]MP Configuration
[P]ort Configuration
[U]ser Interface Configuration
Rapid [S]panning Tree Configuration
[B]andwidth Control Configuration
IP Access [L]ist
Destination MAC [F]ilter
[Q]uit to previous menu




Command>
```

Figure 4. Basic Switch Configuration Menu

2. From the Basic Switch Configuration Menu, type **I** to select **System IP Configuration**.

    The System IP Configuration Menu is shown in Figure 5.

```
Basic Switch Configuration -> System IP Configuration Menu

MAC Address:        00:06:5H:B2:65:84
IP Address:         0.0.0.0
Subnet Mask:        0.0.0.0
Default Gateway:    0.0.0.0
DHCP Mode:          Disabled


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


Command>
```
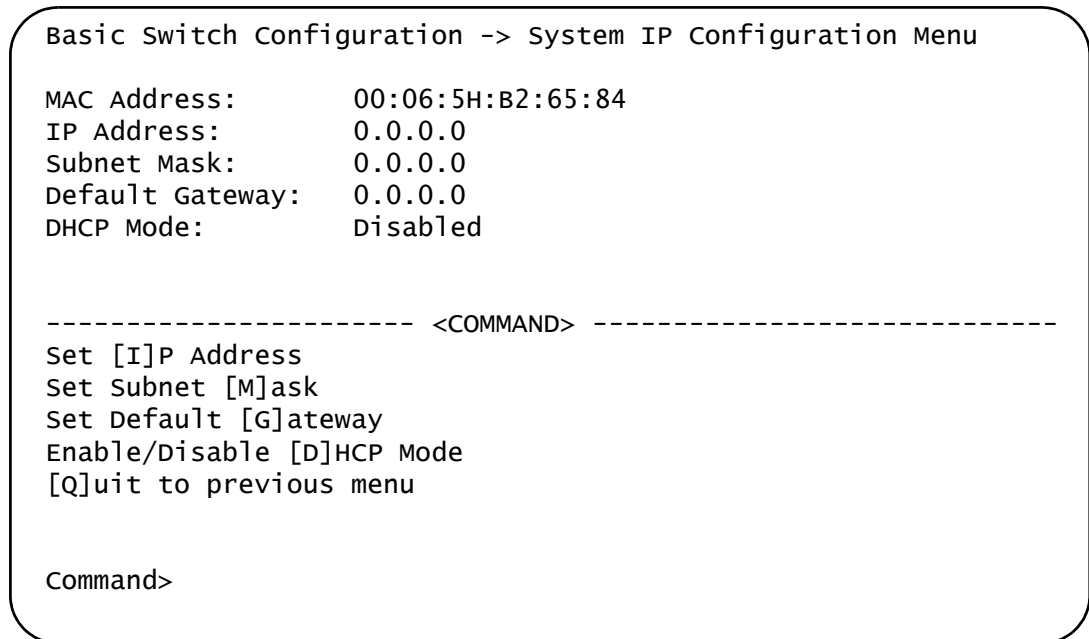
Figure 5. System IP Configuration Menu

The top portion of the menu displays the current IP address, subnet mask, and gateway address for the switch. The menu displays the switch's MAC address, which cannot be changed. The menu also displays the current status of the DHCP client on the switch.

The Enable/Disable DHCP Mode option is described in "Enabling and Disabling the DHCP Client" on page 35.

3. To set the switch's IP address, do the following:

    a. Type **I** to select **Set IP Address**.

        The following prompt is displayed:

        `Enter new IP address>`

    b. Type the IP address for the switch and press Enter.

4. To set the switch's subnet mask, do the following:

    a. Type **M** to select **Set Subnet Mask**.

        The following prompt is displayed:

        `Enter new subnet mask>`

b. Type the subnet mask for the switch and press Enter.

5. To set the switch's gateway address, do the following:

   a. Type **G** to select **Set Default Gateway**.

      The following prompt is displayed:

      `Enter new gateway IP address>`

   b. Type the gateway IP address for the switch and press Enter.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Enabling and Disabling the DHCP Client

This procedure explains how to activate and deactivate the DHCP client on the switch. When the client is activated, the switch obtains its IP configuration from a DHCP server on your network. Note the following before performing the procedure:

❐ The switch does not need an IP address, subnet mask, or default gateway for normal network operations. These parameters must be assigned values only if you plan to remotely manage the device with a web browser from a management workstation on your network.

❐ A gateway address is only required if your remote management station is separated from the switch by a router.

❐ The default setting for the DHCP client is disabled.

❐ The DHCP client does not support BOOTP servers.

To activate or deactivate the DHCP client, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

2. From the Basic Switch Configuration Menu, type **I** to select **System IP Configuration**.

   The System IP Configuration Menu is shown in Figure 5 on page 33.

3. Type **D** to select **Enable/Disable DHCP Mode**.

   The following prompt is displayed:

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

4. Type **E** to select Enable or **D** to select Disable.

   If activated, the client immediately begins to send queries to the DHCP server. It continues to send queries until it receives a response.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Configuring System Administration Information

This section explains how to assign a name to the switch. It also explains how to specify the location of the switch and the name of the switch's administrator. Entering this information is optional.

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

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

    The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

2. From the Basic Switch Configuration Menu, type **A** to select **System Administration Information**.

    The System Administration Configuration Menu is shown in Figure 6.

```
Basic Switch Configuration -> System Admin. Configuration Menu


Description:   AT-FS750/16
Object ID:
Name:
Location:
Contact:




---------------------- <COMMAND> ----------------------------
Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu


Command>
```

Figure 6. System Administration Configuration Menu

The Description parameter displays the model name of the switch. It cannot be changed.

3. To set the system's name, do the following:

    a. Type **N** to select **Set System Name**.

        The following prompt is displayed:

        ```
        Enter system name>
        ```

    b. Type a name for the switch (for example, Sales). The name is optional and can contain up to 50 characters.

Note
Allied Telesis recommends assigning a name to each switch. Names can make it easier for you to identify the various switches in your network and can also help you avoid performing a configuration procedure on the wrong switch.

Note
The Object ID field indicates the SNMP product ID or this switch. It is in the MIB object format. You cannot alter this field.

---

4. To enter the system's location, do the following:

    a. Type **L** to select **Set System Location**.

       The following prompt is displayed:

```
Enter system location>
```

    b. Type information to describe the location of the switch (for instance, Third Floor). The location is optional and can contain up to 50 characters.

5. To enter the administrator's name, do the following:

    a. Type **C** to select **Set System Contact Information**.

       The following prompt is displayed:

```
Enter system contact>
```

    b. Type the name of the network administrator responsible for managing the switch. The contact name is optional and can contain up to 50 characters.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting the User Interface Configuration

This procedure explains how to adjust the user interface and security features on the switch. With this procedure you can:

❐ Change the console timer, used to automatically end inactive local management sessions.

❐ Change the AT-S80 management login user name and password.

❐ Enable and disable the web server, used to manage the switch from a remote management station with a web browser.

For information about how to configure a dial-in user, see Chapter 9, "Dial-in User Configuration" on page 95.

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

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

The User Interface Configuration Menu is shown in Figure 7.

```
Basic Switch Configuration -> User Interface Configuration Menu

Console UI Idle Timeout:  5 Min.

Password Protection: Enabled
SNMP Agent:          Enabled
Web Server:          Enabled

Administrator List:
No. Username     Password   No. Username Password
--  --------     --------   --  ------- --------
1   manager      ******     2
3                           4
5                           6
7                           8


---------------------- <COMMAND> -----------------------------
Set [C]onsole UI Time Out          Enable/Disable [W]eb Server
Enable/Disable [S]NMP Agent        [R]ADIUS Server Configuration
[A]dd Administrator                [D]elete Administrator
[M]odify Administrator             Enable/Disable Password Pr[o]tection
[Q]uit to previous menu

Command>
```

Figure 7. User Interface Configuration Menu

The RADIUS Server Configuration option is described Chapter 18, "RADIUS Authentication Protocol" on page 207.

3. To configure the console idle time out parameter, do the following:

   a. Type **C** to select **Set Console UI Time Out.**

      The following prompt is displayed:

      ```
      Enter console idle timeout>
      ```

   b. Enter a number for the timeout value. The range is 0 to 60 minutes. The default is 5 minutes. A timeout value of 0 causes the switch to never timeout a local management session.

      The console idle time out parameter specifies the length of time a local management session can be inactive before the management software automatically ends it. The purpose of this parameter is to prevent unauthorized individuals from configuring the switch should you leave your management workstation unattended.

This parameter applies to a local management session but not to a remote web management session. A web browser management session remains active so long as your web browser is open.

Note
If you select 0, you must always remember to properly log off from a local management session when you are finished to prevent blocking future management sessions with the switch.

---

4. To enable or disable the web server, do the following:

   a. Type **W** to select **Enable/Disable Web Server**.

   The following prompt is displayed:

   `Enable or Disable web server (E/D)>`

   b. Type **E** to enable the web server or **D** to disable it. The default is enabled. If you disable the web server, you can not manage the switch from a remote management station using a web browser.

5. To enable or disable an SNMP agent, do the following:

   a. Type **S** to select **SNMP Agent**.

   The following prompt is displayed:

   `Enable or Disable SNMP agent (E/D)`

   b. Type **E** to enable an SNMP agent or **D** to disable the SNMP agent.

6. To add a new user and password, do the following:

   a. Type **A** to select **Add Administrator**.

   The following prompt is displayed:

   `Enter entry number>`

   b. Enter the number of the user name. You can select numbers 2 through 8.

   The following prompt is displayed:

   `Enter new user name>`

   c. Enter the name of a user.

   The following prompt is displayed:

   `Enter new password>`

d. Enter a password for the new user. You are prompted to reenter the password.

The following prompt is displayed:

```
Retype new password>
```

e. Retype the password for the new user.

7. To delete a user name, do the following:

a. Type **D** to select **Delete Administrator**.

The following prompt is displayed:

```
Enter entry number>
```

b. Enter the number of the user name that you want to delete. After you enter it, the Administrator List is refreshed.

8. To modify a user name, do the following

a. Type **M** to select **Modify Administrator**.

The following prompt is displayed:

```
Enter entry number>
```

b. Enter the number of the user name. You can select numbers 2 through 8.

The following prompt is displayed:

```
Choose which to be modified (U/P/B)>
```

c. Type **U** to change the user name.

The following prompt is displayed:

```
Enter new user name>
```

d. Enter the name of the new user. Type **P** to change the password.

The following prompt is displayed:

```
Enter new password>
```

e. Type the new password and press Enter. The password can be from 0 to 12 characters. Allied Telesis recommends not using special characters, such as spaces and exclamation points. The password is case sensitive. Not entering a new password deletes the current password without assigning a new one.

The following prompt is displayed:

`Retype new password.`

f. Enter the new password a second time. You must use the new login password the next time you start a local or web browser management session.

g. To change both the user name and its corresponding password, type **B**.

The following prompt is displayed:

`Enter new user name>`

h. Enter the name of the new user.

The following prompt is displayed:

`Enter new password>`

i. Enter the new password.

The following prompt is displayed:

`Retype new password>`

j. Reenter the new password.

9. To enable or disable password protection, type **O**.

The following prompt is displayed:

`Enable or Disable password protection (E/D)?>`

a. Type **E** to enable password protection or **D** to disable password protection.

You can control login authentication by enabling password protection which requires a user to supply a password when logging onto the switch. If you disable password protection, a user can login without inputting a password.

10.Type **Q** to select **Quit to previous menu** and save your changes.

Viewing Switch Information

To view general information about the switch, perform the following procedure:

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

    The General Information menu is shown in Figure 8.

```
Main Menu -> General Information


System up for: 24min(s), 36sec(s)


Runtime Image: Version AT-S80 V2.0.0 [1.1.1.57]
Boot Loader: Version 1.00.03
Hardware Information
  Version:                          DRAM Size:    16MB
  Fixed Baud Rate:   9600bps        Flash Size:   4 MB
Administration Information
  Switch Name: Marketing
  Switch Location: Fourth Floor
  Switch Contact: Ralph
System Address Information
  MAC Address:       00:06:5H:B2:65:84
  IP Address:        149.35.8.237
  Subnet Mask:       255.255.255.0
  Gateway:           149.35.8.1
Automatic Network Features
  DHCP Mode:         Disabled




Press any key to continue...
```

Figure 8. General Information Menu

The General Information Menu displays the following information:

System up for
The number of hours, minutes, and seconds since the last reset or power cycle.

Runtime Image
The version of the runtime software.

Boot Loader
The version of the boot loader software.

Hardware Information Section

Version
The hardware version number.

Fixed Baud Rate
The baud rate of the console port.

DRAM Size
The size of the DRAM, in megabytes.

Flash Size
The size of the flash memory, in megabytes.

Administration Information Section

Switch Name
The name of the switch. To assign a name, refer to "Configuring System Administration Information" on page 36.

Switch Location
The location of the switch. To specify the location, refer to "Configuring System Administration Information" on page 36.

Switch Contact
The contact person responsible for managing the switch. To specify a contact, refer to "Configuring System Administration Information" on page 36.

System Address Information Section

MAC Address
The MAC address of the switch. You cannot change a switch's MAC address.

System IP Address
The switch's IP address. Refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32 to manually assign an IP address or "Enabling and Disabling the DHCP Client" on page 35 to activate the DHCP client.

Subnet Mask
The switch's subnet mask. Refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32 to manually assign a subnet mask or "Enabling and Disabling the DHCP Client" on page 35 to activate the DHCP client.

Gateway
The switch's default gateway IP address. Refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32 to manually assign a gateway address or "Enabling and Disabling the DHCP Client" on page 35 to activate the DHCP client.

Automatic Network Features Section

DHCP Mode
The status of the DHCP client on the switch. For information about setting this parameter, refer to "Enabling and Disabling the DHCP Client" on page 35.

2. Press any key to return to the previous menu.

Rebooting the Switch

This procedure reboots the switch and reloads the AT-S80 management software from flash memory. You can reboot the device if you believe it is experiencing a problem. Rebooting the switch does not change any of the its parameter settings.

⚠ **Caution**
The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To reboot the switch, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 9.

```
Main Menu -> Switch Tools Configuration Menu

Software [U]pgrade...
System [R]eboot
[P]ing Execution
[Q]uit to previous menu




Command>
```

Figure 9. Switch Tools Configuration Menu

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

The System Reboot Menu is shown in Figure 10.

```
Main Menu -> System Reboot Menu

Reboot Status:          Stop
Reboot Type:            Normal


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


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




Command>
```

Figure 10. System Reboot Menu

3. From the System Reboot menu, type **O** to select **Set Reboot Option**.

    The following prompt is displayed:

    Select reboot option (F/I/N)>

4. Type **N** to select **Normal**.

    > **Note**
    > The **F** and **I** options are described in "Returning the AT-S80
    > Management Software to the Factory Default Values" on page 51.

5. Type **R** to select **Start Reboot Process**.

    The following prompt is displayed:

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

6. Type **Y** to start the reboot process or **N** to cancel the reboot.

    The switch immediately begins to reload the AT-S80 management
    software. This process takes approximately one minute to complete.
    You can not manage the device during the reboot. You can log in again
    after the reboot is finished if you want to continue to manage the
    device.

Pinging a Remote System

This procedure instructs the switch to ping a node on your network. This procedure is useful in determining whether an active link exists between the switch and another network device. Note the following before performing the procedure:

❐ The switch must have an IP address and subnet mask.

❐ The device to be pinged by the switch must be a member of the Default VLAN. It must be communicating with the switch through an untagged or tagged port of the Default VLAN.

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

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

   The Switch Tools Configuration Menu is shown in Figure 9 on page 46.

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

   The Ping Execution Menu is shown in Figure 11.

```
Switch Tools Configuration -> Ping Execution

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




----------------------- <COMMAND> -----------------------------
Set Target [I]P Address          [E]xecute Ping
Set [N]umber of Requests         [S]top Ping
Set [T]imeout Value              [Q]uit to previous menu


Command>
```

Figure 11. Ping Execution Menu

3. Type **I** to select **Set Target IP Address**.

   The following prompt is displayed:

   ```
   Enter new target IP address>
   ```

4. Type the IP address of the node the switch is to ping and press Enter.

5. Type **N** to select **Set Number of Requests**.

   The following prompt is displayed:

   ```
   Enter new number of requests>
   ```

6. Enter the number of ping requests you want the switch to perform. The range is 1 to 10. The default is 10.

7. Type **T** to select **Set Timeout Value**.

   The following prompt is displayed:

   ```
   Enter new timeout value>
   ```

8. Enter the length of time in seconds the switch is to wait for a response before assuming that a ping has failed. The range is 1 to 5 seconds. The default is 3 seconds.

9. Type **E** to select **Execute Ping**.

   The following prompt is displayed:

   ```
   Execute ping or Clean ping data (E/C)>
   ```

10. Type **E** to execute the ping or **C** to clear previous ping data.

Figure 12 shows an example of the results of a ping.

```
Switch Tools Configuration -> Ping Execution

Target IP Address:     149.35.8.33
Number of Requests:    4
Timeout Value (sec):   3
================Result=================
      No. 1                20 ms
      No. 2                20 ms
      No. 3                20 ms
      No. 4                20 ms


---------------------- <COMMAND> ----------------------------
Set Target [I]P Address            [E]xecute Ping
Set [N]umber of Requests           [S]top Ping
Set [T]imeout Value                [Q]uit to previous menu


Command>
```

Figure 12. Ping Results

11. To stop the ping, type **S** to select **Stop Ping**.

12. Type **Q** to select **Quit to previous menu**.

Returning the AT-S80 Management Software to the Factory Default Values

This procedure returns all AT-S80 Management Software parameters to their default values. The default values are listed in Appendix A, "AT-S80 Software Default Settings" on page 339.

⚠ **Caution**
This procedure reboots the switch. The device does not forward network traffic during the reboot process. Some network traffic may be lost.

To return the AT-S80 management software to its default settings, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 9 on page 46.

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

   The System Reboot menu is shown in Figure 10 on page 47.

3. Type **O** to select **Set Reboot Option**.

   The following prompt is displayed:

   ```
   Select reboot option (F/I/N)>
   ```

4. Type **F** or **I** to select one of the following:

   F (Factory Default)
   Resets all switch parameters to the factory default settings, including IP address, subnet mask, and gateway address. If the DHCP client is enabled, this selection disables it.

   I (Reset to Defaults Except IP Address)
   Resets all switch parameters to the factory default settings, but retains the IP address, subnet mask, and gateway settings. If the DHCP client is enabled, it remains enabled after this reset.

   Note
   Option **N** is described in "Rebooting the Switch" on page 46.

5. Type **R** to select **Start Reboot Process**.

   The following prompt is displayed:

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

6. Type **Y** to start the reboot process.

   The switch returns its operating parameters to the default values and begins to reload the AT-S80 Management Software. This process takes approximately one minute to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the device.

Chapter 4

Port Configuration

This chapter contains the procedures for viewing and adjusting the parameter settings for the ports on the switch. This chapter contains the following sections:

❐ "Displaying the Port Parameters" on page 54

❐ "Enabling and Disabling a Port" on page 56

❐ "Setting a Port's Speed and Duplex Mode" on page 57

❐ "Changing the Flow Control Setting" on page 59

Displaying the Port Parameters

To display the parameter settings for the ports on the switch, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Port Configuration Menu is shown in Figure 13.

```
Basic Switch Configuration -> Port Configuration Menu

Port   Trunk     Type      Link   Status     Mode             Flow Ctrl
----   -----     ------    ----   ------     --------------------
 1     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
 2     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
 3     ---       10/100TX  Up     Enabled          100-FDx    Enabled
 4     ---       10/100TX  Up     Enabled    Auto  (10F)      Enabled
 5     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
 6     ---       10/100TX  Down   Enabled    Auto             Enabled
 7     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
 8     ---       10/100TX  Down   Enabled    Auto             Enabled
 9     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
10     ---       10/100TX  Up     Enabled          10-FDx     Enabled
11     ---       10/100TX  Up     Enabled          10-FDx     Enabled
12     ---       10/100TX  Up     Enabled    Auto  (100F)     Enabled
----------------------- <COMMAND> ----------------------------------
[N]ext Page             Set [S]tatus       Set [F]low Control
[P]revious Page         Set [M]ode         [Q]uit to previous menu


Command>
```

Figure 13. Port Configuration Menu

The Port Configuration Menu displays the following columns of information:

Port
The port number.

Trunk
The trunk group number. This column contains the number of the port trunk if the port is a member of a trunk. To configure a trunk, refer to Chapter 5, "Port Trunking" on page 61.

Type
The port type. The port type will be one of the following:

❑ 10/100BaseTX - Base ports.

❑ 1000TX - Uplink 10/100/1000Base-TX twisted pair ports.

❑ 1000BaseX - Optional fiber optic SFP module.

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

Up - A link exists between the port and the end node.

Down - The port has not established a link with an end node.

Status
The current operating status of the port. The possible values are:

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

Disabled - The port was manually disabled.

To change a port's status, see "Enabling and Disabling a Port" on page 56.

Mode
The port's speed and duplex mode setting. The possible values are:

Auto - The port is using Auto-Negotiation to set its operating speed and duplex mode. This is the default setting. The actual operating speed and duplex mode are displayed in parentheses (for example, "Auto (100F)" for 100 Mbps full duplex mode).

If the speed and duplex mode were set manually on a port, the Mode column will be one of the following:

❑ 10-HDx - 10 Mbps, half-duplex mode

❑ 100-HDx - 100 Mbps, half-duplex mode

❑ 10-FDx - 10 Mbps, full-duplex mode

❑ 100-FDx - 100 Mbps, full-duplex mode

❑ 1000-FDx - 1000 Mbps, full-duplex mode (uplink ports only)

To change a port's speed and duplex mode setting, see "Setting a Port's Speed and Duplex Mode" on page 57.

Flow Ctrl
Whether flow control is enabled on the port. Flow control is enabled by default. To disable flow control, refer to "Changing the Flow Control Setting" on page 59.

3. Type **Q** to select **Quit to previous menu**.

Enabling and Disabling a Port

This procedure allows you to enable or disable a port. A disabled port does not forward any ingress or egress packets. You may want to disable a port if a problem occurs with the node or cable connected to the port. After the problem is fixed, you can enable the port to resume normal operation. You can also disable an unused port to secure it from unauthorized connections. The default setting for a port is enabled.

To change the port's status, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32

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

   The Port Configuration Menu is shown in Figure 13 on page 54.

3. Type **S** to select **Set Status**.

   The following prompt is displayed:

   ```
   Set Status->Enter port number>
   ```

4. Enter the number of the port to enable or disable. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enable or Disable port n (E/D)>
   ```

5. Type **E** to enable the port or **D** to disable it. The default is enabled. A disabled port immediately stops forwarding all ingress and egress traffic until you enable it again.

   The display is refreshed to show the port's new status.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting a Port's Speed and Duplex Mode

To change a port's speed or duplex mode, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 4 on page 32

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

    The Port Configuration Menu is shown in Figure 13 on page 54.

3. Type **M** to select **Set Mode**.

    The following prompt is displayed:

    ```
    Set Mode -> Enter port number >
    ```

4. Enter the number of the port whose speed or duplex mode you want to change. You can configure only one port at a time.

    The following prompt is displayed:

    ```
    Enter new mode for port n (a/h/H/f/F/T)>
    ```

5. Enter the letter that corresponds to the desired speed and duplex mode setting for the port. The port settings are:

    a - Auto: The port uses Auto-Negotiation to set its speed and duplex mode. This is the default setting for all ports.

    h - 10 Mbps, half-duplex

    f - 10 Mbps, full-duplex

    H - 100 Mbps, half-duplex

    F - 100 Mbps, full-duplex

    T - 1000 Mbps, full-duplex (uplink ports only)

    When selecting a setting, note the following:

    ❒   The selections are case sensitive. For example, you must enter a lowercase letter "a" to select Auto-Negotiation.

    ❒   When a twisted pair port on the switch is set to Auto-Negotiation, the default setting, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a

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

❒ For 1000 Mbps operation on an uplink 10/100/1000Base-T twisted pair uplink port, Allied Telesis recommends using Auto-Negotiation. Setting the speed and duplex mode manually to 1000 Mbps full duplex is not recommended.

❒ The only valid setting for an optional SFP port is Auto-Negotiation.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Changing the Flow Control Setting

Flow control applies to ports operating in full-duplex mode. A switch port uses flow control to control the flow of ingress packets from its end node. A port using flow control issues a special frame, referred to as a PAUSE frame, as specified in the IEEE 802.3x standard, to stop the transmission of data from an end node. When a port needs to stop an end node from transmitting data, it issues this frame. The frame instructs the end node to cease transmission. The port continues to issue PAUSE frames until it is ready again to receive data from the end node.

To change the flow control setting on a port, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32

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

   The Port Configuration Menu is shown in Figure 13 on page 54.

3. Type **F** to select **Set Flow Control**.

   The following prompt is displayed:

   ```
   Set Flow Control -> Enter port number >
   ```

4. Type the port number whose flow control setting you want to change. Then press Enter. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enable or Disable flow control for port <n> (E/D)>
   ```

5. Type **E** to enable flow control or **D** to disable it. The default is enabled.

   The display is refreshed to show the port's new flow control setting.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 5
Port Trunking

This chapter provides information and procedures for creating a port trunk and contains the following sections:

❒ "Port Trunking Overview" on page 62

❒ "Creating a Port Trunk" on page 64

❒ "Modifying a Port Trunk" on page 67

❒ "Enabling and Disabling a Port Trunk" on page 69

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. A port trunk is 2 to 8 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.

Port Trunking Guidelines

Observe the following guidelines when creating a port trunk:

❒ A port trunk can consist of up to 8 ports.

❒ The switch can support up to 7 trunks.

❒ A port can belong to only one trunk at a time.

❒ The ports of a 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 on all the ports in a trunk.

❒ The ports of a trunk must be members of the same VLAN.

❒ The ports of a trunk do not have to be consecutive.

❒ When you cable a trunk, the order of the connection 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-FS750 switches. On the first AT-FS750 switch, select ports 1 through 4 for a trunk. On the second AT-FS750 switch, select ports 6 through 9. To maintain the order of the port connections, connect port 1 on the first AT-FS750 switch to port 6 on the second AT-FS750 switch, port 2 to port 7, and so on.

❒ To avoid compatibility problems, Allied Telesis recommends that both switches connected by a trunk are AT-FS750 switches. A port trunk between an AT-FS750 switch and another switch model might result in undesirable trunk behavior.

❒ Trunk 7 is reserved for the uplink ports 17 and 18 on the AT-FS750/16 switch and ports 25 and 26 on the AT-FS750/24 switch. You cannot add or remove ports from this trunk. To use the uplink ports as a port trunk, activate Trunk 7 as explained in "Enabling and Disabling a Port Trunk" on page 69.

Creating a Port Trunk

This procedure explains how to create a port trunk.

⚠️ **Caution**

Do not connect the cables to the ports on the switches until after you have configured the trunk with the management software. Connecting the cables before configuring the software can create a loop in the network topology. A loop can cause a broadcast storm and poor network performance.

To create a port trunk, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14.

```
Main Menu -> Advanced Switch Configuration Menu

[V]LAN Management
[T]runk Configuration
[I]GMP Snooping Configuration
Static Multicast [A]ddress Configuration
Quality of [S]ervice Configuration
Port [M]irroring Configuration
[D]ial-in User Configuration
802.1[X] Port Based Access Control Configuration
[Q]uit to previous menu



Command>
```

Figure 14. Advanced Switch Configuration Menu

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

The Trunk Configuration Menu is shown in Figure 15.

```
AT-FS750/24 Local Management System
Advanced Switch Configuration -> Trunk Configuration Menu

Group      Status          Port Members            Trunk ID
-------    --------------  --------------------    ----------
  1        Disabled                                    1
  2        Disabled                                    2
  3        Disabled                                    3
  4        Disabled                                    4
  5        Disabled                                    5
  6        Disabled                                    6
  7        Disabled        25, 26                      7




---------------------- <COMMAND> ----------------------------
[A]dd Trunk Member                      [S]et Trunk Status
[R]emove Trunk Member                   [Q]uit to previous menu


Command>
```

Figure 15. Trunk Configuration Menu

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

    The following prompt is displayed:

    ```
    Enter trunk group number>
    ```

4. Select a trunk group number from 1 to 7 and press Enter.

    The following prompt is displayed:

    ```
    Enter port members (up to 8 ports) for trunk n>
    ```

5. Enter the ports you want to include in the trunk and press Enter.

    You can specify the ports individually separated by commas (for example, 1,2,5), as a range of ports separated by a hyphen (for example, 2-4), or both (for example, 4,6,11-14).

6. Type **S** to select **Set Trunk Status**.

    The following prompt is displayed:

    ```
    Enter trunk group number>
    ```

7. Type the trunk group number and press Enter.

The following prompt is displayed:

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

8. Type **E** to enable the trunk.

9. Type **Q** to select **Quit to previous menu** and save your changes.

   The trunk is now operational on the switch.

10. Configure the port trunk on the other switch and connect the cables.

Modifying a Port Trunk

This procedure adds and removes ports from a port trunk.

> ⚠ **Caution**
> Disconnect the cables from the ports of the trunk before you modify the trunk. Leaving the cables connected can create a loop in the network topology. A loop can cause a broadcast storm and poor network performance.

> **Note**
> You cannot modify Trunk 7, which is reserved for the uplink ports. If you want to use the uplink ports as a port trunk, activate Trunk 7 as explained in "Enabling and Disabling a Port Trunk" on page 69.

To add or remove ports from a trunk, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The Trunk Configuration Menu is shown in Figure 15 on page 65.

3. To add ports to a port trunk, type **A** to select **Add Trunk Member**. To remove ports, type **R** to select **Remove Trunk Member**.

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

4. Type the number of the trunk group you want to modify and press Enter.

   The following prompt is displayed where *n* represents the port trunk number:

   ```
   Enter port members (from 1 to 24, up to 8 ports) for
   trunk n >
   ```

5. Type the ports you want to add or remove from the trunk. Then press Enter.

You can specify the ports individually separated by commas (for example, 1,2,5), as a range of ports separated by a hyphen (for example, 2-4), or both (for example, 4,6,11-14).

6. Type **Q** to select **Quit to previous menu** and save your changes.

7. Modify the port trunk on the other switch and reconnect the cables.

Enabling and Disabling a Port Trunk

This procedure enables and disables a port trunk. Note the following before performing this procedure:

❒ Do not enable a port trunk until after you have configured the trunk on both switches.

❒ Do not connect the cables to the ports on the switches until after you have configured and enabled the trunk on both switches.

❒ The ports of a disabled trunk forward traffic as individual ports.

Note
Before disabling a port trunk, disconnect all cables from the ports of the trunk. Leaving the cables connected can create a loop in your network topology. A loop can cause a broadcast storm and poor network performance.

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

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The Trunk Configuration Menu is shown in Figure 15 on page 65.

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

   The following prompt is displayed:

   `Enter trunk group number>`

Note
Port members must be in the same VLAN or you will receive an error message and the ports will not be added to a trunk.

---

4. Type the number of the trunk group you want to enable or disable and press Enter.

   The following prompt is displayed:

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

5. Type **E** to enable the trunk or **D** to disable it.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 6
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" on page 72

❒ "Configuring IGMP Snooping" on page 74

IGMP Snooping Overview

IGMP enables IPv4 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 that wants to become a member of a multicast group responds to a query by sending a *report*. A report indicates an end node's desire to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. After becoming a member of a multicast group, a host node must continue to periodically issue reports to remain a member.

After 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.

There are three versions of IGMP — versions 1, 2, and 3. One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1, it 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*. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets from the port to which the node is connected if it determines there are no further host nodes on the port.

Version 3 adds the ability of host nodes to join or leave specific sources in a multicast group.

The IGMP snooping feature supports IGMP versions 1 and 2. The AT-FS750 switches monitor the flow of queries from a router as well as report leave messages from host nodes to build its own multicast membership lists. Both switches use the lists to forward multicast packets to switch ports where there are host nodes who 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 needs to flood multicast packets from all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact network performance.

The AT-FS750 switches maintain a list of multicast groups through an adjustable timeout 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.

Configuring IGMP Snooping

The procedures in this section describe how to enable or disable IGMP snooping, set the age-out timer, and view group members. See the following procedures:

❑ "Enabling or Disabling IGMP Snooping" on page 74

❑ "Setting the Age-out Timer" on page 76

❑ "Setting Group Members" on page 76

Enabling or Disabling IGMP Snooping

To activate or deactivate IGMP snooping on the switch, perform the following procedure:

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

    The Advanced Switch Configuration Menu is shown in Figure 16.

