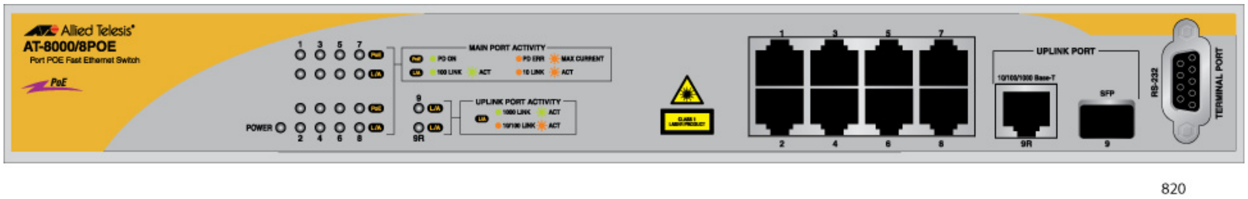
Allied Telesis™

AT-8000/8POE

Layer 2 Fast Ethernet Switch



AT-8000/8POE Layer 2 Fast Ethernet Switch User Guide AT-S81 Version 1.3.0 (V1.1.1.90)

613-001675 Rev.A

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

Contents

Figures

Tables

Preface

This guide contains instructions on how to use the AT-S81 management software to manage and monitor the AT-8000/8POE Layer 2 Fast Ethernet Switch.

The AT-S81 management software has three management interfaces: menus, web browser, and CLI. You access the menus and CLI interfaces through the console port on the switch or through Telnet, and 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 19.

This preface contains the following sections:

❒ “Safety Symbols” on page 14

❒ “Contacting Allied Telesis” on page 15

Safety Symbols

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.

Warning
Warnings inform you that an eye and skin hazard exists due to the presence of a Class 1 laser device.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- ❐ 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about RMAs, and contact Allied Telesis technical experts.
- ❐ USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- ❐ Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- ❐ Replacement Services - Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- ❐ Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- ❐ Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Section I

Using the Menus Interface

The chapters in this section explain how to manage the switch using the menus interface of the AT-S81 management software. The chapters include:

- Chapter 1, “Overview” on page 19
- 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 61
- Chapter 5, “SNMP” on page 71
- Chapter 6, “Port Trunking” on page 81
- Chapter 7, “Port Mirroring” on page 97
- Chapter 8, “Power Over Ethernet” on page 103
- Chapter 9, “Virtual LANs and GVRP” on page 111
- Chapter 10, “Quality of Service (QoS)” on page 133
- Chapter 11, “IGMP Snooping” on page 145
- Chapter 12, “Rapid Spanning Tree Protocol (RSTP)” on page 153
- Chapter 13, “802.1x Network Access Control” on page 175
- Chapter 14, “RADIUS Authentication Protocol” on page 189
- Chapter 15, “Broadcast Storm Control” on page 195
- Chapter 16, “MAC Address Tables” on page 199
- Chapter 17, “Working With System Files” on page 207

Note
The web browser interface is described in Section II, “Using the Web Browser Interface” on page 215, and the command line interface is described in Section III, “Using the Command Line Interface” on page 329.

Chapter 1
Overview

This chapter provides an overview of the AT-S81 management software for the AT-8000/8POE Fast Ethernet switch. This chapter describes the different methods for accessing the software and the management access levels. This chapter contains the following sections:

Management Overview

The AT-S81 management software allows you to view and adjust the operating parameters of the AT-8000/8POE Fast Ethernet switch. Here are a few examples of the functions that you can perform with the management software:

- 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 and tagged virtual LANs
- Configure 802.1x network access control

The AT-S81 management software is preinstalled on the switch with default settings for all of the switch's operating parameters. You do not have to manage the switch 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, as explained in the hardware installation guide, and powering on the unit.

Note
The default settings for the management software are listed in Appendix A, "AT-8000/POE Default Settings" on page 345.

To actively manage the switch and adjust its operating parameters, you must connect to an AT-8000/8POE Fast Ethernet switch and access the switch's AT-S81 management software. There are two ways to connect to the switch:

- Locally
- Remotely

Depending upon the method you choose, specific AT-S81 software interfaces are available. When you have a local connection, you can use the menus (described in Section I of this guide) or the command line interface (CLI) (described in Section III). With a remote connection you can use the menus, CLI, and web browser interfaces, or a third-party network management application. (The web browser interface is described in Section II).

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

Local Connection

To establish a local connection with a switch, you connect a terminal or a PC with a terminal emulator program to the terminal port on the front of the switch using the management cable 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 switch is located.

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

With a local connection, you can manage the switch using the menus or CLI.

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

Remote Connection

You can use any management station on your network that has the Telnet application to manage an AT-8000/8POE Fast Ethernet switch. This is referred to as a remote connection. A remote connection allows you to use any of the AT-S81 software user interfaces: menus, CLI, web browser, or SNMP.

In order for you to manage a switch using the web browser interface, the switch must have an IP address and subnet mask. 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.

For instructions on how to start a remote management session to use the web browser interface, refer to “Establishing a Remote Connection to Use the Web Browser Interface” on page 218.

Note
In order to remotely manage a switch using a web browser, the remote management station must be a member of the switch’s Default VLAN. The switch processes remote management packets only when they are received on an untagged port of the Default VLAN.

Using an SNMP Network Management Application

You can use the Simple Network Management Protocol (SNMP) to run a network management application such as AT-View to manage the switch through a remote connection. A familiarity with how to use management information base (MIB) objects is necessary for this type of management.

The AT-S81 management software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Remote Network MIB (RFC 1757)
- Allied Telesis managed switch MIB

You must download the Allied Telesis managed switch MIB (atiswitch.mib) file from the Allied Telesis web site and compile the files with your SNMP application. For compilation instructions, refer to your third-party application’s documentation. Refer to Chapter 5, “SNMP” on page 71 for information about how to configure SNMP on the switch.

Management Access Level

The AT-S81 management software has one level of management access: manager. When you log in as a manager, you can view and configure all of a switch’s operating parameters. You log in as a manager by entering the appropriate username and password when you start an AT-S81 management session. The default username is “manager” and the default password is “friend”.

Chapter 2

Getting Started with the Menus Interface

This chapter provides information and instructions on how to access the menus interface of the AT-S81 management software by starting a local management session. This chapter contains the following sections:

Starting a Local Management Session

You establish a local management session with the AT-8000/8POE switch by connecting a terminal or personal computer with a terminal emulation program to the RS-232 console port on the front panel of the switch.

Note
You do not need to assign an IP address to the switch to manage the unit 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 AT-8000/8POE switch, as shown in Figure 1.

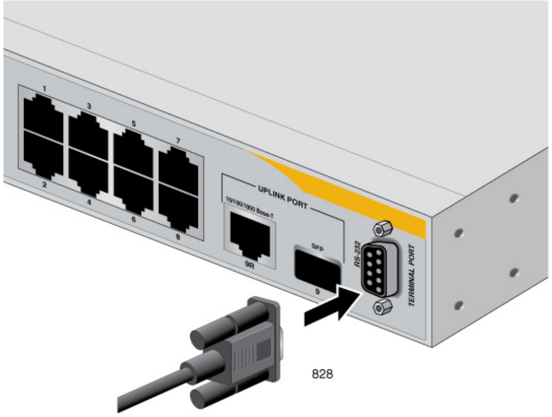


Figure 1. Connecting the Management Cable to the Console Port

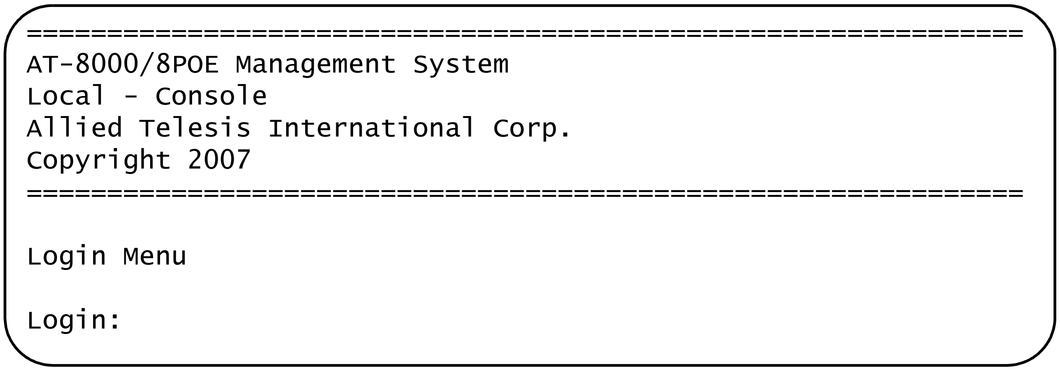
2. Connect the other end of the cable to the RS-232 port on a terminal or PC with a terminal emulator program.

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. You cannot change this.

The Login Menu is shown in Figure 2.



```
==============================================================
AT-8000/8POE Management System
Local - Console
Allied Telesis International Corp.
Copyright 2007
==============================================================

Login Menu

Login:
```

Figure 2. Login Menu

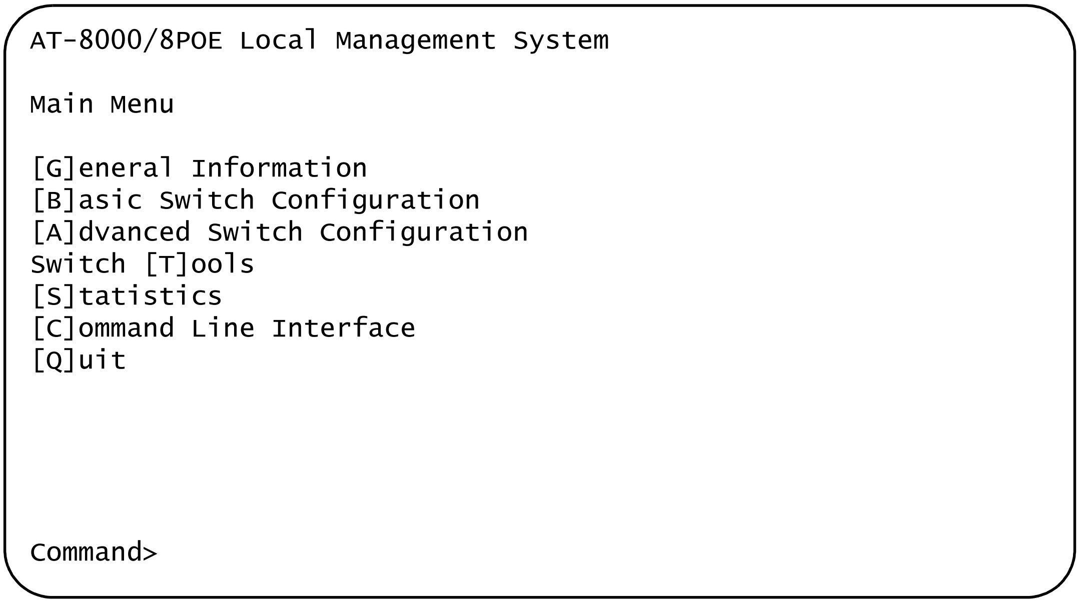
4. Enter the manager login name and press Return. The default name is “manager”.

   You are prompted for a password.

5. Enter the manager password. The default password is “friend”.

> **Note**
> 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.



```
AT-8000/8POE Local Management System

Main Menu

[G]eneral Information
[B]asic Switch Configuration
[A]dvanced Switch Configuration
Switch [T]ools
[S]tatistics
[C]ommand Line Interface
[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
Make a menu selection	Type the menu option letter enclosed in brackets, such as typing P to select [P]ort Configuration.
Enter information (for example, entering a port number)	Enter the information.
Return to previous menu	Type Q for Quit to previous menu.

When you enter a letter to select a field in which you can enter a value, a message 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 AT-8000/8POE switch.

Note
The web browser interface is described in Section II, “Using the Web Browser Interface” on page 215, and the command line interface is described in Section III, “Using the Command Line Interface” on page 329.

Quitting from a Local Management Session

To quit a local management session, return to the Main Menu and type **Q** for **Quit**. When you are finished managing the switch, make sure to exit from a management session. Quitting from a local session prevents unauthorized changes to the switch’s configuration if you leave your workstation unattended.

Note
A local management session automatically times out if there is no management activity during a pre-defined length of time referred to as the 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

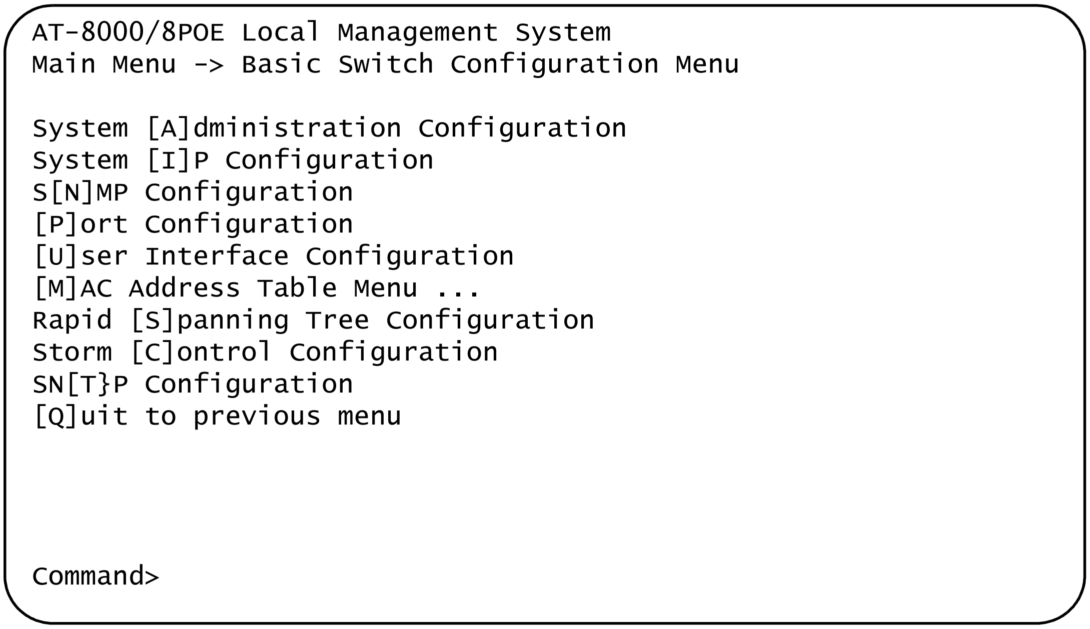
This procedure explains how to manually assign an IP address, subnet mask, and gateway address to the switch. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to “Enabling and Disabling the DHCP Client” on page 35.

To set the switch’s IP 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.

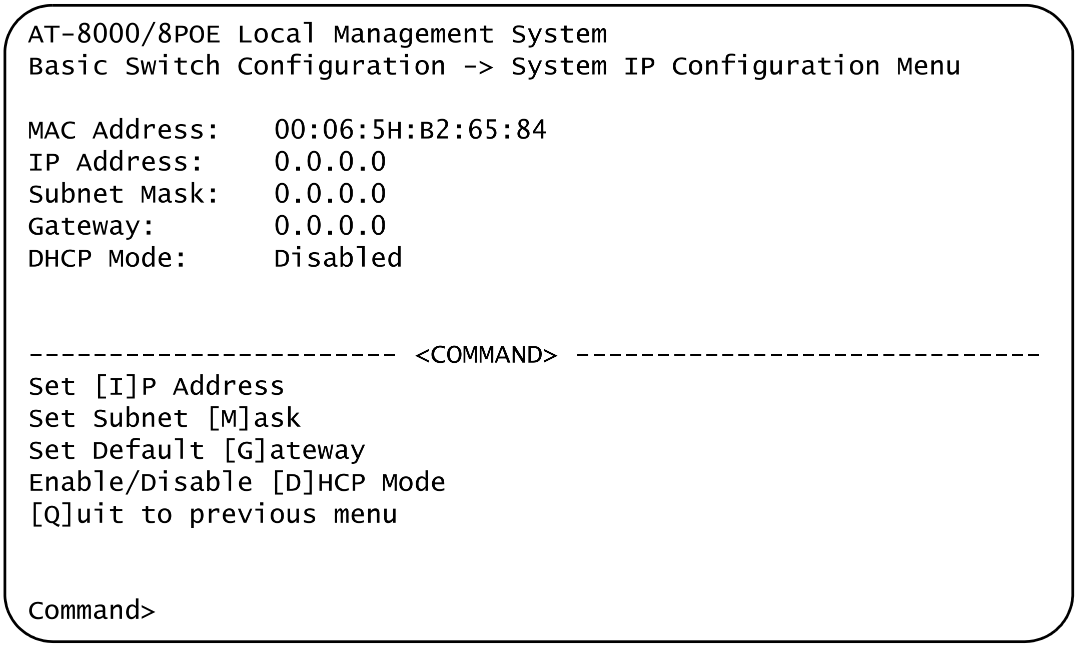


```
AT-8000/8POE Local Management System
Main Menu -> Basic Switch Configuration Menu