```
Main Menu -> Advanced Switch Configuration Menu

[V]LAN Management
[T]runk Configuration
[I]GMP Snooping Configuration
Static Multicast [A]ddress Configuration
Quality of [S]ervice Configuration
Port [M]irroring Configuration
[D]ial-in User Configuration
802.1[X] Port Based Access Control Configuration
[Q]uit to previous menu




Command>
```

Figure 16. Advanced Switch Configuration Menu

2. From the Advanced Switch Configuration Menu, type **I** to select **IGMP Snooping Configuration**.

The IGMP Snooping Configuration Menu is shown in Figure 17.

```
Advanced Switch Configuration -> IGMP Snooping Configuration Menu

IGMP Snooping Status:        Disabled
IGMP Snooping Age-Out Timer:  280 seconds

Multicast Group Address
-----------------------




-------------------------------<COMMAND>-----------------------------
[N}ext Page                          [E]nable/Disable IGMP Snooping
[P]revious Page                      [S]et Age-Out Timer
[V]iew Group Members                 [Q]uit to previous menu


Command>
```

Figure 17. IGMP Snooping Configuration Menu

3. From the SNMP Configuration Menu, type **E** to select **Enable/Disable IGMP Configuration**.

   The following prompt is displayed:

   Enable or Disable IGMP snooping (E/D) >

4. Type **E** to enable IGMP snooping or **D** to disable IGMP snooping.

   By default, IGMP snooping is disabled.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Setting the Age-out Timer

Use the following procedure to set the age-out timer.

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

   The Advanced Switch Configuration Menu is shown in Figure 16 on page 74.

2. From the Advanced Switch Configuration Menu, type **I** to select **IGMP Snooping Configuration**.

   The IGMP Configuration Menu is shown in Figure 17 on page 75.

3. From the SNMP Configuration Menu, type **S** to select **Set Age-Out Timer**.

   The following prompt is displayed:

   ```
   Enter age-out time>
   ```

   For an IGMP member port, the Set Age-Out Timer is set to 280 seconds by default. The range of this parameter is from 280 to 420 seconds.

   For an IGMP router port, the Set Age-Out Timer is set to 130 seconds by default. This value cannot be changed.

4. Type the number of seconds that you want the switch to wait before it purges an inactive dynamic MAC address which is called the aging time. Enter a value between 280 and 420 seconds.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Setting Group Members

To set the MAC addresses of IGMP group members, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 16 on page 74.

2. From the Advanced Switch Configuration Menu, type **I** to select **IGMP Configuration**.

   The IGMP Configuration Menu is shown in Figure 17 on page 75.

3. From the IGMP Configuration Menu, type **V** to select **View Group Members**.

The following prompt is displayed:

`Enter MAC Address (xx:xx:xx:xx:xx:xx)>`

4. Enter a Multicast Group MAC address in the format xx:xx:xx:xx:xx.

   The range of the multicast MAC address is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.

   The IGMP Configuration Menu is updated with the information.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 7
Static Multicast Address

This chapter explains how to assign static multicast addresses. Sections in the chapter include:

❐ "Static Multicast Address Overview" on page 80

❐ "Creating a Static Multicast Address" on page 81

Static Multicast Address Overview

There are 4 ways to populate the database of a MAC address table:

❒ Static unicast addresses which can only be assigned to one port

❒ Static multicast addresses which can be assigned to multiple ports

❒ Broadcast addresses which are broadcast to all of the ports on a switch

❒ Dynamically learned MAC addresses

If you want the MAC address table to act as a forwarding database, configure it with static multicast MAC addresses.

The Static Multicast Address feature allows you to assign an IP address to more than one host. This feature is used for video streaming when you also enable IGMP snooping. For more information about configuring IGMP snooping, see Chapter 6, "IGMP Snooping" on page 71.

For the static multicast address, the MAC addresses are prelearned. This means that you can assign a MAC address before you create a physical connection to a host.

Creating a Static Multicast Address

The procedures in this section describe how to create, delete, and modify static multicast addresses. See the following procedures:

❐ "Adding a Static Multicast Address" on page 81

❐ "Deleting a Static Group" on page 82

❐ "Deleting a Static Member Port" on page 83

Adding a Static Multicast Address

To assign a static multicast address or to assign a group number to an existing group MAC address, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **A** to select **Static Multicast Address Configuration**.

   The Static Multicast Address Table Menu is shown in Figure 18.

```
Advanced Switch Configuration -> Static Multicast Address Table Menu

Group MAC Address    Group Members
-----------------    --------------------------------------------
01:00:5E:00:01:00    1
01:00:5E:00:01:01    2
01:00:5E:00:01:02    3, 4,5,6
01:00:5E:00:01:03    7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18
01:00:5E:00:01:04    19, 20
01:00:5E:00:01:05    21
01:00:5E:00:01:06    22



-----------------------------<COMMAND>-----------------------------
[N}ext Page        [A]dd Static Member Port      Delete Static [G]roup
[P]revious Page    [D]elete Static Member Port   [Q]uit to previous menu


Command>
```

Figure 18. Static Multicast Address Table Menu

3. Type **A** to select **Add Static Member Port**.

The following prompt is displayed:

```
Enter MAC address for multicast entry >
```

4. Type a multicast MAC address. Then press enter. The range of acceptable multicast MAC addresses is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.

    The following prompt is displayed:

    ```
    Select group member >
    ```

5. Enter a group member in the range of 1 to 24.

    You can add more than one group member at a time. You can specify the values individually (for example, 2,5,11), as a range (for example, 4-7), or both (for example, 2,5,11-15).

6. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a Static Group

To delete a group from a Group MAC address, perform the following procedure.

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **A** to select **Static Multicast Address Configuration**.

    The Static Multicast Address Table Menu is shown in Figure 18 on page 81.

3. Type **G** to select **Delete Static Group**.

    The following prompt is displayed:

    ```
    Enter MAC address for multicast entry >
    ```

4. Type a multicast MAC address. Then press enter. The range of acceptable multicast MAC addresses is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.

    The following prompt is displayed:

    ```
    Select group member >
    ```

5. Enter a group member in the range of 1 to 24.

You can add more than one group member at a time. You can specify the values individually (for example, 2,5,11), as a range (for example, 4-7), or both (for example, 2,5,11-15).

6. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a Static Member Port

To delete a group from a Group MAC address, perform the following procedure.

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **A** to select **Static Multicast Address Configuration**.

   The Static Multicast Address Table Menu is shown in Figure 18 on page 81.

3. Type **D** to select **Delete Static Member Port**.

   The following prompt is displayed:

   ```
   Enter MAC address for multicast entry >
   ```

4. Type a multicast MAC address. Then press enter. The range of acceptable multicast MAC addresses is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.

   The following prompt is displayed:

   ```
   Select group member >
   ```

5. Enter a group member in the range of 1 to 24.

   You can add more than one group member at a time. You can specify the values individually (for example, 2,5,11), as a range (for example, 4-7), or both (for example., 2,5,11-15).

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 8

Port Mirroring

This chapter provides a description of the Port Mirroring feature and contains procedures for setting up this feature. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by copying the traffic to another port. This chapter contains the following sections:

❐ "Port Mirroring Overview" on page 86

❐ "Configuring Port Mirroring" on page 87

❐ "Enabling or Disabling Port Mirroring" on page 89

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the ingress and egress traffic on a port by copying the traffic to another port. You can connect a network analyzer to the port where the traffic is copied and monitor it without impacting performance or speed.

The port whose traffic you want to mirror is called the *mirrored port*. The port where the traffic will be copied to is called the *mirroring port*.

Observe the following guidelines when using this feature:

❒ You can mirror only one port at a time.

❒ The mirrored and mirroring ports must be on the same switch.

❒ This feature copies both the ingress and egress traffic of the mirrored port.

❒ The mirroring port cannot be used for normal Ethernet switching.

Configuring Port Mirroring

To set up port mirroring, perform the following procedure:

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

    The Advanced Switch Configuration Menu is shown in Figure 16 on page 70.

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

    The Port Mirroring Menu is shown in Figure 19.

```
Advanced Switch Configuration -> Port Mirroring Configuration Menu


Status:          Disabled
Mirroring Port:   1
Ingress Port:
Egress Port:


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


Command>
```

Figure 19. Port Mirroring Menu

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

    The following prompt is displayed:

    `Set monitoring port-> Enter port number>`

4. Type the number of the port where the network analyzer is connected and press Enter. You can specify only one port.

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

    The following prompt is displayed:

    `Set monitored port-> Enter port number>`

6. Type the number of the port whose ingress and egress traffic you want to monitor and press Enter. You can specify only one port.

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

    The following prompt is displayed:

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

8. Type **E** to enable port mirroring.

    You can now connect your data analyzer to the mirroring port.

9. Type **Q** to select **Quit to previous menu** and save your changes.

Enabling or Disabling Port Mirroring

To enable or disable port mirroring on the switch, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The Port Mirroring Menu is shown in Figure 19 on page 87.

3. Type **E** to select **Set Mirroring Status**.

   The following prompt is displayed:

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

4. Type **D** to disable port mirroring.

   The port that was functioning as the mirroring port can now be used as a normal networking port.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 9
Dial-in User Configuration

This chapter describes the Dial-in User feature and provides procedures for configuring this feature. Sections in the chapter include:

❐ "Dial-in User Configuration Overview" on page 92

❐ "Configuring a Dial-in User" on page 93

Dial-in User Configuration Overview

The Dial-in User Configuration feature allows you to add and delete, and modify dial-in users to the AT-FS750 switch. In addition, you must assign each dial-in user a password and a VLAN. See Chapter 10, "Virtual LANs" on page 97 for more information about VLANs and VIDs.

To configure a system administrator or set user information for the switch, see Chapter 3, "Basic Switch Parameters" on page 31.

Configuring a Dial-in User

The procedures in this section describe how to create, delete, and modify dial-in users. See the following procedures:

- ❑ "Adding a Dial-in User" on page 93
- ❑ "Deleting a Dial-in User" on page 94
- ❑ "Modifying a Dial-in User" on page 95

Adding a Dial-in User

To add a dial-in user, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **D** to select **Dial-in User Configuration**.

   The Dial-in User Configuration Menu is shown in Figure 20.

```
Advanced Switch Configuration -> Dial-in User Configuration Menu

User Name           Password                    Dynamic VLAN
----------------    -----------------------     ------------------
Jenny               *****                       2
Jill                *******                     2
Ellen               *****                       3
MaryAnn             ******                      3
Tom                 *****                       3
Sam                 *****                       1



------------------------------<COMMAND>-----------------------------
[N]ext Page                   [D]elete User
[P]revious Page               [M]odify User
[A]dd User                    [Q]uit to previous menu

Command>
```

Figure 20. Dial-in User Configuration Menu

3. Type **A** to select **Add User**.

   The following prompt is displayed:

   ```
   Enter dial-in user name >
   ```

4. Type a name of a dial-in user. Then press Enter.

   The following prompt is displayed:

   ```
   Enter dial-in user password >
   ```

5. Enter the password of the dial-in user.

   The following prompt is displayed:

   ```
   Enter dial-in user dynamic VLAN ID >
   ```

6. Assign the dial-in user to a VLAN by entering a VID.

7. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a Dial-in User

To delete a dial-in user, perform the following procedure.

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **D** to select **Dial-in User Configuration**.

   The Dial-in User Configuration Menu is shown in Figure 20 on page 93.

3. Type type **D** to select Delete User.

   The following prompt is displayed:

   ```
   Enter dial-in user name >
   ```

4. Type the name of the dial-in user that you want to delete.

   The dial-in user name is removed from the Dial-in User Configuration Menu.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Modifying a Dial-in User

To change the password or the VLAN assignment of a dial-in user, perform the following procedure.

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **D** to select **Dial-in User Configuration**.

    The Dial-in User Configuration Menu is shown in Figure 20 on page 93.

3. Type type **M** to select Modify User.

    The following prompt is displayed:

    ```
    Enter dial-in user name >
    ```

4. Type the name of the dial-in user that you want to modify.

    The following prompt is displayed:

    ```
    Enter dial-in user password >
    ```

5. Type the password of the dial-in user. You may type in a new password or the existing password.

    The following prompt is displayed:

    ```
    Enter dial-in user dynamic VLAN ID >
    ```

6. Type the VID of the dial-in user. You may type in a new VID or the existing VID.

7. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 10

Virtual LANs

This chapter contains the procedures for creating, modifying, and deleting port-based and tagged Virtual Local Area Networks (VLANs). This chapter contains the following sections:

❑ "VLAN Overview" on page 98

❑ "Port-based VLAN Overview" on page 100

❑ "Tagged VLAN Overview" on page 101

❑ "Creating a VLAN" on page 103

❑ "Configuring the PVID of Untagged Ports" on page 107

❑ "Displaying the VLANs" on page 111

❑ "Resetting a VLAN to the Default Value" on page 113

❑ "Modifying a VLAN" on page 114

❑ "Deleting a VLAN" on page 116

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.

With VLANs, you can segment your network through the switch's AT-S80 management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

❐ Improved network performance

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

VLANs improve network perform 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.

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

❐ Increased security

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

❐ Simplified network management

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

But with VLANS, you can change the LAN segment assignment of an end node connected to the switch through the switch's AT-S80 management software. You can change the VLAN memberships through the management software without moving the workstations physically, or changing group memberships by moving cables from one switch port to another.

In addition, 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.

The AT-FS750 switches support the following types of VLANs you can create yourself:

❐ Port-based VLANs

❐ Tagged VLANs

These VLANs are described in the following sections.

Port-based VLAN Overview

As explained in "VLAN Overview" on page 98, a VLAN consists of a group of ports on an Ethernet switch that form an independent traffic domain. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on an AT-FS750 Fast Ethernet Switch that form a logical Ethernet segment.

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.

The parts of a port-based VLAN in the AT-S80 management software are:

❑ VLAN name

❑ Group ID

VLAN Name

To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are be members of the VLAN. Examples include Sales, Production, and Engineering.

Group ID

Each VLAN in a network must have a unique number assigned to it. This number is called the Group ID. This number uniquely identifies a VLAN in the switch.

Each port of a port-based VLAN can belong to as many VLANs as needed. Therefore, traffic can be forwarded to the members of the groups to which the port is assigned. For example, port 1 and port 2 are members of group 1 and ports 1 and 3 are members of group 2. In this case, traffic from port 1 is forwarded to ports 2 and 3, traffic from port 2 is forwarded only to port 1, and traffic from port 3 is forwarded only to port 1.

General Rules for Creating a Port-based VLAN

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

❑ Each port-based VLAN must be assigned a name.

❑ Each port-based VLAN must be assigned to one or more Group IDs. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches should be assigned the same Group ID.

❑ 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.

❑ The AT-FS750/16 and AT-FS750/24 switches can support up to 256 port-based VLANs.

Tagged VLAN Overview

The second type of VLAN supported by the AT-S80 management software is the *tagged VLAN*. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port and the VLAN configuration of each port.

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 Group ID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports whose Group ID equals the VLAN tag.

A port to receive or transmit 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 parts of a tagged VLAN are:

❑ VLAN Name

❑ Group ID

❑ Tagged and Untagged Ports

❑ Port VLAN identifier (PVID)

Tagged and Untagged Ports

When you specify that a port is a member of a tagged VLAN, you need to specify that it is tagged or untagged. You can have a combination of tagged and untagged ports in the same VLAN.

Packet transmission from a tagged port differs from packet transmission from an untagged port. When a packet is transmitted from a tagged port, the tagged information within the packet is maintained when it is transmitted to the next network device. If the packet is transmitted from an untagged port, the VLAN tag information is removed from the packet before it is transmitted to the next network device.

The IEEE 802.1Q standard describes how tagging information within a packet is used to forward or discard traffic throughout the switch. If the incoming packet has a VLAN tag that matches one of the Group IDs of which the port is a member, the packet is accepted and forwarded to the appropriate port(s) within that VLAN. If the incoming packet's VLAN tag does not match one of the Group IDs assigned to the port, the packet is discarded.

Port VLAN Identifier

When an untagged packet is received on a port in a tagged VLAN, it is assigned to one of the VLANs of which that port is a member. The deciding factor in this process is the Port VLAN Identifier (PVID). Both tagged and untagged ports in a tagged VLAN must have a PVID assigned to them. The default value of the PVID for each port is 1. The switch associates a received untagged packet to the Group ID that matches the PVID assigned to the port. As a result, the packet is only forwarded to those ports that are members of that VLAN.

General Rules for Creating a Tagged VLAN

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

❐ Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VID.

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

❐ The AT-FS750/16 and AT-FS750/24 switches can support up to 48 tagged VLANS.

Creating a VLAN

This section contains the procedure for creating a new port-based or tagged VLAN. This procedure assigns the VLAN a name, a VID number, and the untagged and tagged member ports.

After you have performed this procedure, you must configure the untagged ports of the VLAN by adjusting their PVID values to match the virtual LAN's VID number. The PVID value of a port must match its virtual LAN's VID in order for a port to be considered an untagged member of the VLAN. This procedure is found in "Configuring the PVID of Untagged Ports" on page 107.

To create a VLAN, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21.

```
Advanced Switch Configuration -> VLAN Management Menu

Port VLAN Type:

Port    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
-----------------------------------------------------------------------------

802.1Q  * * * * * * * * * *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *

Port-Based




----------------------- <COMMAND> -------------------------------------
802.1Q [V]LAN                 [C]hange Port VLAN Type
[P]ort-Based VLAN             [Q]uit to Previous Menu


Command>
```

Figure 21. VLAN Management Menu

3. Type **V** to select **802.1Q VLAN**.

    The Tagged-based VLAN Configuration Menu is shown in Figure 22.

```
VLAN Management Menu -> Tagged-based VLAN Configuration

VLAN ID   VLAN Name                               VLAN Type
-------   -------------------------------         ---------
1         Default VLAN                            Permanent
2         Sales                                   Static




----------------------- <COMMAND> ------------------------------------
[N]ext Page                   [C]reate VLAN        C[o]nfig VLAN Member
[P]revious Page               [D]elete VLAN         [S]et Port Config
[R]eset VLAN to Default       [Q]uit to Previous Menu



Command>
```

Figure 22. Tagged-based VLAN Configuration Menu

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

    The VLAN Creation Menu is shown in Figure 22.

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

The VLAN Creation Menu is shown in Figure 23.

```
VLAN Management -> VLAN Creation Menu

 VLAN ID:
 VLAN Name:

 Port Member
 ----------------------------------------------------------------------
 Tagged:


 UnTagged:



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



Command>
```

Figure 23. VLAN Creation Menu

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

    The following prompt is displayed:

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

    Note
    You must assign a VLAN a VID.

    ---

7. Type a value from 2 to 4094 and press Enter.

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

    The following prompt is displayed:

    ```
    Enter port number >
    ```

9. Enter the untagged and tagged ports of the VLAN.

    You can specify the ports individually separated by commas, for example, 2,7,15, as a range of ports separated by a hyphen, for example, 2-4, or both, for example, 2-7,15,17.

    The following prompt is displayed:

    ```
    Select port tagging. Type (T/U) >
    ```

10. Type **T** to indicate a tagged port or **U** to indicate an untagged port.

11. When the VLAN is complete, type **A** to select **Apply** and apply the VLAN settings.

    The Tagged-based VLAN Configuration Menu is displayed again with information about the VLAN you just created. The VLAN is now active on the switch.

12. If the VLAN contains untagged ports, perform the next procedure, "Configuring the PVID of Untagged Ports" on page 107, to change the PVID of the untagged ports to match the virtual LAN's VID.

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

    The following prompt is displayed:

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

14. Type a name for the VLAN and press Enter. The VLAN name can contain up to 32 characters including spaces.

15. Type **Q** to select **Quit to previous menu** and save your changes.

Configuring the PVID of Untagged Ports

This procedure adjusts a port's VID value. The PVID value determines the VLAN in which the port is an untagged member. A port can be an untagged member of only one VLAN at a time. A port is an untagged member of the VLAN whose VID value matches its PVID.

The ports of a new VLAN are initially designated as tagged ports by the software. Their PVID values retain their previous settings when you assign them to a new VLAN. You must change their PVID values to match the VID of the VLAN, if you want the ports to function as untagged members of a new VLAN. This is explained in the following procedure.

You can also use this procedure to change the VLAN assignment of an untagged port. With this procedure you can move an untagged port from one VLAN to another by changing its PVID value.

To assign the PVID value of a port, perform the following procedure:

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

    The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **P** to select **Port-Based VLAN**.

The Port-Based VLAN Configuration Menu is shown in Figure 24.

```
VLAN Management -> Port-Based VLAN Configuration Menu

Index       Group Name           Group Member
-------     ------------         --------------------------
3           Sales                3-6
4           Marketing            7,9-11




------------------------- <COMMAND> ---------------------------------
[N]ext Page              [A]dd Member Port       [C]hange VLAN Group Name
[P]revious Page          [D]elete Member Port    [Q]uit to Previous Menu


Command>
```

Figure 24. Port-Based VLAN Configuration Menu

4. Type **A** to select **Add Member Por**t.

    The following prompt is displayed:

    ```
    Enter Group ID >
    ```

5. Enter a Group ID. Enter a value from x to y. Then press Return.

    The following prompt is displayed:

    ```
    Add Member -> Enter port number
    ```

6. Enter a port number or a range of port numbers. You can add more than one port at a time. You can specify the ports individually (for example, 2,5,11), as a range (for example, 4-7), or both (for example, 2,5,11-15).

7. Type **C** to select **Change VLAN Group Name**.

    The following prompt is displayed:

    ```
    Enter Group ID >
    ```

8. Enter a Group ID of an existing group. Then press Enter.

    The following prompt is displayed:

    ```
    Enter new VLAN group name >
    ```

9. Type the name of the VLAN group. The VLAN name can contain up to 32 characters including spaces. Then press Enter.

10. Type **Q** to select **Quit to previous menu** and save your changes.

Changing the PVID

To change the value of a VLAN's PVID, perform the following procedure.

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **V** to select **802.1Q VLAN**.

   The Tagged-based VLAN configuration Menu is shown in Figure 22 on page 104.

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

   The VLAN Port Configuration Menu is shown in Figure 21 on page 103

5. Type **V** to select **Set Port VID**.

   The following prompt is displayed:

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

6. Type the number of the port whose PVID value you want to change and press Enter. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enter PVID for port n
   ```

7. Type the new PVID for the port and press Enter. The PVID should equal the VID of the VLAN where you want the port to be an untagged member.

   > **Note**
   > If you specify a PVID that does not correspond to any VIDs on the switch, the management software creates a new VLAN with a VID that equals the PVID. The VLAN is not assigned any name.

8. Repeat steps 4 through 6 to configure additional ports.

Changing Port VLAN Type

To change the of ports that are assigned to a port-based VLAN on the VLAN Management Menu, perform the following procedure.

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **C** to select **Change Port VLAN Type**.

   The following prompt is displayed:

   ```
   Add member -> Enter port number >
   ```

4. Type a port number (or numbers) that is assigned to a port-based group. Then press Enter.

   You can specify ports individually, separated by commas, for example, 2,7,15, as a range of ports separated by a hyphen, for example, 2-4, or both, for example, 2-7,15,17.

   The following prompt is displayed:

   ```
   Select port VLAN type (1/2) >
   ```

5. Type **1** to indicate the ports belong to a port-based VLAN or **2** to indicate the ports belong to a tagged VLAN.

   You can set ports that are assigned to a port-based group to either **1** a port-based VLAN or **2** a tagged VLAN. However, ports that are not assigned to a port-base group can only be set to **2** to indicate a tagged VLAN.

   The VLAN management Menu is updated with the new port assignments.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Displaying the VLANs

To display a list of the port-based and tagged VLANs on the switch, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **V** to select **802.1Q VLAN**.

   The Tagged-based VLAN configuration Menu is shown in Figure 22 on page 104. The currently configured VLANs are displayed in a table with the following columns of information:

   VLAN ID
   The ID of the VLAN.

   VLAN Name
   The name of the VLAN.

   VLAN Type
   The type of VLAN, either permanent or static. Only the Default VLAN is permanent. All other port-based and tagged VLANs are static.

4. To view the ports of a VLAN, type **O** to select **Config VLAN Member**.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

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

   The range of the VID is from 2 to 4094.

The Config VLAN Member Menu is shown in Figure 25.

```
VLAN Management -> Config VLAN Member

VLAN ID: 3     VLAN Name: Marketing


Port      Tagging
---------------------------------------------------------------------
  4       No
  5       No
  6       No
  7       No
  8       No
  24      Yes



---------------------- <COMMAND> -----------------------------------
[N]ext Page              [C]hange VLAN Name      [A]dd VLAN Member
[P]revious page          [R]emove VLAN Member    [Q]uit to Previous Menu



Command>
```

Figure 25. Config VLAN Member Menu

The menu displays the following information:

VLAN ID
The VID number of the VLAN.

VLAN Name
The name of the VLAN.

Port
The ports of the VLAN.

Tagging
Whether a port is a tagged or untagged member of the VLAN. An untagged port is designated with No and a tagged port with Yes.

The selections in this Config VLAN Member menu are explained in "Modifying a VLAN" on page 114.

Resetting a VLAN to the Default Value

To delete all of the Port-based and Tagged VLANs on the switch and restore the default VLAN with a value of 1, perform the following procedure.

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

    The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **V** to select **802.1Q VLAN**.

    The Tagged-based VLAN configuration Menu is shown in Figure 22 on page 104.

4. Type **R** to select **Reset VLAN to Default**.

    The following prompt is displayed:

    ```
    Are you sure you want to reset VLAN configuration to
    factory default (Y/N) >
    ```

5. Type **Y** to delete all of the configured VLANs on the switch.

    A confirmation message is displayed on the screen.

Modifying a VLAN

This procedure allows you to perform the following functions:

❐ Change the name of a VLAN.

❐ Add or remove tagged ports from a VLAN.

Before performing this procedure, note the following:

❐ You cannot change the VID of a VLAN.

❐ You cannot add an untagged port to a VLAN with this procedure. That function requires changing a port's VID value, as explained in "Configuring the PVID of Untagged Ports" on page 107

❐ You cannot remove an untagged port from a VLAN with this procedure. To remove an untagged port from a VLAN, you must assign it as an untagged member of another VLAN by changing its PVID, as explained in "Configuring the PVID of Untagged Ports" on page 107.

To change the name of a VLAN or to add or remove tagged ports, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **V** to select **802.1Q VLAN**.

   The Tagged-based VLAN configuration Menu is shown in Figure 22 on page 104.

4. Type **O** to select **Config VLAN Member**.

   The Config VLAN Member menu is shown in Figure 25 on page 112.

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

5. Type the number of the VLAN you want to modify and press Enter.

   The range of the VID is from 2 to 4094.

6. To change the VLAN's name, do the following:

   a. Type **C** to select **Change VLAN Name**.

   The following prompt is displayed:

   ```
   Enter new VLAN name>
   ```

   b. Type the new name for the VLAN and press Enter. A VLAN name can be up to 32 characters and can include spaces.

7. To add a tagged port to the VLAN, do the following:

   a. Type **A** for **Add Member** and press Enter.

   The following prompt is displayed:

   ```
   Add member->Enter port number >
   ```

   b. Enter the number of the port and press Enter. You can add more than one port at a time. You can specify the ports individually (that is, 2,5,11), as a range (that is, 4-7), or both (that is, 2,5,11-15).

   The following prompt is displayed:

   ```
   Select port tagging type (T/U)>
   ```

   c. Type **T** to indicate a tagged port or **U** to indicate an untagged port.

8. To remove a tagged port from the VLAN, do the following:

   a. Type **R** for **Remove Member** and press Enter.

   The following prompt is displayed:

   ```
   Delete number -> Enter port number >
   ```

   b. Enter the number of the tagged port you want to remove and press Enter. You can remove more than one port at a time. You can specify the ports individually (that is, 2,5,11), as a range (that is, 4-7), or both (that is, 2,5,11-15).

9. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a VLAN

There are two separate procedures for deleting a VLAN depending on whether it is a Tagged or Port-based VLAN. See the following sections.

Deleting a Port-based VLAN

To delete a port from a Port-based VLAN, perform the following procedure.

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **P** to select **Port-Based VLAN**.

   The Port-Based VLAN Configuration Menu is shown in Figure 24 on page 108.

4. Type **D** to select **Delete Member Por**t.

   The following prompt is displayed:

   ```
   Enter Group ID >
   ```

5. Type the Group ID if the VLAN you want to remove ports from. Then press Enter.

   The following prompt is displayed:

   ```
   Delete member -> Enter port number >
   ```

6. Type the port number or numbers that you want to remove from the VLAN. Then press Enter.

   You can add more than one port at a time. You can specify the ports individually (for example, 2,5,11), as a range (for example, 4-7), or both (for example, 2,5,11-15).

   The Port-Based VLAN Configuration Menu is updated.

7. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a Tagged VLAN

To delete a Tagged VLAN, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

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

   The VLAN Management Menu is shown in Figure 21 on page 103.

3. Type **V** to select **802.1Q VLAN**.

   The Tagged-based VLAN configuration Menu is shown in Figure 22 on page 104.

4. Type **D** to select **Delete VLAN**.

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

5. Type the VLAN ID of the VLAN you want to delete and press Enter. You can enter only one VID.

   The range of the VID is from 2 to 4094.

   Note
   The VLAN is immediately deleted with no confirmation prompt.

   Note
   You cannot delete the Default VLAN which has a VID of 1.

   The VLAN Management Menu is updated to show that the VLAN is deleted. The untagged ports of a deleted VLAN are automatically returned to the Default VLAN.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 11

Simple Network Management Protocol (SNMP)

This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. Sections in the chapter include:

❐ "SNMP Overview" on page 120

❐ "Creating an SNMP Community" on page 124

❐ "Creating an SNMP Host" on page 129

❐ "Enabling and Disabling SNMP Traps" on page 133

SNMP Overview

You can manage a switch by viewing and changing the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). The AT-S80 Management Software supports SNMPv1 and SNMPv2c.

To manage a switch using an SNMP application program, you must do the following:

❒ Activate SNMP management on the switch. The default setting for SNMP management is disabled.

❒ Load the Allied Telesis MIBs for the switch onto your management workstation containing the SNMP application program. The MIBs are available from the Allied Telesis web site at www.alliedtelesis.com.

To manage a switch using SNMP, you need to know the IP address of the switch.

A trap is a message sent by the switch to a management workstation or server to signal an operating event, such as when the device is reset.

An authentication failure trap is similar to other the traps. It too signals an operating event on the switch. But this trap is somewhat special because it relates to SNMP management. A switch that sends this trap could be indicating an attempt by someone to gain unauthorized management access using an SNMP application program to the switch. There are two events that can cause a switch to send this trap:

❒ An SNMP management station attempts to access the switch using an incorrect or invalid community name.

❒ An SNMP management station tried to access a closed access community string, to which its IP address is not assigned.

Given the importance of this trap to the protection of your switch, the management software allows you to disable and enable it separately from the other traps. If you enable it, the switch will send this trap if either of the above events occur. If you disable it, the switch will not send this trap. The default is disabled.

If you enable this trap, be sure to add one or more IP addresses of trap receivers to the community strings so that the switch will know where to send the trap if it needs to.

Community String Attributes

A community string has attributes for controlling who can use the string and what the string will allow a network management to do on the switch. The community string attributes are defined below:

Community String Name A community string must have a name of one to eight alphanumeric characters. Spaces are allowed.

Access Mode This attribute defines the permissions of a community string. There are two access modes: Read and Read/Write. A community string with an access mode of Read can be used to view, but not change the MIB objects on a switch. A community string with a Read/Write access can be used to both view the MIB objects and change them.

Operating Status A community string can be enabled or disabled. When it is disabled, no one can use it to access the switch. You might disable a community string if you suspect someone is using it for unauthorized access to the device. When a community string is enabled, then it is available for use.

Open or Closed Access Status This feature controls which management stations on your network can use a community string. An open access status permits any network manager who knows the community string to use it. A closed access status restricts the string to those network managers who work at particular workstations, identified by their IP addresses. You specify the workstations by assigning the IP addresses of the workstations to the community string. A closed community string can have up to eight IP addresses of management workstations.

If you decide to activate SNMP management on the switch, it is a good idea to assign a closed status to all community strings that have a Read/ Write access mode and then assign the IP addresses of your management workstations to those strings. This helps reduce the chance of someone gaining management access to a switch through a community string and making unauthorized configuration changes.

Trap Receivers A trap is a signal sent to one or more management workstations by the switch to indicate the occurrence of a particular operating event on the device. There are numerous operating events that can trigger a trap. For instance, resetting the switch or the failure of a cooling fan are two examples of occurrences that cause a switch to send a trap to the management workstations. You can use traps to monitor activities on the switch.