System [A]dministration Configuration
System [I]P Configuration
S[N]MP Configuration
[P]ort Configuration
[U]ser Interface Configuration
[M]AC Address Table Menu ...
Rapid [S]panning Tree Configuration
Storm [C]ontrol Configuration
SN[T}P Configuration
[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.



```
AT-8000/8POE Local Management System
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
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 also displays the switch’s MAC address. The MAC address 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. Enter the IP address for the switch.

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. Enter the subnet mask for the switch.

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. Enter the gateway IP address for the switch.

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:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- The DHCP client is disabled by default on the switch.
- The DHCP client does not support BOOTP servers.

To activate or deactivate the DHCP client 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 **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 you enable the client, it immediately begins to send queries to the DHCP server. It continues to send queries until it receives a response.

Configuring System Administration Information

This section explains how to assign a name to the switch, as well as specify the location of the switch and the name of the switch’s administrator. Entering this information is optional.

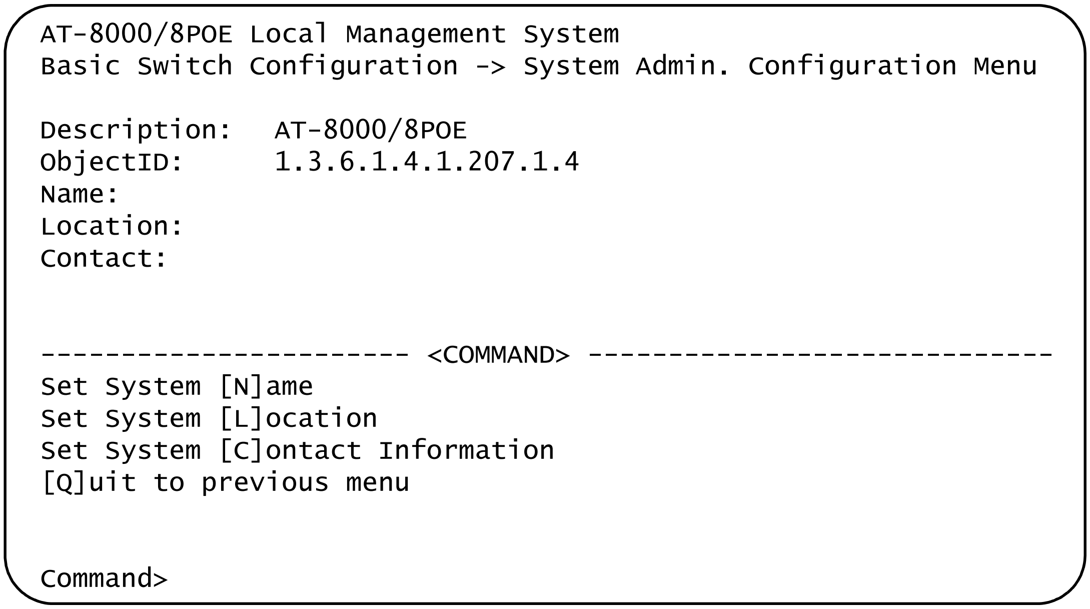
To set a switch’s administration information, perform the following procedure:

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.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> System Admin. Configuration Menu

Description:   AT-8000/8POE
ObjectID:      1.3.6.1.4.1.207.1.4
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 Admin. Configuration Menu

The Description parameter in the top portion of the menu displays the model name of the switch. The System Object ID parameter is the numeric ID of the switch. You cannot change these parameters.

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 that you assign names to the switches. Names can help you identify the switches when you manage them and can also help you avoid performing a configuration procedure on the wrong switch.

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.

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 various settings that control user access to the switch.

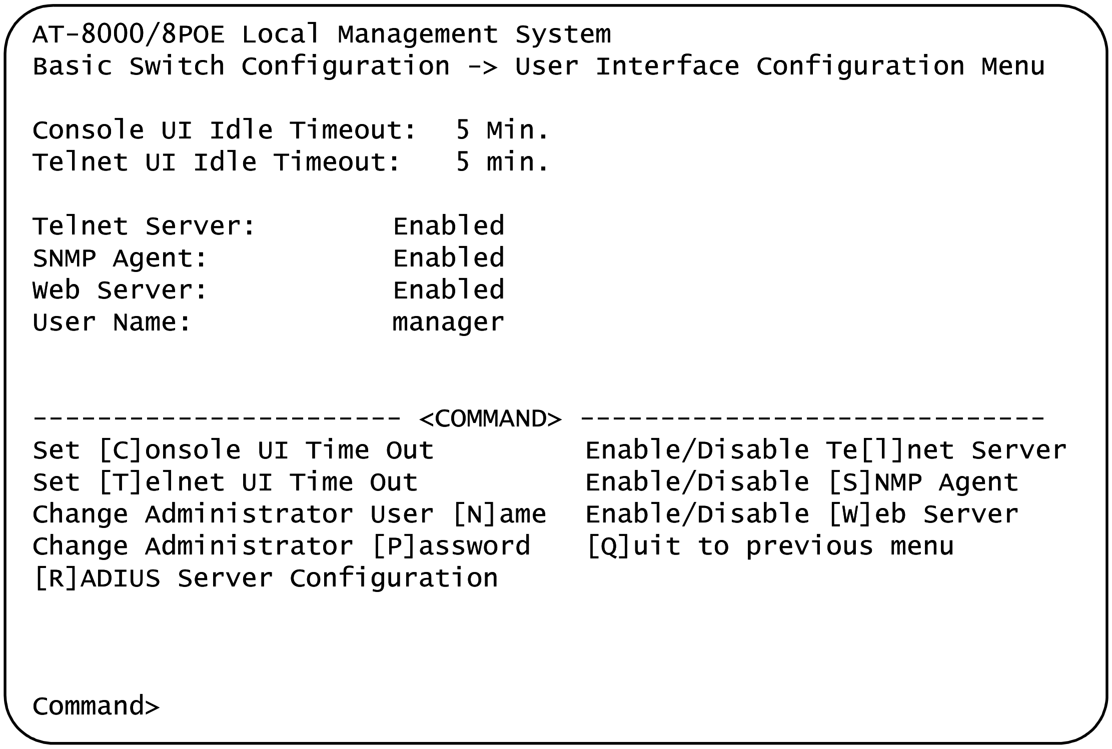
To set the switch's user interface configuration, perform the following procedure:

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.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> User Interface Configuration Menu

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

Telnet Server:         Enabled
SNMP Agent:            Enabled
Web Server:            Enabled
User Name:             manager


----------------------- <COMMAND> -----------------------------
Set [C]onsole UI Time Out          Enable/Disable Te[l]net Server
Set [T]elnet UI Time Out           Enable/Disable [S]NMP Agent
Change Administrator User [N]ame   Enable/Disable [W]eb Server
Change Administrator [P]assword    [Q]uit to previous menu
[R]ADIUS Server Configuration



Command>
```

Figure 7. User Interface Configuration Menu

The Telnet server option is described in "Disabling or Enabling the Telnet Server" on page 43.

The web server option is described in "Disabling or Enabling the Web Server" on page 42.

The SNMP option is described in "Enabling or Disabling the SNMP Agent" on page 74.

The RADIUS Server Configuration option is described Chapter 14, "RADIUS Authentication Protocol" on page 189.

3. To configure the console UI 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, and the default is 5 minutes. A timeout value to 0 causes the switch to never time out a local management session.

      The console UI idle time out parameter specifies the length of time a local management session can be inactive before the management software automatically ends it. This feature prevents unauthorized individuals from configuring the switch if you leave your management workstation unattended.

      This parameter applies to a local management session but not to a remote SNMP or web management session. An SNMP management session remains active as long as the network management application is active. A web browser management session remains active as 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 configure the Telnet UI idle time out parameter, do the following:

   a. Type **T** to select **Set Telnet 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, and the default is 5 minutes. A timeout value to 0 causes the switch to never timeout a local management session.

The Telnet UI idle time out parameter specifies the length of time a remote Telnet management session can be inactive before the management software automatically ends it. This feature prevents unauthorized individuals from configuring the switch if you leave your management workstation unattended.

This parameter applies to a local management session but not to a remote SNMP or web management session. An SNMP management session remains active as long as the network management application is active. A web browser management session remains active as long as your web browser is open.

5. To change the AT-S81 management login user name, do the following:

   a. Type **N** to select **Change Administrator User Name**.

      The following prompt is displayed:

      ```
      Enter current password>
      ```

   b. Enter the current login password. The management software prompts you for the password to prevent an unauthorized individual from changing the login name.

   c. Enter the new user name. The default name is “manager.” The name can be from 0 to 12 characters. Spaces are allowed. The login name is case sensitive. Not entering a new login name deletes the current login name without assigning a new one.

      The new user name appears in the User Field in the top portion of the menu. You must use the new login user name the next time you start a local or web browser management session.

6. To change the manager login password, do the following:

   a. Type **P** to select **Change Administrator Password**.

      The following prompt is displayed:

      ```
      Enter old password>
      ```

   b. Enter the current manager password.

      The following prompt is displayed:

      ```
      Enter new password>
      ```

c. Enter the new password. 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>
   ```

d. Retype the new password.

   You must use the new login password the next time you start a local or remote management session.

Disabling or Enabling the Web Server

The AT-S81 management software is shipped with web server software. The software is available so that you can remotely manage the switch with a web browser from any management station on your network. (The instructions for managing a switch with a web browser are described in Chapter 18, “Starting a Web Browser Management Session” on page 217.)

The default setting for the web server is enabled,

To disable or enable the web server, 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 38.

3. From the User Interface Configuration Menu, type **W** to select **Enable/ Disable Web Server**.

   The following prompt is displayed:

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

4. Type **D** to disable the web server or **E** to enable it.

Disabling or Enabling the Telnet Server

This procedure describes how to enable or disable the Telnet server on the switch. The default setting for the Telnet server is enabled,

To disable or enable the Telnet server, 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 **User Interface Configuration**.

   The User Interface Configuration Menu is shown in Figure 7 on page 38.

3. From the User Interface Configuration Menu, type **L** to select **Enable/ Disable Telnet Server**.

   The following prompt is displayed:

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

4. Type **D** to disable the Telnet server or **E** to enable it.

Configuring SNTP

The AT-S81 software is shipped with the client version of the Simple Network Time Protocol (SNTP). You can configure AT-S81 to obtain the current time and date from an SNTP or Network Time Protocol (NTP) server located on your network or on the internet.

SNTP is a reduced version of the NTP. However, the SNTP client software is interoperable with NTP servers.

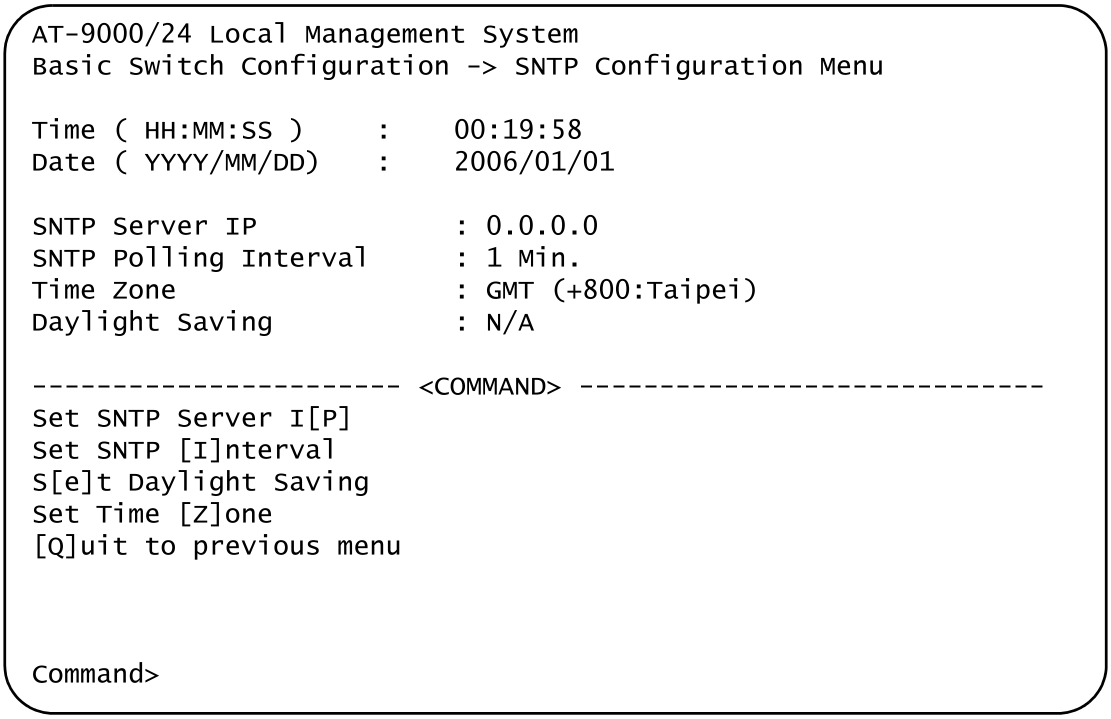
To configure SNTP, perform the following procedure:

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 **T** to select **Set SNTP Server IP**.

   The SNTP Configuration Menu is shown in Figure 8



```
AT-9000/24 Local Management System
Basic Switch Configuration -> SNTP Configuration Menu

Time ( HH:MM:SS )     :    00:19:58
Date ( YYYY/MM/DD)    :    2006/01/01

SNTP Server IP             : 0.0.0.0
SNTP Polling Interval      : 1 Min.
Time Zone                  : GMT (+800:Taipei)
Daylight Saving            : N/A

------------------------ <COMMAND> -----------------------------
Set SNTP Server I[P]
Set SNTP [I]nterval
S[e]t Daylight Saving
Set Time [Z]one
[Q]uit to previous menu



Command>
```

Figure 8. SNTP Configuration Menu

3. Configure the SNTP server's IP address:

   a. Type **P** to select **Set SNTP Server IP**.

      The following prompt is displayed:

Enter new IP address>

b. Type the IP address for the SNTP server you want to use.

4. To set the SNTP interval:

   a. Type **I** to select **Set SNTP Interval**.

      The following prompt is displayed:

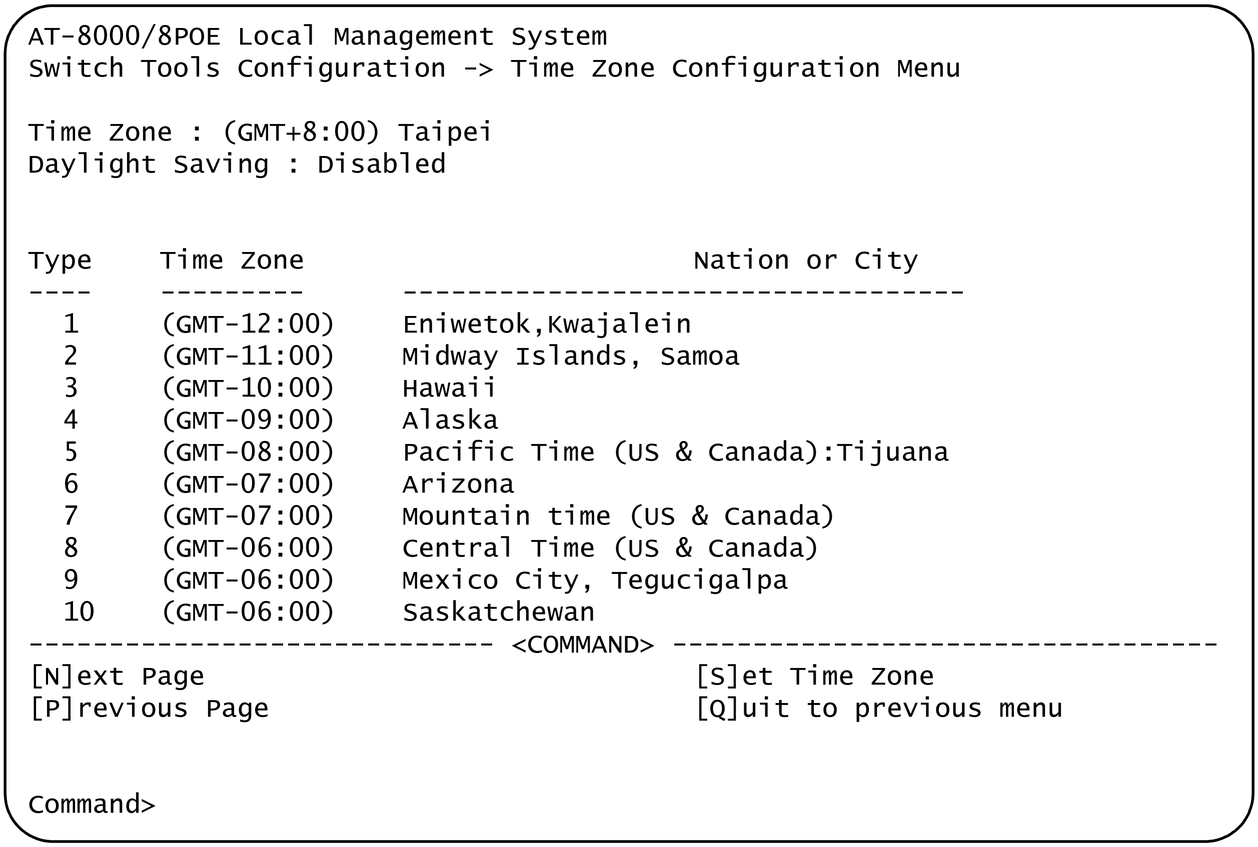
      Enter Interval Time>

   b. Type a number to specify the number of minutes between occurrences of polling the SNTP server. The range is 1 to 60 minutes and the default is 1 minute.

5. To set the time zone:

   a. Type **Z** to select **Set Time Zone**.

   The Time Zone Configuration Menu is shown in Figure 9.



```
AT-8000/8POE Local Management System
Switch Tools Configuration -> Time Zone Configuration Menu

Time Zone : (GMT+8:00) Taipei
Daylight Saving : Disabled


Type    Time Zone                       Nation or City
----    ---------       -----------------------------------
  1     (GMT-12:00)     Eniwetok,Kwajalein
  2     (GMT-11:00)     Midway Islands, Samoa
  3     (GMT-10:00)     Hawaii
  4     (GMT-09:00)     Alaska
  5     (GMT-08:00)     Pacific Time (US & Canada):Tijuana
  6     (GMT-07:00)     Arizona
  7     (GMT-07:00)     Mountain time (US & Canada)
  8     (GMT-06:00)     Central Time (US & Canada)
  9     (GMT-06:00)     Mexico City, Tegucigalpa
  10    (GMT-06:00)     Saskatchewan
----------------------------- <COMMAND> ----------------------------------
[N]ext Page                             [S]et Time Zone
[P]revious Page                         [Q]uit to previous menu


Command>
```

Figure 9. Time Zone Configuration Menu

   b. Scroll through the list of time zones until you find one that matches your time zone.

c. Type **S** to choose **Set Time Zone**.

   The following message is prompt is displayed:

   Select time zone>

d. Type the number that corresponds to the time zone you want.

   If you selected a time zone that observes daylight saving time, the following prompt is displayed:

   Enable or Disable Daylight Saving (E/D)>

e. Type **D** to disable the daylight saving time or **E** to enable it.

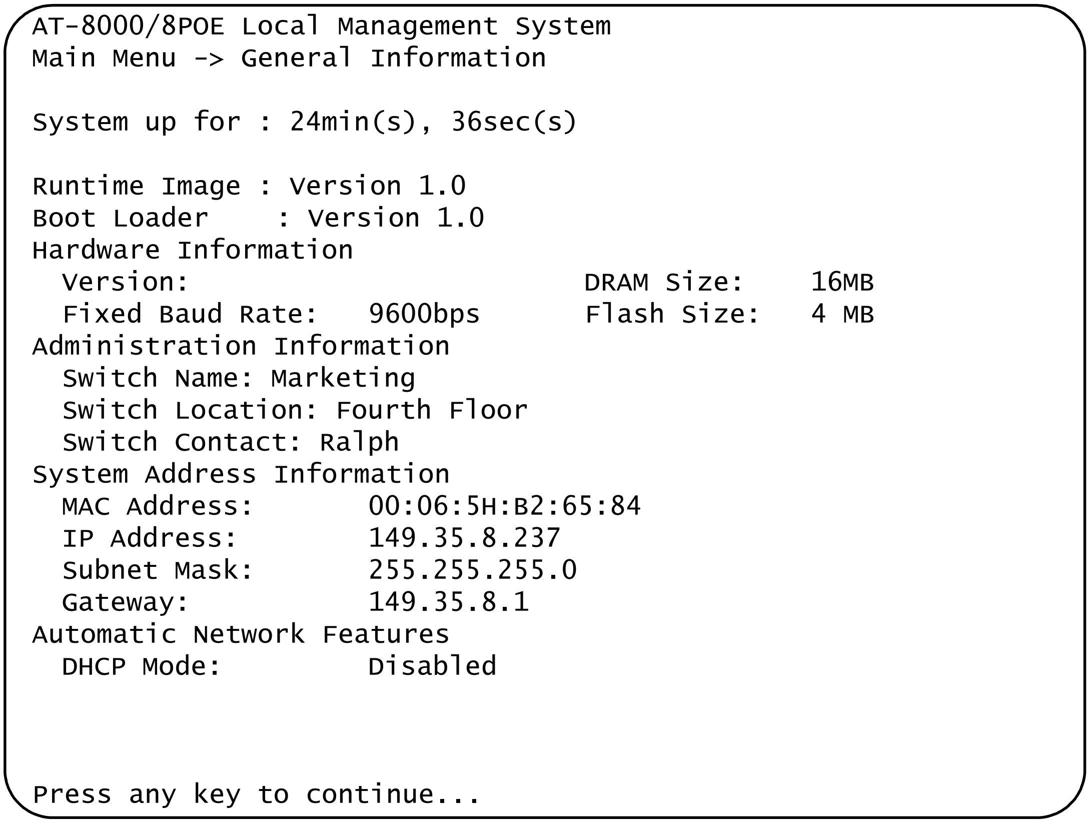
Note
You must set the time zone in order to display the daylight saving time option. If the time zone you previously selected is located in DST area, you can set this anytime.

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 10.