Trap receivers are the devices, typically management workstations or servers, that you want to receive the traps sent by the switch. You specify the trap receivers by their IP addresses. You assign the IP addresses to the community strings.

Each community string can have up to eight trap IP addresses.

It does not matter which community strings you assign your trap receivers. When the switch sends a trap, it looks at all the community strings and sends the trap to all trap receivers on all community strings. This is true even for community strings that have a access mode of only Read.

If you are not interested in receiving traps, then you do not need to enter the IP addresses of trap receivers.

Default SNMP Community Strings

The AT-S80 Management Software provides two default community strings: public and private. The public string has an access mode of Read-Only and the private string has an access mode of Read/Write. If you activate SNMP management on the switch, you should delete or disable the private community string, which is a standard community string in the industry. Or, change the status of the community string from open to closed to prevent unauthorized changes to the switch.

Creating an SNMP Community

The procedures in this section describe how to create, delete, and modify an SNMP community. See the following procedures:

❐ "Adding an SNMP Community" on page 124

❐ "Deleting an SNMP Community" on page 126

❐ "Modifying an SNMP Community" on page 127

Adding an SNMP Community

To create an SNMP community, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 26.

```
Main Menu -> Basic Switch Configuration Menu

System [A]dministration Configuration
System [I]P Configuration
S[N]MP Configuration
[P]ort Configuration
[U]ser Interface Configuration
Rapid [S]panning Tree Configuration
[B]andwidth Control Configuration
IP Access [L]ist
Destination MAC [F]ilter
Storm [C]ontrol Configuration
[Q]uit to previous menu




Command>
```

Figure 26. Basic Switch Configuration Menu

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

The SNMP Configuration Menu is shown in Figure 27.

```
Basic Switch Configuration -> SNMP Configuration Menu

[C]ommunity Configuration
[H]ost Configuration
[T]rap Receiver Configuration
[Q]uit to previous menu




Command>
```

Figure 27. SNMP Configuration Menu

3. From the SNMP Configuration Menu, type **C** to select **Community Configuration**.

The Community Configuration Menu is displayed as show in Figure 28.

```
SNMP Configuration Menu -> Community Configuration Menu

No.        Access          Community
----       --------        --------------
1          Read-Only       public
2          Read-Write      private
3
4
5
6
7
8


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

[A]dd New Community Entry              [D]elete Community Entry
[M]odify Community Entry               [Q]uit to previous menu



Command>
```

Figure 28. Community Configuration Menu

4. To add a new community, type **A** to select **Add New Community Entry**.

The following prompt is displayed:

```
Enter entry number>
```

a. Type an available entry number from 1 through 8.

The following prompt is displayed:

```
Enter community name>
```

b. Type the name of the new SNMP community.

The following prompt is displayed:

```
Enter community access (R/W)>
```

c. Enter **R** to indicate Read-Only access and **W** to indicate Read-Write access.

5. Type **Q** to select **Quit to previous menu** and save your changes.

The new SNMP community is now operational on the switch.

Deleting an SNMP Community

To delete an SNMP community, perform the following procedure.

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

The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. Type **D** to select **Delete Community Entry**.

The following prompt is displayed:

```
Enter entry number>
```

a. Enter the number of the SNMP community (from 1 through 8) that you want to delete followed by Enter.

The entry is removed from the Community Configuration Menu.

4. Type **Q** to select **Quit to previous menu** and save your changes.

Modifying an SNMP Community

Use the following procedure to modify an existing SNMP community.

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

    The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. Type **M** to select **Modify Community Entry**.

    The following prompt is displayed:

    ```
    Enter entry number>
    ```

    a. Enter the entry number (from 1 through 8) that you want to modify. Then press Enter.

    The following prompt is displayed:

    ```
    Choose which to be modified (A/C/B)?
    ```

    > **Note**
    > In the above prompt, **A** represents the access level, **C** represents the community name, and **B** represents both the access level and community name.

    b. Select **A** to modify the access level of a community.

    The following prompt is displayed:

    ```
    Enter community access (R/W)>
    ```

    c. Enter **R** to indicate Read-Only access and **W** to indicate Read-Write access.

    The Community Configuration Menu is updated with the new access level.

4. Select **C** to change the community name.

    The following prompt is displayed:

    ```
    Enter entry number>
    ```

    a. Enter a number from 1 through 8.

The following prompt is displayed:

```
Enter community name>
```

b. Enter the new name of the SNMP community. You can enter a name of up to 20 characters in length. Special characters such as *, $, and @ are permitted.

The Community Configuration Menu is updated with the new SNMP community name.

c. Select **B** to modify both the name and access of a community.

The following prompt is displayed:

```
Enter community name>
```

d. Enter the name of an exiting SNMP community.

The following prompt is displayed:

```
Enter community access (R/W)>
```

5. Type **Q** to select **Quit to previous menu** and save your changes.

The new SNMP community is now operational on the switch.

Creating an SNMP Host

This procedures in this section adds, removes, and modifies SNMP hosts.

Adding an SNMP Host

To add or remove ports from a trunk, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

    The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **H** to select **Host Configuration**.

    The Host Configuration Menu is displayed in Figure 29.

```
SNMP Configuration Menu -> Host Configuration Menu

No.        IP Address      Community
----       -----------     ---------------
1
2
3
4
5
6
7
8
9
10
----------------------------<COMMAND>-----------------------------

[A]dd New Host Entry                   [D]elete Host Entry
[M]odify Host Entry                    [Q]uit to previous menu



Command>
```

Figure 29. Host Configuration Menu

4. Type **A** to select **Add New Host Entry**.

    The following prompt is displayed:

    ```
    Enter entry number>
    ```

    a. Enter a value between 1 and 10. Then press Enter.

    The following prompt is displayed:

    ```
    Enter IP address for host>
    ```

    b. Enter an IP address for an SNMP community that you previously defined in the Community Configuration menu. The IP address format must be in the xxx.xxx.xxx.xxx format. See "Creating an SNMP Community" on page 124.

    The following prompt is displayed:

    ```
    Enter community name>
    ```

    c. Enter the community name for an existing SNMP community that you previously defined in the Community Configuration menu. See "Creating an SNMP Community" on page 124.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting an Host Entry

To delete an entry from the Host Community Menu, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

    The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **H** to select **Host Configuration**.

    The Host Configuration Menu is displayed in Figure 29 on page 129.

4. Type **D** to select **Delete Host Entry**.

    The following prompt is displayed:

    ```
    Enter entry number>
    ```

    a. Enter the number of the SNMP community that you want to remove from the list of SNMP hosts. Then press Enter.

The Host Configuration Menu is updated.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Modifying an Host Entry

To modify an entry from the Host Community Menu, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

    The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **H** to select **Host Configuration**.

    The Host Configuration Menu is displayed in Figure 29 on page 129.

4. Type **M** to select **Modify Host Entry**.

    The following prompt is displayed:

    ```
    Enter entry number>
    ```

    a. Enter a number between 1 and 10. Then press enter.

    The following prompt is displayed:

    ```
    Choose which to be modified (I/C/B)>
    ```

    Note
    In the prompt above, **I** represents the IP address, **C** represents the community name, and **B** represents both the IP address and the community name.

    ---

    b. Select **I** to change the IP address.

    The following prompt is displayed:

    ```
    Enter IP address for host>
    ```

    c. Type the IP address for the host in the format xxx.xxx.xxx.xxx. Then press Enter.

    d. Select **C** to change the community name.

The following prompt is displayed:

```
Enter community name>
```

e. Enter the new community name followed by Enter.

f. Select **B** to change both the IP address and Community.

The following prompt is displayed:

```
Enter IP address for host>
```

g. Type the IP address for the host in the format xxx.xxx.xxx.xxx. Then press Enter.

The following prompt is displayed:

```
Enter community name>
```

h. Enter the new community name followed by Enter.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Enabling and Disabling SNMP Traps

The procedures in this section describe how to enable, disable, and modify traps. See the following procedures:

❒ "Enabling an SNMP Trap" on page 133

❒ "Deleting a Trap Receiver" on page 135

❒ "Modifying a Trap Receiver" on page 135

Enabling an SNMP Trap

To enable an SMNP trap, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

   The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **T** to select **Trap Receiver Configuration**.

The Trap Receiver Configuration Menu is displayed in Figure 29.

```
SNMP Configuration Menu -> Trap Receiver Configuration Menu

Authentication Trap:Enabled
No.        Version    IP Address            Community
----       -------    ------------          --------------
1          V1         167.114.71.1          Tech Com
2          V2c        167.114.71.2          Tech Com
3          V2c        167.114.71.3          System Test
4
5
6
7
8
9
10
----------------------------<COMMAND>-----------------------------

[A]dd New Trap Receiver             [D]elete Trap Receiver
[M]odify Trap Entry                 [E]nable/Disable Authentication Trap
[Q]uit to previous menu


Command>
```

Figure 30. Trap Receiver Configuration Menu

4. Type **A** to select **Add New Trap Receiver**.

   The following prompt is displayed:

   Enter entry number>

   a. Type a trap number between 1 and 10. Then press Enter.

   The following prompt is displayed:

   Enter trap version (1/2) >

   b. Type the trap version and then press Enter. Select **1** for SNMP version 1 or select **2** for SNMP version 2vc.

   The following prompt is displayed:

   Enter IP address for trap receiver>

   c. Enter an IP address in the xxx.xxx.xxx.xxx format.

   The following prompt is displayed:

   Enter community name >

     d. Enter a previously defined community name followed by Enter. See "Adding an SNMP Community" on page 124.

The Trap Receiver Configuration Menu is redrawn with the new trap displayed.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Deleting a Trap Receiver

To delete a trap receiver, perform the following procedure:

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

The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **T** to select **Trap Receiver Configuration Menu**.

The Trap Receiver Configuration Menu is displayed in Figure 29 on page 129.

4. Type **D** to select **Delete Trap Receiver**.

The following prompt is displayed:

```
Enter entry number>
```

     a. Enter a trap number between 1 and 10. Then press Enter.

The Trap Receiver Configuration Menu is updated.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Modifying a Trap Receiver

To modify a trap receiver, perform the following procedure:

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

The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **T** to select **Trap Receiver Configuration Menu**.

The Trap Receiver Configuration Menu is displayed in Figure 29 on page 129.

4. Type **M** to select **Modify Trap Receiver Entry**.

The following prompt is displayed:

```
Enter entry number>
```

a. Enter a trap number between 1 and 10. Then press Enter.

The following prompt is displayed:

```
Choose which to be modified (V/I/C/A) >
```

> **Note**
> In the above prompt, V represents Trap Version, I represents IP address, C represents community name, and A represents all of the previous choices.

The following prompt is displayed:

```
Enter entry number>
```

b. Enter a trap number between 1 and 10. Then press Enter.

c. Type **V** to change the Trap SNMP version number.

The following prompt is displayed:

```
Enter trap version (1/2) >
```

d. Type the trap version and then press Enter. Select **1** for SNMP version 1 or select **2** for SNMP version 2vc.

The Trap Receiver Configuration Menu is updated.

e. Type **I** to change the IP address.

The following prompt is displayed:

```
Enter IP address for trap receiver>
```

f. Enter an IP address in the xxx.xxx.xxx.xxx format.

The Trap Receiver Configuration Menu is updated.

g. Type **C** to change the community name.

The following prompt is displayed:

```
Enter community name >
```

h. Enter a previously defined community name followed by Enter. See "Adding an SNMP Community" on page 124.

i. Type **A** to change the trap version, IP address, and community name. Then press Enter.

The following prompt is displayed:

```
Enter trap version (1/2) >
```

j. Type the trap version and then press Enter. Select **1** for SNMP version 1 or select **2** for SNMP version 2vc.

The following prompt is displayed:

```
Enter IP address for host >
```

k. Enter an IP address in the xxx.xxx.xxx.xxx format.

The following prompt is displayed:

```
Enter community name >
```

l. Enter a previously defined community name followed by Enter. See "Adding an SNMP Community" on page 124.

The Trap Receiver Configuration Menu is updated.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Enabling or Disabling Traps

To enable or disable a trap, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

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

    The SNMP Configuration Menu is shown in Figure 27 on page 125.

3. From the SNMP Configuration Menu, type **T** to select **Trap Receiver Configuration Menu**.

    The Trap Receiver Configuration Menu is displayed in Figure 29 on page 129.

4. Type **E** to select **Enable/Disable Authentication Trap**.

    The following prompt is displayed:

```
Enable or Disable SNMP Authentication Trap (E/D) >
```

a. Enter **E** to enable all configured traps. Or, enter **D** to disable all configured traps.

Note
You can only enable or disable all traps. You may not enable or disable traps individually.

---

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 12

Quality of Service (QoS)

This chapter contains the procedures for configuring Quality of Service (QoS). This chapter contains the following sections:

❐ "QoS Overview" on page 140

❐ "Mapping CoS Priorities to Egress Queues" on page 143

❐ "Changing the Temporary Priority Level of Untagged Traffic" on page 146

QoS 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, resulting in the delay of packets from reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are often of no consequence to a network or its performance. But there are 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 QoS can be of value. It allows you to manage the flow of traffic through a 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.

QoS actually consists of several different elements. The element supported by the AT-FS750/16 and AT-FS750/24 switches is called Class of Service (CoS). CoS applies primarily to tagged packets. As explained in "Tagged VLAN Overview" on page 101, a tagged packet contains information within it that specifies the VLAN to which the packet belongs.

A tagged packet can also contain a priority level. This priority level is used by network switches and other networking devices to know how important (delay sensitive) that packet is in comparison 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-S80 software for its priority. The switch software uses the priority to determine which egress priority queue the packet should be stored in on the egress port.

Each port on the AT-FS750/16 and AT-FS750/24 switches has four priority queues, 0 (low) to 3 (high). When a tagged packet enters a switch port, the switch responds by placing the packet into one of the queues according to the assignments shown in Table 2. A packet in a high priority egress queue is typically transmitted out a port sooner than a packet in a low priority queue.

Table 2. Default Mappings of IEEE 802.1p Priority Levels
to Egress Port Priority Queues

IEEE 802.1p Traffic Class	AT-FS750 Switch Egress Port Priority Queue
0	0
1	0
2	0
3	1
4	2
5	2
6	3
7	3

For example, a tagged packet with a priority tag of 6 is placed in the egress port's highest priority queue of 3, while a packet with a priority tag of 1 is placed in the lowest priority queue.

Note
QoS is disabled by default on the switch.

You can customize these priority-to-queue assignments using the AT-S80 management software. The procedure for changing the default mappings is found in "Mapping CoS Priorities to Egress Queues" on page 143. Note that because all ports must use the same priority-to-egress queue mappings, they are applied at the switch level. They cannot be set on a per-port basis.

CoS primarily relates to tagged packets rather than untagged packets because untagged packets do not contain a priority level. By default, all untagged packets are temporarily assigned a priority level of 0 as they enter a port and, at the default settings, are placed in a port's Q0 egress queue, the queue with the lowest priority. But you can override this by assigning a different temporary priority level to a port so that all of the untagged packets are stored in a different egress queue. The procedure for this is explained in "Changing the Temporary Priority Level of Untagged Traffic" on page 146.

One last thing to note is that the switch 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.

The default setting for Quality of Service is disabled. When the feature is disabled, all tagged packets are stored in the lowest priority egress queue of a port.

Mapping CoS Priorities to Egress Queues

This procedure changes the mappings of CoS priority levels to egress priority queues. The default mappings are shown in Table 2 on page 141. This is set at the switch level and applies to all ports. This procedure also enables and disables QoS.

To change the mappings or to activate or deactivate QoS, perform the following procedure:

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **S** to select **Quality of Service Configuration**.

    The Quality of Service Configuration Menu is shown in Figure 31.

```
Advanced Switch Configuration -> Quality of Service Configuration Menu

[T]raffic Class Configuration
[P]ort Priority Configuration
[Q]uit to previous menu




        Command>
```
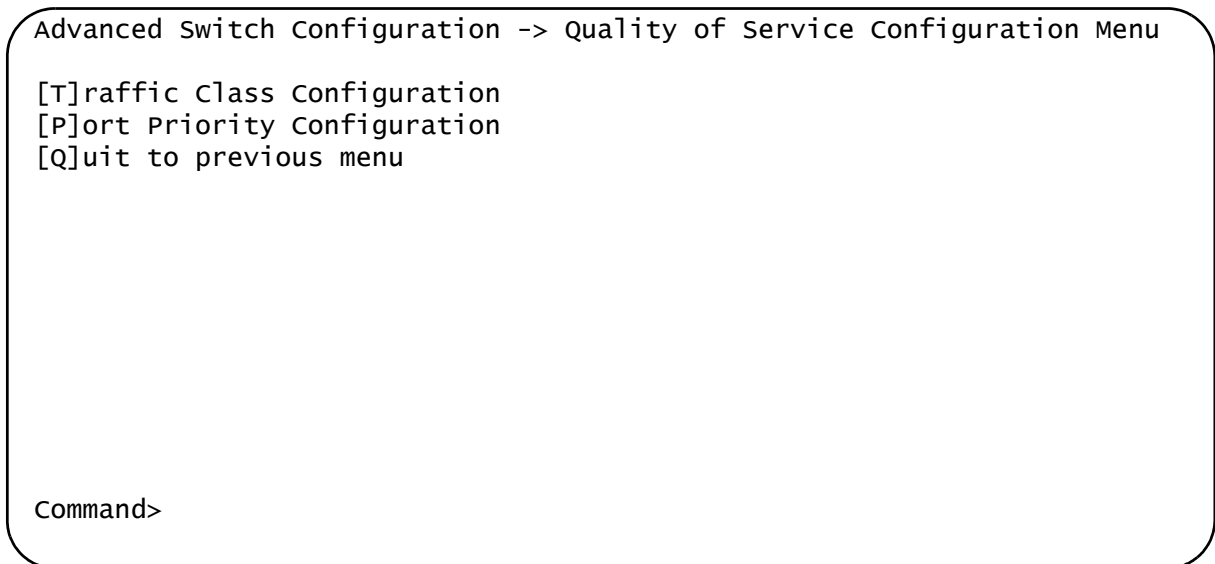
Figure 31. Quality of Service Configuration Menu

3. From the Quality of Service Configuration Menu, type **T** to select **Traffic Class Configuration**.

The Traffic Class Configuration Menu is shown in Figure 32.

```
Quality of Service Configuration -> Traffic Class Configuration Menu

QoS Status: Disabled

Traffic Class      Queue
-------------      -----
     0               0
     1               0
     2               0
     3               1
     4               2
     5               2
     6               3                3: Highest
     7               3                0: Lowest


---------------------- <COMMAND> -----------------------------------
Set [S]tatus
Set [P]riority Queue
[Q]uit to previous Page


Command>
```

Figure 32. Traffic Class Configuration Menu

4. To enable or disable QoS, do the following:

    a. Type **S** to select **Set Status**.

        The following prompt is displayed:

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

    b. Type **E** to enable QoS or **D** to disable it. The default setting is disabled. When disabled, all tagged packets are stored in the lowest priority queue of a port.

5. To change the egress priority queue assignment of a tagged 802.1p traffic class, do the following:

    a. Type **P** to select **Set Priority Queue**.

        The following prompt is displayed:

        `Enter traffic class>`

    b. Enter the traffic class whose egress priority queue you want to change. The range is 0 to 7. You can specify only one traffic class at a time. Specifying traffic class 0 affects untagged traffic as well as tagged traffic with a priority level of 0.

The following prompt is displayed:

```
Enter queue for traffic class n >
```

    c. Enter the new egress queue number for the traffic class. The range is 0 to 3 *where* 0 is the lowest priority queue and 3 is the highest. You can specify only one egress queue.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Changing the Temporary Priority Level of Untagged Traffic

This procedure explains how to change the temporary priority level of untagged packets that enter a port, and so change the egress queue where the packets are stored. For example, you could assign a temporary priority value of 5 to the untagged packets received on a port so that the packets are stored in queue 2 on the egress port. The default priority level for untagged packets is 0.

To change the temporary priority level of untagged traffic received on a port, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **S** to select **Quality of Service Configuration**.

   The Quality of Service Configuration Menu is shown in Figure 31 on page 143.

3. From the Quality of Service Configuration Menu, type **P** to select **Port Priority Configuration**.

The Port Priority Configuration Menu is shown in Figure 33.

```
Quality of Service Configuration -> Port Priority Configuration Menu

QoS Status: Enabled

Port    Trunk      Traffic Class    Queue     Override
----    -----      -------------    -----     --------
 1      ---                          0        Disabled
 2      ---        5                 2        Enabled
 3      ---                          0        Disabled
 4      ---                          0        Disabled
 5      ---                          0        Disabled
 6      ---                          0        Disabled
 7      ---                          0        Disabled
 8      ---        7                 3        Enabled
 9      ---                          0        Disabled
10      ---                          0        Disabled
11      ---                          0        Disabled    3: Highest
12      ---                          0        Disabled    0: Lowest
---------------------- <COMMAND> ------------------------------------------
[N]ext Page             Set P[r]iority Queue     Set [T]runk Priority Queue
[P]revious Page         Set [O]verride Status    Set Trun[k] Override Status
[Q]uit to previous Page


Command>
```

Figure 33. Port Priority Configuration Menu

The columns in the menu display the following information:

Port
Displays the port number.

Trunk
Displays the trunk number if the port is a member of a trunk.

Traffic Class
Displays the temporary priority level applied to the untagged traffic that enters the port. For example, in the figure above the untagged traffic received on port 2 is assigned a temporary priority value of 5.

Queue
Displays the queue where the untagged packets received on the port are stored on the egress port. For example, in the figure above the untagged traffic received on port 2 is assigned a temporary priority level of 5 and is stored in queue 2 on the egress port.

Override
Displays whether the temporary priority value is being applied to the untagged packets on the port. If this field is set to Disable, all untagged

packets received on the port are stored in queue 0 on the egress port. If this field is set to Enable, all untagged packets received on the port are stored in the egress queue specified in the table.

4. To configure a port that is not a member of a trunk, type **R** to select **Set Traffic Class**. To configure the ports of a port trunk, type **T** to select **Set Trunk Traffic Class**.

   The following prompt is displayed if you are configuring a port:

   ```
   Set Traffic Class->Enter port number>
   ```

   The following prompt is displayed if you are configuring a trunk:

   ```
   Enter trunk group number>
   ```

5. Enter the port or trunk number to be configured. You can configure only one port or trunk at a time.

   A prompt similar to the following is displayed:

   ```
   Enter queue for port n>
   ```

6. Enter the priority level (0 to 7) you want assigned to the untagged traffic on the port or trunk. The default is 0.

7. To activate the assignment of a temporary priority level to the untagged traffic on the port, type **O** to select **Set Override Status** to configure a port or **K** to select **Set Trunk Override Status** to configure a trunk.

   The following prompt is displayed if you are configuring a port:

   ```
   Set Priority Queue->Enter port number>
   ```

   The following prompt is displayed if you are configuring a trunk:

   ```
   Enter trunk group number>
   ```

8. Enter the port or trunk number to be configured.

   You can configure only one port or trunk at a time.

   A prompt similar to the following is displayed:

   ```
   Enable or Disable override for port n (E/D)>
   ```

9. Type **E** to enable the new priority level or **D** to disable it. The default is disabled.

Chapter 13

Rapid Spanning Tree Protocol (RSTP)

This chapter describes how to configure the Rapid Spanning Tree Protocol (RSTP) on the switch and includes the following sections:

RSTP Overview

The performance of a Ethernet network can be negatively impacted by the formation of a data loop in the 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 path. 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 can significantly reduce network performance.

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

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.

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 communications between the various network segments. This is the process of convergence.

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

At this time, only RSTP is available on the switch.

The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how RSTP operates 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 the *bridge priority* number, and sometimes the bridge's MAC address, also referred to as the bridge identifier. 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.

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 offline, and assign that bridge the second lowest bridge identifier number. You can change the bridge priority number for the switch.

The bridge priority has a range of 0X0000 to 0XF000 and is specified in multiples of 0x1000.

After the convergence process has completed, there is only one path between the switch and the root bridge. The active port on the switch through which the bridge is communicating with the root bridge is called the *root port*. Each switch in the spanning tree domain has a root port with the exception of the root bridge, which has no root port.

Designated Bridge and Designated Port

The switch that is directly connected to the root port of the switch is called the designated bridge. The port on the designated bridge that is connected to the switch's root port is called the designated port.

Path Costs and Port Costs

After 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.

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 the sum of the port costs between a bridge and the root bridge.

Port cost also has an Auto-Detect feature. This feature allows spanning tree 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.

Table 3 lists the RSTP port costs with Auto-Detect.

Table 3. RSTP Auto-Detect Port Costs

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

Table 4 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 4. RSTP Auto-Detect Port Trunk Costs

Port Speed	No. of Ports/ Trunk	Port Cost
10/100/1000	2	10,000
10/100/1000	3	6,666
10/100/1000	4	5,000
10/100/1000	5	4,000
10/100/1000	6	3,333
10/100/1000	7	2,857
10/100/1000	8	2,500

You can override Auto-Detect and set the port cost manually. However, you must assign the same port cost to all ports that are members of a trunk.

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 is used as a tie breaker when two paths have the same cost.

The range for port priority, in hexadecimal format, is 0 to 240, with 240 being the highest priority. As with bridge priority, this range is broken into multiples of 16. To select a port priority for a port, you enter the desired value.

Table 5 lists the values. The default value is 0.

Table 5. Port Priority Value Increments

Port Priority	Port Priority
0	128
16	144
32	160
48	176
64	192
80	208
96	224
112	240

If two paths have the same port cost and the same priority, then the ports with the lowest port MAC addresses become the root ports of their respective bridges.

Hello Time and Bridge Protocol Data Units (BPDUs)

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 protocol data unit (BPDU). When a bridge is brought online, it issues 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 periodically transmits 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 in the AT-S80 Management Software. The interval is measured in seconds and the default is two seconds. Consequently, if an AT-FS750 switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

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 the port types defined, RSTP can quickly reconfigure a network when a change in network topology is detected.

There are two possible selections:

❑ Point-to-point port

❑ Edge port

The default setting for the RSTP port point-to-point status is automatic. With the automatic setting, the point-to-point status is True of the port is operating in full-duplex mode. If the port is operating in half-duplex mode, then the point-to-point status is False.

Figure 34 illustrates two AT-FS750/24 switches that have been connected with one data link. With the link operating in full-duplex, the ports are point-to-point ports.

Point-to-Point Ports
(Full-duplex Mode)
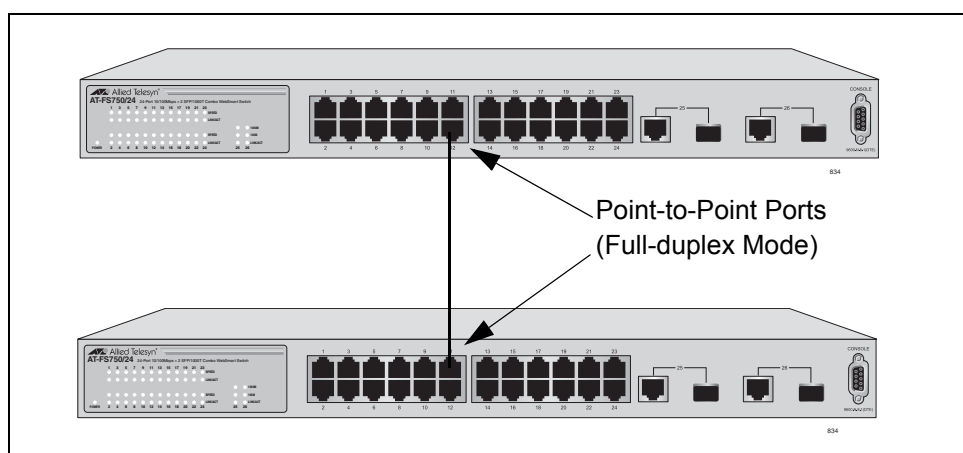
Figure 34. Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any additional bridges participating in STP or RSTP, then you need to manually define the port as an edge port. The default setting for the edge port status is False. For each port, you must manually configure this setting. There is no automatic mode for the edge port setting.

Figure 35 illustrates an edge port on an AT-FS750/24 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.
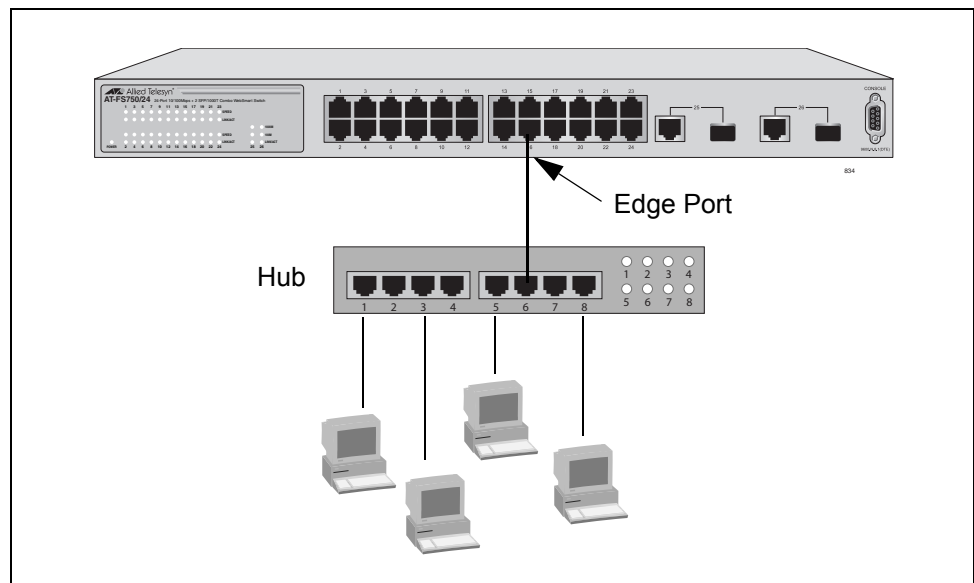
Figure 35. Edge Port

A port can be both a point-to-point and an edge port at the same time. Figure 36 illustrates a port functioning as both a point-to-point and edge port. You must manually configure the edge port status.
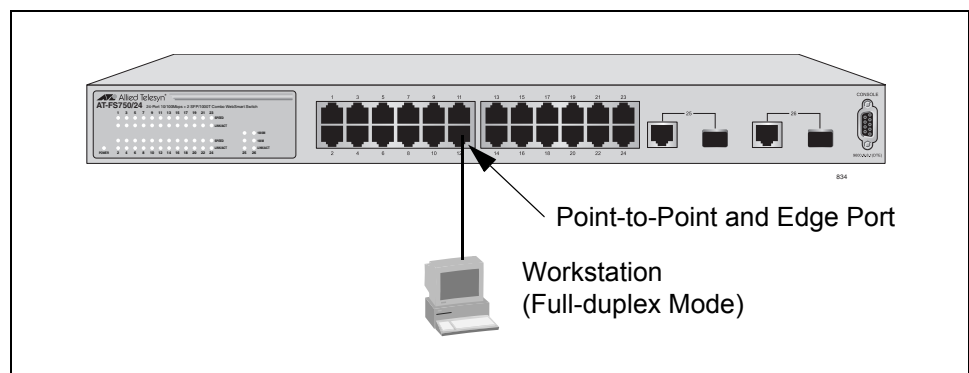
Figure 36. Point-to-Point and Edge Port

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

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 can operate together to create a single spanning tree domain.

The switch monitors the traffic on each port for BPDU packets. When you set the switch to RSTP mode, all the ports operate in that mode and reject STP BPDU packets. When you set the switch to operate in STP-

compatible mode, the ports can receive either RSTP or STP BPDU packets.