```
AT-8000/8POE Local Management System
Main Menu -> General Information

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

Runtime Image : Version 1.0
Boot Loader    : Version 1.0
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 10. 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. You cannot change this parameter.

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 assigned to the switch. To assign the switch 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 the name of 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 this information.

System IP Address
The IP address of the switch. 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 subnet mask for the switch. 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
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

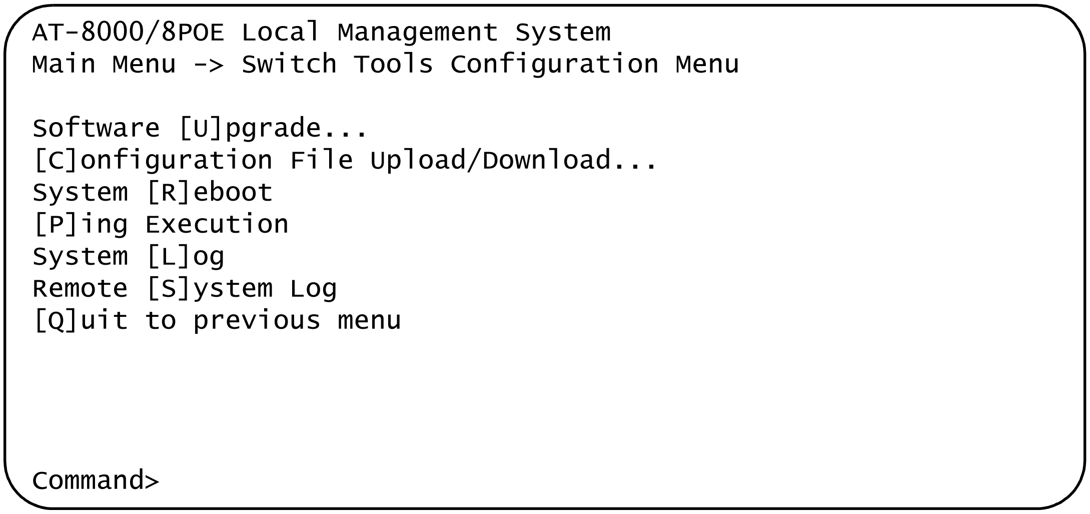
This procedure reboots the switch and reloads the AT-S81 management software from flash memory. You might reboot the device if you believe it is experiencing a problem. Rebooting the device does not change any of the device’s parameter settings.

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 11.



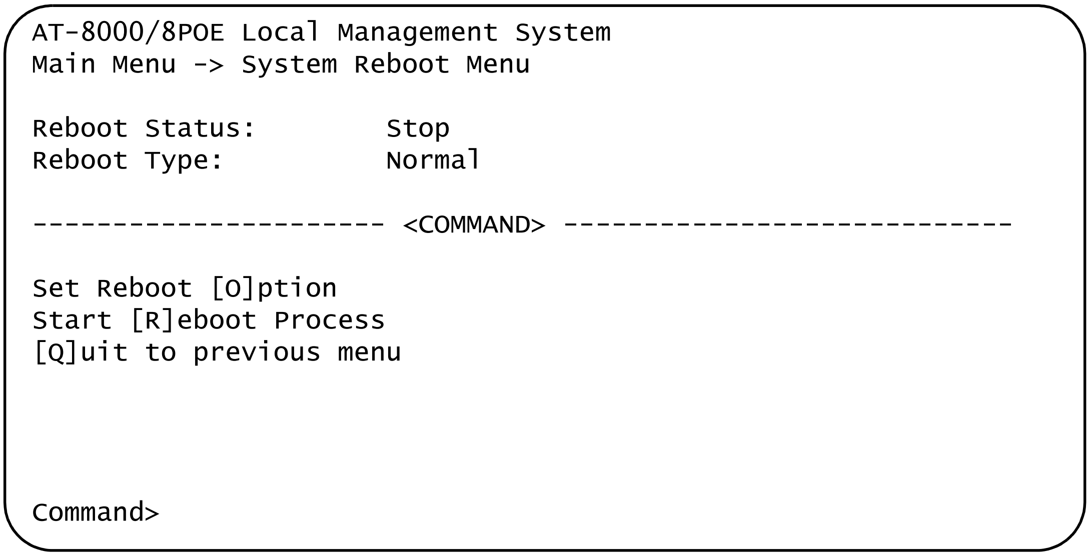
```
AT-8000/8POE Local Management System
Main Menu -> Switch Tools Configuration Menu

Software [U]pgrade...
[C]onfiguration File Upload/Download...
System [R]eboot
[P]ing Execution
System [L]og
Remote [S]ystem Log
[Q]uit to previous menu




Command>
```

Figure 11. Switch Tools Configuration Menu

Note
The Software Upgrade option is described in “Downloading a New Management Software Image Using TFTP” on page 208, the Configuration File Upload/Download option is described in “Uploading or Downloading the Configuration File” on page 211, and the system log options are described in “Working with the System Log” on page 55.

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

The System Reboot Menu is shown in Figure 12.



```
AT-8000/8POE Local Management System
Main Menu -> System Reboot Menu

Reboot Status:        Stop
Reboot Type:          Normal

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

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




Command>
```

Figure 12. 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**.

   This reboot type does not change the current configuration.

   Note
   The **F** and **I** options are described in “Returning the AT-S81 Management Software to the Factory Default Values” on page 59.

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-S81 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 where you are initiating the ping must have an IP address and subnet mask.
- The device you are pinging must be a member of the Default VLAN. This means that the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

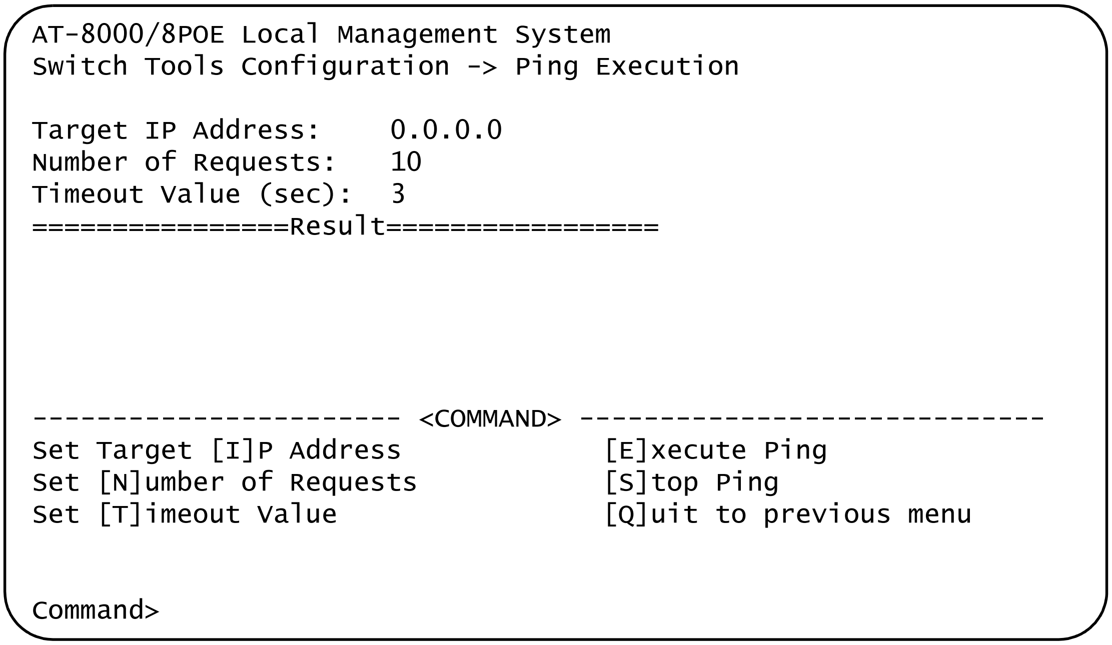
To ping a network device, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

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

   The Ping Execution Menu is shown in Figure 13.



```
AT-8000/8POE Local Management System
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 13. Ping Execution Menu

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

   The following prompt is displayed:

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

4. Enter the IP address of the node you want the switch to ping.

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.

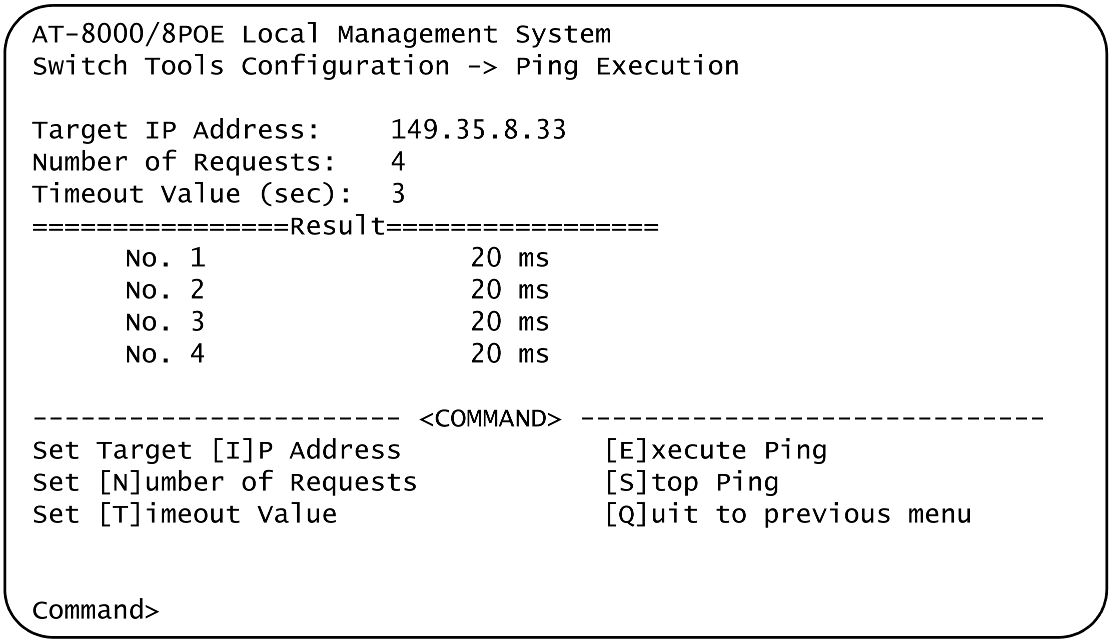
9. Type **E** to select **Execute Ping**.

   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 before performing this ping.

    Figure 14 shows an example of the results of a ping.



```
AT-8000/8POE Local Management System
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 14. Ping Results

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

Working with the System Log

The system log displays system-level events in the switch, such as logging in to the management software. You can view the system log locally, or send the system log file to a remote location. This section contains the following procedures:

❐ "Viewing the System Log," next

❐ "Sending the System Log to a Remote Server" on page 57

Viewing the System Log

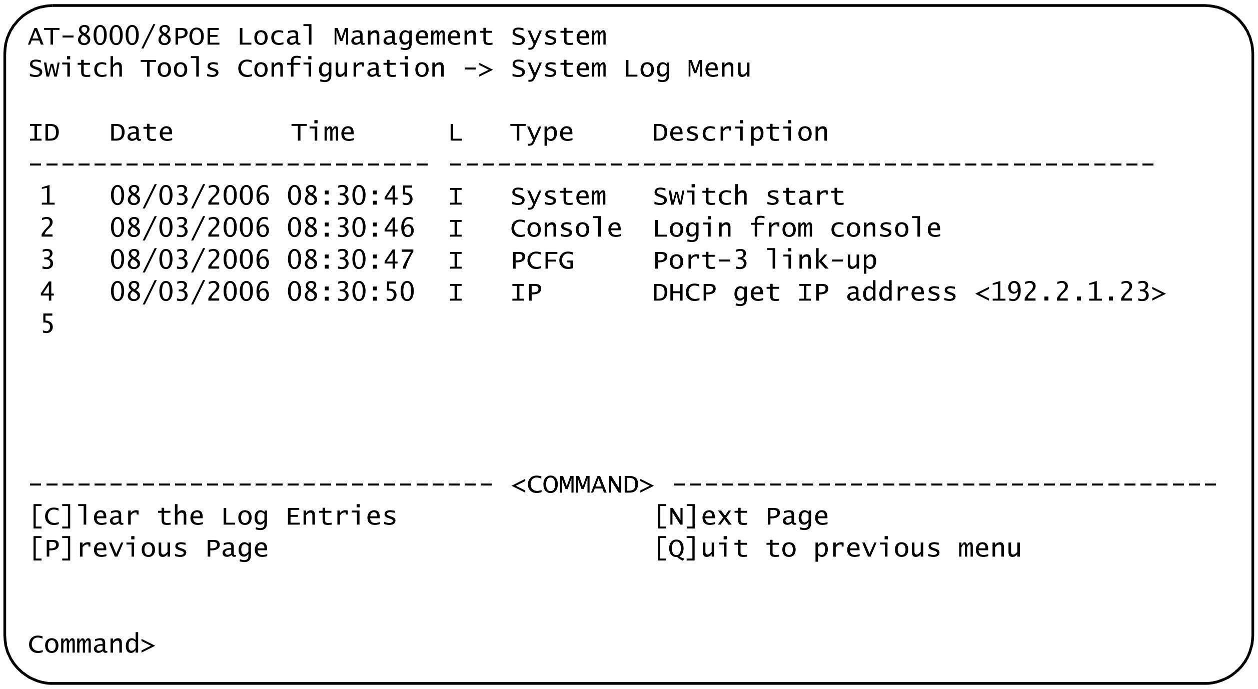
To view the system log, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

2. From the Switch Tools Configuration Menu, type **L** to select **System Log**.

   The System Log Menu is shown in Figure 15.



```
AT-8000/8POE Local Management System
Switch Tools Configuration -> System Log Menu

ID   Date       Time      L   Type     Description
------------------------- ---------------------------------------------
 1   08/03/2006 08:30:45  I   System   Switch start
 2   08/03/2006 08:30:46  I   Console  Login from console
 3   08/03/2006 08:30:47  I   PCFG     Port-3 link-up
 4   08/03/2006 08:30:50  I   IP       DHCP get IP address <192.2.1.23>
 5





----------------------------- <COMMAND> ----------------------------------
[C]lear the Log Entries                [N]ext Page
[P]revious Page                        [Q]uit to previous menu


Command>
```

Figure 15. System Log Menu

The System Log Menu contains a table that displays the following information:

ID
An indentifying number for the event.

Date
The date that the event occurred.

Time
The time that the event occurred.

> **Note**
> When you enable the SNTP protocol, switch startup events show the default system date until SNTP polls for the current date and time.

L
Severity level of the event. The severity levels are:

(I)nformation - Useful information that you can ignore during normal operation.

(W)arning - An issue that may require a manager’s attention.
(E)rror - Switch operation is severely impaired.

Type
The type provides more information about the event. The possible types are:

802.1X - An 802.1X event.

CFG - Configuration event.

CLI - CLI login.

Console - A console login by a user.

IP - Change to the IP information.

PCFG - Port configuration.

PoE - PoE configuration or event.

SNTP - SNTP configuration.

STP - Spanning tree.

SwUpg - Software upgrade.

System - General system event.

Telnet - Access via Telnet.

Description
A description of the event.

3. To remove the current log entries, type **L** to select **Clear the Log Entries**.

Sending the System Log to a Remote Server

The syslog protocol allows you to collect messages and events produced by a wide variety of network equipment in a single place. For instance, instead of viewing the event logs of several separate AT-8000/8POE Fast Ethernet switches, you can have those events sent to a single syslog server on your network. The destination for the events is referred to as a facility.

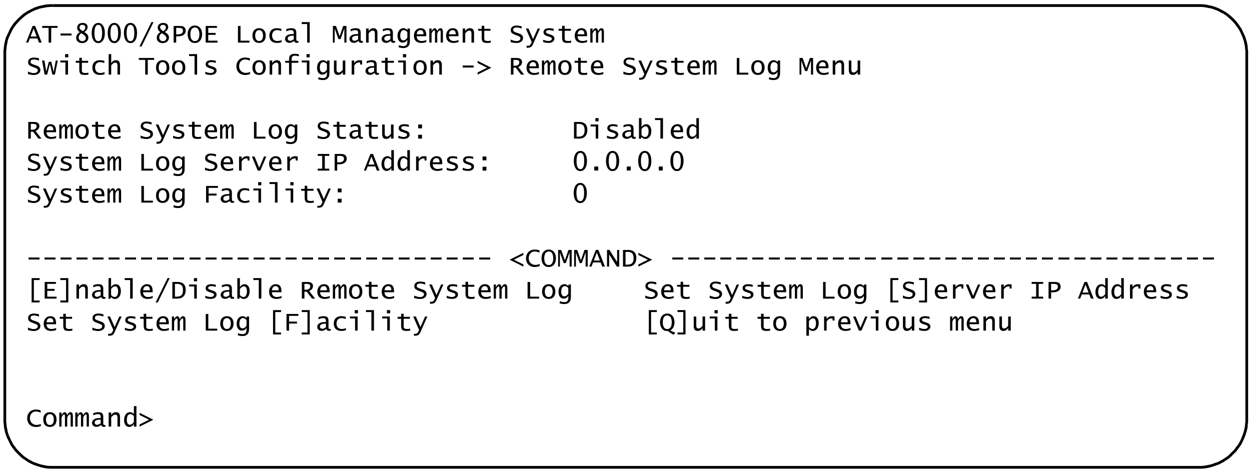
To transmit the system events to a syslog server, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

2. From the Switch Tools Configuration Menu, type **S** to select **Remote System Log.**

   The Remote System Log Menu is shown in Figure 16.



```
AT-8000/8POE Local Management System
Switch Tools Configuration -> Remote System Log Menu

Remote System Log Status:         Disabled
System Log Server IP Address:     0.0.0.0
System Log Facility:              0

----------------------------- <COMMAND> ---------------------------------
[E]nable/Disable Remote System Log    Set System Log [S]erver IP Address
Set System Log [F]acility             [Q]uit to previous menu


Command>
```

Figure 16. Remote System Log Menu

3. Type **S** to select **Set System Log Server IP Address**.

   The following prompt is displayed:

   ```
   Enter IP address of system log server>
   ```

4. Type the IP address of the system log server.

5. Type **F** to select **Set System Log Facility**.

   ```
   Enter system log facility (0-7)>
   ```

6. Type a number from 0 to 7 that corresponds to the facility number on your network.

7. Type **E** to select **Enable/Disable Remote System Log**.

   The following prompt is displayed:

   ```
   Enable or Disable remote system log (E/D)>
   ```

8. Type **E** to enable events to be sent to the remote system log, or **D** to disable this feature.

Returning the AT-S81 Management Software to the Factory Default Values

This procedure returns all AT-S81 management software parameters to their default values and deletes all tagged and VLANs on the switch. The AT-S81 management software default values are listed in Appendix A, ”AT-8000/POE Default Settings” on page 345.

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-S81 management software to the 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 11 on page 50.

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

   The System Reboot menu is shown in Figure 12 on page 51.

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.

   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 50.

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-S81 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

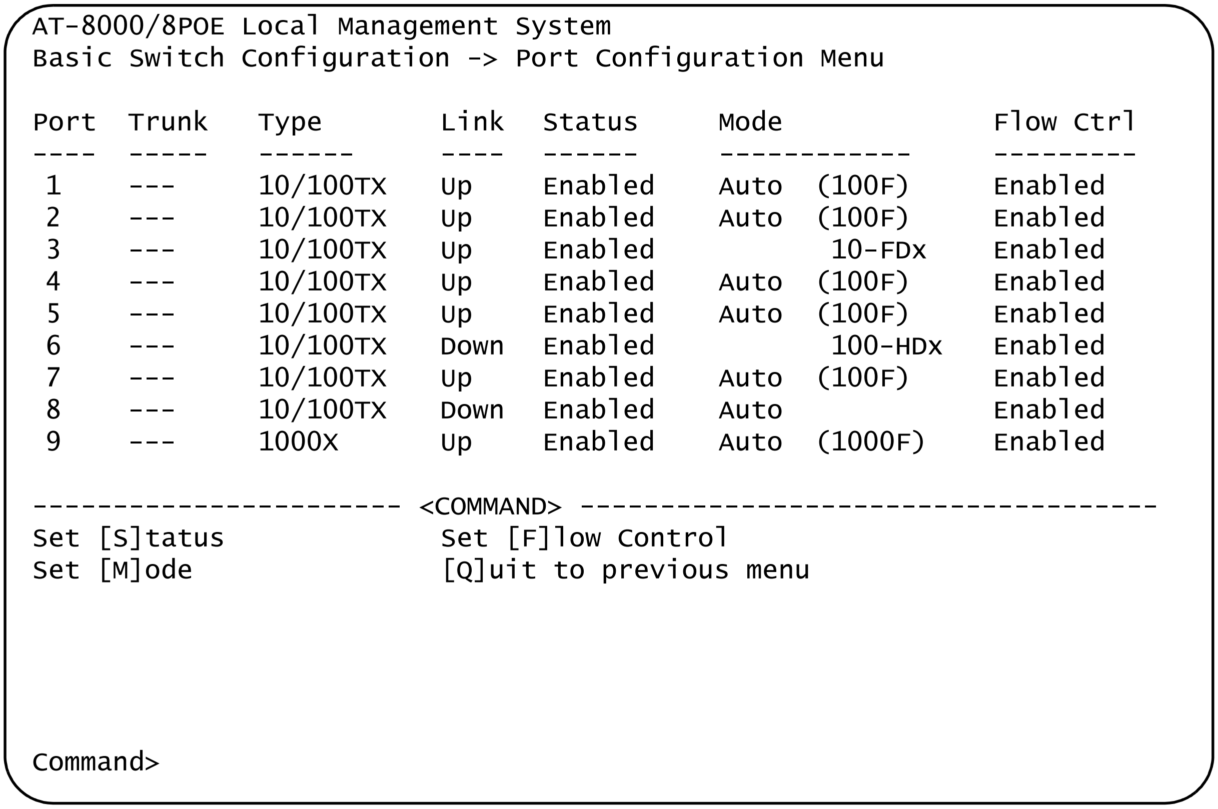
To display the parameter settings for the ports on the switch, perform the following procedure:

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 17.



```
AT-8000/8POE Local Management System
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           10-FDx    Enabled
 4    ---     10/100TX   Up     Enabled    Auto  (100F)     Enabled
 5    ---     10/100TX   Up     Enabled    Auto  (100F)     Enabled
 6    ---     10/100TX   Down   Enabled           100-HDx   Enabled
 7    ---     10/100TX   Up     Enabled    Auto  (100F)     Enabled
 8    ---     10/100TX   Down   Enabled    Auto             Enabled
 9    ---     1000X      Up     Enabled    Auto  (1000F)    Enabled

----------------------- <COMMAND> ------------------------------------
Set [S]tatus             Set [F]low Control
Set [M]ode               [Q]uit to previous menu




Command>
```

Figure 17. Port Configuration Menu

The Port Configuration Menu displays the following columns of information about the status of the ports:

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 6, "Port Trunking" on page 81.

Type
The port type. The type for an RJ-45 copper port is 10/100TX. The port type for the fiber optic ports is 1000BaseX.

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 has been manually disabled.

To change a port's status, see "Enabling and Disabling a Port" on page 64.

Mode
The port's speed and duplex mode setting. For information about the modes or to change a port's speed and duplex mode setting, see "Setting a Port's Speed and Duplex Mode" on page 65.

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 67.

Enabling and Disabling a Port

This procedure enables and disables 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 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 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 17 on page 62.

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

   The following prompt is displayed:

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

4. Enter the number of the port you want 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.

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 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 17 on page 62.

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/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

   H - 100 Mbps, half-duplex

   f - 10 Mbps, full-duplex

   F - 100 Mbps, full-duplex

   When you select a setting, note the following:

   ❒ When a twisted pair port on the switch 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.

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

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 17 on page 62.

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

   The following prompt is displayed:

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

4. Enter the port number whose flow control setting you want to change. 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.

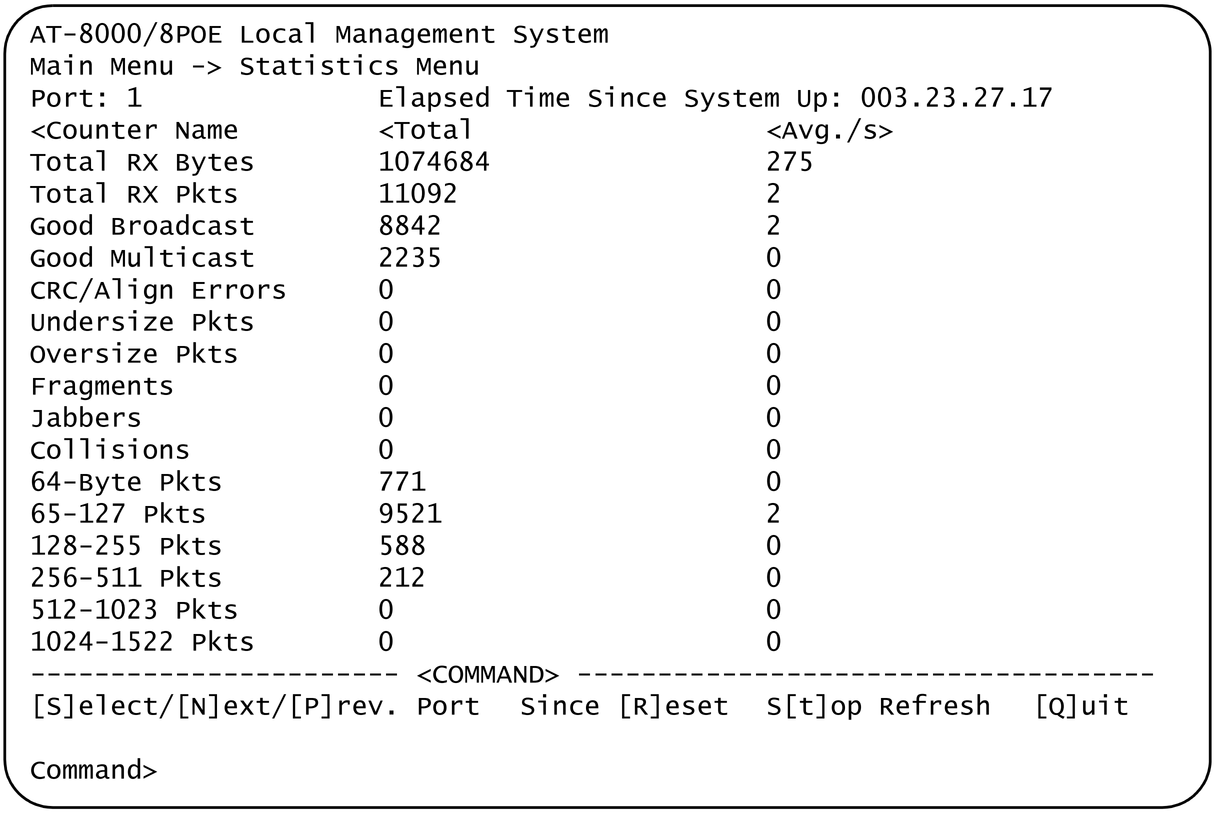
   The display is refreshed to show the port’s new flow control setting.

Displaying Port Statistics

To display statistics about a port, perform the following procedure:

1. From the Main Menu, select **Statistics**.

   The **Statistics** menu is shown in Figure 18.



```
AT-8000/8POE Local Management System
Main Menu -> Statistics Menu
Port: 1               Elapsed Time Since System Up: 003.23.27.17
<Counter Name         <Total                  <Avg./s>
Total RX Bytes        1074684                 275
Total RX Pkts         11092                   2
Good Broadcast        8842                    2
Good Multicast        2235                    0
CRC/Align Errors      0                       0
Undersize Pkts        0                       0
Oversize Pkts         0                       0
Fragments             0                       0
Jabbers               0                       0
Collisions            0                       0
64-Byte Pkts          771                     0
65-127 Pkts           9521                    2
128-255 Pkts          588                     0
256-511 Pkts          212                     0
512-1023 Pkts         0                       0
1024-1522 Pkts        0                       0
----------------------- <COMMAND> ------------------------------------
[S]elect/[N]ext/[P]rev. Port  Since [R]eset  S[t]op Refresh   [Q]uit

Command>
```

Figure 18. Statistics Menu

The statistics for port 1 are displayed in a table that contains the following columns of information:

Total
The total count for this statistic.

Avg/s
The average count of that statistic per second.

The table contains the following items of information:

Total RX Bytes
Number of bytes received on the port.

Total RX Pkts
Number of packets received on the port.

Good Broadcast
Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Pkts
Number of packets that were less than the minimum length specified by IEEE 902.3 (64 bytes including the CRC) received on the port.

Oversize Pkts
Number of packets that exceeded the maximum length specified by IEEE 902.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
Number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1024-1522 Pkts
Number of 1024- to 1522-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.

The statistics are refreshed every 30 seconds,

2. To select a specific port:

   a. Type **S** to select **Select**.

The following prompt is displayed:

```
Select port number>
```

b. Type the number of the port whose statistics you want to view.

3. Type **N** for **Next** or **P** for **Previous** to move between ports.

4. To view the statistics for a particular port since the switch was last reset, select the port and then type **R** for **Since Reset**.

5. To stop refreshing the statistics, type **T** for **Stop Refresh**.

Chapter 5
SNMP

This chapter contains the following sections:

SNMP Overview

The Simple Network Management Program (SNMP) is another way for you to manage the switch. This type of management involves viewing and changing the management information base (MIB) objects on the device using an SNMP application program. The AT-S81 management software supports SNMPv1 and SNMPv2c which is always disabled on the switch.

The procedures in this chapter show you how to create and manage SNMPv1 and SNMPv2c community strings through which your SNMP application program at your management workstation can access the switch's MIB objects.

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. The procedure for this can be found in "Enabling or Disabling the SNMP Agent" on page 74.

❒ 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 and at least one of the switch's community strings. A community string is a string of alphanumeric characters that gives you access to the switch.

A community string has several attributes that you can use to control who can use the string and what the string will allow a network manager to do on the switch. The community string attributes are defined below:

Community String Name
The SNMP community string is similar to a user ID or password, which allows access to a network device's statistics. You must assign a name to the community string. The name can be from one to eight alphanumeric characters. Spaces are allowed.

Access Mode
This defines what the community string will allow a network manager to do. There are two access modes: Read and Read/Write. A community string with an access mode of Read can only 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.

Status
A community string can be enabled, disabled, or deleted. When 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. You can enable it again later, or even delete it. When a community string is enabled, then it is available for use.

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 four 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 any IP addresses of trap receivers.

Default SNMP Community Strings

The AT-S81 management software provides two default community strings: SNMP Read Community and SNMP Write Community. The read community string is called “public” and has an access mode of just Read. The write community string is named “private” and has an access mode of write only.

Enabling or Disabling the SNMP Agent

To disable or enable the SNMP agent, 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 38.

3. From the User Interface Configuration Menu, type **S** to select **Enable/ Disable SNMP Agent**.

   The following prompt is displayed:

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

4. Type **D** to disable the SNMP agent or **E** to enable it. The default is Enabled.

Enabling Authentication Traps

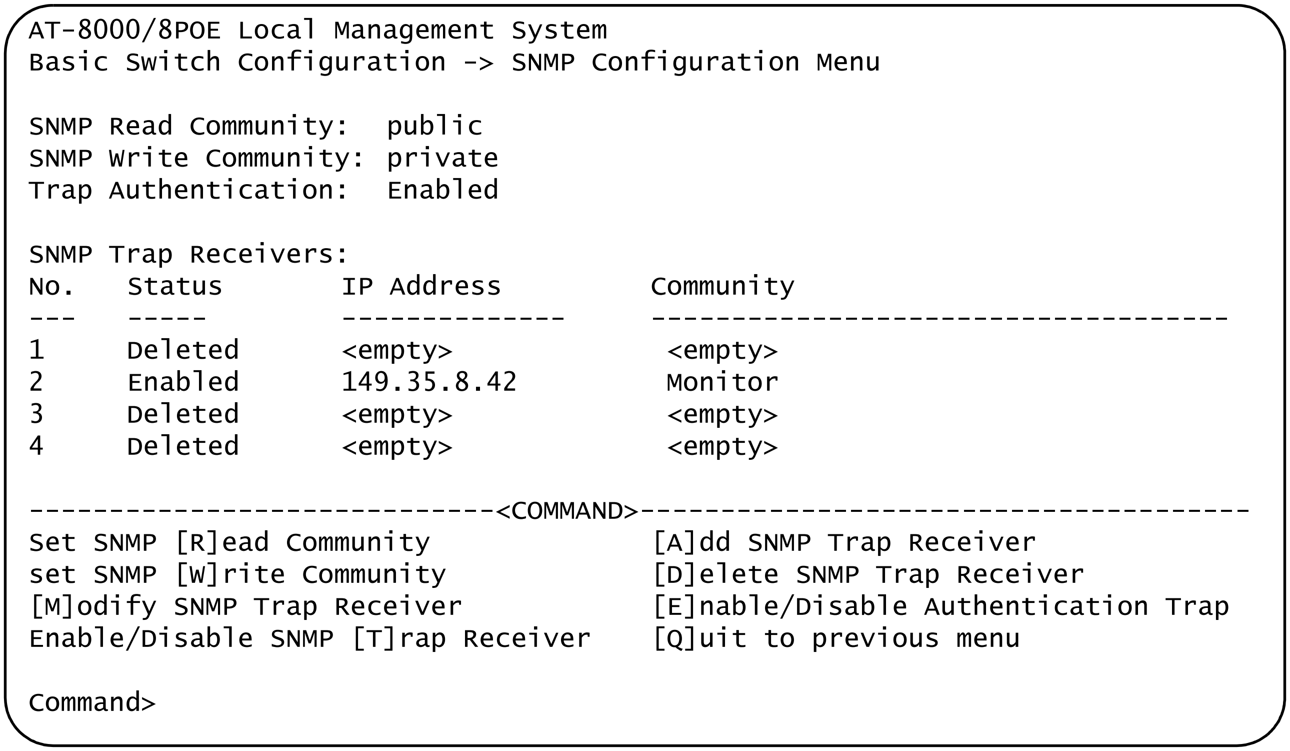
To enable SNMP authentication traps, perform the following procedure:

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 **N** to select **SNMP Configuration**.

   The SNMP Configuration menu is shown in Figure 19.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> SNMP Configuration Menu

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

SNMP Trap Receivers:
No.   Status      IP Address         Community
---   -----       --------------     -------------------------------------
1     Deleted     <empty>             <empty>
2     Enabled     149.35.8.42         Monitor
3     Deleted     <empty>             <empty>
4     Deleted     <empty>             <empty>

-----------------------------<COMMAND>--------------------------------------
Set SNMP [R]ead Community              [A]dd SNMP Trap Receiver
set SNMP [W]rite Community             [D]elete SNMP Trap Receiver
[M]odify SNMP Trap Receiver            [E]nable/Disable Authentication Trap
Enable/Disable SNMP [T]rap Receiver    [Q]uit to previous menu