Rapid Spanning Tree and VLANs

The spanning tree implementation in the AT-S80 Management Software 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. In this situation, STP blocks a data link because it detects a data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 37. Two VLANs, Sales and Production, span two switches. Two links consisting of untagged ports connect the separate parts of each VLAN. If RSTP is activated on the switches, one of the links is disabled. In the example, the port on the top switch that links the two parts of the Production VLAN is changed to the block state. This leaves the two parts of the Production VLAN unable to communicate with each other.
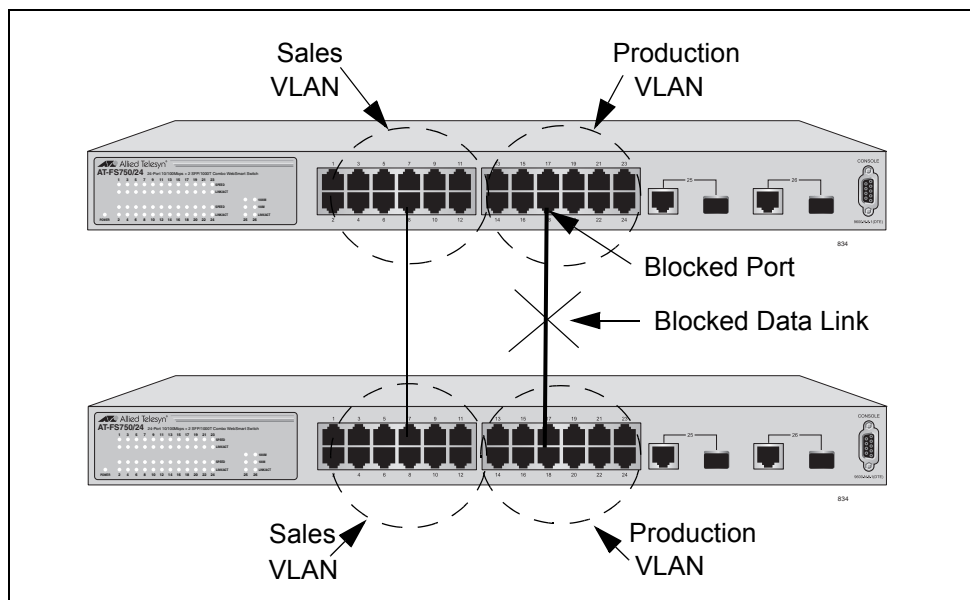
Figure 37. VLAN Fragmentation

You can avoid this problem by not activating rapid spanning tree or by connecting VLANs using tagged port members instead of untagged ports. (For information on tagged and untagged ports, refer to Chapter 10, "Virtual LANs" on page 97.)

Enabling or Disabling RSTP

To enable or disable RSTP, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Rapid Spanning Tree Configuration Menu is shown in Figure 38.

```
Basic Switch Configuration -> Rapid Spanning Tree Configuration Menu

Global RSTP Status: Disabled          Protocol Version: RSTP

Root Port:        0                   Time Since Topology Change: 118  Sec.
Root Path Cost:  0                    Topology Change Count:       1

Designated Root: 8000 00C08F1211BB    Bridge ID:            8000 010203AABB04
Hello Time:      2 Sec.               Bridge Hello Time:    2 Sec.
Maximum Age:     20 Sec.              Bridge Maximum Age:   20 Sec.
Forward Delay:   15 Sec.              Bridge Forward Delay: 15 Sec.


----------------------- <COMMAND> -----------------------------
[E]nable/Disable Global RSTP          Set Bridge [F]orward Delay
Set RSTP Protocol [V]ersion           RSTP [B]asic Port Configuration
Set Bridge [P]riority                 RSTP [A]dvanced Port Configuration
Set Bridge [H]ello Time               Topology [I]nformation
Set Bridge [M]aximum Age              [Q]uit to previous menu


Command>
```

Figure 38. RSTP Configuration Menu

The RSTP menu allows you to configure RSTP as well as to view the current settings and contains the following items of information in the middle portion:

Root Port
The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port and the root port parameter will be 0.

Root Path Cost

The sum of all the root port costs of all the bridges between the switch's root port and the root bridge including the switch's root port cost.

Time Since Topology Change

The time in seconds since the last topology change took place. When RSTP detects a change to the LAN's topology or when the switch is rebooted, this parameter is reset to 0 seconds and begins incrementing until the next topology change is detected.

Topology Change Count

An integer that reflects the number of times RSTP has detected a topology change on the LAN since the switch was initially powered on or rebooted.

The following parameters refer to the designated root bridge:

Designated Root

This parameter includes two fields: the root bridge priority and the MAC address of the root bridge. For example, 1000 00C08F1211BB shows the root bridge priority as 1000, and 00C08F1211BB as the MAC address.

Hello Time

The hello time. See "Hello Time and Bridge Protocol Data Units (BPDUs)" on page 153. This parameter affects only the root bridge.

Maximum Age

The maximum amount of time that BPDUs are stored before being deleted on the root bridge.

Forward Delay

The time interval between generating and sending configuration messages by the root bridge.

The following parameters refer to the switch.

Bridge ID

The MAC address of the bridge. The bridge identifier is use as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority. You cannot change this setting.

Bridge Hello Time

This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Bridge Maximum Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge.

Bridge Forward Delay
This is the time interval between generating and sending configuration messages by the bridge.

3. Type **E** to select **Enable/Disable Global RSTP**.

   The following prompt is displayed:

   ```
   Enable or Disable Global RSTP (E/D)>
   ```

4. Type **E** to enable RSTP or **D** to disable RSTP.

Configuring the RSTP Bridge Settings

To configure the RSTP bridge settings, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

    The Rapid Spanning Tree Configuration Menu is shown in Figure 38 on page 157.

3. Type **P** to select **Set Bridge Priority**.

    The following prompt is displayed:

    ```
    Enter bridge priority>
    The value is in the range from 0x0000 to 0xF000 and in
    increments of 0x1000.
    ```

    Indicates the priority number for the bridge, in hexadecimal format. This number is used to determine the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, that is, the lowest of all the bridges, then the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes offline, the bridge with the lowest priority number automatically takes over as the root bridge. This parameter can be from 0X0000 to 0XF000, with 0XF000 being the highest priority.

    The bridge priority is shown as the first field in the "Designated Root" and "Bridge ID" parameters.

4. Enter a number for the bridge priority.

5. Type **H** to select **Set Bridge Hello Time**.

    The following prompt is displayed:

    ```
    Enter bridge hello time>
    ```

    This is 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.

6. Enter a number for the bridge hello time.

7. Type **M** to select **Set Bridge Maximum Age**.

The following prompt is displayed:

```
Enter bridge maximum age>
```

Indicates the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All of the 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 value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

When you select a value for maximum age, observe the following rules:

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.

---

8. Enter a number for the bridge maximum age.

9. Type **F** to select **Set Bridge Forward Delay**.

    The following prompt is displayed:

    ```
    Enter bridge forward delay>
    ```

    The bridge forwarding delay is the waiting period in seconds 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.

10. Enter a number for the bridge forward delay, between 4 and 30 seconds.

Configuring STP Compatibility

Choosing an RSTP protocol version allows you to determine if the switch ports will operate in RSTP-only mode or are STP-compatible. This setting applies to all of the ports; you cannot set this on a per-port basis.

To configure the STP compatibility, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Rapid Spanning Tree Configuration Menu is shown in Figure 38 on page 157.

3. Type **V** to select **Set RSTP Protocol Version**.

   The following prompt is displayed:

   ```
   Set RSTP protocol version (S/R)>
   ```

4. Type **S** to make the ports STP-compatible, or **R** to make the ports operate only in RSTP mode.

Configuring RSTP Port Settings

This section contains the following topics:

❑ "Configuring the Basic RSTP Port Settings," next

❑ "Configuring the Advanced RSTP Port Settings" on page 165

Configuring the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Rapid Spanning Tree Configuration Menu is shown in Figure 38 on page 157.

3. From the Rapid Spanning Tree Configuration Menu, type **B** to select **RSTP Basic Port Configuration**.

   The RSTP Basic Port Configuration menu is shown in Figure 39.

```
 Rapid Spanning Tree Configuration -> RSTP Basic Port Configuration

 Port  Trunk  Link  State       Role       Priority   Path Cost      STP Status
 ----  -----  ----  ----------  ---------  --------   ----------------------   ----------
 1     ---    Up    Forwarding  Disabled   128        200000         Disabled
 2     ---    Down  Forwarding  Disabled   128        200000         Enabled
 3     ---    Up    Forwarding  Root       128        200000         Enabled
 4     ---    Down  Forwarding  Disabled   128        200000         Enabled
 5     ---    Down  Forwarding  Disabled   128        200000         Enabled
 6     ---    Down  Forwarding  Disabled   128        200000         Enabled
 7     ---    Down  Forwarding  Disabled   128        200000         Enabled
 8     ---    Down  Forwarding  Disabled   128        200000         Enabled
 9     ---    Down  Forwarding  Disabled   128        20000          Enabled
 10    ---    Down  Forwarding  Disabled   128        20000          Enabled
 11    ---    Down  Forwarding  Disabled   128        20000          Enabled
 12    ---    Down  Forwarding  Disabled   128        20000          Enabled
 ----------------------------- <COMMAND> -------------------------------
 [N]ext Page                                    Set Path [C]ost
 [P]revious Page                                Set Port STP [S]tatus
 Set Port Pr[i]ority                            [Q]uit to previous menu

 Command>
```

Figure 39. RSTP Basic Port Configuration Menu

4. Type **I** to select **Set Port Priority**.

    The following prompt is displayed:

    ```
    Select port number to be changed>
    Port number is in range from 1 to 9, 0 to set all ports
    ```

5. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

    The following prompt is displayed:

    ```
    Enter priority for port n>
    ```

    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 5 on page 153.

    Note
    If two or more ports have the same cost and priorities, then the port with the lowest MAC address becomes the forwarding port.

    ---

6. Enter a number for the priority.

7. Type **C** to select **Set Path Cost**.

    The following prompt is displayed:

    ```
    Select port number to be changed>
    Port number is in range from 1 to 9, 0 to set all ports
    ```

8. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

    The following prompt is displayed:

    ```
    Enter path cost for port n>
    ```

    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 from 0 to 240, with 240 being the highest priority. For a list of the increments, refer to Table 5 on page 153.

    The default setting is based on the Auto-Detect Port Cost feature, which sets port cost depending on the speed of the port. The default values are shown in Table 3 on page 152.

9. Enter a number for the path cost.

10. Type **S** to select **Set Port STP Status**.

```
Select port number to be changed>
Port number is in range from 1 to 9, 0 to set all ports
```

This parameter enables or disables RSTP on a specified port or a group of ports in a trunk.

11. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

The following prompt is displayed:

```
Enable or Disable STP for port n (E/D)>
```

12. Type **E** to enable or **D** to disable STP on the port.

Configuring the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Rapid Spanning Tree Configuration Menu is shown in Figure 38 on page 157.

3. From the Rapid Spanning Tree Configuration Menu, type **A** to select **RSTP Advanced Port Configuration**.

The RSTP Advanced Port Configuration menu is shown in Figure 39.

```
Rapid Spanning Tree Configuration -> RSTP Advanced Port Configuration

Port  Trunk Link  State       Role      Admin/OperEdge  Admin/OperPtoP  Migrat
----  ----- ----  ----------  --------  --------------  --------------  ------
 1    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 2    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 3    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 4    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 5    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 6    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 7    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 8    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
 9    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
10    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
11    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
12    ---   Down  Forwarding  Disabled  False/False     Auto/False      Init.
------------------------------- <COMMAND> -------------------------------
[N]ext Page                              Set Port P-[t]o-P Status
[P]revious Page                          Restart Port [M]igration
Set Port [E]dge Status                   [Q]uit to previous menu

Command>
```

Figure 40. RSTP Advanced Port Configuration Menu

4. Type **E** to select **Edge Status**.

    The following prompt is displayed:

    The following prompt is displayed:

    ```
    Select port number to be changed>
    Port number is in range from 1 to 9, 0 to set all ports
    ```

5. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

    The following prompt is displayed:

    ```
    Set edge port for port n >(T/F)>
    ```

    This parameter defines whether the port is functioning as an edge port. The possible settings are True and False. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" on page 153.

6. Enter **T** for True or **F** for False to change the Admin/OperEdge status.

7. Type **P** to select **P-to-P Status**.

The following prompt is displayed:

```
Select port number to be changed>
Port number is in range from 1 to 9, 0 to set all ports
```

8. Enter the number of the port you want to change, or type 0 (zero) to apply the settings to all ports on the switch.

The following prompt is displayed:

```
Set point-to-point for port n >(A/T/F)
```

This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Auto, True, and False. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" on page 153.

9. Enter **A** for Auto, **T** for True, or **F** for False, according to the operating status your network requires, following the guidelines in Table 6.

Table 6. RSTP Point-to-Point Status

Admin	**Operation**	**Port Duplex Operation**
Auto	True	Full
	False	Half
True	True	Full or Half
False	False	Full or Half

10. Type **M** to select **Restart Port Migration**.

The following prompt is displayed:

```
Select port number to be changed>
```

11. Enter the number of the port you want to change.

The following prompt is displayed:

```
Restart the protocol migration process for port n? (Y/N)
```

This parameter resets an RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely.

12. Enter **T** for True or **F** for False.

Displaying the RSTP Topology

To display the RSTP topology, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The Rapid Spanning Tree Configuration Menu is shown in Figure 38 on page 157.

3. From the Rapid Spanning Tree Configuration Menu, type **I** to select **Topology Information**.

   The Topology Information menu is shown in Figure 39.

```
Rapid Spanning Tree Configuration -> Designated Topology Information

 PortTrunk Link  Desig. Root          Desig. Cost  Desig. Bridge     Desig. Port
 --------- ----  --------------------------------------------------------------
 1         Up    8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 2         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 3         Up    8000 000c46aa7fal  200000         8000 003084000000 00 03
 4         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 5         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 6         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 7         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 8         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
 9         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
10         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
11         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00
12         Down  8000 00c08f1211bb  0              8000 00c08f1211bb 00 00


-------------------------------- <COMMAND> --------------------------------
[N]ext Page              [P]revious Page      [Q]uit to previous menu

Command>
```

Figure 41. Topology Information Menu

This menu displays the following information about the ports:

Trunk
The trunk of which the port is a member.

Link
Whether the link on the port is up or down.

Desig. Root
The designated root bridge is the switch that is directly connected to the local switch. The MAC address of the designated root bridge is displayed. In the network topology, the designated bridge is located between the local switch and the root bridge.

Desig. Cost
The sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Desig. Bridge
An adjacent bridge to which the root port of the switch is actively connected.

Desig. Port
The port on the designated bridge that is directly connected to the root port of the local switch.

Chapter 14

Bandwidth Control

This chapter explains how to activate and configure the Internet Group Management Protocol (IGMP) snooping feature on the switch. Sections in the chapter include:

❒ "Bandwidth Control Overview" on page 172

❒ "Configuring Bandwidth Control" on page 173

Bandwidth Control Overview

If the performance of your network is affected by heavy traffic, you can use bandwidth control to set the rate of various types of packets that a port receives. You can control ingress packet types, including broadcast, multicast, and DLF packets or a combination of all three types, and limit their rates. (DLF packets are unicast packets that are broadcast because of a destination address lookup failure.)

Configuring Bandwidth Control

The procedures in this section describe how to set bandwidth control options on the switch and on the ports. See the following sections:

❒ "Assigning Broadcast or Multicast Packets" on page 173

❒ "Setting the Ingress Limit Rate" on page 174

❒ "Setting Ingress Status" on page 174

❒ "Setting Ingress DLF Status" on page 175

Assigning Broadcast or Multicast Packets

To assign broadcast or multicast packets to a port, perform the following procedure:

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

2. From the Basic Switch Configuration Menu, type **B** to select **Bandwidth Control**.

The Bandwidth Control Configuration Menu is shown in Figure 42.

```
Basic Switch Configuration -> Bandwidth Control Configuration Menu

Broad/Multicast Packet Threshold: Low   DLF Ingress Packet Status: Enabled
Port    Ingress       Mode
----    ---------     -----------
1       Disabled      Bcast/Mcast
2       Disabled      Bcast/Mcast
3       Disabled      Bcast/Mcast
4       Disabled      Bcast/Mcast
5       Disabled      Bcast/Mcast
6       Disabled      Bcast/Mcast
7       Disabled      Bcast/Mcast
8       Disabled      Bcast/Mcast
9       Disabled      Bcast/Mcast
10      Disabled      Bcast/Mcast
11      Disabled      Bcast/Mcast
12      Disabled      Bcast/Mcast


-------------------------------<Command>----------------------------
[N]ext Page      Set Ingress [M]ode         [Q]uit to previous menu
[P]revious Page  Set Ingress [L]imit Rate
Set [I]ngress    Set Ingress [D]LF Status
Command>
```

Figure 42. Advanced Switch Configuration Menu

3. From the Advanced Switch Configuration Menu, type **M** to select **Set Ingress Mode**.

   The following prompt is displayed:

   `Set Bandwidth Control-> Enter port number>`

4. Type a port number. Then press Enter.

   The following prompt is displayed for port 12:

   `Enter Ingress Mode for port 12 (B/M) >`

5. Type **B** to select broadcast or **M** to select multicast.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting the Ingress Limit Rate

To set the ingress limit rate on the switch, perform the following procedure.

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

2. From the Basic Switch Configuration Menu, type **B** to select **Bandwidth Control**.

   The Advanced Switch Configuration Menu is shown in Figure 42 on page 173.

3. Type **L** to select **Set Limit Rate**.

   The following prompt is displayed:

   `Enter threshold level for all ports (L/M/H)>`

4. Type **L** for a low threshold level, **M** for a medium threshold level, or **H** for a high threshold level.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Setting Ingress Status

To enable or disable ingress status on a port, perform the following procedure.

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

2. From the Basic Switch Configuration Menu, type **B** to select **Bandwidth Control**.

   The Advanced Switch Configuration Menu is shown in Figure 42 on page 173.

3. Type **I** to select **Set Ingress**.

    The following prompt is displayed:

    ```
    Set Bandwidth Control-> Enter port number>
    ```

4. Type a port number. Then press Enter.

    The following prompt is displayed if you select port 12:

    ```
    Enable or Disable Ingress Bandwidth Control for port 12
    (E/D)>
    ```

5. Type **E** to enable ingress or **D** to disable ingress on a port.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Setting Ingress DLF Status

To enable or disable DLF ingress status on a switch, perform the following procedure.

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

2. From the Basic Switch Configuration Menu, type **B** to select **Bandwidth Control**.

    The Advanced Switch Configuration Menu is shown in Figure 42 on page 173.

3. Type **D** to select **Set DLF Ingress Status**.

    The following prompt is displayed:

    ```
    Enable or Disable DLF Bandwidth Control for all ports
    (E/D)>
    ```

4. Type **E** to enable DLF Bandwidth Control or **D** to disable DLF Bandwidth Control.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 15

IP Access List

This chapter explains how to activate and configure the IP Access List feature on the switch. Sections in the chapter include:

❒ "IP Access List Overview" on page 178

❒ "Configuring IP Access List" on page 179

IP Access List Overview

The IP Access List feature, when enabled, restricts remote (web) access to the management software by means of a user-configured list of IP addresses. It does not restrict the management ping response activity.

Note
By default, the IP Access List feature is disabled.

Configuring IP Access List

The procedures in this section describe how to enable or disable the IP Access List Restriction feature and how to add or remove IP addresses from the list. See the following sections:

❑ "Enabling or Disabling IP Access List Restriction" on page 179

❑ "Adding or Removing IP Addresses" on page 180

Enabling or Disabling IP Access List Restriction

To enable or disable the IP Access List feature, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

2. From the Basic Switch Configuration Menu, type **L** to select IP Access List.

    The IP Access List Menu is shown in Figure 43.

```
Basic Switch Configuration -> IP Access List Menu

IP Restriction: Disabled

Accessible IP      Accessible IP      Accessible IP      Accessible IP
------------       ------------       ------------       ------------
100.10.10.4


[Q]uit to previous menu




------------------------------<Command>------------------------------
Set IP Restriction [S]tatus               Set [I]P Address
[Q]uit to previous menu

Command>
```

Figure 43. IP Access List Menu

3. To enable the IP Access List feature, type **S** to select **Set IP Restriction Status**.

    The following prompt is displayed:

    ```
    Enable or Disable IP Restriction (E/D) >
    ```

4. Type **E** to enable the IP Restriction feature or **D** to disable the IP Restriction feature.

    By default, IP Restriction feature is disabled.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Adding or Removing IP Addresses

To add or remove IP addresses from the IP Access List, perform the following procedure:

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

    The Basic Switch Configuration Menu is shown in Figure 26 on page 124.

2. From the Basic Switch Configuration Menu, type **L** to select **IP Access List**.

    The IP Access List Menu is shown in Figure 43 on page 179.

3. To add or remove an IP address, type **I** to select **Set IP Address**.

    The following prompt is displayed:

    ```
    Add or Delete accessible IP (A/D) >
    ```

4. Type **A** to add an IP address or **D** to delete an IP address.

    The following prompt is displayed:

    ```
    Enter allowed accessible IP>
    ```

5. Type an IP address in the following format:

    XXX.XXX.XXX.XXX.

6. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 16
Destination MAC Filter

This chapter explains how to activate the Destination MAC filter on the switch. Sections in the chapter include:

❒ "Destination MAC Filtering Overview" on page 182
❒ "Configuring Destination MAC Filtering" on page 183

Destination MAC Filtering Overview

Destination MAC Filtering is a security feature that prevents AT-FS750/16 or AT-FS750/24 switches from receiving packets from a particular device which is specified by its MAC address. After you add a MAC address of a device to the list of Destination MAC Filtering, then the AT-FS750 switch drops or discards packets sent from this device.

To reverse this process and allow an AT-FS750 switch to receive packets from a device on the Destination MAC Filtering list, you must remove the MAC address of the device from the list.

Note
By default, Destination MAC Filtering is disabled on the switch.

Configuring Destination MAC Filtering

The procedures in this section describe how to add or remove MAC addresses from the Destination MAC filtering addresses. See the following procedures:

❐ "Setting Destination MAC Filtering" on page 183

❐ "Removing Destination MAC Filtering Addresses" on page 184

Setting Destination MAC Filtering

To add a MAC address to the destination MAC filtering addresses on the switch, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

2. From the Basic Switch Configuration menu, type **F** to select **Destination MAC Filter**.

   See the Destination MAC Filter Menu in Figure 44.

```
Basic Switch Configuration -> Destination MAC Filter

MAC Address      MAC Address      MAC Address      MAC Address
-----------      -----------      -----------      ------------




                        -------------------<COMMAND>---------------------------
[N]ext Page         [A]dd MAC Address      [Q]uit to previous menu
[P]revious Page     [R]emove MAC Address


Command>
```

Figure 44. Destination MAC Filter Menu

3. To add a destination MAC address filter, type **A** to select **Add MAC Address**.

   The following prompt is displayed:

   ```
   Add MAC Address to filter >
   ```

4. Enter a MAC address in the following format:

xx:xx:xx:xx:xx:xx

The MAC address is displayed in the Destination MAC Filter menu.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Removing Destination MAC Filtering Addresses

To remove a destination MAC filtering address on the switch, perform the following procedure:

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

The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

2. From the Basic Switch Configuration menu, type **F** to select **Destination MAC Filter**.

See the Destination MAC Filter Menu in Figure 44 on page 183.

3. Type **R** to select **Remove MAC Address**.

The following prompt is displayed:

```
Delete MAC address from filter >
```

4. Enter a MAC address in the following format:

xx:xx:xx:xx:xx:xx

The MAC address is removed from the Destination MAC Filter menu.

5. Type **Q** to select **Quit to previous menu** and save your changes.

Chapter 17

802.1x Port-based Network Access Control

This chapter contains information about and the procedure for configuring 802.1x Port-based Network Access Control. It includes the following sections:

❐ "802.1x Port-based Network Access Control Overview" on page 186

❐ "Guest VLANs" on page 192

❐ "Configuring 802.1x Port-based Network Access Control Feature" on page 193

❐ "Configuring MAC Based Access Control Feature" on page 197

802.1x Port-based Network Access Control Overview

802.1x Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch port. With this feature, the switch does not allow an end node to send or receive traffic through a port until the user of the node logs on by entering a username and password.

This feature can prevent an unauthorized individual from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users to whom you have assigned a username and password are able to use the switch to access the network.

This feature must be used with the RADIUS authentication protocol and requires a RADIUS server on your network. The RADIUS server performs the authentication of the username and password combinations.

> **Note**
> RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

Following are several 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 switch 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 does the actual authenticating of the user names and passwords from the supplicants.

The AT-FS750/16 and AT-FS750/24 switches do not authenticate the usernames and passwords from the end users. Instead, they act 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.

❒ Either the authenticator (that is, a switch port) or the supplicant can initiate an authentication prompt 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.

❒ The supplicant responds with an EAP-Response/Identity packet to the authentication server via the authenticator.

❒ The authentication server responds with an EAP-Request packet to the supplicant via the authenticator.

❒ The supplicant responds with an EAP-Response/MDS packet containing a username and password.

❒ The authentication server sends either an EAP-Success packet or EAP-Reject packet to the supplicant.

❒ 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.

❒ When the supplicant sends an EAPOL-Logoff prompt, 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.

Authenticator Ports

All of the ports on the AT-FS750/16 and AT-FS750/24 switches are authenticator ports. An authenticator port can have one of three settings. These settings are referred to as the port control settings. The settings are:

❒ Auto - Activates 802.1x port-based authentication. An authenticator port with this setting does not forward network traffic to or from the end node until the client has entered a username and password that the authentication server must validate. The port begins in the unauthorized state, sending and receiving only EAPOL frames. All other frames, including multicast and broadcast frames, are discarded. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication

server. Each client that attempts to access the network is uniquely identified by the switch using the client's MAC address.

❒ Force-unauthorized - Places the port in the unauthorized state, ignoring all attempts by the client to authenticate. This port control setting blocks all users from accessing the network through the port and is similar to disabling a port and can be used to secure a port from use. The port continues to forward EAPOL packets, but discards all other packets, including multicast and broadcast packets.

❒ Force-authorized - Disables IEEE 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. This is the default setting. Use this port control setting for those ports where there are network devices that are not to be authenticated.

Figure 45 illustrates the concept of the authenticator port control settings.
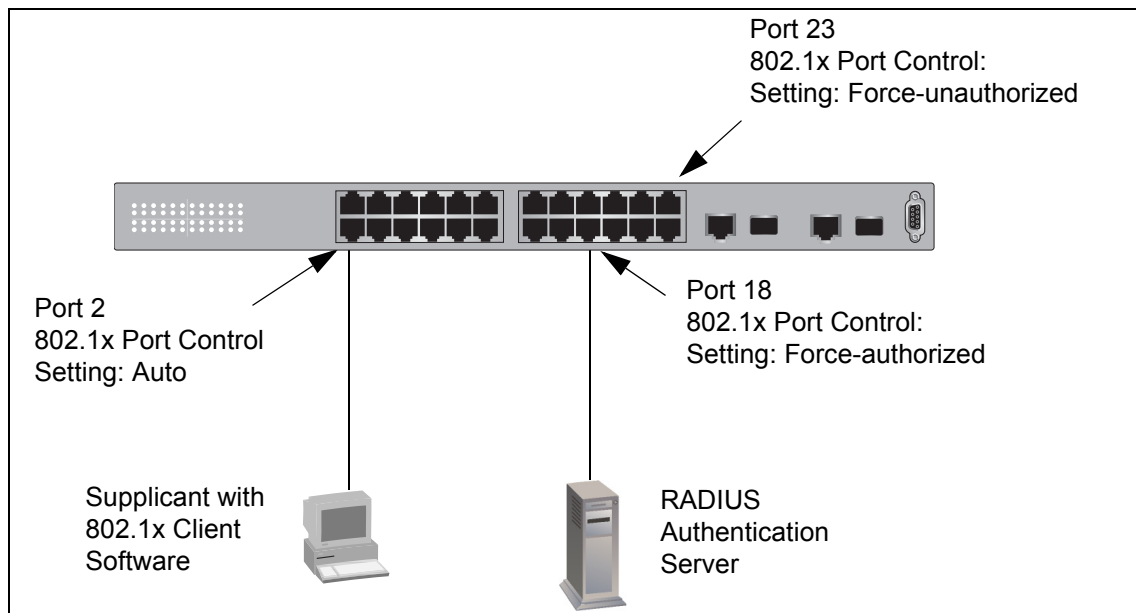
Figure 45. Example of the Authenticator Role

❒ Port 2 is set to Auto. The end node connected to the port must use its 802.1x client software and provide a username and password to send or receive traffic from the switch.

❒ Port 18 is set to the Force-authorized setting so that the end node connected to the port does not have to provide a user name or password to send or receive traffic from the switch. In the example, the node is the RADIUS authentication server. Since the server cannot authenticate itself, its port must be set to Force-authorized in order for it to pass traffic through the port.

❒ Port 23 is set to Force-unauthorized to prevent anyone for using the port.

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 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

Following are the general steps to implementing 802.1x Port-based Network Access Control:

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 Telesis. Consult the vendor's documentation for server installation instructions.

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-S80 management software.

3. You must configure and activate the RADIUS client software in the AT-S80 management software. The default setting for the authentication protocol is disabled. You will need to provide the following information:

   ❑ The IP address of a RADIUS servers.

   ❑ The encryption key used by the authentication server.

   For instructions, refer to Chapter 18, "RADIUS Authentication Protocol" on page 201.

4. You must configure the authenticator port settings, as explained in "Configuring 802.1x Port-based Network Access Control Feature" on page 193 in this chapter.

Port-based Network Access Control Guidelines

Following are the guidelines for using this feature:

❑ Ports set to Auto do not support port trunking or dynamic MAC address learning.

❑ The appropriate setting for a port on an AT-FS750/16 or AT-FS750/24 switch connected to an authentication server is Force-authorized, the default setting. This is because an authentication server cannot authenticate itself.

❑ The authentication server must be a member of the Default VLAN by communicating with the switch through a port that is an untagged member of the Default VLAN.

❑ Allied Telesis does not support connecting more than one supplicant to an authenticator port on the switch. The switch allows only one supplicant to log on per port.

Note
Connecting multiple supplicants to a switch port set to the Auto setting does not conform to the IEEE 802.1x standard. This can introduce security risks and can result in undesirable switch behavior. To avoid this, Allied Telesis recommends use the Force-authorized setting of the Port Control feature on ports that are connected to more than one end node, such as a port connected to another switch or to 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.

❒ After 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. 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 prevents unauthorized individuals from accessing the network through unattended network workstations.

❒ There should be only one port in the authenticator port control setting of Auto between a client and the authentication server.

❏ Ports used to interconnect switches should be set to the port control setting of Force-authorized. This is illustrated in Figure 46.

Switch A

Port 6:
802.1x Port Control
Setting: Force-authorized

Port 22:
802.1x Port Control
Setting: Force-authorized

Port 15:
802.1x Port Control
Setting: Force-authorized

RADIUS
Authentication
Server

Switch B

Ports 1 to 12:
802.1x Port Control
Setting: Auto

Supplicants with
802.1x Client Software
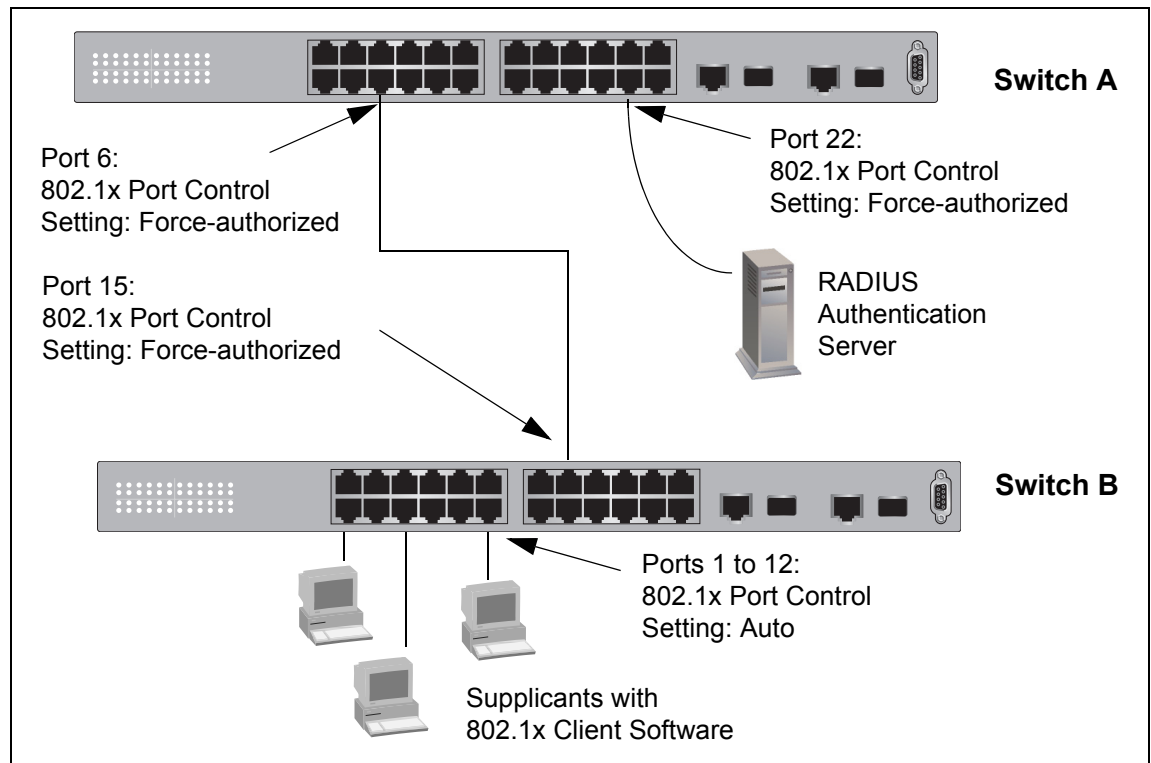
Figure 46. Port-based Authentication Across Multiple Switches

Guest VLANs

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a supplicant. However, you can configure an authenticator port to be a member of a Guest VLAN when no supplicant is logged on. Any client using the port is not required to log on and has full access to the resources of the Guest VLAN.