Command>
```

Figure 19. SNMP Configuration Menu

3. Type **E** to select **Enable/Disable Authentication Trap**.

   The following prompt is displayed:

   ```
   Enable or Disable SNMP Authentication Trap (E/D)>
   ```

4. Type **E** to enable SNMP or **D** to disable SNMP. The default is Enabled.

Changing the Default SNMP Community Names

To change the names of the default SNMP communities, 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 **N** to select **SNMP Configuration**.

   The SNMP Configuration menu is shown in Figure 19 on page 75.

3. Type **R** to select **Set SNMP Read Community**.

   The following prompt is displayed:

   ```
   Enter read community name>
   ```

4. Type the name of the read community. The default is “public.”

5. Type **W** to select **Set SNMP Write Community**.

   The following prompt is displayed:

   ```
   Enter write community name>
   ```

6. Type the name of the write community. The default name is “private”.

Working with Trap Receivers

This section contains procedures for working with SNMP trap receivers and includes the following topics:

❒ "Adding a Trap Receiver," next

❒ "Enabling or Disabling Trap Receivers" on page 77

❒ "Modifying a Trap Receiver" on page 78

❒ "Deleting a Trap Receiver" on page 79

Adding a Trap Receiver

You must add a trap receiver before you can enable it.

To add 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 4 on page 32.

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

   The SNMP Configuration menu is shown in Figure 19 on page 75.

3. Type **A** to select **Add SNMP Trap Receiver**.

   The following prompt is displayed:

   ```
   Add SNMP trap receivers->Enter entry number>
   ```

4. Enter 1 through 4 for the trap receiver you want to configure.

   The following prompt is displayed:

   ```
   Enter IP address for trap receiver>
   ```

5. Enter the IP address of the workstation that you want to receive traps.

   The following prompt is displayed:

   ```
   Enter community name for trap receiver>
   ```

6. Enter a name for the workstation that you want to receive traps.

   A new trap receiver is automatically enabled.

Enabling or Disabling Trap Receivers

You can disable a trap receiver or enable one that was previously disabled. To enable or disable 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 4 on page 32.

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

   The SNMP Configuration menu is shown in Figure 19 on page 75.

3. Type **T** to select **Enable/Disable SNMP Trap Receiver**.

   The following prompt is displayed:

   ```
   Set SNMP trap receivers status->Enter entry number>
   ```

4. Enter the number of the trap receiver you want to enable or disable.

   The following prompt is displayed:

   ```
   Set SNMP trap receivers status->Enter entry number>
   ```

5. Enter the number for the trap you want to enable or disable.

   The following prompt is displayed:

   ```
   Enable or Disable SNMP Trap Receiver (E/D)>
   ```

   Note
   The trap receiver must be one whose status is not “deleted.”

6. Type **E** to enable the trap receiver or **D** for disable to disable the trap receiver.

   You can also delete a trap receiver, as described in “Deleting a Trap Receiver” on page 79

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 4 on page 32.

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

   The SNMP Configuration menu is shown in Figure 19 on page 75.

3. Type **M** to select **Modify SNMP Trap Receiver**.

   The following prompt is displayed:

   ```
   Modify SNMP trap receivers->Enter entry number>
   ```

Note
The trap receiver must be one whose status is not “deleted.”

4. Enter the number for the trap you want to modify.

   The following prompt is displayed:

   ```
   Modify trap receiver entry number (I/C/B)>
   ```

   The options are:

   I - Modify the IP address of the trap receiver. To modify only the IP address, type **I** and follow the prompts.

   C - Modify the community name of the trap receiver. To modify only the community name, type **C** and follow the prompts.

   B - Modify both the IP address and community name of the trap receiver. To modify both the IP address and the community name, type **B** and follow the prompts.

Deleting a Trap Receiver

When you delete a trap receiver, all the settings are removed from the entry in the table. Instead of deleting a trap receiver, you may want to disable it, as described in “Enabling or Disabling Trap Receivers” on page 77.

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 4 on page 32.

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

   The SNMP Configuration menu is shown in Figure 19 on page 75.

3. Type **D** to select **Delete SNMP Trap Receiver**.

   The following prompt is displayed:

   ```
   Delete SNMP trap receivers->Enter entry number>
   ```

4. Type the number of the entry you want to delete.

Chapter 6

Port Trunking

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

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.

Static Port Trunk Overview

A static port trunk consists of two to eight ports on the switch that function as a single virtual link between the switch and another device. A static port trunk improves performance by distributing the traffic across multiple ports between the devices and enhances reliability by reducing the reliance on a single physical link.

A static trunk is easy to configure. You designate the ports on the switch that are to be in the trunk and the management software on the switch automatically groups them together.

The example in Figure 20 illustrates a static port trunk of four links between two AT-8000/8POE Fast Ethernet switches.

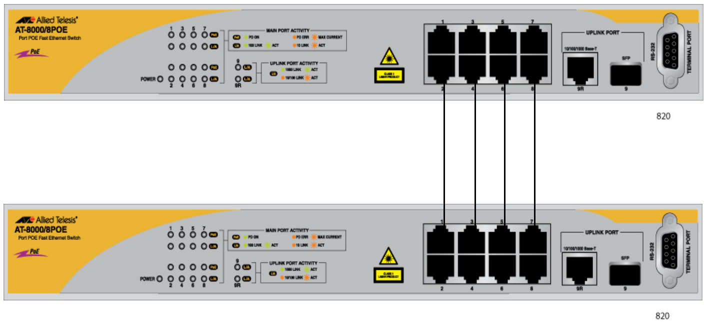


Figure 20. Static Port Trunk Example

Network equipment vendors tend to employ different techniques to implement static trunks. Consequently, a static trunk on one device might not be compatible with the same feature on a device from a different manufacturer. For this reason static trunks are typically employed only between devices from the same vendor. That is not to say that an Allied Telesis layer 2 managed switch cannot form a static trunk with a device from another manufacturer; but there is the possibility that the implementations of static trunking on the two devices might not be compatible.

Also note that a static trunk does not provide for redundancy or link backup. If a port in a static trunk loses its link, the trunk's total bandwidth is diminished. Though the traffic carried by the lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until the lost link is reestablished or you reconfigure the trunk by adding another port to it.

Port Trunking Guidelines

Observe the following guidelines when creating a port trunk:

- ❒ A port trunk can consist of up to 8 ports, but must have a minimum of 2 ports.
- ❒ The switch can support up to 4 trunks at a time.
- ❒ A port can belong to only one trunk at a time.
- ❒ 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. A port trunk cannot consist of ports from different VLANs.
- ❒ 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-8000/8POE Fast Ethernet switches. On the first switch you select ports 1 through 4 for a trunk. On the second switch you select ports 5 through 8. To maintain the order of the port connections, connect port 1 on the first switch to port 5 on the second switch, port 2 to port 6, and so on.
- ❒ To avoid compatibility problems, Allied Telesis recommends creating a port trunk only between AT-8000/8POE Fast Ethernet switches. A port trunk between an AT-8000/8POE Fast Ethernet switch and a device from another manufacturer might result in undesirable trunk behavior.

LACP Trunks

An LACP (Link Aggregation Control Protocol) trunk is another type of port trunk. It performs the same function as a static trunk. It increases the bandwidth between two network devices by distributing the traffic load over multiple physical links.

The advantage of an LACP trunk over a static port trunk is its flexibility. While implementations of static trunking tend to be vendor specific, the AT-S81 implementation of LACP is compliant with the IEEE 802.3ad standard. This makes it interoperable with equipment from other vendors that also comply with the standard. Therefore, you can create a trunk between an Allied Telesis device and networking devices from other manufacturers.

LACP Trunk Status

The AT-8000/8POE Fast Ethernet switch can have up to four trunks. A maximum of eight ports of each trunk can be assigned by the switch administrator. You can configure each trunk's status as Active, Passive, Manual, or Disabled.

When a trunk is created, its default status is Disabled. This means that the trunk does not pass network traffic or send/receive LACP data units (LACPDU) until the trunk status is changed accordingly.

When a trunk is set to Active status, the trunk ports are all available as part of the active LACP trunk. The trunk ports of an active trunk will all send and receive LACPDUs. A minimum number of trunk ports determined by the bandwidth requirements of the network traffic will pass network traffic. Additional ports within an active trunk will dynamically be added or deleted by the LACP feature depending on the increase or decrease of the network traffic.

When a trunk is set to Passive status, the trunk ports are available to be activated by their link partners. If the trunk receives LACP data unit packets from an Active link partner, it automatically transitions to an Active status. The trunk ports will not transmit LACP data units unless the link partners are in the Active status.

A trunk set to Manual status is effectively a static trunk and has none of the benefits of the LACP feature. The trunk ports of an active trunk will not send or receive LACPDUs. The switch administrator must manually add or delete trunk ports from a trunk.

LACP Port Priority Parameter

The switch uses this parameter to determine which ports are to be active and which are to be in the standby mode in situations where the number of ports in the aggregate trunk exceeds the highest allowed number of active ports. This parameter can be adjusted on each port and is a number from 1 to 255. The lower the number, the higher the priority. Ports with the highest priorities are designated as the active ports in an aggregate trunk.

For example, if both 802.3ad-compliant devices support up to four active ports and there are a total of eight ports in the trunk, the four ports with the lowest priority settings are designated as the active ports, and the others are placed in standby mode. If an active link goes down on a active port, the standby port with the highest priority is automatically activated to take its place.

The default value of a port's priority number is equal to 1.

The selection of the active links in an aggregate trunk is dynamic. It changes as links are added, removed, lost or reestablished. For example, if an active port loses its link and is replaced by another port in the standby mode, the reestablishment of the link on the originally active port causes it to return to the active state by virtue of its having a higher priority, while the port that replaced it is returned to the standby mode.

In the unusual event that you set this parameter to the same value for some or all of the ports of an aggregate trunk, the selection of active ports is based on port numbering. The lower the port number, the higher the priority.

Two conditions must be met in order for a port that is a member of an aggregate trunk to function in the standby mode. First, the number of ports in the trunk must exceed the highest allowed number of active ports and, second, the port must be receiving LACPDU packets from the other device. A port functioning in the standby mode does not forward network traffic, but it does continue to send LACPDU packets. If a port that is part of a trunk group does not receive LACPDU packets, it functions as a normal Ethernet port and forwards network packets along with LACPDU packets.

LACP Trunk Guidelines

Following are the guidelines for creating aggregators:

- ❐ LACP must be activated on both the switch and the other device.
- ❐ The other device must be 802.3ad-compliant.
- ❐ The AT-8000/8POE Fast Ethernet switch supports up to eight active ports in a trunk group at a time.
- ❐ The switch supports a maximum of four trunks.
- ❐ The ports of a trunk group must be of the same medium type: all twisted pair ports or all fiber optic ports.
- ❐ The ports of a trunk can be consecutive (for example ports 2-6) or nonconsecutive (for example, ports 2, 4, 6, 8).
- ❐ A port can belong to only one trunk group at a time.

- ❒ The ports of an trunk group must be untagged members of the same VLAN.
- ❒ An LACP trunk does not forward VLAN ID information.
- ❒ 10/100Base-TX twisted pair ports must be set to Auto-Negotiation or 100 Mbps, full-duplex mode. LACP trunking is not supported in half-duplex mode.
- ❒ 1000Base-X fiber optic ports must be set to full-duplex mode.
- ❒ You can create a trunk group that includes transceivers with 1000Base-X fiber optic ports.
- ❒ Only those ports that are members of a trunk group transmit LACPDU packets.
- ❒ A port that is a member of a trunk group functions as part of an aggregate trunk only if it receives LACPDU packets from the remote device. If it does not receive LACPDU packets, it functions as a regular Ethernet port, forwarding network traffic while also continuing to transmit LACPDU packets.
- ❒ The port with the highest priority in a trunk group carries broadcast packets and packets with an unknown destination. For background information, refer to “LACP Port Priority Parameter” on page 84.
- ❒ Prior to creating a trunk group between an AT-8000/8POE Fast Ethernet switch and another vendor’s device, refer to the vendor’s documentation to determine the maximum number of active ports the device can support in a trunk. If the number is less than eight, the maximum number for the AT-8000/8POE Fast Ethernet switch, you should probably assign a higher system LACP priority to the other vendor’s switch. If it is more than eight, assign the higher priority to the AT-8000/8POE Fast Ethernet switch. This can avoid a possible conflict between the devices if some ports are placed in the standby mode when the devices create the trunk. For background information, refer to “LACP Port Priority Parameter” on page 84.
- ❒ LACPDU packets are transmitted as untagged packets.

Setting Up a Port Trunk

This section contains the following procedures for working with port trunks:

- “Creating a Port Trunk” on page 87
- “Modifying a Port Trunk” on page 89
- “Enabling or Disabling a Port Trunk” on page 90

Creating a Port Trunk

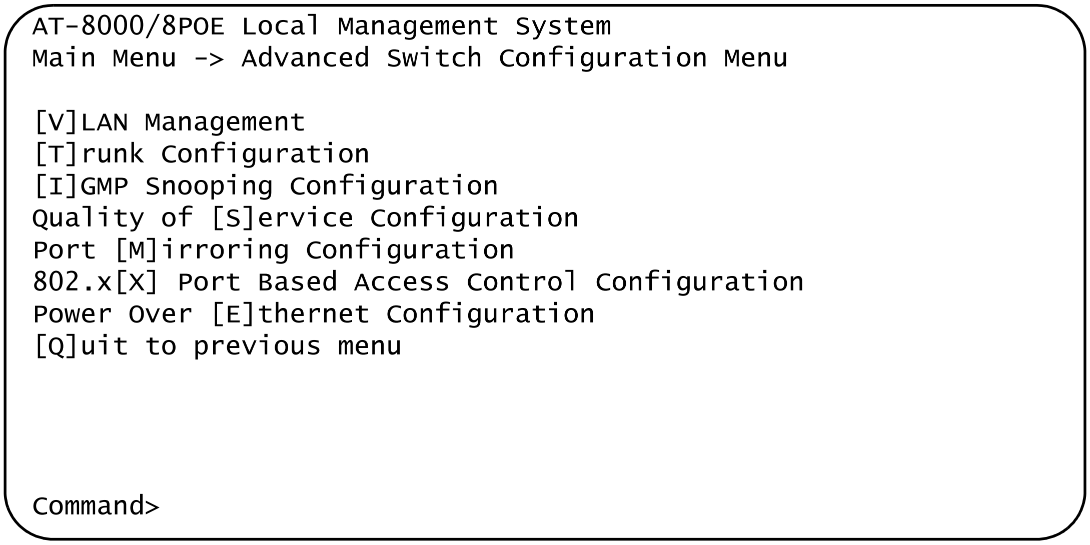
This procedure explains how to create a port trunk.

Caution
Do not connect the cables to the ports on the switches until after you have configured and enabled the trunk with the management software. Connecting the cables before configuring the software creates a loop in your network topology, which can result in broadcast storms and poor network performance.

To create and enable 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 21.

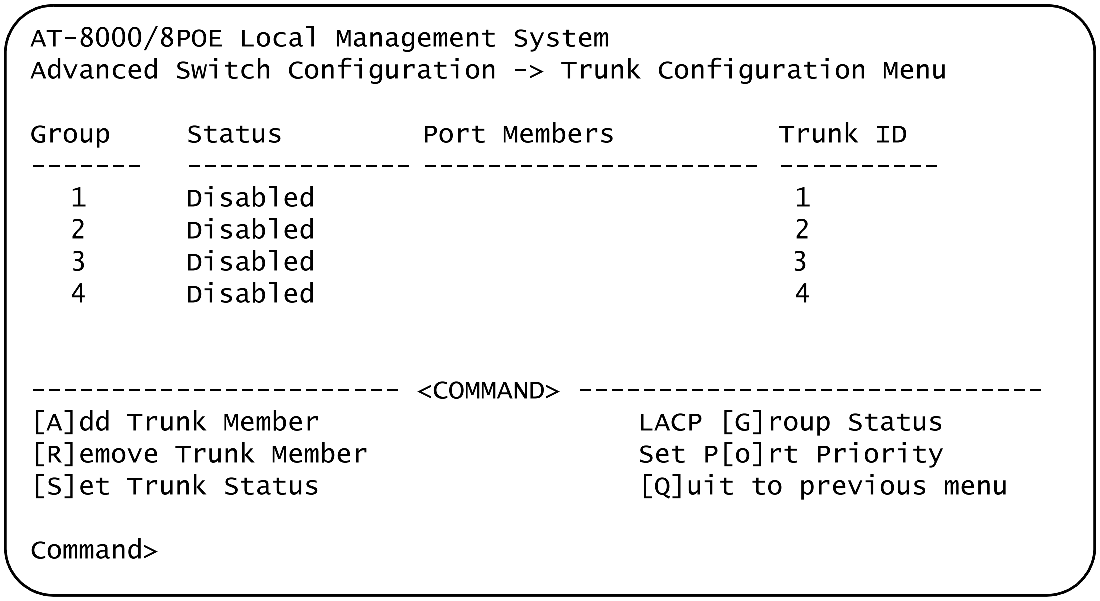


```
AT-8000/8POE Local Management System
Main Menu -> Advanced Switch Configuration Menu

[V]LAN Management
[T]runk Configuration
[I]GMP Snooping Configuration
Quality of [S]ervice Configuration
Port [M]irroring Configuration
802.x[X] Port Based Access Control Configuration
Power Over [E]thernet Configuration
[Q]uit to previous menu




Command>
```

Figure 21. 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 22.



```
AT-8000/8POE 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



----------------------- <COMMAND> -----------------------------
[A]dd Trunk Member                    LACP [G]roup Status
[R]emove Trunk Member                 Set P[o]rt Priority
[S]et Trunk Status                    [Q]uit to previous menu

Command>
```

Figure 22. Trunk Configuration Menu

3. To add a trunk member, 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 4.

   The following prompt is displayed:

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

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

   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, 1,3, 5-8).

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

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

7. Type the trunk group number.

The following prompt is displayed:

```
Set trunk group n status (A/P/M/D)>
```

8. Type **M** to select **Manual Trunk** for a basic trunk without LACP handling.

   The **A** and **P** options apply to LACP trunks. See "Setting Up an LACP Trunk" on page 92 for more information.

   The trunk is now operational on the switch.

9. 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.

Note
Disconnect the cables from the ports of the trunk on the switch before modifying it. Adding or removing ports from a trunk without first disconnecting the cables can create loops in your network topology, which can cause broadcast storms and poor network performance.

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 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

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.

   The following prompt is displayed:

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

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

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, 1,3, 6-8).

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

Enabling or 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.

Note
If you are disabling a port trunk, be sure to first disconnect all cables from the ports of the trunk. Leaving the cables connected can create loops in your network topology because the ports of a disabled port trunk function as normal network ports, forwarding individual network traffic.

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 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

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

   The following prompt is displayed:

```
Enter trunk group number>
```

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

   The following prompt is displayed:

   ```
   Set trunk group n status (A/P/M/D)>
   ```

5. Type **M** to enable a manual trunk, or **D to** disable the trunk.

Setting Up an LACP Trunk

This section contains the following procedures to work with LACP trunks:

- “Creating an LACP Trunk,” next
- “Configuring the LACP Port Priority” on page 93
- “Viewing the LACP Group Settings” on page 94
- “Disabling an LACP Trunk” on page 95

> **Note**
> Create the trunk before you make it an LACP trunk. For more information, see “Setting Up a Port Trunk” on page 87.

Creating an LACP Trunk

To create an LACP 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 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

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

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

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

   The following prompt is displayed:

   ```
   Set trunk group n status (A/P/M/D)>
   ```

5. Choose one of the four following settings:

   A - LACP Active: Ports are in an active negotiation state.

   P - LACP Passive: Ports are in a passive state where the port negotiates a bundle by exchanging LACP packets to the peer only if the far end initiates it.

Note
LACP must be enabled at both ends of the link to be operational.

Configuring the LACP Port Priority

LACP port priority determines which port is the backup port to another port when the link to that port is down. The port with the lowest value has the highest value, and is selected to join the link aggregation group first.

To configure the LACP port priority, perform the following procedure:

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

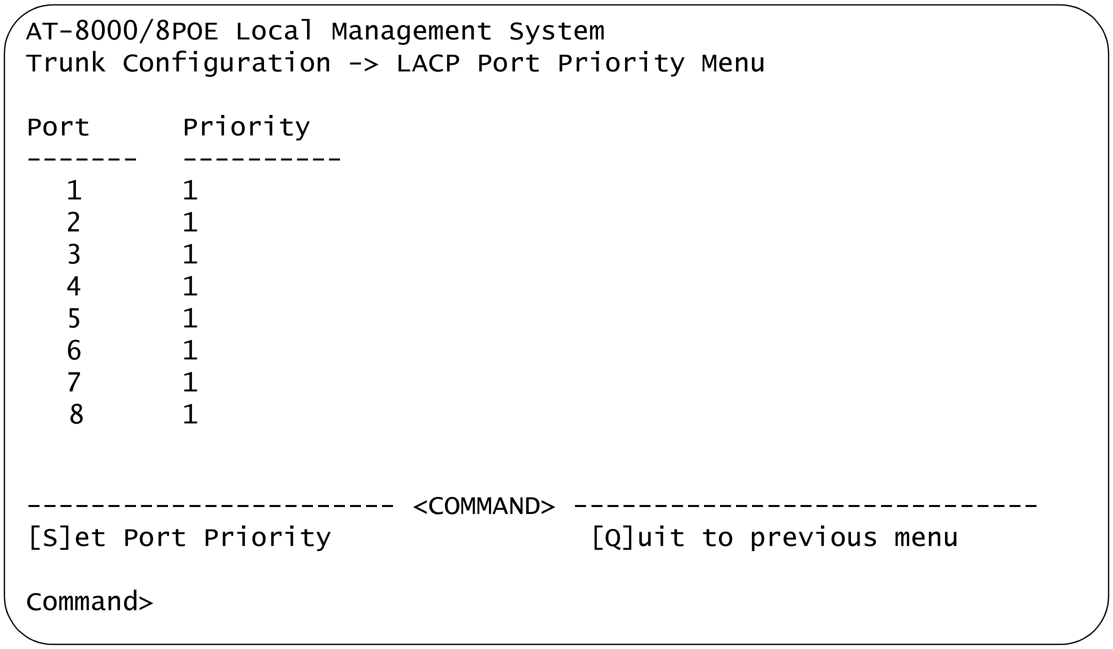
   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

3. From the Trunk Configuration Menu, type **O** to select **Set Port Priority.**

   The LACP Port Priority Menu is shown in Figure 23.



```
AT-8000/8POE Local Management System
Trunk Configuration -> LACP Port Priority Menu

Port      Priority
-------   ----------
   1      1
   2      1
   3      1
   4      1
   5      1
   6      1
   7      1
   8      1


----------------------- <COMMAND> -----------------------------
[S]et Port Priority               [Q]uit to previous menu

Command>
```

Figure 23. LACP Port Priority Menu

4. From the LACP Port Priority Menu, type **S** to select **Set Port Priority**.

   The following prompt is displayed:

```
Enter port no>
```

5. Type the number of the port whose priority you want to set.

   The following prompt is displayed:

   ```
   Enter port priority>
   ```

6. Enter a number for the priority of the port.

   The range is 1 to 255, and the default is 1.

Viewing the LACP Group Settings

To view the LACP group settings, 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 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

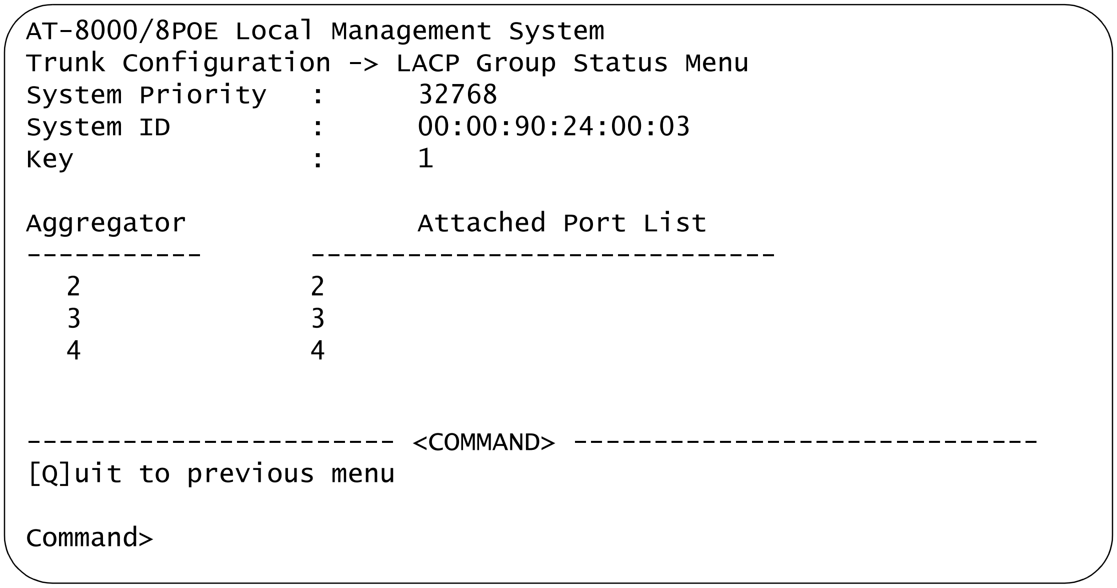
3. From the Trunk Configuration Menu, type **G** to select **LACP Group Status**.

   The following prompt is displayed:

   ```
   Enter trunk group admin key
   ```

4. Type a number from 1 to 4 to specify the admin key of the trunk you want to view.

   The LACP Group Status Menu opens, as shown in Figure 24.



```
AT-8000/8POE Local Management System
Trunk Configuration -> LACP Group Status Menu
System Priority   :      32768
System ID         :      00:00:90:24:00:03
Key               :      1

Aggregator               Attached Port List
-----------       ----------------------------
   2              2
   3              3
   4              4


----------------------- <COMMAND> -----------------------------
[Q]uit to previous menu

Command>
```

Figure 24. LACP Group Status Menu

The LACP Group Status Menu displays the following information about the LACP group:

System Priority
The system priority as defined by IEE 802.3ad. You cannot change this.

System ID
The MAC address of the system.

Key
The key for this trunk group.

The menu also contains a table that displays the following information:

Aggregator
The port that is operating as the aggregator.

Attached Port List
The ports assigned to the aggregator.

Disabling an LACP Trunk

To disable an LACP 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 21 on page 87.

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

   The Trunk Configuration Menu is shown in Figure 22 on page 88.

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

   The following prompt is displayed:

   ```
   Enter trunk group number>
   ```

4. Enter the trunk group number.

   ```
   Set trunk group n status (A/P/M/D)>
   ```

5. Type **D** to select **Disabled**.

Chapter 7
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:

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the ingress and egress traffic on a port on the switch by having the traffic copied to another switch port. By connecting a network analyzer to the port where the traffic is being copied to, you can monitor the traffic on the other port without impacting its 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

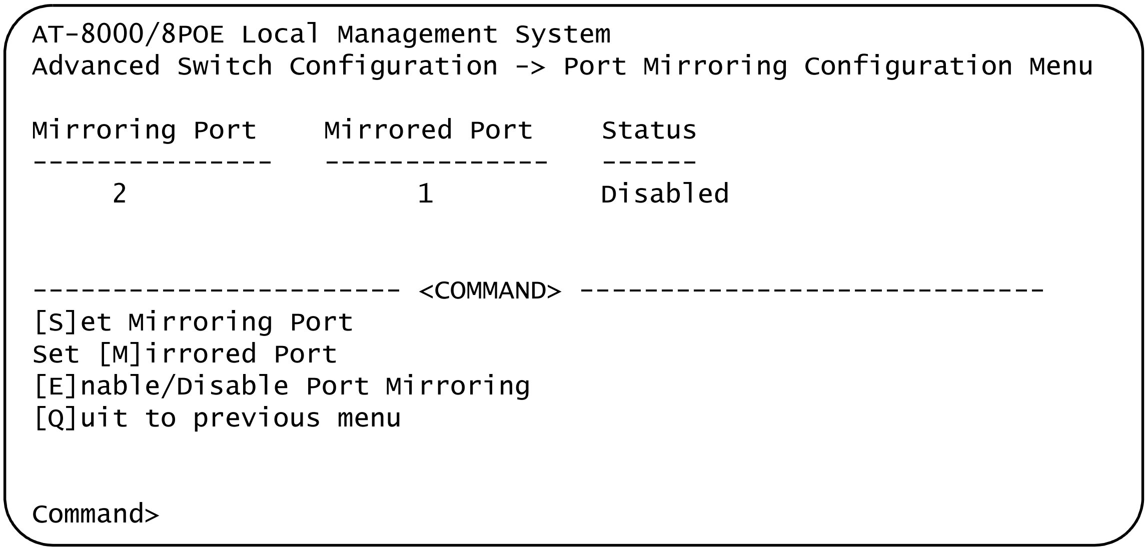
To set up port mirroring, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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

   The Port Mirroring Configuration Menu is shown in Figure 25.



```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> Port Mirroring Configuration Menu

Mirroring Port    Mirrored Port    Status
---------------   --------------   ------
     2                  1          Disabled


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


Command>
```

Figure 25. 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. 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. You can specify only one port.

7. To enable or disable Port Mirroring, See “Enabling or Disabling Port Mirroring” on page 101.

Enabling or Disabling Port Mirroring

To enable or disable 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 21 on page 87.

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

   The Port Mirroring Menu is shown in Figure 25 on page 99.

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

   The following prompt is displayed:

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

4. Type **E** to enable port mirroring or **D** to disable port mirroring. Port mirroring is disabled by default.

   When you disable port mirroring, the port that was functioning as the mirroring port can then be used as a normal networking port.

Chapter 8

Power Over Ethernet

This chapter contains the following sections:

PoE Overview

The twisted pair ports on the AT-8000/8POE Fast Ethernet Switch feature Power over Ethernet (PoE). PoE is a mechanism for supplying power to network devices over the same twisted pair cables used to carry network traffic. This feature can simplify network installation and maintenance by allowing you to use the switch as a central power source for other network devices.

A device that receives its power over an Ethernet cable is called a *powered device*. Examples of such devices can be wireless access points, IP telephones, webcams, and even other Ethernet switches. An example of the latter is the unmanaged AT-FS705PD Ethernet switch from Allied Telesis. A powered device connected to a port on the switch will receive both network traffic and power over the same twisted pair cable.

The switch automatically determines whether a device connected to a port is a powered device or not. A powered device has a signature resistor or signature capacitor that the switch can detect over the Ethernet cabling. If the resistor or capacitor is present, the switch assumes that the device is a powered device.

Note
The uplink ports (9 and 9R) do not provide PoE.

Power Budgeting

The AT-8000/8POE Fast Ethernet Switch provides a maximum of 15.4 W of power per port on six of the eight ports for a total power consumption of 95 W, while at the same time furnishing standard 10/100 Mbps Ethernet functionality. A port connected to a network node that is not a powered device (that is, a device that receives its power from another power source) functions as a regular Ethernet port, without PoE. The PoE feature remains enabled on the port but no power is delivered to the device.

You can, using the AT-S81 management software, enable or disable PoE on a per-port basis, but you cannot change the amount of power a port can receive.

The AT-S81 management software also allows you to prioritize the ports in the event that there is not enough PoE power for all the powered devices. This feature helps ensure that the most important powered devices connected to the switch are guaranteed to have power.

The default setting for PoE on the switch is enabled at the port level.

Port Prioritization for Power Allocation

The AT-S81 management software also allows you to prioritize the ports in the event that the powered devices require more power than the switch can deliver. This feature ensures that the most important powered devices connected to the switch are guaranteed to have power.

If the powered devices connected to the switch require more power than the switch is capable of delivering, the switch denies power to some ports based on a system called *port prioritization*. You can use this system to ensure that powered devices that are critical to your network are given preferential access to the available power.

There are three priority levels:

- Critical
- High
- Low

Ports designated as critical receive power before any other ports with a lower priority. Always assign the critical priority level to your most important network devices. If there is not enough power to support all the ports set to the critical priority level, then power is provided to the ports based on port number, in ascending order.

Ports set to the high level receive power only after all the critical ports receive their power. If there is not enough power to support all the ports set to the high priority level, then power is provided to the ports based on port number, in ascending order.

The lowest priority setting is low, the default setting for all ports. Ports with low priority receive power only after the critical and high level ports receive their power. If there is not enough power to support all the ports set to the high priority level, then power is provided to the ports based on port number, in ascending order.

PoE Device Classes

The IEEE 802.3af standard specifies four classes for powered devices based on their power usage. The classes are defined in Table 2.

Table 2. Power Classes for Powered Devices

Class	Power Usage
0 (Default)	0.44 W to 12.95 W
1	0.44 W to 3.84 W
2	3.84 W to 6.49 W
3	6.49 W to 12.95 W

Note
The standard specifies five classes, but the fifth is reserved for future use.

Manufacturers set the power class of their PoE powered devices. You cannot adjust this. You can view the power class of each device in the Power Over Ethernet menu, shown in Figure 26 on page 107.

Even though each port is capable of supplying up to 15.4 W, the standard calls for a maximum power consumption of 12.95 W, 2.45 W less than the port can supply. This extra capability is to compensate for possible line loss. Some power is likely to be lost on the twisted pair cable as it travels from the switch to the device. For devices that require 12.95 W, the extra watts act as compensation for this possible loss.

Configuring PoE

This section contains the following procedures:

❒ “Displaying the PoE Configuration,” next

❒ “Changing the PoE Port’s Admin Setting” on page 108

❒ “Setting the PoE Port’s Priority” on page 109

Displaying the PoE Configuration

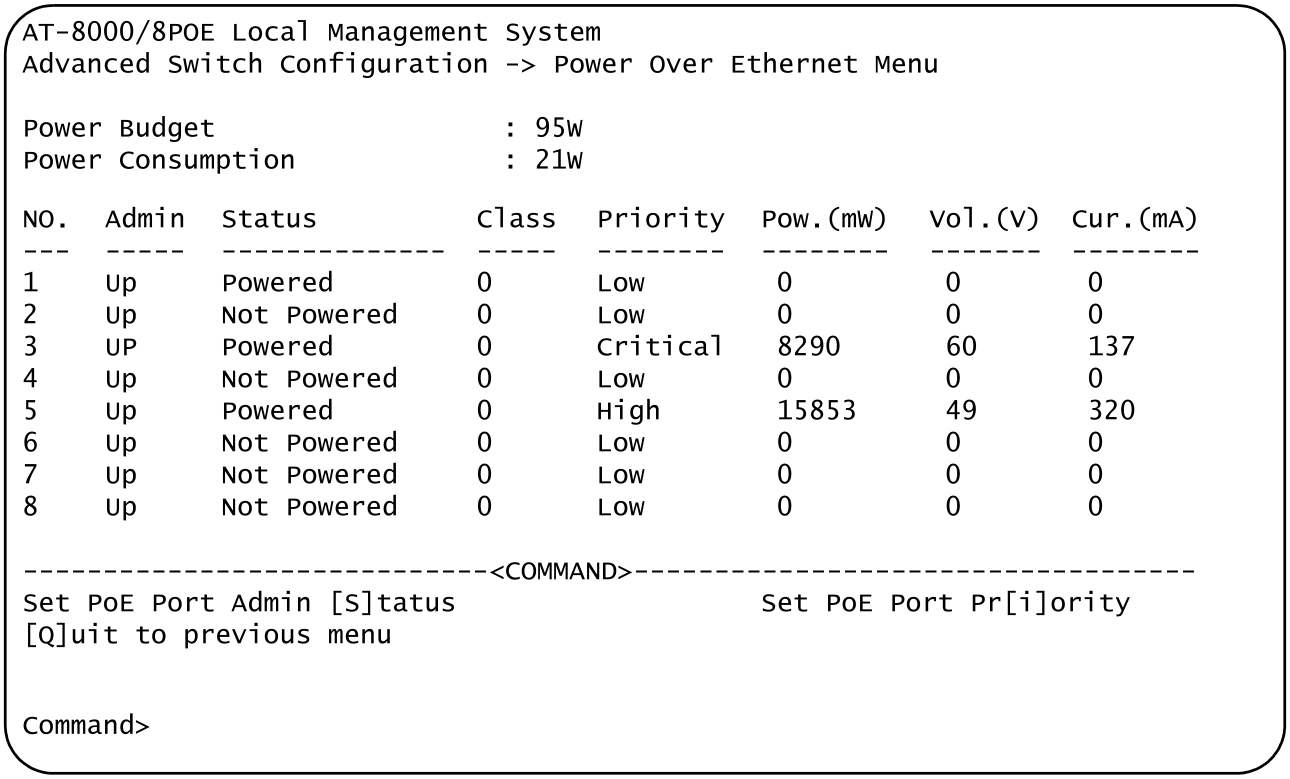
To display the current PoE Configuration, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

2. From the Advanced Switch Configuration menu, type **E** to select **Power Over Ethernet.**

   The Power Over Ethernet menu is shown in Figure 26.



```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> Power Over Ethernet Menu

Power Budget                  : 95W
Power Consumption             : 21W

NO.  Admin  Status          Class  Priority  Pow.(mW)  Vol.(V)  Cur.(mA)
---  -----  --------------  -----  --------  --------  -------  --------
1    Up     Powered         0      Low        0         0        0
2    Up     Not Powered     0      Low        0         0        0
3    UP     Powered         0      Critical   8290      60       137
4    Up     Not Powered     0      Low        0         0        0
5    Up     Powered         0      High       15853     49       320
6    Up     Not Powered     0      Low        0         0        0
7    Up     Not Powered     0      Low        0         0        0
8    Up     Not Powered     0      Low        0         0        0

-----------------------------<COMMAND>-----------------------------------
Set PoE Port Admin [S]tatus                   Set PoE Port Pr[i]ority
[Q]uit to previous menu