If the switch receives 802.1x packets on the port, signalling that a supplicant is logging on, it moves the port to its predefined VLAN and places it in the unauthorized state. The port remains in the unauthorized state until the log on process between the supplicant and the RADIUS server is completed. When the supplicant logs off, the port automatically returns to the Guest VLAN.

Note
The Guest VLAN feature is only supported on an authenticator port in the Single operating mode.

Configuring 802.1x Port-based Network Access Control Feature

To configure 802.1x Port-based Network Access Control feature, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **X** to select **802.1x Port Based Access Control Configuration**.

   The Port Based Access Control Configuration Menu is shown in Figure 47.

```
Advanced Switch Configuration -> Port Based Access Control Configuration Menu

NAS ID                     : Nas1
Authentication Method      : 1
Port No                    : 1
Port Status                : Authorized
Port Control               : Force Authorized
Transmission Period        : 30    seconds
Maximum Request            : 2
Quiet Period               : 60    seconds
Re-authentication Period   : 3600  seconds
Re-authentication Status   : Disabled
Multi-host                 : Disabled
Current PVID               : 1
Guest VLAN ID              : Disabled


---------------------- <COMMAND> -----------------------------------
[N]AS ID                    [M]aximum Request        [I]nitialize Port
[N]ext Page                 Q[u]iet Period           [G]uest VLAN ID
Pre[v]ious Page             R[e]-auth Period         Auth [M]ode
[P]ort No                   Re-[a]uth Status         Aut[h]entication Method
Port [C]ontrol              Multi-h[o]st             [Q]uit to previous Page
[T]ransmission Period


Command>
```

Figure 47. Port Based Access Control Configuration Menu

3. Type **P** to select **Port No**.

   The following prompt is displayed:

   ```
   Enter port number>
   ```

4. Enter the number of the port on the switch you want to configure. You can configure only one port at a time.

   The Port Based Access Control Configuration Menu is updated with the current settings of the selected port.

5. Configure the 802.1x settings for the port. A change to a parameter takes affect immediately on the port. The settings are described here:

   NAS ID.
   This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

   Port Status.
   Displays the current 802.1 status of the port as either authorized or unauthorized. This is not an adjustable parameter.

   Port Control.
   Sets the 802.1x port control setting. The possible settings are:

   A (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 or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server.

   U (Force-unauthorized) - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.

   F (Force-authorized) - Disables IEEE 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. This is the default setting.

   Transmission 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.

Maximum Request.
Sets 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.

Quiet Period.
Sets the number of seconds that the port 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.

Re-auth Period.
Specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Re-auth Status.
Specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

Current PVID
Displays the current port VLAN identifier or PVID assignment of the port. You cannot change this value from the Port Based Access Control Configuration Menu. See Chapter 10, "Virtual LANs" on page 97 for information about assigning a PVID.

Multi-host
Permits you to enable or disable multi-host status.

6. To permit a guest VLAN ID, type **G**.

   The following prompt is displayed:

   ```
   Enter guest VLAN ID >
   ```

   a. Type a VLAN ID and then press Enter.

   The Port Based Access Control Configuration Menu is updated with the new guest VLAN ID.

7. To enable 802.1x to support multiple hosts, type **O**.

   The following prompt is displayed:

   ```
   Enable or disable multi-host status? >
   ```

   a. Select **E** to enable multi-host status and **D** to disable multi-host status.

   The Port Based Access Control Configuration Menu is updated with the status of the multi-host feature.

8. To select between port-base or MAC address based authentication, type **M** to select Auth Mode.

   The following prompt is displayed:

   ```
   Select the Port based or MAC based auth mode (P/M) >
   ```

   a. Select **P** and the menu is redrawn.

   b. Select **M** and the MAC Based Access Control Configuration Menu is displayed.

   Authentication Method
   Select an authentication method that is enabled on the switch either R (RADIUS) or L (local).

9. If the port control setting is Auto and you want to return the EAPOL machine state on the port to the initialized state, do the following:

   a. Type **I** to select **Initialize Port**.

      The following prompt is displayed:

      ```
      Would you initialize authenticator? (Y/N)>
      ```

   b. Typing **Y** returns the EAPOL machine state on the port to the initialize state. Typing **N** cancels the step.

10. Type **Q** to select **Quit to previous menu** and save the settings.

Configuring MAC Based Access Control Feature

To configure the MAC Based Access Control feature, perform the following procedure.

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

    The Advanced Switch Configuration Menu is shown in Figure 14 on page 64.

2. From the Advanced Switch Configuration Menu, type **X** to select **802.1x Port Based Access Control Configuration**.

    The Port Based Access Control Configuration Menu is shown in Figure 47 on page 193.

3. From the **802.1x Port Based Access Control Configuration Menu,** type **M** to select **Auth Mode.**

    The following prompt is displayed:

    ```
    Select Port based or Mac based auth mode (P/M) >
    ```

4. Type **M** to select MAC Based Access Control.

The MAC Based Access Control Configuration Menu is displayed. See Figure 48.

```
Advanced Switch Configuration -> MAC Based Access Control Configuration Menu
 Port No: 1      Port Control: Forced Authorized    Authentication Method: Local
Transmit Period: 30 sec Max Request: 2 Quiet Period: 60 sec
Re-auth Period : 3600 sec  Re-auth Status: Disabled
Supplicant MAC Addr        MAC Control             Auth Status
-------------------        -----------             -----------




   
                                    



 ----------------------- <COMMAND> ------------------------------------
 [N]AS ID                   [M]aximum Request        [I]nitialize Port
 [N]ext Page                Q[u]iet Period           [G]uest VLAN ID
 Pre[v]ious Page            R[e]-auth Period         Auth [M]ode
 [P]ort No                  Re-[a]uth Status         Aut[h]entication Method
 Port [C]ontrol             Multi-h[o]st             [Q]uit to previous Page
 [T]ransmission Period


 Command>
```

Figure 48. MAC Based Access Control Configuration Menu

5. Type **P** to select **Port No**.

    The following prompt is displayed:

    `Enter port number>`

6. Enter the number of the port on the switch you want to configure. You can configure only one port at a time.

    The MAC Based Access Control Configuration Menu is updated with the current settings of the selected port.

7. Configure the 802.1x settings for the port. A change to a parameter takes affect immediately on the port. The settings are described here:

    NAS ID
    This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

Port Control
Sets the 802.1x port control setting. The possible settings are:

A (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 or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server.

U (Force-unauthorized) - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.

F (Force-authorized) - Disables IEEE 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. This is the default setting.

Transmission 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.

Maximum Request.
Sets 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.

Quiet Period.
Sets the number of seconds that the port 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.

Re-auth Period.
Specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Re-auth Status.
Specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

Multi-host
Permits you to enable or disable multi-host status.

Authentication Method
Select an authentication method that is enabled on the switch either R (RADIUS) or L (local).

8. To permit a guest VLAN ID, type **G**.

    The following prompt is displayed:

    ```
    Enter guest VLAN ID >
    ```

    a. Type a VLAN ID and then press Enter.

    The MAC Based Access Control Configuration Menu is updated with the new guest VLAN ID.

9. If the port control setting is Auto and you want to return the EAPOL machine state on the port to the initialized state, do the following:

    a. Type **I** to select **Initialize Port**.

        The following prompt is displayed:

        ```
        Would you initialize authenticator? (Y/N)>
        ```

    b. Typing **Y** returns the EAPOL machine state on the port to the initialize state. Typing **N** cancels the step.

10. Type **Q** to select **Quit to previous menu** and save the settings.

Chapter 18
RADIUS Authentication Protocol

This chapter describes how to configure the RADIUS client software on the switch. You can use the RADIUS client with 802.1x port-based network access control to control who can forward packets through the switch. Sections in the chapter include:

❒ "RADIUS Overview" on page 202

❒ "Configuring the RADIUS Client" on page 203

❒ "Displaying the RADIUS Client Settings" on page 205

RADIUS Overview

RADIUS (Remote Authentication Dial In User Services) is an authentication protocol for enhancing the security of your network. The protocol transfers the task of authenticating network access from a network device to an authentication protocol server.

The AT-S80 management software comes with RADIUS client software. You can use the client software together with 802.1x port-based network access control to control which end users and end nodes can send packets through the switch. See Chapter 17, "802.1x Port-based Network Access Control" on page 185.

RADIUS Implementation Guidelines

What do you need to use the RADIUS protocol? Following are the main points.

❑ You must install RADIUS server software on a network server or management station. Authentication protocol server software is not available from Allied Telesis.

❑ The RADIUS server must be communicating with the switch through a port that is an untagged member of the Default VLAN.

❑ If the RADIUS server is on a different subnet from the switch, be sure to specify a default gateway in the System IP Configuration Menu, shown in Figure 5 on page 33, so that the switch and server can communicate with each other.

❑ You need to configure the RADIUS server software on the authentication server by specifying the username and password combinations. The maximum length of a username or password is 12 alphanumeric characters.

> **Note**
> This manual does not explain how to configure RADIUS server software. Refer to the documentation that came with the software for instructions.

❑ You must activate the RADIUS client software on the switch using the AT-S80 Management Software and configure the settings. This is explained in "Configuring the RADIUS Client" on page 203. By default, authentication protocol is disabled.

> **Note**
> For more information on the RADIUS authentication protocol, refer to the RFC 2865 standard.

Configuring the RADIUS Client

To configure the RADIUS client, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The User Interface Configuration Menu is shown in Figure 7 on page 39.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 49.

```
User Interface Configuration -> RADIUS Server Configuration


Server IP Address      :   0.0.0.0
Server Port            :   1812
Shared Secret          :


---------------------- <COMMAND> ----------------------------
Set Server [I]P
Set UDP [P]ort Number
Set Shared Se[c]ret
[Q]uit to previous menu


Command>
```

Figure 49. RADIUS Server Configuration Menu

4. Type **I** to select **Set Server IP**.

   The following prompt is displayed:

   Enter IP address for RADIUS server>

5. Type the IP address of the RADIUS server and press Enter.

6. Type **P** to select **UDP Port Number**.

   The following prompt is displayed:

   Enter port number>

7. Enter the port number that you want to assign to UDP. You may only assign one port number to this parameter. The default value is 1812.

8. Type **C** to select **Shared Secret**.

   The following prompt is displayed:

   ```
   Enter secret string for server>
   ```

9. Enter the encryption key of the RADIUS server and press Enter.

10. Type **Q** to select **Quit to previous menu** and save your changes.

Displaying the RADIUS Client Settings

To display the RADIUS client status and settings, perform the following procedure:

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

   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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

   The User Interface Configuration Menu is shown in Figure 7 on page 39.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 49 on page 203. The top of the menu shows the current RADIUS server configuration.

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

Chapter 19

Management Software Updates

This chapter explains how to download a new version of the AT-S80 Management Software onto the switch. The procedure is:

❐ "Downloading a New Management Software Image Using TFTP" on page 208

Note
For information on how to obtain new releases of the AT-S80 Management Software, refer to "Management Software Updates" on page 16.

Note
For procedures to download software from the web interface using TFTP or HTTP, see Chapter 36, "Management Software Updates" on page 323.

Downloading a New Management Software Image Using TFTP

Before downloading a new version of the AT-S80 management software onto the switch, note the following:

❒ Both models of the AT-FS750 Series use the same AT-S80 management software image.

❒ The current configuration of a switch is retained when a new AT-S80 software image is installed. To return a switch to its default configuration values, refer to "Returning the AT-S80 Management Software to the Factory Default Values" on page 51.

❒ Your network must have a node with TFTP server software.

❒ You must store the new AT-S80 image file on the server.

❒ You should start the TFTP server software before you begin the download procedure.

❒ The switch where you are downloading the new image file must have an IP address and subnet mask. For instructions on how to configure the IP address on a switch, refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32 or "Enabling and Disabling the DHCP Client" on page 35.

⚠️ **Caution**
Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

The following procedure assumes you have already obtained the new software from Allied Telesis and stored it on the TFTP server.

To download the AT-S80 image software onto the switch, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 9 on page 46.

2. From the Switch Tools Menu, type **U** to select **Software Upgrade**.

The Software Upgrade Menu is shown in Figure 50.

```
Switch Tools Configuration -> Software Upgrade Menu


 [T]FTP Software Upgrade
 [Q]uit to previous menu




 Command>
```

Figure 50. Software Upgrade Menu (1 of 2)

3. Type **T** to select **TFTP Upgrade**.

The Software Upgrade Menu (2 of 2) is shown in Figure 51.

```
Main Menu -> Software Upgrade Menu

Image Version/Date:   AT-S80 V2.0.0 [1.1.1.57/Dec 6 2007 14:39:48

TFTP Server IP:   0.0.0.0
Image File Name:  FS750_1_1_1_57
Retry Count:      5


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

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image and Reboot
Set [R]etry Count
[Q]uit to previous menu




 Command>
```

Figure 51. Software Upgrade Menu (2 of 2)

4. Type **S** to select **Set TFTP Server IP Address**.

The following prompt is displayed:

Enter IP address of TFTP server:

5. Type the IP address of the TFTP server and press Enter.

6. Type **F** to select **Set Image File Name**.

    The following prompt is displayed:

    ```
    Enter file name >
    ```

7. Enter the file name of the AT-S80 image file on the TFTP server and press Enter.

8. Type **R** to select **Set Retry Count**.

    The following prompt is displayed:

    ```
    Enter retry count >
    ```

9. Enter the number of times you want the switch to retry in the event a problem occurs during the download process. The range is 1 to 20. The default is 5 times.

10. To begin the download, type **U** to select **Upgrade Image and Reboot**.

    The following prompt is displayed:

    ```
    Download file? (Y/N) >
    ```

11. Type **Y** for yes to begin the upgrade or **N** for no to cancel the procedure.

    If you select yes, the software immediately begins to download the file onto the switch. After the software download is complete, the switch initializes the software and reboots. You will lose your local management connection to the switch during the reboot process.

Section II
Using the Web Browser Interface

The chapters in this section provide information and procedures for using the web browser interface of the AT-S80 Management Software. The chapters include:

❒ Chapter 20, "Starting a Web Browser Management Session" on page 213

❒ Chapter 21, "Basic Switch Parameters" on page 219

❒ Chapter 22, "Port Configuration" on page 241

❒ Chapter 23, "Port Trunking" on page 245

❒ Chapter 24, "Port Mirroring" on page 251

❒ Chapter 25, "Static Multicast Address Table" on page 255

❒ Chapter 26, "IGMP Snooping" on page 261

❒ Chapter 27, "Destination MAC Address Filter" on page 265

❒ Chapter 28, "Bandwidth Control" on page 269

❒ Chapter 29, "Virtual LANs" on page 273

❒ Chapter 30, "Simple Network Management Protocol (SNMP)" on page 285

❒ Chapter 31, "Quality of Service (QoS)" on page 295

❒ Chapter 32, "Rapid Spanning Tree Protocol (RSTP)" on page 301

❒ Chapter 33, "802.1x Port-based Network Access Control Feature" on page 311

❒ Chapter 34, "Dial-in User" on page 317

❒ Chapter 35, "RADIUS Authentication Protocol" on page 321

❒ Chapter 37, "Statistics" on page 329

❒ Chapter 36, "Management Software Updates" on page 323

Chapter 20

Starting a Web Browser Management Session

This chapter contains the procedures for starting, using, and quitting a web browser management session on the AT-FS750/16 and AT-FS750/24 switches. Sections in the chapter include:

❑ "Establishing a Remote Connection to Use the Web Browser Interface" on page 214

❑ "Web Browser Tools" on page 217

❑ "Quitting a Web Browser Management Session" on page 218

Establishing a Remote Connection to Use the Web Browser Interface

To manage an AT-FS750/16 or AT-FS7950/24 switch using the web browser interface, you must assign an IP address and a subnet mask to the switch. To manually assign an IP address, refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32. To configure the switch to obtain its IP configuration from a DHCP server, refer to "Enabling and Disabling the DHCP Client" on page 35. The initial assignment of an IP address must be made through a local management session.

> **Note**
> The remote management station must be a member of the switch's Default VLAN. The switch responds and processes management packets only if they are received on an untagged port of the Default VLAN.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

2. In the URL field of the browser, enter the IP address of the switch to be managed.
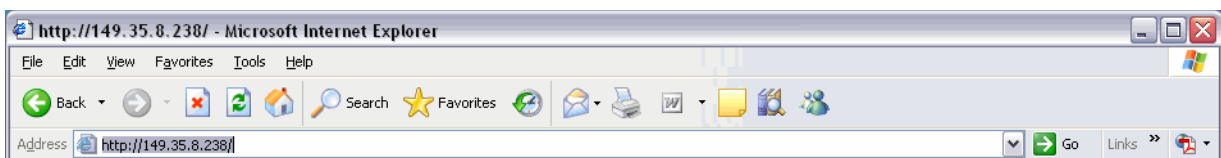
Switch's IP Address

Figure 52. Entering a Switch's IP Address in the URL Field

The AT-S80 Management Software displays the login dialog box, shown in Figure 53.
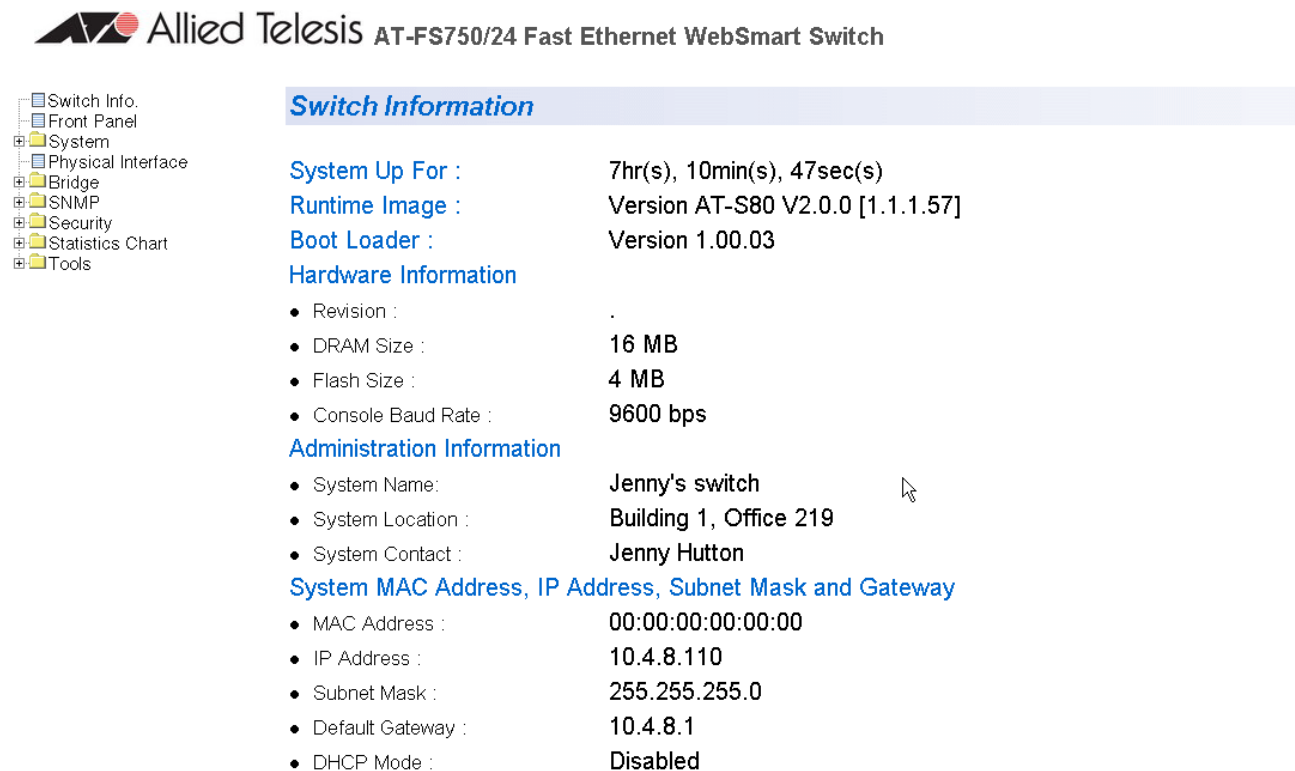
Figure 53. AT-S80 Login Dialog Box

3. Enter the AT-S80 management login user name and password. The default user name is "manager" and the password is "friend." The login name and password are case-sensitive.

To change the user name and password, refer to "Configuring System Management Information" on page 226.

The AT-S80 management software displays the home page which is called the Switch Information Page. See Figure 54.

For more information about the Switch Information Page, see "Viewing System Information" on page 233.

Allied Telesis AT-FS750/24 Fast Ethernet WebSmart Switch

- Switch Info.
- Front Panel
- System
- Physical Interface
- Bridge
- SNMP
- Security
- Statistics Chart
- Tools

Switch Information

System Up For :	7hr(s), 10min(s), 47sec(s)
Runtime Image :	Version AT-S80 V2.0.0 [1.1.1.57]
Boot Loader :	Version 1.00.03

Hardware Information

- Revision : .
- DRAM Size : 16 MB
- Flash Size : 4 MB
- Console Baud Rate : 9600 bps

Administration Information

- System Name: Jenny's switch
- System Location : Building 1, Office 219
- System Contact : Jenny Hutton

System MAC Address, IP Address, Subnet Mask and Gateway

- MAC Address : 00:00:00:00:00:00
- IP Address : 10.4.8.110
- Subnet Mask : 255.255.255.0
- Default Gateway : 10.4.8.1
- DHCP Mode : Disabled

Figure 54. Home Page for the AT-FS750/24 Switch

The main menu is on the sidebar of the home page. It consists of the following folders:

❑ System

❑ Bridge

❑ SNMP

❑ Security

❑ Statistics

❑ Tools

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.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature to save the link to the switch.

Quitting a Web Browser Management Session

To exit a web browser management session, close the web browser.

Chapter 21

Basic Switch Parameters

This chapter contains the following sections:

❒ "Configuring an IP Address, Subnet Mask and Gateway Address" on page 220

❒ "Setting Up the IP Access List" on page 222

❒ "Enabling and Disabling the DHCP Client" on page 225

❒ "Configuring System Management Information" on page 226

❒ "Configuring System Administration Information" on page 228

❒ "Setting the User Interface Configuration" on page 231

❒ "Viewing System Information" on page 233

❒ "Rebooting a Switch" on page 236

❒ "Pinging a Remote System" on page 238

❒ "Returning the AT-S80 Management Software to the Factory Default Values" on page 240

Configuring an IP Address, Subnet Mask and Gateway Address

This procedure explains how to change the IP address, subnet mask, and gateway address to the switch. Before performing the procedure, note the following:

❏ The switch needs an IP address, subnet mask, or default gateway if you plan to manage the device remotely with a web browser from a management workstation on your network.

❏ A gateway address is only required if your remote management station is separated from the switch by a router.

❏ To configure the switch to automatically obtain its IP configuration from a DHCP server, go to "Enabling and Disabling the DHCP Client" on page 225.

❏ The initial assignment of an IP address must be made through a local management session using the menus interface.

To change the switch's IP configuration, perform the following procedure:

1. From the book marks on the left side of the page, select **System**.

   The System folder expands.

2. From the **System** folder, select **IP Setup**.

   The IP Setup Page is shown in Figure 55.

Figure 55. IP Setup Page

3. Change the IP configuration parameters by entering new information in the fields:

System MAC Address
This parameter displays the MAC address of the switch. You cannot change this parameter.

System IP Address
Enter the IP address for the switch.

System Subnet Mask
Enter the subnet mask for the switch.

System Default Gateway
Enter the default gateway's IP address.

DHCP Mode
For information about setting this parameter, refer to "Enabling and Disabling the DHCP Client" on page 225.

4. Click **Apply**.

Note
Changing the IP address ends your management session. To resume managing the device, enter the new IP address of the switch in the web browser's URL field, as shown in Figure 52 on page 214.

Setting Up the IP Access List

The procedures in this section describe how to enable or disable the IP Access List feature on the switch and how to add or remove IP addresses from the list. See the following sections:

❒ "Creating an IP Access List" on page 222

❒ "Deleting an IP Address" on page 224

For background information regarding the IP Access List feature, see Chapter 15, "IP Access List" on page 183.

Creating an IP Access List

To create a list of restricted IP addresses, perform the following procedure:

1. From the book marks on the left side of the page, select **System**.

   The System folder expands.

2. From the **System** folder, select **IP Access List**.

   The IP Access List Page is shown in Figure 56.
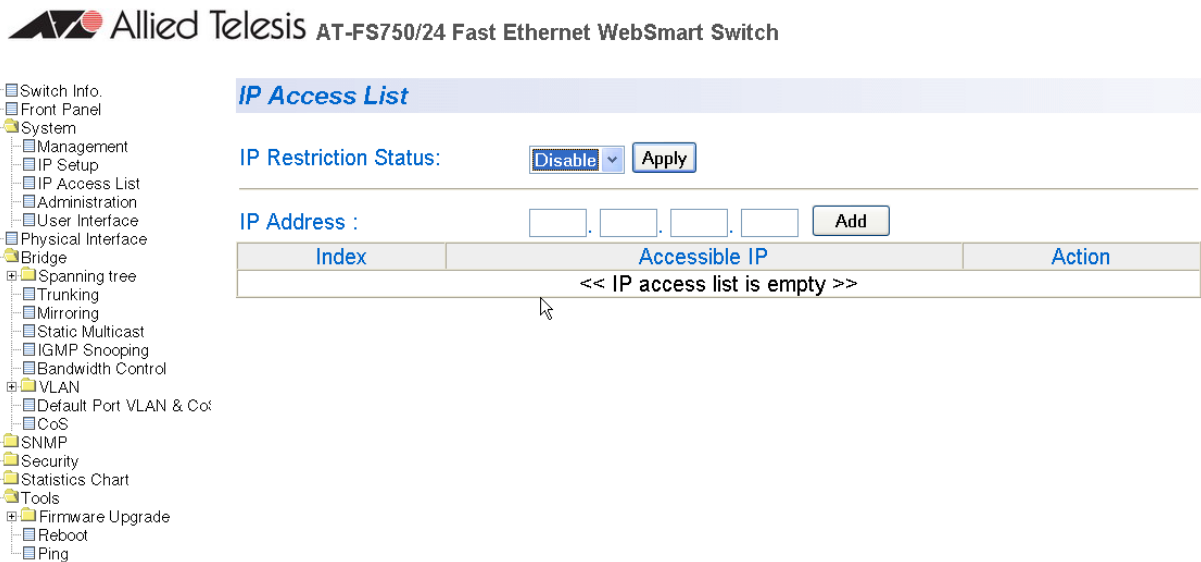
Figure 56. IP Access List Page

3. To set the IP restriction status, select Disable or Enable in the pull-down menu next to the **IP Restriction Status** field. Then click **Apply**.

   By default, the IP Restriction Status field is set to Disable.

4. Enter an IP address that you want to prevent from accessing the switch in the xxx.xxx.xxx.xxxx format next to the **IP Address** field. Then click **Add**.

   The IP address is added to the IP Access List Table.

Deleting an IP Address

To delete an IP address from the IP Access List, perform the following procedure:

To create a list of restricted IP addresses, perform the following procedure:

1. From the book marks on the left side of the page, select **System**.

   The System folder expands.

2. From the System folder, select **IP Access List**.

3. Select **delete** next to the IP address that you want to remove.

   The IP address is removed from the IP Access List Table.

Enabling and Disabling the DHCP Client

This procedure explains how to activate and deactivate the DHCP client on the switch. When the client is activated, the switch obtains its IP configuration, such as its IP address and subnet mask, from a DHCP server on your network. Before performing the procedure, note the following:

❒ The switch needs an IP address, subnet mask, or default gateway if you plan to manage the device remotely with a web browser from a management workstation on your network.

❒ A gateway address is only required if your remote management station is separated from the switch by a router.

❒ The default setting for the DHCP client is disabled.

❒ The DHCP client does not support BOOTP.

❒ The initial assignment of the IP address must be made through a local management session using the menus interface.

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

1. From the book marks on the left side of the page**,** select **System**.

   The System folder expands.

2. From the System folder, select **IP Setup**.

   The IP Setup Page is shown in Figure 55 on page 220.

3. Select the pull-down menu next to the **DHCP Mode** field. Then select **Enable** or **Disable**.

4. Click **Apply**.

   If you enable the client, it immediately begins to send queries to the DHCP server. It continues to send queries until it receives a response.

   > **Note**
   > Enabling DHCP ends your management session. To resume managing the device, enter the IP address assigned to the switch by the DHCP server in the web browser's URL field.

Configuring System Management Information

This section explains how to assign a name to the switch, as well as the location of the switch and the name of the switch's administrator. Entering this information is optional.
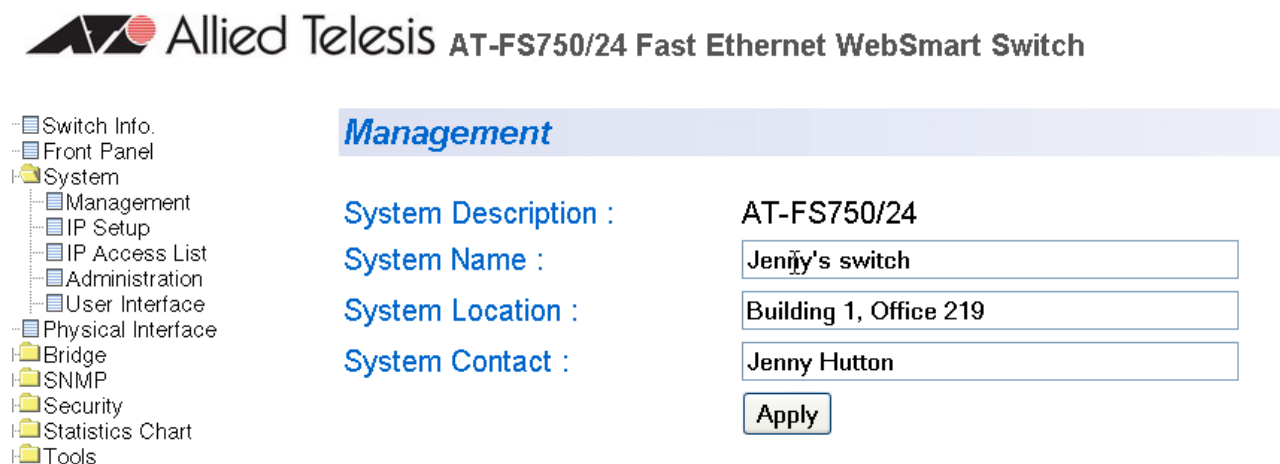
To set a switch's administration information, perform the following procedure:

1. From the book marks on the left side of the page, select **System**.

   The System folder expands.

2. From the System folder, select **Management**.

   The Management Page is shown in Figure 56.

Figure 57. Management Page

3. Configure the following parameters as necessary:

   System Description
   Specifies the model number of the switch. You cannot change this parameter.

   System Name
   Specifies a name for the switch, for example, Sales. The name is optional and may contain up to 50 characters.

Note
Allied Telesis recommends assigning a name to each switch. Names can make it easier for you to identify the various switches in your network and can also help you avoid performing a configuration procedure on the wrong switch.

System Location
Specifies the location of the switch. The location is optional and may contain up to 50 characters.

System Contact
Specifies the name of the network administrator responsible for managing the switch. This contact name is optional and may contain up to 50 characters.

4. Click **Apply**.

Configuring System Administration Information

This section explains how to enable password protection and create users in the web interface. See the following sections:

❒ "Adding System Administration Information" on page 228

❒ "Modifying Administration Information" on page 229

❒ "Deleting Administration Information" on page 230

Adding System Administration Information

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

1. From the book marks on the left side of the page, select **System**.

   The System folder expands.

2. From the System folder, select **Administration**.

   The Administration Page is shown in Figure 58.

Figure 58. Administration Page
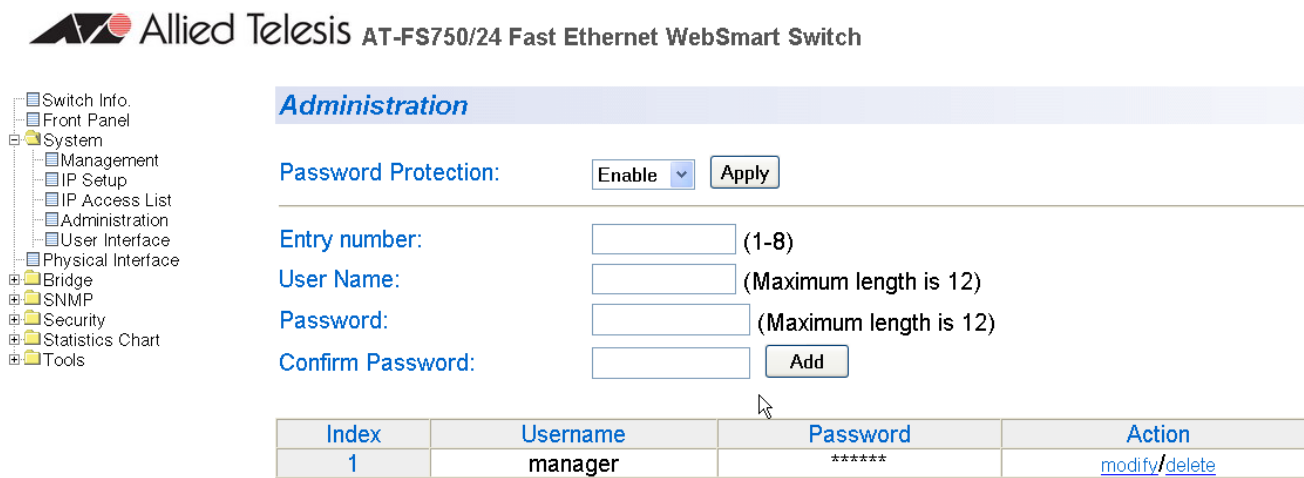
3. To enable or disable password protection, select Enable or Disable from the pull-down menu next to the **Password Protection** field.

   You can control login authentication by enabling password protection which requires a user to supply a password when logging onto the switch. If you disable password protection, a user can login without inputting a password. By default, this field is set to Enable.

4. To create an entry number, type 1 through 8 in the box next to the Entry number field.

This value appears as the Index value in the Administration table.

5. To create a user name, enter a user name in the box next to the **User Name** field.

    You can enter a value of up to 12 alphanumeric characters.

6. To add a password to the above user name, enter a password of up to 12 alphanumeric characters in the box next to the **Password** field.

7. To confirm the above password, retype the password in the box next to the **Confirm Password** field.

8. Click **Add** to activate your changes on the switch.

Modifying Administration Information

To modify the password of a user name, perform the following procedure.

1. From the book marks on the left side of the page**,** select **System**.

    The System folder expands.

2. From the **System** folder, select **Administration**.

    The Administration Page is shown in Figure 58 on page 228.

3. Select the user name that you want to change and click **modify**. The Modify Administration Page is displayed. See Figure 59.

Figure 59. Modify Administration Page

4. Click **Apply** to activate your changes on the switch.

Deleting Administration Information

To delete a user name, perform the following procedure.

1. From the book marks on the left side of the page**,** select **System**.

    The System folder expands.

2. From the **System** folder, select **Administration**.

    The Administration Page is shown in Figure 58 on page 228.

3. Select the user name that you want to delete and click **delete**.

    The user name is removed from the Administration Table.

4. Click **Add** to activate your changes on the switch.

Setting the User Interface Configuration

This procedure explains how to adjust the user interface and security features on the switch. With this procedure you can:

❏ Change the console timer, used to automatically end inactive local management sessions.

❏ Change the AT-S80 management login user name and password.

❏ Enable and disable the web server, used to manage the switch from a remote management station with a web browser.

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

1. From the book marks on the left side of the page, select **System**.

    The System folder expands.

2. From the System folder, select **User Interface**.

    The User Interface Page is shown in Figure 60.

Figure 60. User Interface Page

Note
If the page includes a Telnet UI Idle Time Out parameter, you can ignore it. The parameter does not apply to these switches.

3. To configure the console idle time out parameter, do the following:

    a. Click the **Console UI Time Out** field and enter a new value. The range is 0 to 60 minutes. The default is 5 minutes. A timeout value to 0 causes the console connection to never time out.

        The console idle time out parameter specifies the length of time a local management session can be inactive before the management software automatically ends it. The purpose of this parameter is to prevent unauthorized individuals from configuring the switch should you leave your management workstation unattended.

        This parameter applies to a local management session but not to a web management session. A web browser management session remains active so long as your web browser is open.

        Note
        If you select 0, you must remember to properly log off from a local management session when you are finished to prevent blocking future management sessions with the switch.

    b. Click **Apply**.

4. To enable or disable an SNMP agent, do the following:

    a. Click the **SNMP Agent** parameter and choose **Enable** or **Disable** from the list. The default is Enable. When you enable this parameter, the SNMP agent is enabled.

    b. Click **Apply**.

5. To enable or disable the web server, do the following:

    a. Click the **Web Server** parameter and choose **Enable** or **Disable** from the list. The default is Enable. When you enable this parameter, an individual can manage the switch remotely using a web browser.

        Note
        Disabling the web browser automatically ends your remote management session.

    b. Click **Apply**.

Viewing System Information

To view general information about the switch, perform the following procedure:

1. The Switch Information Page is the page that appears after you log on to the web interface. The Switch Information Page is shown in Figure 61.

Figure 61. Switch Information Page

The Switch Information page displays the following information:

System Up For
The number of days, hours, and minutes that the switch has been running since it was last rebooted.

Runtime Image
The version number and build date of the runtime firmware.

Boot Loader
The version number and build date of the bootloader firmware.

Hardware Information Section:

Revision
The hardware version number.

DRAM Size
The size of the DRAM, in megabytes.

Flash Size
The size of the flash memory, in megabytes.

Console Baud Rate
The baud rate of the console port.

Administration Information Section:

Switch Name
The name assigned to the switch. To give the switch a name, refer to "Configuring System Management Information" on page 226.

Switch Location
The location of the switch. To specify the location, refer to "Configuring System Management Information" on page 226.

Switch Contact
The contact person responsible for managing the switch. To specify the name of a contact, refer to "Configuring System Management Information" on page 226.

System MAC Address, IP Address, Subnet Mask, and Gateway Section:

MAC Address
The MAC address of the switch. You cannot change this value.

IP Address
The IP address of the switch. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 220 to manually assign an IP address or "Enabling and Disabling the DHCP Client" on page 225 to activate the DHCP client.

Subnet Mask
The subnet mask for the switch. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 220 to manually assign a subnet mask or "Enabling and Disabling the DHCP Client" on page 225 to activate the DHCP client.

Default Gateway
Default gateway's IP address. Refer to "Configuring an IP Address, Subnet Mask and Gateway Address" on page 220 to manually assign

a gateway address or "Enabling and Disabling the DHCP Client" on page 225 to activate the DHCP client.

DHCP Mode
The status of the DHCP client on the switch. For information about setting this parameter, refer to "Enabling and Disabling the DHCP Client" on page 225.

Rebooting a Switch

This procedure reboots the switch and reloads the AT-S80 management software from flash memory. You can reboot the device if you believe it is experiencing a problem. Rebooting the switch does not change any of its parameter settings.

⚠ **Caution**
The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To reboot a switch, perform the following procedure:

1. From the **Tools** folder, select **Reboot**.

    The Reboot Page is shown in Figure 62.
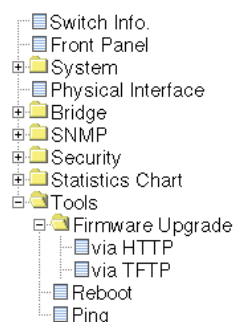
Figure 62. Reboot Page

2. For the Reboot Type, select **Normal Reset**.This is the default setting.

    Note
    The two Reboot Type options **Reset to Factory Default** and are **Reset to Factory Default Except IP Address** are described in "Returning the AT-S80 Management Software to the Factory Default Values" on page 240.

3. For the Reboot Status, select **Start** to start the reboot.

4. Click **Apply**. The switch immediately begins to reload the AT-S80 management software. This process takes approximately one minute to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the device.

Pinging a Remote System

This procedure instructs the switch to ping a node on your network. This procedure is useful in determining whether an active link exists between the switch and another network device. Note the following before performing the procedure:

❏ The switch must have an IP address and subnet mask.

❏ The device to be pinged by the switch must be a member of the Default VLAN. It must be communicating with the switch through an untagged or tagged port of the Default VLAN.

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

1. From the **Tools** folder, select **Ping**.

   The Ping Page is shown in Figure 63.

Figure 63. Ping Page

2. Configure the following parameters:

   Destination IP Address
   The IP address of the node you want to ping.

   Timeout Value
   Specifies the length of time in seconds the switch waits for a response before assuming that a ping has failed. The default is 3 seconds.

   Number of Ping Requests
   Specifies the number of ping requests you want the switch to perform. The default is 10.

3. Click **Start**.

4. To view the ping results, click **Show Ping Results**.

   A sample Ping Test Results page is shown in Figure 64.
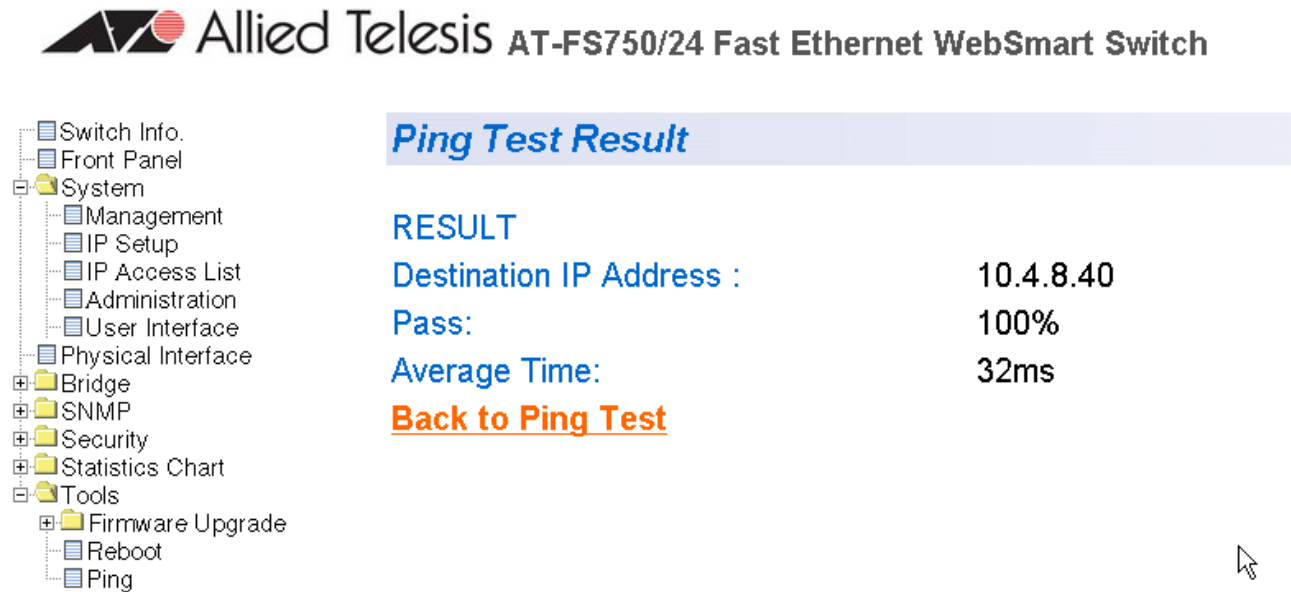
Figure 64. Ping Test Results Page

5. Click **Back to Ping Test** to return to the Ping Test Configuration page.

Returning the AT-S80 Management Software to the Factory Default Values

This procedure returns all AT-S80 Management Software parameters to their default values. The default values are listed in Appendix A, "AT-S80 Software Default Settings" on page 339.

⚠ **Caution**
This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

To return the AT-S80 Management Software to the default settings, perform the following procedure:

1. From the **Tools** menu, select **System Reboot**.

    The Reboot Page is shown in Figure 62 on page 236.

2. For the Reboot Type, select one of the following:

    Reset to Factory Default
    Resets all switch parameters to the factory default settings, including IP address, subnet mask, and gateway address.

    Reset to Factory Default Except IP Address
    Resets all switch parameters to the factory default settings, but retains the IP address, subnet mask, and gateway settings. If the DHCP client is enabled, it remains enabled after this reset.

3. For the Reboot Status, select **Start** to start the reboot.

4. Click **Apply**.

    The switch is rebooted. You must wait for the switch to complete the reboot process before reestablishing your management session.

Chapter 22

Port Configuration

The section in this chapter explains how to view and change the parameter settings of the individual ports on the switch:

❒ "Viewing and Configuring Ports Using the Physical Configuration Page" on page 242

Viewing and Configuring Ports Using the Physical Configuration Page

This procedure explains how to configure the ports on the switch using the Physical Interface Page. This page allows you to view and configure the parameter settings of all the switch ports at one time.

To configure the ports, perform the following procedure:

1. From the book marks on the left side of the page, select **Physical Interface**.

   The Physical Interface Page is shown in Figure 65. The page lists all the ports on the switch and their current settings.

Allied Telesis AT-FS750/24 Fast Ethernet WebSmart Switch

☐Switch Info.
☐Front Panel
⊞☐System
☐Physical Interface
⊞☐Bridge
⊞☐SNMP
⊞☐Security
⊞☐Statistics Chart
⊞☐Tools

Physical Interface

Port Index	Trunk	Type	Link Status	Admin. Status	Mode	Flow Ctrl	
All	-	-	-	Enable	Auto	Disable	Apply
1	-	10/100TX	Up	Enable	Auto (100	Enable	Apply
2	-	10/100TX	Down	Enable	Auto	Enable	Apply
3	-	10/100TX	Down	Enable	Auto	Enable	Apply
4	-	10/100TX	Down	Enable	Auto	Enable	Apply
5	-	10/100TX	Up	Enable	Auto (100	Enable	Apply
6	-	10/100TX	Down	Enable	Auto	Enable	Apply
7	-	10/100TX	Down	Enable	Auto	Enable	Apply
8	-	10/100TX	Down	Enable	Auto	Enable	Apply
9	-	10/100TX	Down	Enable	Auto	Enable	Apply
10	-	10/100TX	Down	Enable	Auto	Enable	Apply
11	-	10/100TX	Down	Enable	Auto	Enable	Apply
12	-	10/100TX	Down	Enable	100M/Full	Enable	Apply
13	-	10/100TX	Down	Enable	Auto	Enable	Apply
14	-	10/100TX	Down	Enable	Auto	Enable	Apply
15	-	10/100TX	Down	Enable	Auto	Enable	Apply
16	-	10/100TX	Down	Enable	Auto	Enable	Apply
17	-	10/100TX	Down	Enable	Auto	Enable	Apply
18	-	10/100TX	Down	Enable	Auto	Enable	Apply
19	-	10/100TX	Down	Enable	Auto	Enable	Apply
20	-	10/100TX	Down	Enable	Auto	Enable	Apply
21	-	10/100TX	Down	Enable	Auto	Enable	Apply
22	-	10/100TX	Down	Enable	Auto	Enable	Apply
23	-	10/100TX	Down	Enable	Auto	Enable	Apply
24	-	10/100TX	Down	Enable	Auto	Enable	Apply
25	-	1000TX	Down	Enable	Auto	Enable	Apply
26	-	1000TX	Down	Enable	Auto	Enable	Apply

Figure 65. Physical Interface Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are defined here:

Port Index
The port number. You cannot change this parameter.

Trunk
The trunk group number. A number in this column indicates that the port has been added to a trunk. For information about configuring a trunk, refer to Chapter 23, "Port Trunking" on page 245.

Type
The port type. The port type will be one of the following:

❒ 10/100BaseTX - Base ports.

❒ 1000TX - Uplink 10/100/1000Base-TX twisted pair ports.

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

Up - A valid link exists between the port and the end node.

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

Admin. Status
The operating status of the port.

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

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for a port.

Disabled - The port is disabled.

Mode
The speed and duplex mode settings for the port.

You can use this parameter to set the speed and duplex mode of a port. Possible settings are:

Auto - The port is using Auto-Negotiation to set the operating speed and duplex mode. This is the default setting for all ports. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.

1000M/Full - 1000 Mbps in full-duplex mode (Uplink ports only.)

100M/Full - 100 Mbps in full-duplex mode

10M/Full - 10 Mbps in full-duplex mode

100M/Half - 100 Mbps in half-duplex mode

10M/Half - 10 Mbps in half-duplex mode

When selecting a setting, note the following:

❏ When a twisted pair port is set to Auto-Negotiation, the default setting, the end node should also be using Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a 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, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

❏ For 1000 Mbps operation on an uplink 10/100/1000Base-T twisted pair uplink port, Allied Telesis recommends using Auto-Negotiation. Setting the speed and duplex mode manually to 1000 Mbps full duplex is not recommended.

❏ The only valid setting for an optional SFP port is Auto-Negotiation.

Flow Control
The current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:

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

Disabled - The port does not use flow control.

3. Click **Apply** to save the configuration.

Chapter 23

Port Trunking

This chapter contains the following procedures for working with port trunking:

❏ "Creating a Port Trunk" on page 246

❏ "Modifying a Port Trunk" on page 248

❏ "Enabling and Disabling a Port Trunk" on page 249

Note
For background information on this feature, refer to "Port Trunking Overview" on page 62.

Creating a Port Trunk

This procedure explains how to create a port trunk.

⚠ **Caution**
Do not connect the cables to the ports on the switches until after you have configured the trunk with the management software. Connecting the cables before configuring the software can create a loop in the network topology. A loop can cause a broadcast storm and poor network performance.

To create a port trunk, perform the following procedure:

1. From the **Bridge** folder, select **Spanning Tree**.

   The System folder expands.

2. From the **Spanning Tree** folder, select **Trunking**.

   The Trunking Page is shown in Figure 66.

Figure 66. Trunking Page

If the switch does not contain a port trunk, all of the ports on the switch are unchecked. If there is a port trunk, the ports in the trunk are checked.

Note
Trunk 7 is reserved for ports 17 and 18 on the AT-FS750/16 and ports 25 and 26 on the AT-FS750/24.

---

3. In any one of the unused Trunk ID rows, click the dialog boxes of the ports that will make up the port trunk. A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to eight ports.

4. Change the status of the trunk from **Disable** to **Enable**.

5. Click **Apply**.

   The trunk is now operational on the switch.

6. Configure the port trunk on the other switch and connect the cables.

Modifying a Port Trunk

This procedure adds and removes ports from a port trunk.

⚠ **Caution**
Disconnect the cables from the ports of the trunk before you modify the trunk. Leaving the cables connected can create a loop in the network topology which, in turn, can cause a broadcast storm and poor network performance.

Note
You cannot modify Trunk 7, which is reserved for the uplink ports. If you want to use the uplink ports as a port trunk, activate Trunk 7 as explained in "Enabling and Disabling a Port Trunk" on page 249.

To add or remove ports from a trunk, perform the following procedure:

1. From the **Bridge** folder, select **Spanning Tree**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **Trunking**.

   The Trunking Page is shown in Figure 66 on page 246.

3. Click the status of the port trunk that you want to modify and change the status from Enable to Disable.

   Note
   Allied Telesis recommends disabling a port trunk before adding or removing ports.

4. Click **Apply**.

5. To add or remove a port from a trunk, click the dialog box for the port in the corresponding trunk row. A check in a box indicates the port is a member of the trunk. No check means the port is not a member.A port trunk can contain up to eight ports.

6. Click **Apply**.

7. Modify the port trunk on the other switch and reconnect the cables.

Enabling and Disabling a Port Trunk

This procedure enables and disables a port trunk. Note the following before performing this procedure:

❒ Do not enable a port trunk until after you have configured the trunk on both switches.

❒ Do not connect the cables to the ports on the switches until after you have configured and enabled the trunk on both switches.

❒ The ports of a disabled trunk forward traffic as individual ports.

⚠ **Caution**
Disconnect the cables from the ports of the trunk before you modify the trunk. Leaving the cables connected can create a loop in the network topology which, in turn, can cause a broadcast storm and poor network performance.

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

1. From the **Bridge** folder, select **Spanning Tree**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **Trunking**.

   The Trunking Page is shown in Figure 66 on page 246.

3. Click the status of the port trunk and change it to **Enable** or **Disable**.

4. Click **Apply**.

Chapter 24

Port Mirroring

This chapter contains the procedure for setting up port mirroring. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by having the traffic copied to another port. This chapter contains the following sections:

❐ "Configuring Port Mirroring" on page 252

❐ "Disabling Port Mirroring" on page 253

> **Note**
> For background information on this feature, refer to "Port Mirroring Overview" on page 86.

Configuring Port Mirroring

To set up port mirroring, perform the following procedure:

1. From the **Bridge** folder, select **Spanning Tree**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **Mirroring**.

   The Mirroring Page is shown in Figure 67.

Figure 67. Mirroring Page

3. In the **Mirroring Port** field, select the port where the network analyzer is connected from the pull-down menu.

4. In the **Ingress Port** field, select the port whose ingress traffic you want to monitor from the pull-down menu. You can select only one port.

5. In the **Egress Port** field, select the port whose egress traffic you want to monitor from the pull-down menu. You can select only one port.

6. Click **Apply** on the right-hand side of the page.

7. From the **Status** field, select **Enable**. Then click **Apply**.

   Port mirroring is immediately enabled on the switch. You can now connect a data analyzer to the mirroring port to monitor the traffic on the other port.

Disabling Port Mirroring

To disable port mirroring, perform the following procedure:

1. From the **Bridge** folder, select **Spanning Tree**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder**,** select **Mirroring**.

   The Mirroring Page is shown in Figure 67 on page 252.

3. From the Status field, select **Disable** from the pull-down menu. Then click **Apply**.

   Port mirroring is disabled on the switch immediately. You can now use the mirroring port for regular network operations.

Chapter 25

Static Multicast Address Table

This chapter contains the following procedures for setting group MAC addresses in the web interface:

❒ "Configuring Static Multicast Address Table" on page 256

❒ "Modifying a Static Multicast Address Table" on page 258

❒ "Deleting a Group MAC Address" on page 259

> **Note**
> For background information, refer to Chapter 7, "Static Multicast Address" on page 79.

Configuring Static Multicast Address Table

This procedure explains how to add group MAC addresses to the Static Multicast Address Table.

To configure the Static Multicast Address Table, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **Static Multicast**.

   The Static Multicast Address Table Page is shown in Figure 68.

Figure 68. Static Multicast Address Table Page

3. To add a group MAC address to the Static Multicast Address table, enter a MAC address in the Group MAC Address field. Use the xx:xx:xx:xx:xx:xx format.

   Enter a value between 01:00:5E:00:01 to 01:00:5E:7F:FF:FF.

   > **Note**
   > Use the Tab key to advance from one MAC address segment to the next.

4. To set the group member of the group MAC address, click a number next to the **Group Member** field. Then press **Add**.

   The Static Multicast Address Table is updated with the new information. See Figure 69 on page 257 for an example.

Figure 69. Static Multicast Table with Group MAC Addresses

Modifying a Static Multicast Address Table

This procedure explains how to change the group number of the Static Multicast Address Table.

To modify the group number in the Static Multicast Address Table, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **Static Multicast**.

   The Static Multicast Address Table Page is shown in Figure 68 on page 256.

3. Click **modify** next to the group number that you want to change.

   The Modify Static Multicast Address Table Page is displayed. See Figure 70.
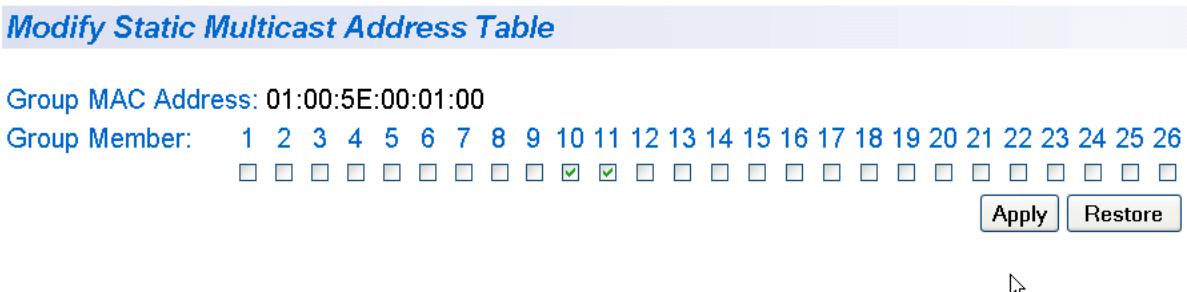
Figure 70. Modify Static Multicast Address Table Page

4. Click the new Group Member number and deselect the original Group Member number.

   Note
   To restore the previous Group Member number, click **Restore**.
   ---

5. Click **Apply**.

Deleting a Group MAC Address

To delete a Group MAC Address from the Static Multicast Address Table, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder**,** select **Static Multicast**.

   The Static Multicast Address Table Page is shown in Figure 68 on page 256.

3. Click **delete** next to the group number that you want to remove.

   The Static Multicast Address Table Page is updated.

Chapter 26

IGMP Snooping

This chapter contains the following procedures for working with IGMP Snooping in the web interface. Sections in the chapter include:

❑ "Configuring IGMP Snooping" on page 262

Note
For background information, refer to "IGMP Snooping Overview" on page 72.

Configuring IGMP Snooping

This procedure explains how to set IGMP snooping and the IGMP Snooping age-out timer on the switch.

To configure IGMP snooping, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Spanning Tree folder expands.

2. From the Spanning Tree folder, select **IGMP Snooping**.

   The IGMP Snooping Page is shown in Figure 71.
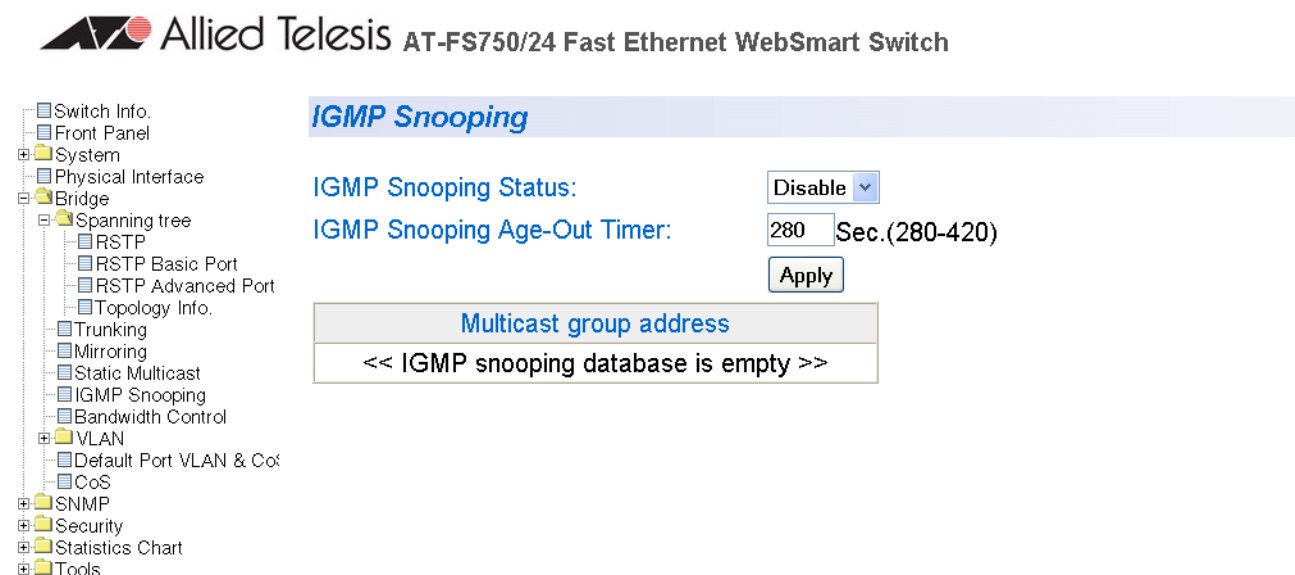
Figure 71. IGMP Snooping Page

3. To enable or disable IGMP Snooping on the switch, select **Enable** or **Disable**. Then press **Apply**.

   By default, IGMP is disabled.

4. To set the age-out timer, type the number of seconds you want the switch to wait before it purges an inactive dynamic MAC address. Then press **Apply**.

   For an IGMP member port, the Set Age-Out Timer is set to 280 seconds by default. The range of this parameter is from 280 to 420 seconds.

   For an IGMP router port, the Set Age-Out Timer is set to 130 seconds by default. This value cannot be changed.

Note
The **Multicast Group Address** field contains MAC addresses of nodes that are members of multicast groups. To set a Multicast Group Address, see "Setting Group Members" on page 76. You cannot configure this field in the web interface.

Chapter 27

Destination MAC Address Filter

This chapter contains the following procedures for setting MAC addresses in the Destination MAC Filter in the web interface:

❒ "Setting a Destination MAC Filter" on page 266

❒ "Removing a MAC Address" on page 268

Note
For background information, refer to "Destination MAC Filtering Overview" on page 182.

Setting a Destination MAC Filter

This procedure explains how to set a Destination MAC Filter on the switch.

To add a MAC address from a Destination MAC Filter list, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Security**.

    The Security folder expands.

2. From the Security folder, select **Destination MAC Filter**.

    The Destination MAC Filter Page is shown in Figure 72.

Figure 72. Destination MAC Filter Page

3. To add a device, type in a MAC address in the xx:xx:xx:xx:xx:xx format. Then click **Add**.

    > **Note**
    > Use the Tab key to advance from one MAC address segment to the next.

The Destination MAC Filter table is updated with the new MAC address. See Figure 73 for an example.

Figure 73. Destination MAC Address with Entries

Removing a MAC Address

To remove a MAC address from a Destination MAC Filter list, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Security**.

   The Security folder expands.

2. From the Security folder, select **Destination MAC Filter**.

   The Destination MAC Filter Page is shown in Figure 73 on page 267

3. To remove a device, click **delete** next to the MAC address you want to remove.

   The Destination MAC Filter table is updated.

Chapter 28

Bandwidth Control

This chapter contains the following procedures for working with Bandwidth Control in the web interface. Sections in the chapter include:

❒ "Configuring Bandwidth Control" on page 270

> **Note**
> For background information, refer to "Bandwidth Control Overview" on page 172.

Configuring Bandwidth Control

This procedure explains how to set Bandwidth Control on a port.

To configure Bandwidth Control, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

    The options under the Bridge folder expand to include Spanning Tree.

2. From the Spanning Tree folder, select **Bandwidth Control**.

    The Bandwidth Control Page is shown in Figure 74.

Figure 74. Bandwidth Control Page

3. To change the status of the packet threshold for all the ports on the switch, select the pull-down menu next to the Broad/Multicast Packet Threshold field. Choose **Low**, **Medium**, and **High** from the pull-down menu. Then press **Apply**.

   By default, the packet threshold is set to **Low**.

4. To set the DLF Ingress Packet Status for all the ports on the switch, select the pull-down menu next to the DLF Ingress Packet Status field. Choose **Enable** or **Disable**. Then press **Apply**.

   By default, the packet status is set to **Disable**.

5. To select the Ingress mode of a port, select the pull-down menu next to the **Ingress** field. Choose **Enable** or **Disable**. Then press **Apply**.

   By default, the Ingress field is set to **Disable**.

6. To select the mode of a port, select the select the pull-down menu next to the **Mode** field. Choose **Bcast** for broadcast mode or **Bcast/Mcast** for multicast mode. Then press **Apply**.

   By default, the Mode field is set to **Bcast/Mcast**.

Chapter 29

Virtual LANs

This chapter contains the procedures for creating, modifying, and deleting port-based and tagged Virtual Local Area Networks (VLANs) from a web browser management session. This chapter contains the following sections:

❐ "Assigning Ports to a VLAN" on page 274

❐ "Creating a Tagged VLAN" on page 275

❐ "Modifying a Tagged VLAN" on page 277

❐ "Deleting a Tagged VLAN" on page 279

❐ "Creating a Port-Based VLAN" on page 280

❐ "Modifying a Port-Based VLAN" on page 281

❐ "Deleting a Port-Based VLAN" on page 283

> **Note**
> For background information, refer to "Port-based VLAN Overview" on page 100 and "Tagged VLAN Overview" on page 101.

Assigning Ports to a VLAN

To assign ports to a tagged or port-based VLAN, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

    The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

    The VLAN folder expands.