Command>
```

Figure 26. Power Over Ethernet Menu

The Power Over Ethernet Configuration menu displays information about the PoE status of each port and also allows you to configure the port's status and priority. The table includes the following items of information:

Admin
The status of the port, either up or down. To change the Admin selection, refer to "Changing the PoE Port's Admin Setting" on page 108.

Status
The status of PoE power on that port, including:

Powered - The port is providing power to a powered device.

Not Powered - The device is not a powered device or that no device is connected to the port.

Over Budget - The power budget of 95W has been exceeded.

Overload - The power supplied to the port exceeds the maximum of 15.4W.

Class
The IEEE 802.3af class of the device. You cannot change this setting. For more information, refer to "PoE Device Classes" on page 105.

Priority
The port's priority for receiving power from the switch. For more information about port priority, refer to "Port Prioritization for Power Allocation" on page 105. To set the priority, refer to "Setting the PoE Port's Priority" on page 109.

Power (mW)
The amount of power being delivered to the device, in Milliwatts.

Voltage (V)
The amount of voltage being delivered to the device, in Volts.

Current (mA)
The amount of current being delivered to the device, in Milliampere.

Changing the PoE Port's Admin Setting

To change a port's admin setting from up (online) to down (offline), perform the following procedure:

1. Type **S** to select **Set PoE Port Admin Status**.

   The following prompt is displayed:

   ```
   Enter port number >
   ```

2. Enter the number of the port you whose status you want to change.

   The following prompt is displayed:

   ```
   Up or Down port n (U/D) >
   ```

3. Type **U** to change the status to Up (online), or type **D** to change the status to Down (offline).

Setting the PoE Port's Priority

The priority defines which port and its attached PoE powered device should receive priority for the available power over other PoE devices. For more information about port priority, refer to "Port Prioritization for Power Allocation" on page 105.

To set the port priority, perform the following procedure:

1. Type **I** to select **Set PoE Port Priority**.

   The following prompt is displayed:

   ```
   Enter port number >
   ```

2. Enter the number of the port you whose priority you want to change.

   The following prompt is displayed:

   ```
   Enter the selection (L/H/C) >
   ```

3. Type one of the following:

   L - To change the port priority to low. This is the default.

   H - To change the port priority to high.

   C - To change the port priority to critical, so that this device continues to receive power even if others do not.

Chapter 9

Virtual LANs and GVRP

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

VLAN Features

A Virtual Local Area Network (VLAN) is a logical grouping of devices on different physical LAN segments that allows users to communicate as if they were physically connected to a single LAN, independent of the physical configuration of the network.

With VLANs, you can segment your network and group end-nodes with related functions into their own separate, logical LAN segments. For example, the marketing personnel in your company may be spread throughout a building. Assigning marketing to a single VLAN allows marketing personnel to share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be visible to the marketing VLAN members, accessible, or accessible only to specified individuals.

A few benefits of a VLAN architecture are described in the following sections.

Increased Performance

In traditional Layer 2 switched networks, broadcast packets are sent to each and every individual port. Grouping users into logical networks limits broadcast traffic to users performing similar functions or users within individual workgroups. High traffic, the danger of broadcast storms, router latency, and data collisions are significantly reduced, and the efficiency of the entire network is improved.

Improved Manageability

VLANs provide a fundamental improvement in the design, administration, and management of LANs. Before VLANs, physical changes to a network were made at the switch in the wiring closet.

For example, if an employee transferred to a new department, changing that employee’s LAN segment assignment often required a physical wiring change at the switch.

As a software-base solution, VLANs eliminate the restriction of existing network design and cabling infrastructure and allow the centralized configuration of switches located in many different locations. VLAN memberships are changed quickly and efficiently from the management console rather than in a wiring closet.

Increased Security

VLANs provide additional security not available in a shared media network environment. Because a switched network only delivers frames to intended recipients, and only broadcast frames to other members of the VLAN, a network administrator can segment users requiring access to sensitive information into separate VLANs from the rest of the general user community.

VLANs can be used to control the flow of data in your network, since the traffic generated by an end-node in a VLAN is restricted to the other end-nodes in the same VLAN. In addition, VLANs can prevent data from flowing to unauthorized end-nodes

VLAN Overview

This VLAN overview contains the following sections:

❒ “VLAN Name,” next

❒ “VLAN Identifier” on page 114

❒ “VLAN Port Members” on page 114

❒ “Port VLAN Identifier” on page 114

❒ “Incoming and Outgoing Tagged and Untagged Frames” on page 115

❒ “Guidelines for Creating a VLAN” on page 116

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.

VLAN Identifier

Every VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network. The factory VID is 1 for all ports.

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

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

For example, if you had a VLAN titled Marketing that spanned three AT-8000/8POE Fast Ethernet switches, you would assign the Marketing VLAN on each switch the same VID.

Port VLAN Identifier

The Port VLAN Identifier (PVID) is the VLAN identifier associated with a specific port. The PVID provides a VLAN assignment for each untagged frame received by the switch. (See “Incoming and Outgoing Tagged and Untagged Frames” on page 115.) The switch internally associates the untagged frame with the VID that is equal to the PVID. The switch then forwards this frame to one of the other member ports of that VLAN. The default PVID value is 1.

VLAN Port Members

You need to specify which ports on the switch are to be members of a VLAN. A port can be specified as a member of one or more VLANs up to 255, the maximum number of VLANs supported by the switch. The factory default VID is 1. Therefore, each port is initially configured to be a member of VLAN 1, which is known as the default VLAN.

Note
The switch is preconfigured with the Default_VLAN only. All ports on the switch are initially members of the Default_VLAN.

If a port is assigned to be a new member of a VLAN, its membership can be defined as either tagged or untagged.

Tagged Port Members

A port is a tagged member of a VLAN when the PVID does not equal the VID. In this case, the port must be a member of two or more VLANs. If a port is a tagged member of one VLAN, then the same port is also an untagged member of another VLAN where the PVID matches its VID.

Untagged Port Members

A port is an untagged member of a VLAN if the PVID is equal to the VID of that VLAN. A port can be an untagged member of only one VLAN. An example of this is the Default_VLAN configuration where all ports are initially configured to be untagged members of VLAN 1 only. A port can be an untagged member of one VLAN and be a tagged member of one or more VLANS at the same time. (See Figure 28 on page 119.)

Incoming and Outgoing Tagged and Untagged Frames

The VLAN information within an Ethernet frame is referred to as a tag or tagged header. An Ethernet frame can contain VLAN information within its header. Likewise, a frame that does not contain this VLAN tag information is referred to as an untagged or standard frame. A tag contains the VID information of the VLAN to which the frame belongs, according to the IEEE802.1Q VLAN tagging standard.

When a switch receives a frame, it examines the frame header to see if it contains a VLAN tag (tagged frame) or no tag (untagged frame). After switching the frame to an outgoing port and before transmitting it, the switch determines if the tag information should be kept in the header or should be stripped out and made into an untagged frame.

Incoming Frames

Tagged frames received by the switch are only accepted (not dropped or discarded) if the tag information contained in the frame is equal to one of the VIDs of which the port is a member. If the tag information contained in the frame does not match one of these VIDs, the frames are dropped or discarded.

Untagged frames received by the switch are always accepted by all ports on the switch. As described in “Port VLAN Identifier” on page 114, each untagged frame received by the switch is assigned a VLAN number equal to the PVID. The switch then forwards this frame to one of the other member ports of that VLAN.

Outgoing Frames

Frames being transmitted from the switch retain their VLAN tag information in the frame header if the frame’s tag does not match the PVID of the port (a tagged member of that VLAN). These frames are untagged after transmission from the switch.

The VLAN tag information in the header of the frame is stripped from the frame’s header if the tag matches the PVID of the port (an untagged member of the VLAN). These frames are untagged after transmission from the switch.

Guidelines for Creating a VLAN

The following are guidelines for creating a VLAN.

- ❐ Each VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches should be assigned the same VID.
- ❐ A port can be an untagged member of only one VLAN at a time.
- ❐ Each port must be assigned a PVID (the default is 1). This value must match one of the VIDs assigned to the port. If you need to change the PVID value, you must configure it on a port after you assign a port to a VLAN. For instructions, refer to “Configuring the Port PVID” on page 124.
- ❐ A VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside.
- ❐ This port may be defined as an untagged member of a VLAN where the port is connected to another switch via another untagged port member of the VLAN. This means that all traffic on this inter-switch port contains traffic for that VLAN only.
- ❐ Another scenario is where the port could be an untagged member of one VLAN and a tagged member of one or more VLANs. The port would then be connected to another switch via a port with the same VLAN membership. This means that the traffic on this inter-switch port is for any or all of the VLANs of which the port is a member.
- ❐ If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.
- ❐ The switch can support up to a total of 255 VLANs.

Untagged VLAN

Figure 27 illustrates how VLANs with untagged port members can be interconnected. In this example, the Sales VLAN spans two AT-8000/8POE Fast Ethernet switches via a router , while the Production-VLAN is limited to just one switch.

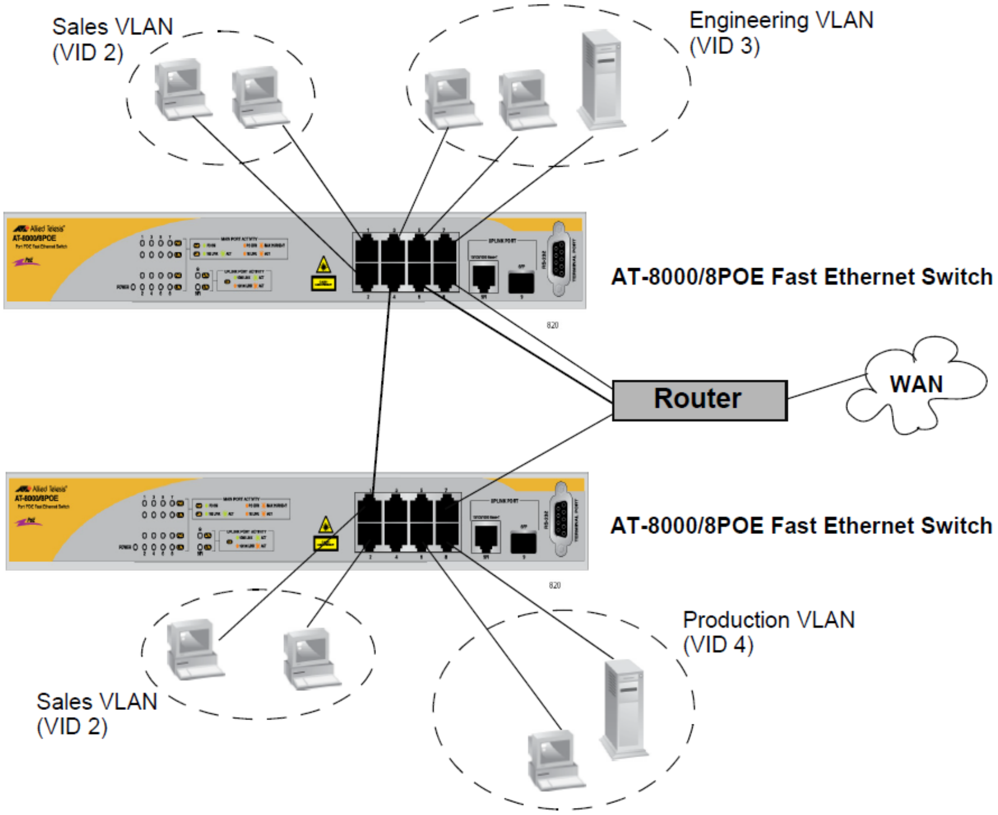


Figure 27. VLAN - Example 2

The table below lists the port numbers for the Sales, Engineering, and Production VLANs on the switches. In this example, all ports are untagged members of their respective VLANS.

Table 3. Port Numbers for VLAN Example 2

	Sales VLAN (VID 2)	**Engineering VLAN (VID 3)**	**Production VLAN (VID 4)**
AT-8000/8POE Fast Ethernet Switch (top)	Ports 1, 2, 4 & 6 (PVID 2)	Ports 3, 5, 7 & 8 (PVID 3)	None
AT-8000/8POE Fast Ethernet Switch (bottom)	Ports 1, 2, & 4 (PVID 2)	None	Ports 6, 7 & 8 (PVID 4)

Note the following concerning the example:

- Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of four untagged port members on the top switch and three untagged port members on the bottom switch. The two parts of the VLAN are connected by a direct link from port 4 on the top switch to port 1 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.
- Engineering VLAN - This VLAN is on the top switch only and consists of four untagged port members. The workstations are connected to ports 3, 5, and 7. Port 8 is used as a connection to the router, other VLANs, and the WAN.
- Production VLAN - This VLAN has the VLAN of 4 and is on the bottom switch only. The workstations are connected to ports 3, 6, and 8. Port 7 is used as a connection to the router, other VLANS, and the WAN.

Tagged VLAN Example

Figure 28 illustrates how tagged and untagged ports can be used to interconnect IEEE 802.1Q-based products.

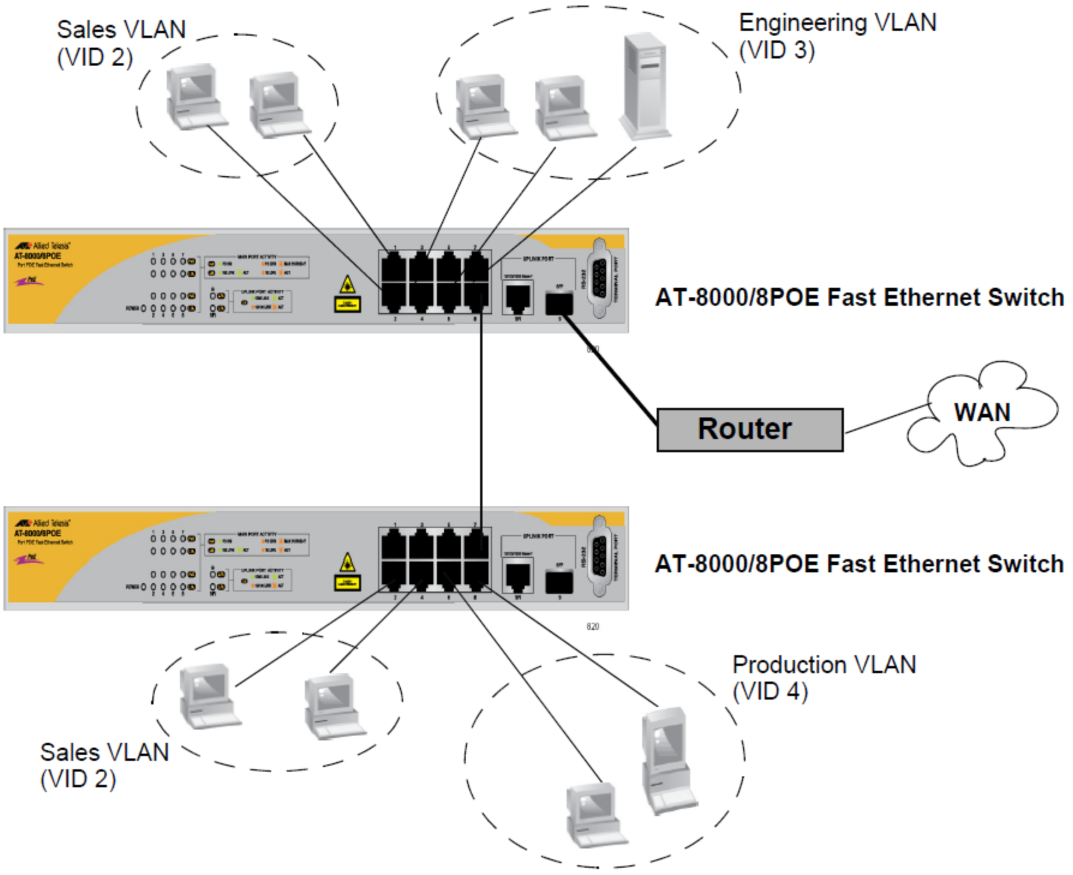


Figure 28. Example of a Tagged VLAN

The port assignments for the VLANs are as follows:

Table 4. Ports for Tagged VLAN Example

	Sales VLAN (VID 2)		Engineering VLAN (VID 3)	
	Untagged Port Members	Tagged Port Members	Untagged Port Members	Tagged Port Members
AT-8000/8POE Fast Ethernet Switch (top)	1, 2 (PVID 2)	6, 9	3, 5, & 7 (PVID 3)	6, 9
AT-8000/8POE Fast Ethernet Switch (bottom)	2, 4 (PVID 2)	5	3, 6,& 8 (PVID 3)	5

Ports 1 and 3 on the top switch and ports 2 and 4 on the bottom switch are assigned a PVID of 2 and are untagged members of only VLAN 2. These ports are connected to workstations from Sales.

Ports 2 and 4 on the top switch and ports, 3, 6, and 8 on the bottom switch are assigned a PVID of 3 and are untagged members of VLAN 3 only. These ports are connected to workstations from Engineering.

Ports 6 and 9 on the top switch and port 5 on the bottom switch are tagged members of both VLANs 2 and 3. Traffic passed between the switches and the router consist of tagged packets from both VLANs. These ports provide a common connection that enables different member ports of the same VLAN to communicate with each other while maintaining data separation between VLANs.

Working with VLANS

This section contains the following procedures:

- ❒ “Creating a VLAN,” next
- ❒ “Configuring the Port PVID” on page 124
- ❒ “Restricting Management VLAN Access” on page 125
- ❒ “Displaying the VLANs” on page 126
- ❒ “Modifying a VLAN” on page 128
- ❒ “Deleting a VLAN” on page 129
- ❒ “Resetting to the Default VLAN” on page 130

Creating a VLAN

This section contains the procedure for creating a new 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 members 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 Port PVID” on page 124.

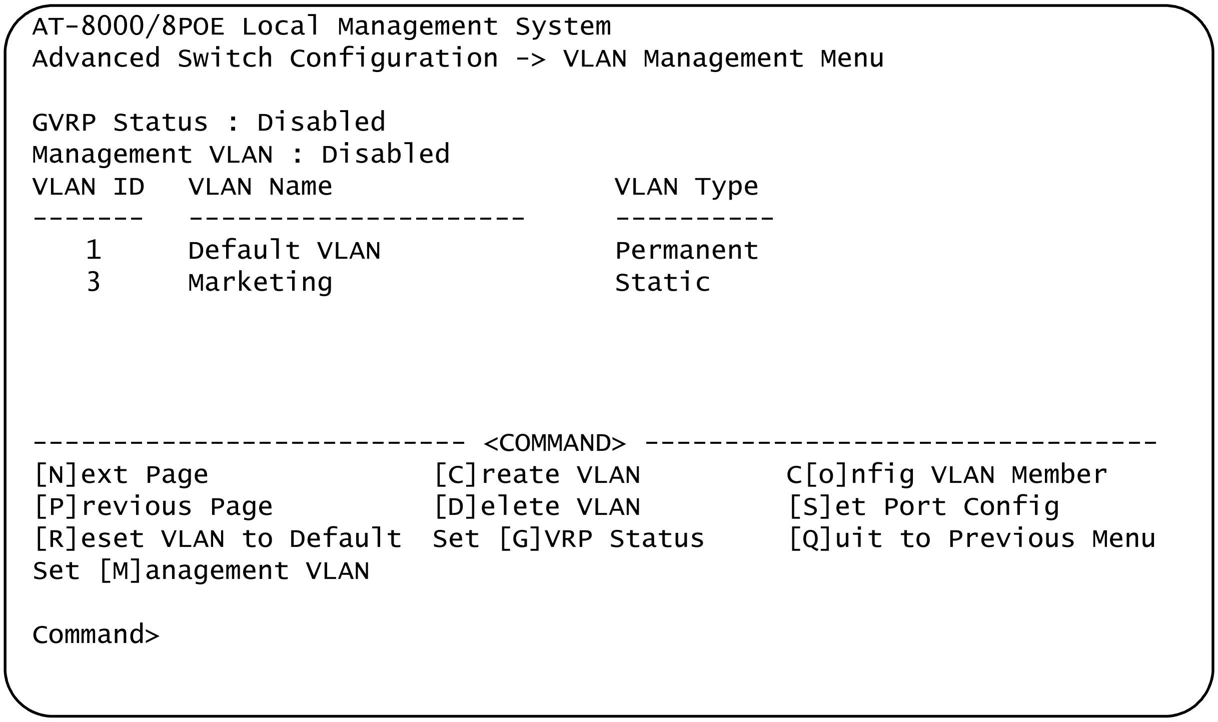
To create a VLAN, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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

The VLAN Management Menu, which displays any existing VLANs, is shown in Figure 29.



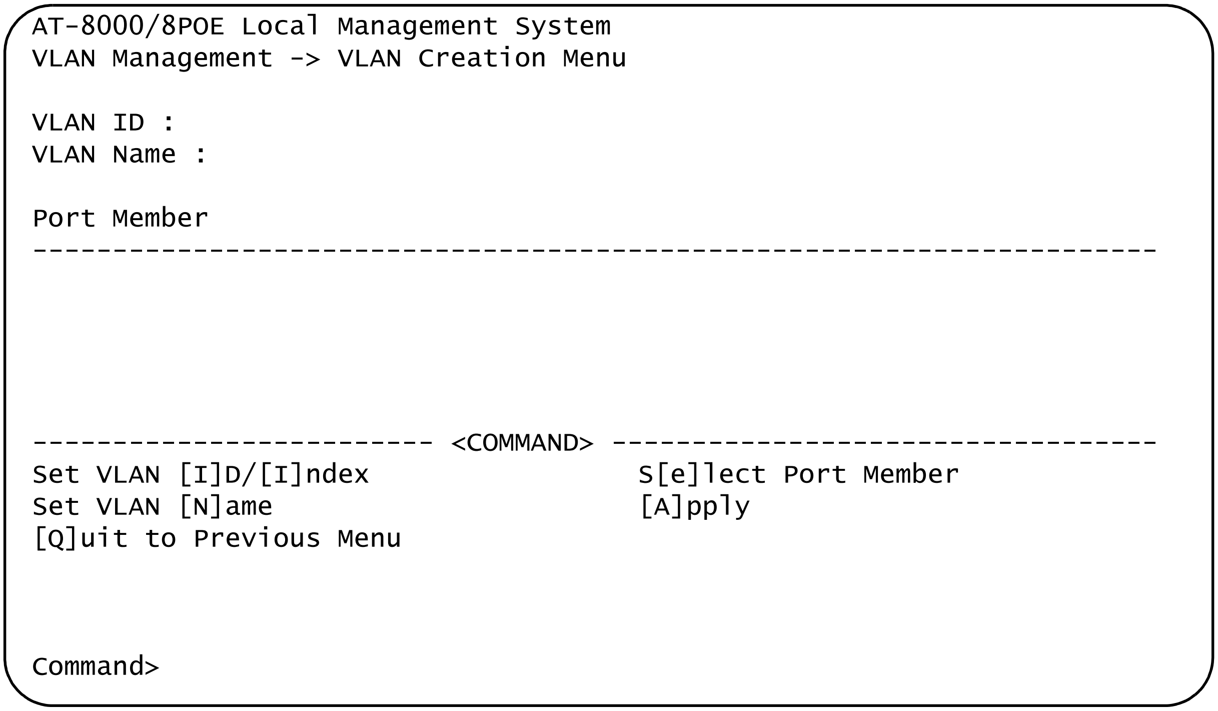
```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> VLAN Management Menu

GVRP Status : Disabled
Management VLAN : Disabled
VLAN ID   VLAN Name                 VLAN Type
-------   ---------------------     ----------
   1      Default VLAN              Permanent
   3      Marketing                 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  Set [G]VRP Status     [Q]uit to Previous Menu
Set [M]anagement VLAN

Command>
```

Figure 29. VLAN Management Menu

Note
The Set GVRP Status option is described in “Enabling or Disabling GVRP” on page 132.

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

The VLAN Creation Menu is shown in Figure 30.