3. From the VLAN folder, select **VLAN Mode**.

    The VLAN Mode Page is shown in Figure 75.
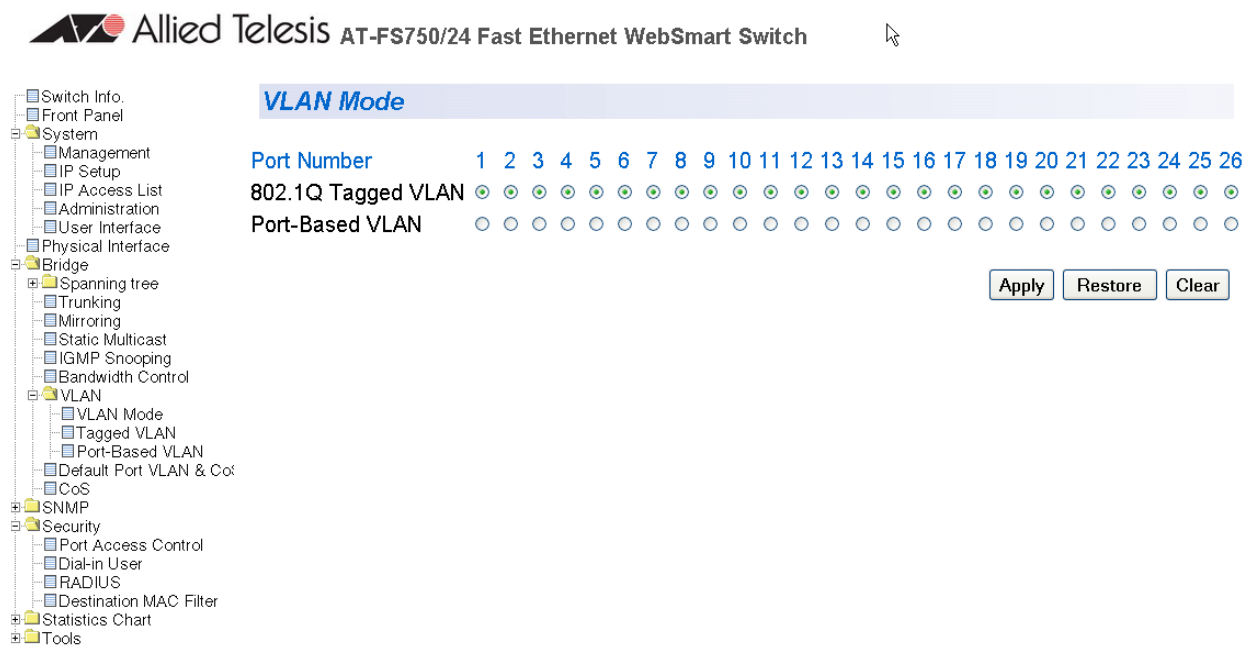
Figure 75. VLAN Mode Page

4. To add ports to a Tagged or Port-Based VLAN, select the ports and then click **Apply**.

Creating a Tagged VLAN

To create a tagged VLAN, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

    The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

    The VLAN folder expands.

3. From the VLAN folder, select **Tagged VLAN**.

    The Tagged VLAN Page is shown in Figure 76

Figure 76. Tagged VLAN Page

4. To assign a VLAN ID, type in a VLAN ID in the **VLAN ID** field.

    Choose a value between 2 and 4,000.

5. To assign a name to the VLAN, type in a name in the **VLAN Name** field.

6. To assign ports to the VLAN, click on the port numbers labeled either Static Tagged or Static Untagged. Then click **Apply**.

    By default, all the ports are assigned to the **Not Member** category.

For an example of Tagged VLANs, see Figure 77.

Figure 77. Example of Tagged VLAN Page

Modifying a Tagged VLAN

To modify a tagged VLAN, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

    The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

    The VLAN folder expands.

3. From the VLAN folder, select **Tagged VLAN**.

    An Example of a Tagged VLAN page is shown in Figure 77 on page 276.

4. In the VLAN Action column, click **modify** next to the VLAN that you want to change.

    The Modify VLAN Page is displayed, see Figure 78

Figure 78. Modify VLAN Page

5. To change the VLAN ID, type in a VLAN ID in the **VLAN ID** field.

    You can choose a value between 2 and 4,000.

6. To change the name of the VLAN, type in a name in the **VLAN Name** field.

7. To assign ports to the VLAN, click on the port numbers labeled either Static Tagged or Static Untagged. Then click **Apply**.

Deleting a Tagged VLAN

To delete a tagged VLAN, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

   The VLAN folder expands.

3. From the VLAN folder, select **Tagged VLAN**.

   An example of the Tagged VLAN page is shown in Figure 77 on page 276.

4. In the VLAN Action column, click **delete** next to the VLAN that you want to delete.

   A confirmation prompt is displayed.

5. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

   Note
   You cannot delete the Default VLAN which has a VID of 1.

Creating a Port-Based VLAN

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

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

   The VLAN folder expands.

3. From the VLAN folder, select **Port-Based VLAN**.

   The Port-Based VLAN Page is shown in Figure 79.
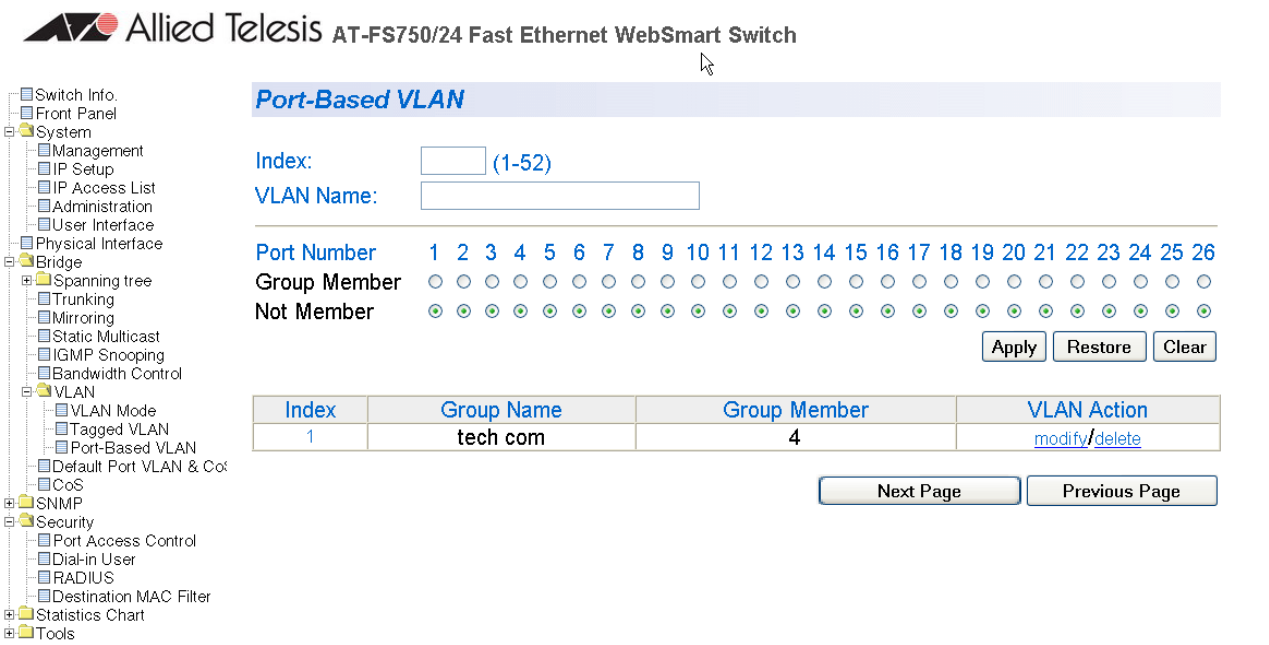
Figure 79. Port-Based VLAN Page

4. To assign a VLAN ID, type a VLAN ID in the **VLAN ID** field.

   You can choose a value between 2 and 4,000.

5. To assign a name to a VLAN, type in a name in the **VLAN Name** field.

6. To assign ports to the VLAN, click on the port numbers labeled either Static Tagged or Static Untagged. Then click **Apply**.

Modifying a Port-Based VLAN

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

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

   The VLAN folder expands.

3. From the VLAN folder, select **Port-Based VLAN**.

   The Port-Based VLAN Page is shown in Figure 79 on page 280.

4. In the VLAN Action column, click **modify** next to the VLAN that you want to change.

   The Modify Port-based VLAN Page is shown in Figure 80.

Figure 80. Modify Port-based VLAN

5. To change the VLAN ID, type a VLAN ID in the **Index** field.

   You can choose a value between 2 and 4,000.

6. To change the name of the VLAN, type in a name in the **VLAN Name** field.

7. To assign ports to the VLAN, click on the port numbers labeled either Static Tagged or Static Untagged. Then click **Apply**.

Deleting a Port-Based VLAN

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

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **VLAN**.

   The VLAN folder expands.

3. From the VLAN folder, select **Port-Based VLAN**.

   The Port-Based VLAN Page is shown in Figure 79 on page 280.

4. In the VLAN Action column, click **delete** next to the VLAN that you want to delete.

   A confirmation prompt is displayed.

5. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

   Note
   You cannot delete the Default VLAN which has a VID of 1.

Chapter 30
Simple Network Management Protocol (SNMP)

This chapter contains the following procedures for working with SNMP:

Note
For background information, refer to "SNMP Overview" on page 120.

Creating an SNMP Community

This procedure explains how to create an SNMP community with the web interface.

To create an SNMP community, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

    The SNMP folder expands.

2. From the SNMP folder, select **Community Table**.

    The Community Table Page is shown in Figure 81.

Figure 81. Community Table Page

3. Type an available entry number from 1 through 8 next to the Entry number field.

4. To select the read/write access for the community, use the pull-down menu next to the Access field to select Read-Only access or Read-Write access.

5. Type the name of the new SNMP community in the Community field. Then click **Add**.

    Enter a name between 1 and 20 characters in length.

Modifying an SNMP Community

Use the following procedure to modify the name and the access level of an existing SNMP community. You cannot change the Index entry.

To change the name and access level of a community, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the **SNMP** folder**,** select **Community Table**.

   The Community Table Page is shown in Figure 81 on page 286.

3. To change the access level of an SNMP community, select the pull-down menu under the Access column in the Community table for the community you want to modify. Select **Read-Only** access or **Read-Write** access.

4. To change the community name, type over an existing community name. Then click **Apply**.

Deleting an SNMP Community

Use the following procedure to delete an SNMP community in the Community Table.

1. From the bookmarks on the left side of the page, select **SNMP**.

    The SNMP folder expands.

2. From the **SNMP** folder**,** select **Community Table**.

    The Community Table Page is shown in Figure 81 on page 286.

3. To delete a community, select **delete** in the Community Table next to the community that you want to remove.

    The Community Table Page is updated.

Creating a Host Table

Use the following procedure to create a Host Table.

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the **SNMP** folder**,** select **Host Table**.

   The Host Table Page is shown in Figure 82.

Figure 82. Host Table Page

3. To specify an entry number, type a value between 1 and 10 in the Entry number field.

4. Enter an IP address for an SNMP community that you previously defined in the Community Table Page.

   The IP address must be in the xxx.xxx.xxx.xxx format.

5. Select a community name from the pull-down menu next to the Community Name field. Then click **Add**.

   The new host is added to the table.

Modifying a Host Table Entry

Use the following procedure to modify the community name assignment or the IP address of an entry in the Host Table.

To modify an entry in the Host Table, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the **SNMP** folder**,** select **Host Table**.

   The Host Table Page is shown in Figure 82 on page 289.

3. To change the IP Address, type in the new IP address in the Host Table.

4. To change the community name, use the pull-down menu to select a new community name in the Host Table.

5. To activate your changes on the switch, click **Apply** next to the entry that you want to modify.

Deleting a Host Table Entry

Use the following procedure to delete a Host Table entry.

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the **SNMP** folder**,** select **Host Table**.

   The Host Table Page is shown in Figure 82 on page 289.

3. To delete an entry in the host table, click **<u>delete</u>** next to the entry in the table that you want to remove.

Enabling or Disabling Traps

This procedure enables or disables traps for an SNMP community that was previously defined. For more information, see "Creating an SNMP Community" on page 286.

To enable or disable a trap, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the SNMP folder**,** select **Trap Setting**.

   The Trap Setting Page is displayed in Figure 83.

Figure 83. Trap Setting Page

3. Type a trap number between 1 and 10 in the Entry number field.

4. Select the SNMP version of the trap by selecting **V1** for SNMP version 1 or **V2c** for SNMP version 2vc in the **Version** field.

5. Enter an IP address, in the xxx.xxx.xxx.xxx format, in the **IP Address** field.

6. Enter a previously defined community name in the **Community** field. Then click **Add**.

   A new trap is displayed in the Trap Setting table.

Modifying Traps

Use this procedure to modify the IP address and the SNMP version of a trap for an SNMP community.

To modify a trap, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

   The SNMP folder expands.

2. From the SNMP folder, select **Trap Setting**.

   The Trap Setting Page is shown in Figure 83 on page 292.

3. Within the Trap Setting table, select a pull-down menu in the Version column to the change the SNMP version of a trap that you want to modify.

   Select the SNMP version of the trap by selecting **V1** for SNMP version 1 or **V2c** for SNMP version 2vc.

4. Change an IP address by typing in the new IP address for a particular community within the Trap Setting table.

   Use the IP address format: xxx.xxx.xxx.xxx

5. To activate your changes on the switch click **Apply**.

   The Trap Setting Page is updated.

Deleting Traps

Use this procedure to delete traps from an SNMP community.

To delete a trap, perform the following procedure:

1. From the bookmarks on the left side of the page, select **SNMP**.

    The SNMP folder expands.

2. From the SNMP folder**,** select **Trap Setting**.

    The Trap Setting Page is shown in Figure 83 on page 292.

3. In the Trap table, click delete next to the trap you want to delete from the table.

    The Trap Setting Page is updated.

Chapter 31

Quality of Service (QoS)

This chapter contains the procedure for configuring Quality of Service (QoS). This chapter includes the following procedures:

❒ "Mapping CoS Priorities to Egress Queues" on page 296

❒ "Configuring CoS" on page 298

Note
For background information, refer to "QoS Overview" on page 140

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, as shown in Table 2 on page 141. This is set at the switch level. You cannot set this at the per-port level. This procedure also enables and disables QoS.

To change the default mappings of CoS priorities to egress priority queues or to enable or disable QoS, perform the following procedure:

1. From the bookmarks on the left side of the page, click on **Bridge**.

   The Bridge folder expands to include the VLAN folder.

2. From the **VLAN** folder, select **CoS**.

   The CoS Page is shown in Figure 84.

Figure 84. CoS Page

3. To enable or disable QoS, select **Enable** or **Disable** from the QoS Status pull-down menu. The default is Disable.

4. To change the egress priority queue assignment of an 802.1p priority class, click the dialog circle of the queue for the corresponding priority. For example, to direct all tagged traffic with a priority of 4 to egress queue 3 on the ports, click the dialog circle for queue 3 in the priority 4 row.

5. Click **Apply**.

Note

The switch does not alter the original priority level in tagged frames. Frames leave the switch with the same priority level they had when they entered the switch.

Configuring CoS

As explained in "QoS Overview" on page 140, a packet received on a port is placed it into one of four priority queues on the egress port according to the switch's mapping of 802.1p priority levels to egress priority queues. The default mappings are shown in Table 2 on page 141.

You can override the mappings at the port level by assigning a new default egress queue to a port. Note that this assignment is made 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, you can configure a switch port so that all ingress frames are stored in egress queue 3 of the egress port, regardless of the priority levels that might be in the frames themselves, as found in tagged frames.

> **Note**
> The switch does not alter the original priority level in tagged frames. Frames leave the switch with the same priority level they had when they entered the switch.

To configure CoS for a port, perform the following procedure:

1. From the bookmarks on the left side of the page, click on **Bridge**.

   The Bridge folder expands to include the VLAN folder.

2. From the VLAN folder, select **Default Port VLAN & CoS**.

The Default Port VLAN & CoS Page is shown in Figure 85.

Figure 85. Default Port VLAN &CoS Page

The columns in the menu display the following information:

Port Index
Displays the port number.

Trunk
Displays the trunk number if the port is a member of a trunk.

Traffic Class
Displays the traffic class whose egress priority queue you want to change. The range is 0 to 7. You can specify only one traffic class at a time. Specifying traffic class 0 affects untagged traffic as well as tagged traffic with a priority level of 0. The default value is 0.

Queue

Displays the number of the queue where untagged packets received on the port are stored on the egress queue. In this field, 0 is the lowest value and 3 is the highest value.

Override

Displays whether the priority level in ingress tagged frames is being used or not. If No, the override is deactivated and the port is using the priority levels contained within the frames to determine the egress queue. If Yes, the override is activated and the tagged packets are stored in the egress queue specified in the Queue column.

3. To assign a PVID to a port, type a PVID between 1 and 4,000 in the **PVID** field.

    For information about the PVID, see "Port VLAN Identifier" on page 102.

4. To change the egress queue where ingress untagged frames received on a port are to be stored on the egress port, use the pull-down menu in the Queue column and select the desired queue. The range is 0 (lowest) to 3 (highest). The default is 0. For example, if you select 3 for queue 3 for a port, all ingress untagged packets received on the port are stored in egress queue 3 on the egress port. (If you perform Step 3 and override the priority level in ingress tagged packets, this also applies to tagged packets as well.)

    If the selected port is part of a port trunk, all ports in the trunk are automatically assigned the same egress queue.

5. To configure a tagged port so that the switch ignores the priority tag in ingress tagged frames, select **Enable** from the Override column for the corresponding port.

    The default for this parameter is disabled, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.

6. Click **Apply**.

    > **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.

Chapter 32

Rapid Spanning Tree Protocol (RSTP)

This chapter contains the following procedures for working with the Remote Spanning Tree Protocol (RSTP):

❒ "Basic RSTP Configuration" on page 302

❒ "Configuring RSTP Port Settings" on page 305

❒ "Viewing the RSTP Topology" on page 309

> **Note**
> For background information on RSTP, refer to "RSTP Overview" on page 150.

Basic RSTP Configuration

To configure the RSTP settings, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **Spanning Tree.**

3. From the Spanning Tree folder, select **RSTP**.

   The Rapid Spanning Tree Configuration Page is shown in Figure 86.
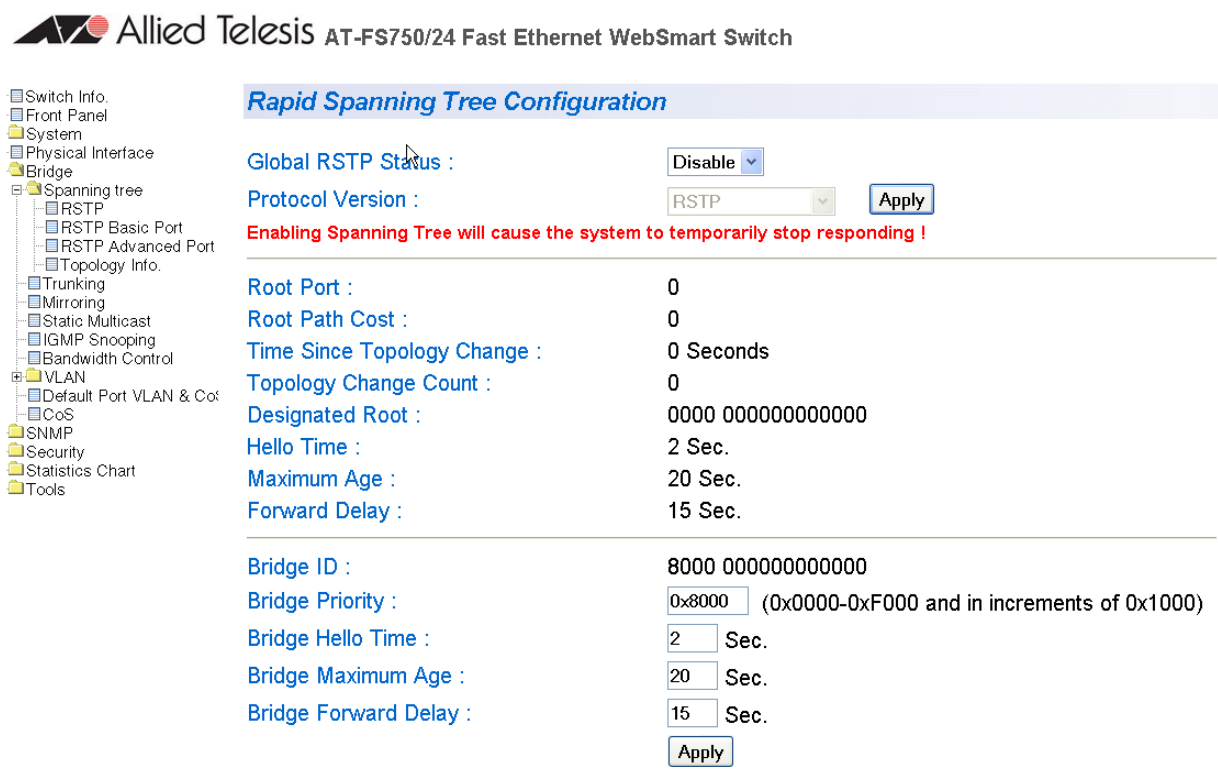
Figure 86. Rapid Spanning Tree Configuration Page

The RSTP Configuration page allows you to configure RSTP as well as to view the current settings. In the upper portion of the page, you can set the following parameters:

Global RSTP Status
Set this field to enable to activate RSTP on the switch. The default is disable.

Protocol Version
Set this field to enable to activate RSTP on the switch. This field is greyed out until you set the Global RSTP Status to enable. To activate this field click **Apply**.

This page contains the following items of information in the middle portion of the page. You cannot change these fields.

Root Port
The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port and the root port parameter is set to 0.

Root Path Cost
The sum of all the root port costs of all the bridges between the switch's root port and the root bridge including the switch's root port cost.

Time Since Topology Change
The time in seconds since the last topology change took place. When RSTP detects a change to the LAN's topology or when the switch is rebooted, this parameter is reset to 0 seconds and begins incrementing until the next topology change is detected.

Topology Change Count
An integer that reflects the number of times RSTP has detected a topology change on the LAN since the switch was initially powered on or rebooted.

The following parameters refer to the designated root bridge. You cannot change these fields.

Designated Root
This parameter includes two fields: the root bridge priority and the MAC address of the root bridge. For example, 1000 00C08F1211BB shows the root bridge priority as 1000, and 00C08F1211BB as the MAC address.

Hello Time
The hello time. See "Hello Time and Bridge Protocol Data Units (BPDUs)" on page 153. This parameter affects only the root bridge.

Maximum Age
The maximum amount of time that BPDUs are stored before being deleted on the root bridge.

Forward Delay
The time interval between generating and sending configuration messages by the root bridge.

The lower section provides information about the bridge. The following parameters appear in the bottom third of the page.

Bridge ID

The MAC address of the bridge. The bridge identifier is use as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority. You cannot change this setting.

Bridge Priority

The priority number for the bridge, in hexadecimal format. This number is used to determine the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, that is, the lowest value of all the other bridges, then the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes offline, the bridge with the lowest priority number automatically takes over as the root bridge. This parameter can be from 0X0000 to 0XF000, with 0XF000 being the highest priority.

Bridge Hello Time

This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Bridge Maximum Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge.

Bridge Forward Delay

This is the time interval between generating and sending configuration messages by the bridge.

Configuring RSTP Port Settings

This section contains the following topics:

❐ "Configuring the Basic RSTP Port Settings," next

❐ "Configuring the Advanced RSTP Port Settings" on page 307

Configuring the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **Spanning Tree.**

   The Spanning Tree folder expands.

3. From the Spanning Tree folder, select **RSTP Basic Port**.

The RSTP Basic Port Configuration Page is shown in Figure 87.

RSTP Basic Port Configuration

Port	Trunk	Link Status	Port State	Role	STP Status	Priority	Path Cost	
All	-	-	-	-	Enable			Apply
1	-	Up	Forwarding	Disabled	Enable	128	200000	Apply
2	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
3	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
4	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
5	-	Up	Forwarding	Disabled	Enable	128	200000	Apply
6	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
7	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
8	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
9	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
10	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
11	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
12	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
13	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
14	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
15	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
16	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
17	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
18	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
19	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
20	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
21	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
22	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
23	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
24	-	Down	Forwarding	Disabled	Enable	128	200000	Apply
25	-	Down	Forwarding	Disabled	Enable	128	20000	Apply
26	-	Down	Forwarding	Disabled	Enable	128	20000	Apply

Figure 87. RSTP Basic Port Configuration Page

4. In the STP Status column for the port you want to configure, select the STP status from the list, either Enable or Disable.

5. In the Priority column for the port you want to configure, type a number for the port priority.

Port priority is described in "Port Priority" on page 152.

6. In the Path Cost column for the port you want to configure, type a number for the Path Cost.

   Path cost is described in "Path Costs and Port Costs" on page 151.

7. Click **Apply**.

8. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: STP Status, Priority, and Path Cost. Then click **Apply**.

Configuring the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

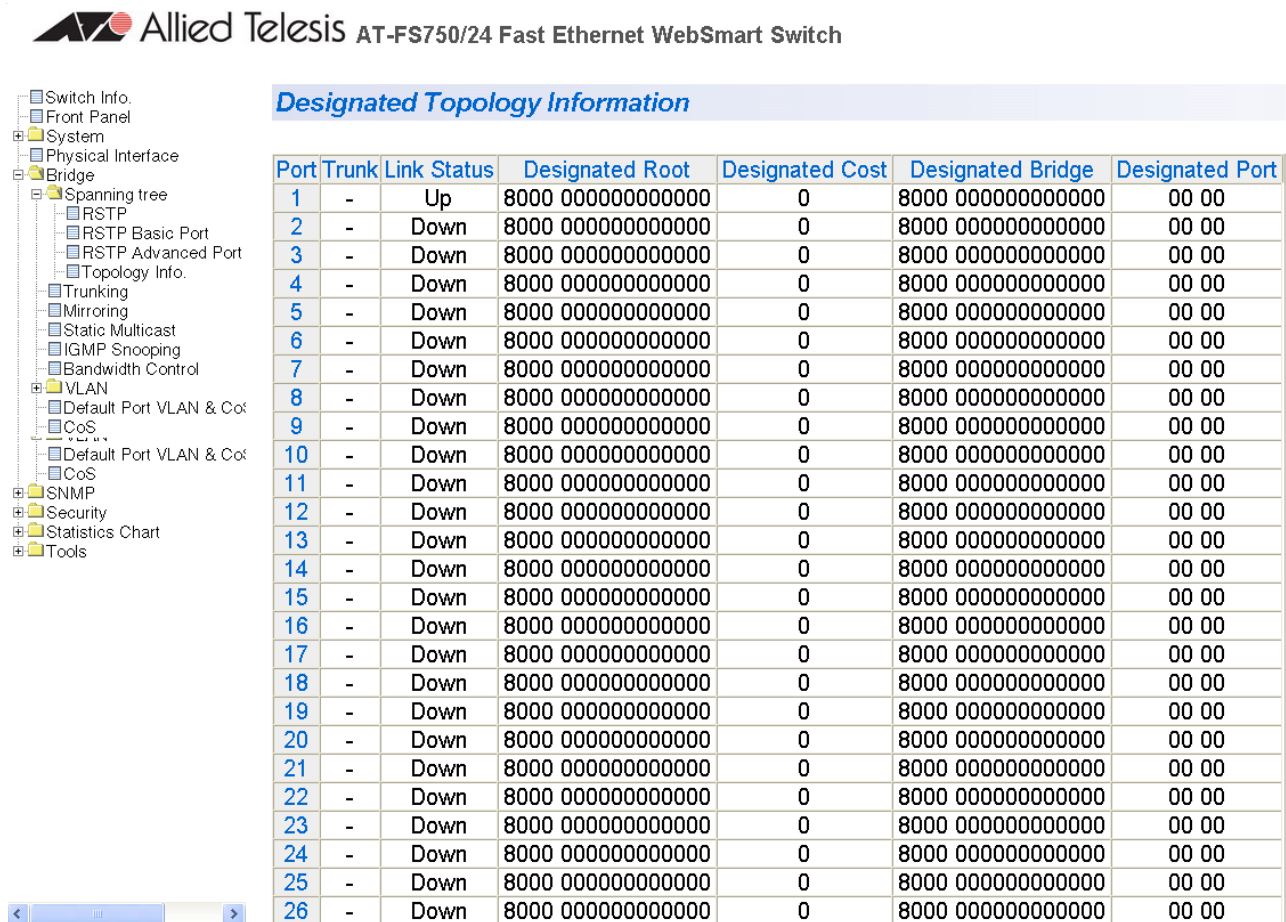1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Spanning Tree folder, select **Spanning Tree.**

   The Spanning Tree folder expands.

3. From the Spanning Tree folder, select **RSTP Advanced Port**.

The RSTP Advanced Port Configuration Page is shown in Figure 88.

RSTP Advanced Port Configuration

Port	Trunk	Link	State	Role	Admin/OperEdge	Admin/OperPtoP	Migration	
All	-	-	-	-	True ▾	Auto ▾	Restart	Apply
1	---	Up	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
2	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
3	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
4	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
5	---	Up	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
6	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
7	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
8	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
9	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
10	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
11	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
12	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
13	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
14	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
15	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
16	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
17	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
18	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
19	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
20	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
21	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
22	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
23	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
24	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
25	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply
26	---	Down	Forwarding	Disabled	False ▾ /False	Auto ▾ /False	Init / Restart	Apply

Figure 88. RSTP Advanced Port Configuration Page

4. In the Admin/OperEdge column for the port you want to configure, choose True or False to set whether or not the port will operate as an edge port.

5. In the Admin/OperPtoP column for the port you want to configure, choose a setting based on the information in Table 6 on page 167.

6. In the Migration column for the port you want to configure, click **Restart** to reset the port.

7. Click **Apply**.

8. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: Admin/OperEdge, Admin/OperPtoP, and Migration. Then click **Apply**.

Viewing the RSTP Topology

To view the current RSTP topology, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Bridge**.

   The Bridge folder expands.

2. From the Bridge folder, select **Spanning Tree.**

   The Spanning Tree folder expands.

3. From the Spanning Tree folder, select **Topology Info**.

   The Designated Topology Information Page is shown in Figure 89.

Figure 89. Designated Topology Information Page

This page displays the following information about the ports:

Port Trunk
Indicates the trunk of which the port is a member.

Link Status
Indicates the whether the link on the port is up or down.

Designated Root
Indicates the designated root bridge to which the switch's root port is actively connected.

Designated Cost
Indicates the sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Designated Bridge
Indicates the an adjacent bridge to which the root port of the switch is actively connected.

Designated Port
Indicates the root bridge to which the root port of the switch is actively connected.

Chapter 33

802.1x Port-based Network Access Control Feature

This chapter contains the procedure for configuring 802.1x Port-based Network Access Control:

❒ "Configuring 802.1x Port-based Network Access Control Feature" on page 312

> **Note**
> For background information, refer to "802.1x Port-based Network Access Control Overview" on page 186.

Configuring 802.1x Port-based Network Access Control Feature

To configure the 802.1x Port-based Network Access Control feature, perform the following procedure:

1. From the bookmarks on the left side of the page, click **Security.**

   The Security folder expands.

2. From the Security folder, select **Port Access Control**.

   The 802.1x Access Control Configuration Page is shown in Figure 90.
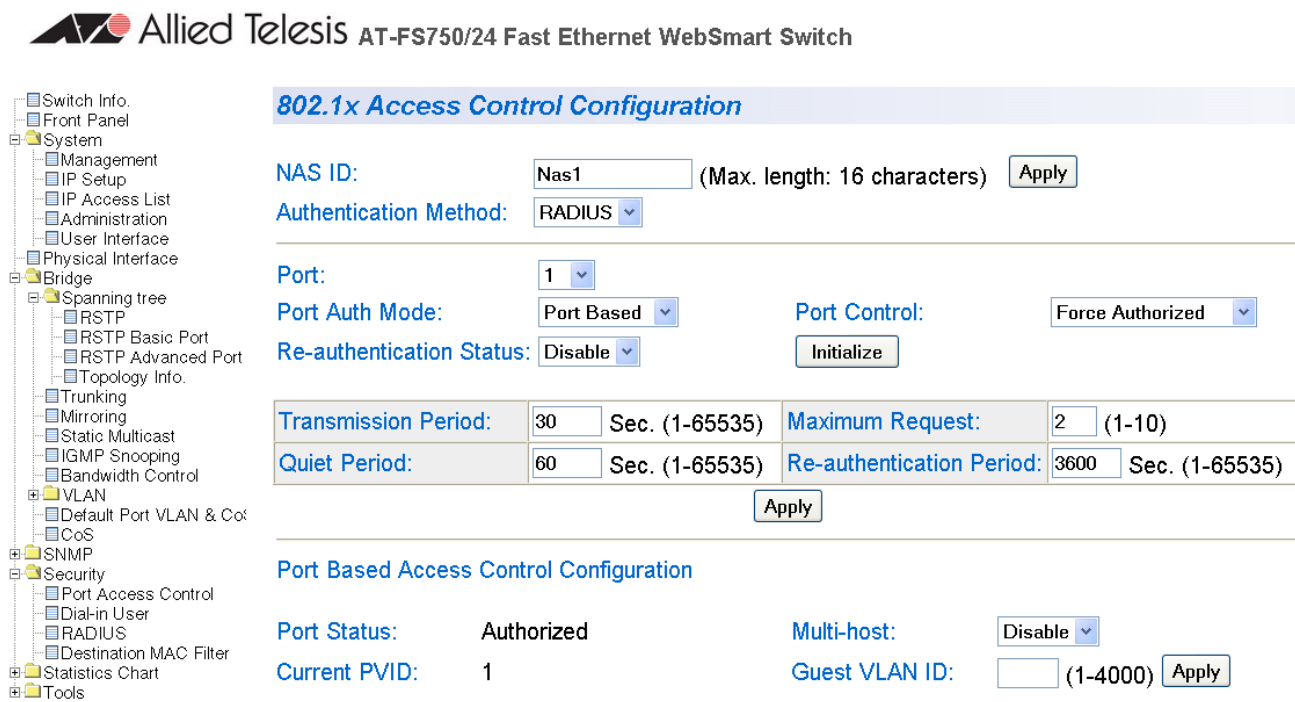
Figure 90. 802.1x Access Control Configuration Page

Note
The Initialize and Re-auth Initialize parameters are described in Steps 5 and 6, respectively.

---

3. To select a port, click the **Port** field and select the port you want to configure from the pull-down menu. You can configure only one port at a time.

   The current settings for the selected port are displayed.

4. Configure the following parameters as needed. The parameters are defined here:

NAS ID
This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional. Click **Apply**.

Authentication Method
Displays the current authentication method setting. The possible settings are:

RADIUS - The authentication method is set to an external RADIUS server. The default setting is RADIUS.

Local - The authentication method is set to the local switch.

Note
For information about the RADIUS protocol, see "RADIUS Overview" on page 202

Port Auth Mode
The possible settings are:

Port Based - Indicates the port authentication mode is set to a port based method. The default value is Port Based. For guidelines, see "Configuring 802.1x Port-based Network Access Control Feature" on page 193.

MAC Based - Indicates the port authentication mode is set to a MAC address based method. See Chapter 17, "Configuring MAC Based Access Control Feature" on page 197.

Re-authentication Status
Specifies if reauthentication should occur according to the reauthentication period. The options are Enable or Disable. By default, this field is set to Disable.

Port Control
Sets the 802.1x port control setting. The possible settings are:

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 or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication prompts between the client and the authentication server.

Force-unauthorized - Places the port in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Force-authorized - Disables IEEE 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. This is the default setting

Transmission 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.

Quiet Period
Sets the number of seconds that the port 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.

Maximum Request
Sets 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.

Re-authentication Period
Specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Port Status
Displays the current 802.1 status of the port as either authorized or unauthorized. This is not an adjustable parameter.

Current PVID
Displays the current port VLAN identifier or PVID assignment of the port. You cannot change this value from the Port Based Access Control Configuration Menu. See Chapter 10, "Virtual LANs" on page 97 for information about assigning a PVID.

Multi-host
Displays the current status of the multi-host status. The options are Enable or Disable. By default, this field is set to Disable.

Guest VLAN ID
Displays the guest VLAN ID set for the port. Select a value between 1 and 4,000. By default, this field is blank. For more information about guest VLAN IDs, see "Guest VLANs" on page 192.

5. When you are finished configuring the parameters, click **Apply** at the bottom of the 802.1x Access Control Configuration Page.

6. If the port control setting is Auto and you want to return the EAPOL machine state on the port to the initialized state, select **Yes** for the Initialize parameter and click **Apply**.

7. If the port control setting is Auto and you want the node connected to the port to reauthenticate with the RADIUS server, select **Yes** for the Re-auth Initialize parameter and click **Apply**.

Chapter 34

Dial-in User

This chapter contains the following procedure for setting the Dial-in User feature in the web interface.

❒ "Adding a Dial-in User" on page 318

❒ "Modifying a Dial-in User" on page 319

❒ "Deleting a Dial-in User" on page 320

Note

For background information, refer to "Dial-in User Configuration Overview" on page 92.

Adding a Dial-in User

This procedure explains how to add a Dial-in User on the switch. For each user, you must assign an user name, password, and a VLAN.

To configure a Dial-in User, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Security**.

    The Security folder expands.

2. From the Security folder, select **Dial-in User**.

    The Dial-in User Page is shown in Figure 91.
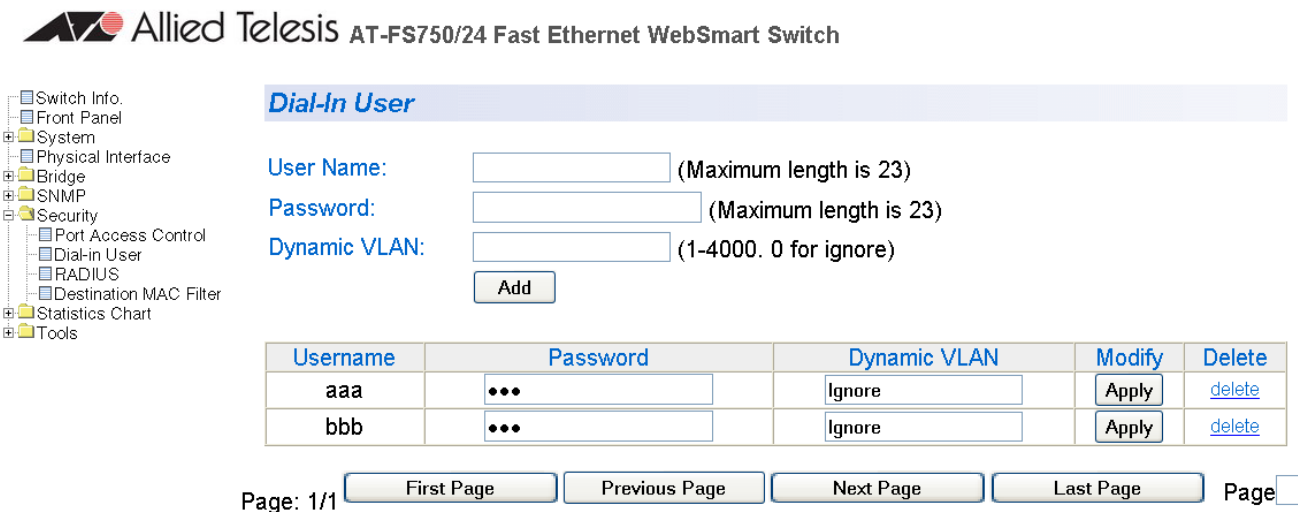
Figure 91. Dial-in User Page

3. To create a new user, enter a user name in the **User Name** field.

    You can enter an alphanumeric value of up to 23 characters. Special characters are permitted.

4. To assign a password to the user name, enter a password in the **Password** field.

    You can enter an alphanumeric value of up to 23 characters. Special characters are permitted.

5. Assign the user name to a VLAN, by entering a VLAN to the **Dynamic VLAN** field.

    Enter a value between 1 and 4,000. Type "0" to ignore this field.

6. Click **Add** to save the user information.

Modifying a Dial-in User

This procedure explains how to modify an existing Dial-in User on the switch. For each user, you may change the password and the VLAN assignment. However, you cannot change the user name.

To modify a Dial-in user, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Security**.

   The Security folder expands.

2. From the Security folder, select **Dial-in User**.

   The Dial-in User Page is shown in Figure 91 on page 318.

3. To change the password for a particular user, type the new password in the **Password** field.

4. To change the VLAN assignment, type the new VLAN number in the **Dynamic VLAN** field.

5. Click **Apply** to save your changes on the switch.

Deleting a Dial-in User

This procedure explains how to delete an existing Dial-in User on the switch.

To delete a Dial-in user, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Security**.

   The Security folder expands.

2. From the Security folder, select **Dial-in User**.

   The Dial-in User Page is shown in Figure 91 on page 318.

3. To delete a user name and its associated password and VLAN assignment, click <u>delete</u> next to the user that you want to remove.

4. Click **Apply** to save your changes on the switch.

Chapter 35
RADIUS Authentication Protocol

This chapter explains how to configure the RADIUS client on the switch. You can use the RADIUS client with 802.1x Port-based Network Access Control feature to control who can forward packets through the switch. The chapter contains the following section:

❒   "Configuring the RADIUS Client" on page 322

> **Note**
> For background information on this feature, refer to "802.1x Port-based Network Access Control Overview" on page 186 and "RADIUS Overview" on page 202.

Configuring the RADIUS Client

To configure the RADIUS client, perform the following procedure:

1. From the book marks on the left side of the page, select **Security**.

   The Security folder expands.

2. From the Security folder, select **RADIUS**.

   The RADIUS Page is shown in Figure 92.

Figure 92. RADIUS Page

3. To enter the RADIUS server's IP address, enter the address in the **Server IP Address** field in the xxx.xxx.xxx.xxx format.

4. To select the port number that you want to assign to UDP, type in the port number in the **Server Port** field. You may only assign one port number to this parameter. The default value is 1812.

5. To specify the server's encryption key, click the **Shared Secret** field and enter the encryption key. Then click **Apply**.

Chapter 36

Management Software Updates

The procedures in this chapter explain how to download a new version of the AT-S80 Management Software update onto the switch. The procedures are:

❒ "Upgrading a Firmware Image With TFTP" on page 324

❒ "Upgrading a Firmware Image With HTTP" on page 326

Note
For information on how to obtain new releases of the AT-S80 Management Software, refer to "Management Software Updates" on page 16.

Note
For procedures to download software from the web interface using TFTP or HTTP, see Chapter 36, "Management Software Updates" on page 323.

Upgrading a Firmware Image With TFTP

Before downloading a new version of the AT-S80 Management Software onto the switch using TFTP, note the following:

❒ Both models of the AT-FS750 switch use the same AT-S80 software image.

❒ The current configuration of a switch is retained when a new AT-S80 software image is installed. To return a switch to its default configuration values, refer to "Returning the AT-S80 Management Software to the Factory Default Values" on page 51.

❒ Your network must have a node with TFTP server software.

❒ You must store the new AT-S80 image file on the server.

❒ You should start the TFTP server software before you begin the download procedure.

❒ The switch where you are downloading the new image file must have an IP address and subnet mask. For instructions on how to configure the IP address on a switch, refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 32 or "Enabling and Disabling the DHCP Client" on page 35.

⚠ **Caution**
Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S80 image software onto the switch, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Tools.**
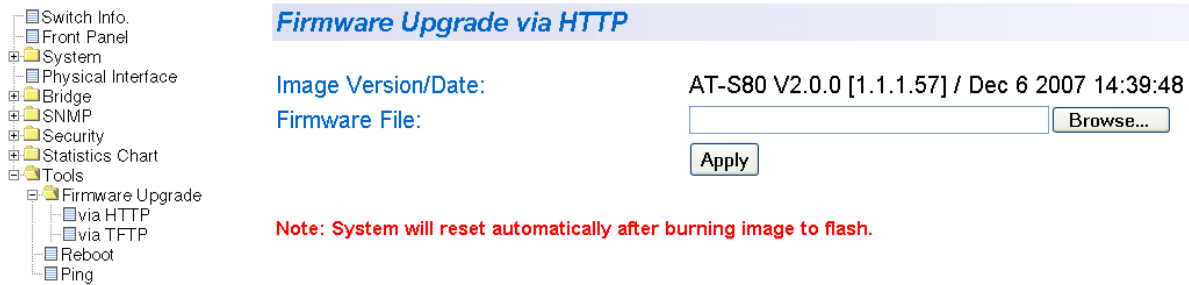
   The Tools folder expands.

2. From the Tools folder, menu, select **Firmware Upgrade**.

   The Firmware Upgrade folder expands**.**

3. From the Firmware Upgrade folder, select **via TFTP.**

The Firmware Upgrade via TFTP Page is shown in Figure 93.

Figure 93. Firmware Upgrade via TFTP Page

4. Change the following parameters as necessary:

Image/Version Date
Displays the current version and date of software installed on the switch. This field cannot be changed.

Download Server IP
The IP address of the TFTP server from which you are downloading the new software.

Download File Name
The name of the AT-S80 file you are downloading.

Retry Count:
The number of times the firmware upgrade is retried. The default number of tries is 5. The range is 1 through 20.

5. Click **Apply**.

The software immediately begins to download onto the switch. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Upgrading a Firmware Image With HTTP

Before downloading a new version of the AT-S80 Management Software onto the switch with HTTP, note the following:

❒ The current configuration of a switch is retained when a new AT-S80 software image is installed. To return a switch to its default configuration values, refer to "AT-S80 Software Default Settings" on page 339.

❒ Assign an IP address and subnet mask to the switch that you are downloading the new image file to. For instructions on how to set the IP address on a switch, refer to "Configuring the IP Address, Subnet Mask, and Gateway Address" on page 34 or "Enabling and Disabling the DHCP Client" on page 37.

⚠ **Caution**
Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S80 image software onto the switch using HTTP, perform the following procedure:

1. From the bookmarks on the left side of the page, select **Tools.**

   The Tools folder expands.

2. From the Tools folder, menu, select **Firmware Upgrade**.

   The Firmware Upgrade folder expands**.**

3. From the Firmware Upgrade folder, select **via HTTP**

The Firmware Upgrade via HTTP Page is shown in Figure 94.

Figure 94. Firmware Upgrade via HTTP Page

4. Change the following parameters as necessary:

    Image/Version Date
    Displays the current version and date of software installed on the switch. This field cannot be changed.

    Firmware File:
    Enter the path of the firmware file or click the **Browse** button and select the filename.

5. Click **Apply**.

    The software immediately begins to download onto the switch. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Chapter 37

Statistics

This chapter provides procedures to display traffic, error, and history statistics. This chapter contains the following section:

❑ "Displaying Switch Statistics" on page 330

Displaying Switch Statistics

Statistics provide important information for troubleshooting switch problems at the port level. The AT-S80 Management Software provides a versatile set of statistical charts that you can customize for your needs, including (depending upon the chart) the ports whose statistics you want to view and the color to use in drawing the statistics in the chart.

The three types of statistics charts provided are:

❐ Traffic Comparison. This chart allows you to display a specified traffic statistic for all ports. You can select 24 statistical types and 12 colors for the ports. The Traffic Comparison statistics chart is described in "Displaying Traffic Comparison Statistics" on page 330.

❐ Error Group. The Error Group chart displays the discard and error counts for a specified port and is described in "Displaying Error Group Statistics" on page 335.

❐ Historical Status. This chart allows you to select from 12 statistics to view for a selection of ports for as long as this chart is running on the management workstation. The Historical Status chart is described in "Displaying Historical Status Charts" on page 337.

Displaying Traffic Comparison Statistics

To display traffic comparison statistics, perform the following procedure:

1. From the book marks on the left side of the page, select **Statistics Chart**.

   The Statistics Chart folder expands.

2. From the Statistics Chart folder, select **Traffic Comparison**.

The Traffic Comparison Chart Page opens as shown in Figure 95.
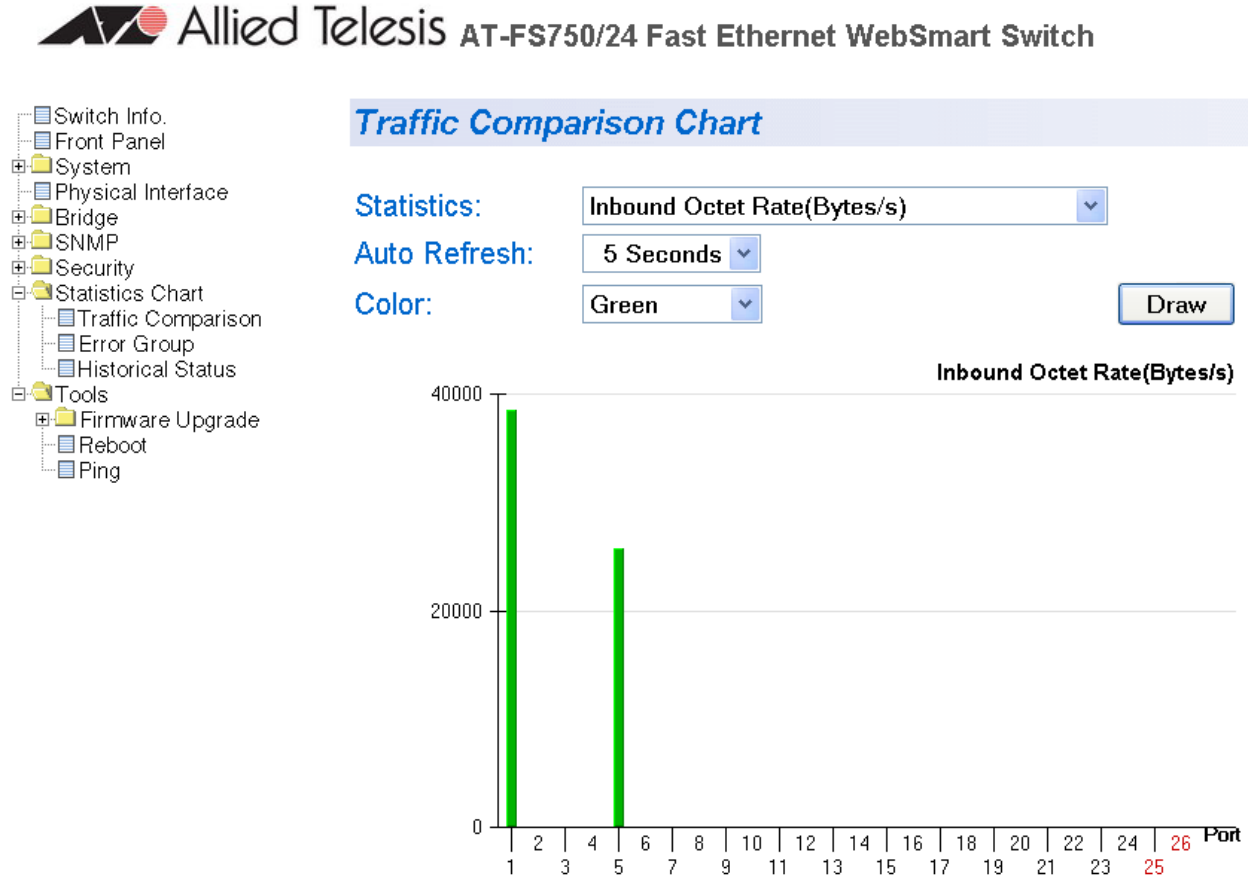
Figure 95. Traffic Comparison Chart Page

3. To view traffic statistics, click on the arrow next to "Statistics" and select one of the options in Table 7.

Table 7 Traffic Comparison Options

Option	Definition
Inbound Octet Rate (Bytes/s)	Measures the rate of inbound octet bits in bytes per second.
Inbound Unicast Packet Rate (Pkts/s)	Measures the rate of inbound unicast packets in packets per second.
Inbound Non-unicast Packet Rate (Pkts/s)	Measures the rate of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.

Table 7 Traffic Comparison Options (Continued)

Option	Definition
Inbound Discard Rate (Pkts/s)	Measures the rate of inbound discarded packets in packets per second.
Inbound Error Rate (Pkts/s)	Measures the number of inbound errors in packets per second.
Outbound Octet Rate (Bytes/s)	Measures the number of outbound octet bits in bytes per second.
Outbound Unicast Packet Rate (Pkts/s)	Measures the number of outbound unicast packets in packets per second.
Outbound Non-unicast Packet Rate (Pkts/s)	Measures the number of outbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Outbound Discard Rate (Pkts/s)	Measures the rate of outbound discarded packets in packets per second.
Outbound Error Rate (Pkts/s)	Measures the rate of outbound errors in packets per second.
Ethernet Undersize Packet Rate (Pkts/s)	Measures the rate of undersized Ethernet packets in packets per second.
Ethernet Oversize Packet Rate (Pkts/s)	Measures the rate of oversized Ethernet packets in packets per second.
Inbound Octet (Bytes/s)	Measures the number of inbound octet bits in bytes per second.
Inbound Unicast Packets (Pkts/s)	Measures the number of inbound unicast packets in packets per second.
Inbound Non-unicast Packets (Pkts/s)	Measures the number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Inbound Discard (Pkts)	Measures the number of inbound discarded packets in packets per second.
Inbound Error (Pkts/s)	Measures the number of inbound errors in packets per second.
Outbound Octet (Bytes/s)	Measures the rate of outbound octet bits in bytes per second.
Outbound Unicast Packets (Pkts/s)	Measures the number of inbound unicast packets in packets per second.

Table 7 Traffic Comparison Options (Continued)

Option	Definition
Outbound Non-unicast Packets (Pkts)	Measures the number of outbound non-unicast (such as broadcast and multicast packets) packets.
Outbound Discards (Pkts)	Measures the number of outbound discarded packets.
Outbound Errors (Pkts/s)	Measures the number of outbound error packets.
Ethernet Undersize Packets (Pkts)	Measures the number of undersized Ethernet packets.
Ethernet Oversize Packets (Pkts/)	Measures the number of oversized Ethernet packets.

4. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:

   – 5 seconds

   – 10 seconds

   – 15 seconds

   – 30 seconds

5. To select the color of the traffic comparison graph, select **Color**. Choose one of the following colors:

   – Green (This is the default.)

   – Blue

   – Red

   – Purple

   – Yellow

   – Orange

   – Gray

   – Light Red

   – Light Blue

   – Light Green

–   Light Yellow

–   Light Gray

6. To create the traffic comparison graph, select **Draw.**

Displaying Error Group Statistics

To display error group statistics for a port, perform the following procedure:

1. From the book marks on the left side of the page, select the **Statistics Chart** folder.

   The Statistics Chart folder expands.

2. From the Statistics Chart folder, select **Error Group**.

   The Error Group Chart Page is displayed in Table 96.
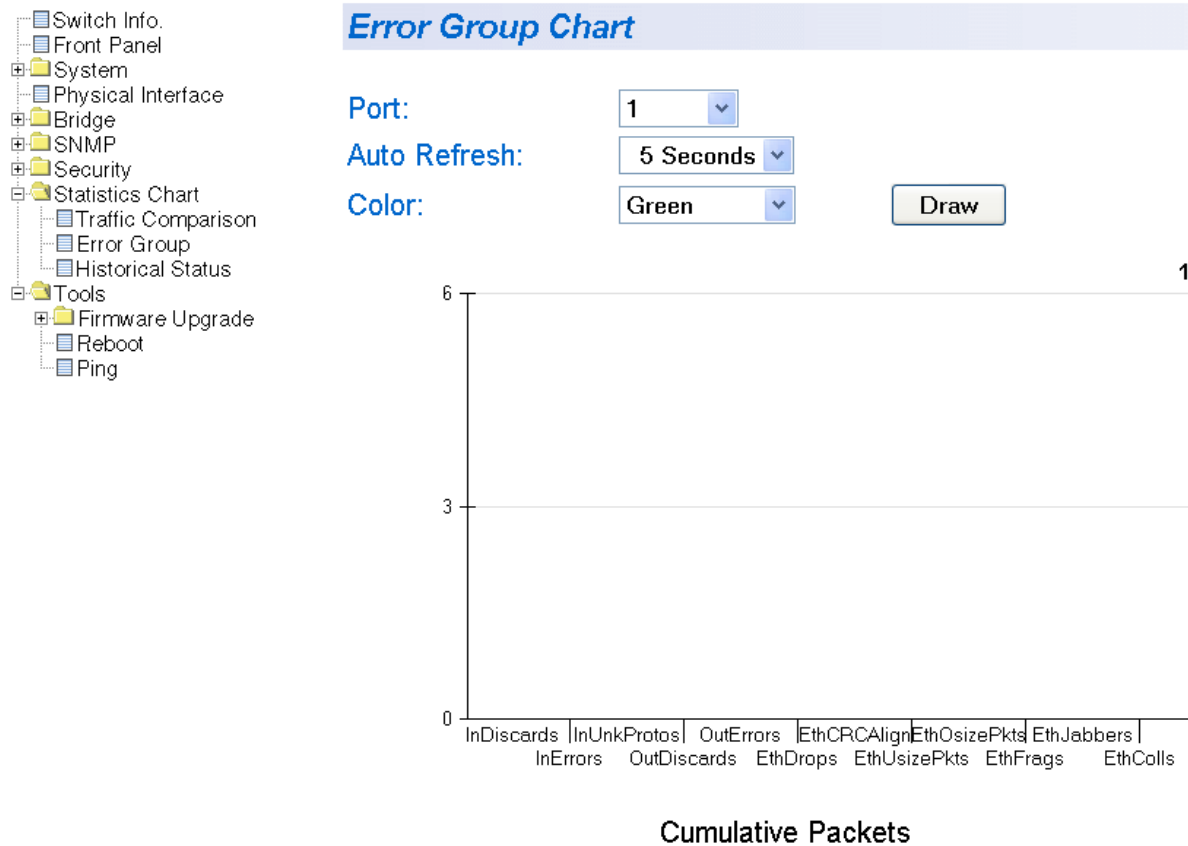
Figure 96. Error Group Chart Page

3. Select a port number from the pull down menu next to Port.

4. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:

   – 5 seconds

   – 10 seconds

        –   15 seconds

        –   30 seconds

5. To select the color of the traffic comparison graph, select **Color**. Choose one of the following colors:

        –   Green (This is the default.)

        –   Blue

        –   Red

        –   Purple

        –   Yellow

        –   Orange

        –   Gray

        –   Light Red

        –   Light Blue

        –   Light Green

        –   Light Yellow

        –   Light Gray

6. To create the Error Group Chart, select **Draw.**

Displaying Historical Status Charts

To display historical status charts statistics for a port, perform the following procedure:

1. From the book marks on the left side of the page, select the **Statistics Chart** folder.

   The Statistics Chart folder expands.

2. From the Statistics Chart folder, select **Historical Status**.

   The Historical Status Chart Page is displayed in Table 97.
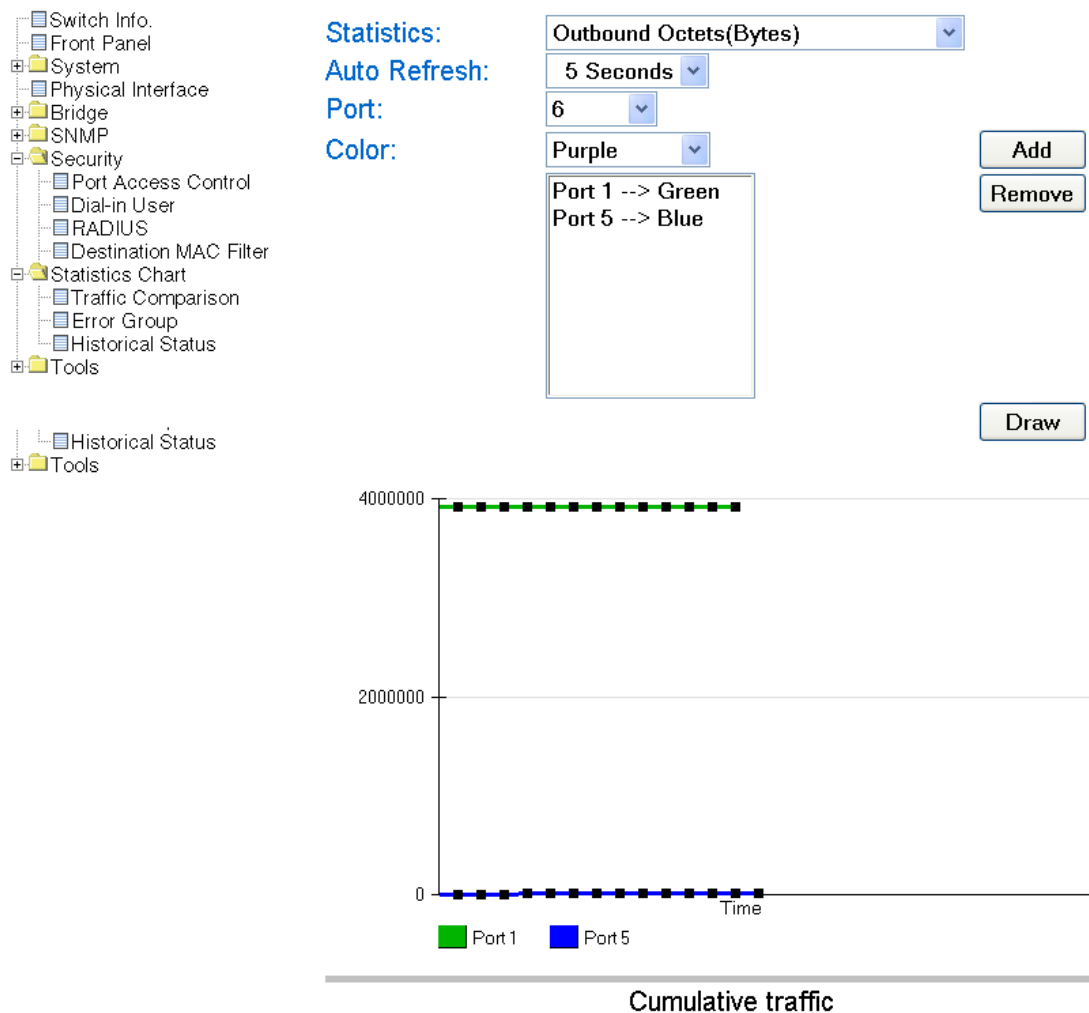
Figure 97. Historical Status Chart Page

3. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:

    – 5 seconds

    – 10 seconds

    – 15 seconds

    – 30 seconds

4. To select the color of the traffic comparison graph, select **Color**. Choose one of the following colors:

    – Green (This is the default.)

    – Blue

    – Red

    – Purple

    – Yellow

    – Orange

    – Gray

    – Light Red

    – Light Blue

    – Light Green

    – Light Yellow

    – Light Gray

5. To create the history group chart, select **Add**. Then click **Draw.**

6. To draw the historical group chart, select **Draw.**

Appendix A

AT-S80 Software Default Settings

Table 8 lists the factory default settings for the management software.

Table 8. AT-S80 Management Software Default Settings

Parameter	Default Setting
IP Configuration	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway Address	0.0.0.0
DHCP Client	Disabled
System Administration	
System Name	(blank)
System Location	(blank)
System Contact	(blank)
Manager Interface	
Manager Username	manager
Manager Password	friend
Console Idle Timeout	5 minutes
Web Server	Enabled
Ping Configuration	
Target IP Address	0.0.0.0
Number of Requests	10
Timeout	3 seconds
Port Configuration	
Port Status	Enabled
Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation

Table 8. AT-S80 Management Software Default Settings (Continued)

Parameter	Default Setting
Flow Control (Full-duplex Mode)	Enabled
Back pressure (Half-duplex Mode)	Enabled (not adjustable)
Port Trunking	
Status	Disabled
IGMP Snooping	
Status	Disabled
IGMP Snooping Age-Out Timer	280 seconds
Port Mirroring	
Status	Disabled
VLAN	
Name	Default VLAN
VID	1
Ports	All Ports (Untagged)
SNMP	
public community	Enabled, Read Only
private community	Enabled, Read Write
Quality of Service	
Status	Disabled
Mappings of IEEE 802.1p Priority Levels to Egress Port Priority Queues	See Table 2 on page 141.
Priority Override Status	Disabled
Priority Queue	Queue 0
RSTP	
Status	Disabled
Bandwidth Control	
DLF Ingress Packet Status	Disabled
Broadcast/Multicast Packet Threshold	Low
Packet Threshold Mode	Broadcast/Multicast

Table 8. AT-S80 Management Software Default Settings (Continued)

Parameter	Default Setting
IP Access List	
IP Restriction	Disabled
802.1x Port-based Network Access Control	
NAS ID	Nas1
Port Control	Force Authorized
Transmission Period	30 seconds
Supplicant Timeout	30 seconds
Server Timeout	30 seconds
Maximum Requests	2
Quiet Period	60 seconds
Re-authentication Period	3600 seconds
Re-authentication Status	Disabled
RADIUS Client	
Server IP Address	0.0.0.0
Shared Secret	(blank)
Response Time	10 seconds
Maximum Retransmissions	3
Upgrade Configuration	
TFTP Server IP Address	0.0.0.0
Image Filename	(blank)
Retry Count	5

Index