```
AT-8000/8POE Local Management System
VLAN Management -> VLAN Creation Menu

VLAN ID :
VLAN Name :

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






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



Command>
```

Figure 30. VLAN Creation Menu

4. To specify the VLAN ID, do the following:

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

      The following prompt is displayed:

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

      Note
      A VLAN must have a VID.

   b. Enter a value from 2 to 4094.

5. To specify the VLAN name, do the following:

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

      The following prompt is displayed:

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

   b. Enter a name for the VLAN. The VLAN name can contain up to 32 characters including spaces.

6. To add ports to the VLAN, do the following:

a. Type **S** to select **Select Port Number**.

   The following prompt is displayed:

   ```
   Enter port number >
   ```

b. Enter the 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.

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

   The VLAN Management Menu is displayed again with information about the VLAN you just created. The VLAN is now active on the switch.

8. If you intend to define a port as an untagged member of a VLAN, you will need to change the PVID of the port to match the VLAN’s VID. Refer to “Configuring the Port PVID” on page 124.

Configuring the Port PVID

This procedure adjusts a port’s VID value. The PVID value determines if a port is a tagged or untagged member of a VLAN. A port is an untagged member of a VLAN whose VID value matches its PVID. A port is a tagged member of a VLAN whose VID does not match the PVID. (The PVID must equal on of the port’s VIDs.) A port can be a tagged member of a VLAN only if the port is a member of more than one VLAN at the same time.

When you create a new VLAN, the ports of the new VLAN are initially designated as tagged members of the new VLAN. The PVIDs of the ports retain the previous settings after the ports become members of a new VLAN. If you want the ports to function as untagged members of a new VLAN, you must change the PVID values to match the VID of the VLAN, as shown in the following procedure.

To adjust 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

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

The VLAN Port Configuration Menu is shown in Figure 29 on page 122

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

   The following prompt is displayed:

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

5. Type the number of the port whose PVID value you want to configure. You can configure only one port at a time.

   The following prompt is displayed:

   ```
   Enter PVID for port n
   ```

6. Enter the new PVID for the port. 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.

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

Restricting Management VLAN Access

Management access can be restricted to the default vlan (VLAN 1) or made available on any vlan. This feature is activated when you select **ENABLE** in the **Management VLAN** field. If this field is set to **DISABLED**, the management access is available on any vlan.

To set the Management access value, 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

3. Type **M** to select **Set Management VLAN**.

4. Select **E** for enable to restrict the management access to the default vlan (VLAN 1) only or **D** for disable to allow management access on any vlan.

Displaying the VLANs

To display a list of the 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

   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 and tagged VLANs are static.

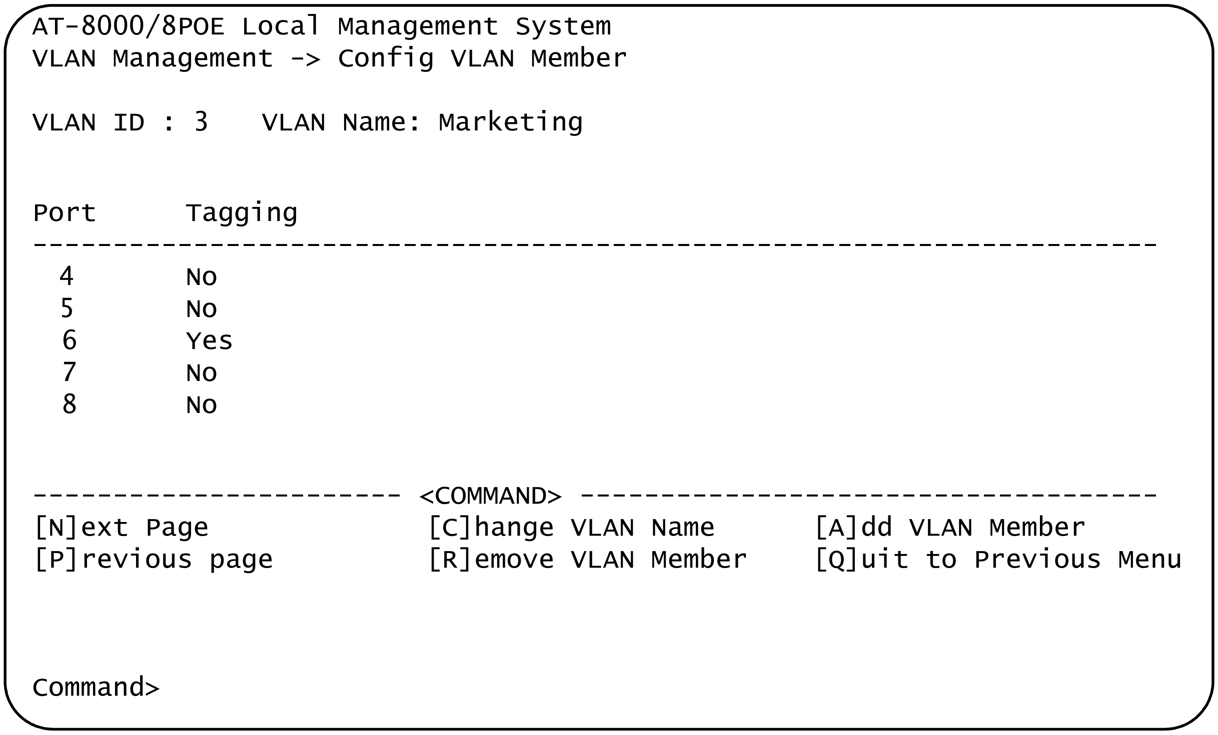
3. To view the ports of a VLAN, type **O** to select **Config VLAN Member**.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

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

The Config VLAN Member Menu is shown in Figure 31.



```
AT-8000/8POE Local Management System
VLAN Management -> Config VLAN Member

VLAN ID : 3   VLAN Name: Marketing


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


----------------------- <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 31. 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 128.

Modifying a VLAN

The topics in this section include:

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 Port PVID" on page 124
- ❐ 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 Port PVID" on page 124.

Changing the VLAN Name

To change the name of 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

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

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

   Enter the number of the VLAN you want to modify.

   The Config VLAN Member menu is shown in Figure 31 on page 127.

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

   The following prompt is displayed:

   ```
   Enter new VLAN name>
   ```

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

Adding or Removing a Tagged Port in a VLAN

To add a tagged port to the 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

3. To add a tagged port, type **A** for **Add Member**.

   The following prompt is displayed:

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

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

5. To remove a tagged port, type **R** for **Remove Member**.

   The following prompt is displayed:

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

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

Deleting a VLAN

To delete 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

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

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

4. Enter the VLAN ID of the VLAN you want to delete. You can enter only one VID.

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 port members of a deleted VLAN are automatically returned to the Default_VLAN with a PVID of 1.

Resetting to the Default VLAN

The following procedure for deletes all VLANs, except the Default_VLAN, on a switch. To delete selected VLANs, refer to “Deleting a VLAN” on page 129.

To reset to the default 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

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

   The following prompt is displayed:

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

4. Type **Y** for Yes.

   The following prompt is displayed:

   ```
   Reset to factory default completed, press any key to
   continue.
   ```

5. Press any key.

GVRP

This section describes GVRP and contains the following topics:

- “GVRP Overview,” next
- “Enabling or Disabling GVRP” on page 132

GVRP Overview

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information. The main purpose of GVRP is to allow switches to automatically discover some of the VLAN information that would otherwise need to be manually configured in each switch. This is helpful in networks where VLANs span more than one switch. Without GVRP, you must manually configure your switches to ensure that the various parts of a VLAN can communicate across the different switches. GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), does this for you automatically.

Figure 32 provides an example of how the GVRP feature works:

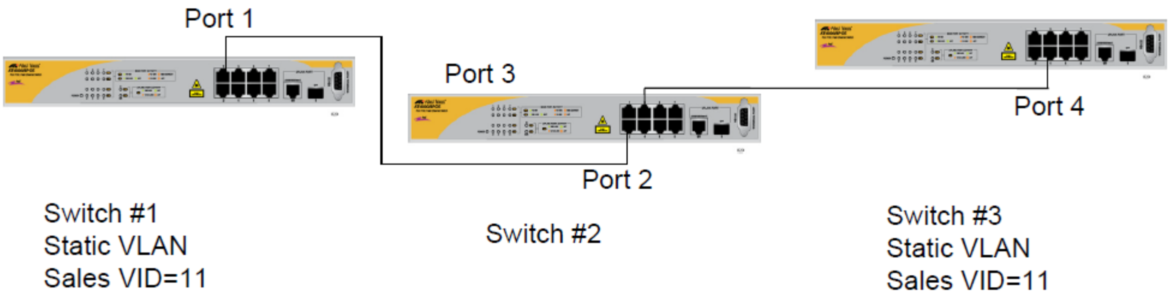


Figure 32. GVRP Example

Switches 1 and 3 contain the Sales VLAN, but switch 2 does not. Consequently, the end nodes of the two parts of the Sales VLANs are unable to communicate with each other.

Without GVRP, you would need to configure switch 2 by creating a Sales VLAN on the switch and adding ports 2 and 3 as members of the VLAN. If you have a large network and a large number of VLANS, this type of manual configuration can be cumbersome and time consuming. Instead, let GVRP set up the communications path for you.

Guidelines

Following are guidelines to observe when you use GVRP:

- Both ports that constitute a data link between the switch and the other device must be running GVRP.
- You cannot modify a GVRP VLAN; you can only enable or disable it.

- ❒ GVRP is only aware of those VLANs that have active nodes, or where at least one end node of a VLAN has established a valid link with a switch. GVRP is not aware of a VLAN if there are no active end nodes or if no end nodes have established a link with the switch.

Enabling or Disabling GVRP

GVRP is disabled by default.

To enable or disable GVRP, 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 21 on page 87.

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

   The VLAN Management Menu is shown in Figure 29 on page 122.

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

   The following prompt is displayed:

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

4. Type **E** to enable GVRP or **D** to disable it.

Chapter 10

Quality of Service (QoS)

This chapter contains the procedures for configuring the Quality of Service (QoS) parameters of the switch. This chapter contains the following sections:

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-8000/8POE Fast Ethernet Switch is called Class of Service (CoS). CoS applies primarily to tagged packets. As explained in “Incoming and Outgoing Tagged and Untagged Frames” on page 115, 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-S81 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 switch 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 5. A packet in a high priority queue is typically transmitted out a port sooner than a packet in a low priority queue.

Table 5. Default Mappings of IEEE 802.1p Priority Levels to Egress Port Priority Queues

IEEE 802.1p Traffic Class	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-S81 management software. The procedure for changing the default mappings is found in "Mapping CoS Priorities to Egress Queues" on page 137.

You can configure a port to completely ignore the priority levels in its tagged packets and instead use a temporary priority level assigned to the port. For instance, perhaps you decide that all tagged packets received on port 4 should be assigned a priority level of 5, regardless of the priority level in the packets themselves. The procedure for overriding priority levels is explained in "Configuring CoS" on page 140.

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain a priority level. By default, all untagged packets are placed in a port's Q0 egress queue, the queue with the lowest priority. But you can override this and instruct a port's untagged frames to be stored in a higher priority queue. The procedure for this is also explained in "Configuring CoS" on page 140.

One last thing to note is that CoS 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 queue of a port.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, shown in Table 5 on page 135. This is set at the switch level and applies to all ports. This procedure also enables and disables QoS.

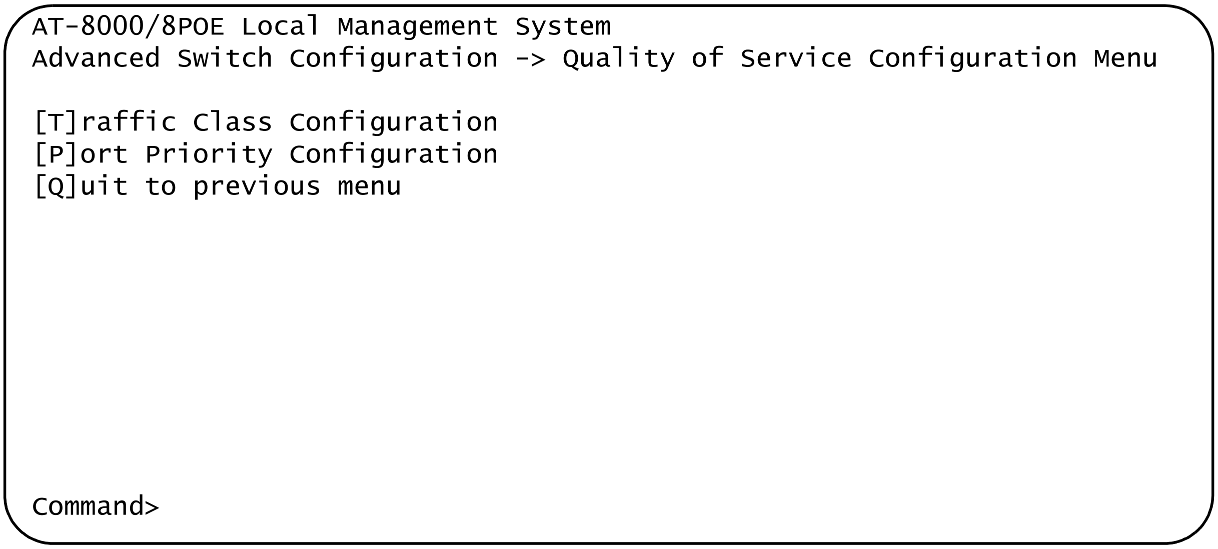
To change the mappings, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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 33.

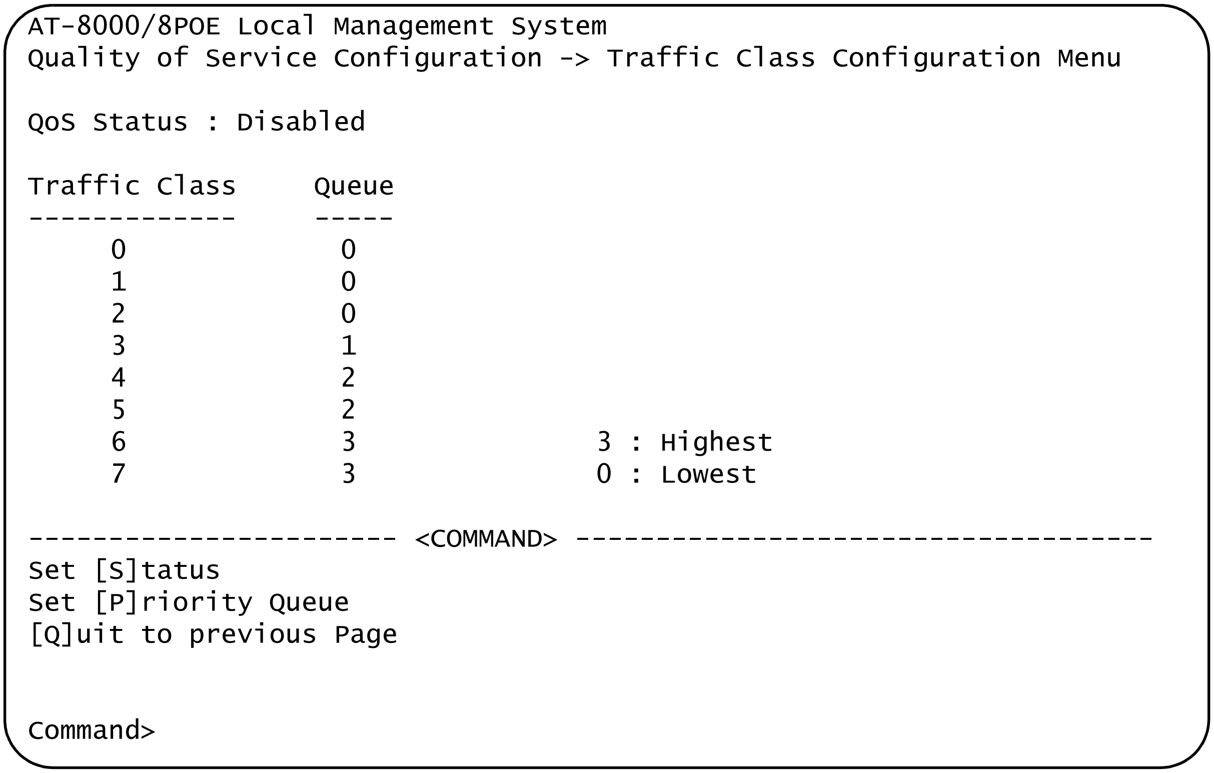


```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> Quality of Service Configuration Menu

[T]raffic Class Configuration
[P]ort Priority Configuration
[Q]uit to previous menu









Command>
```

Figure 33. 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 34.



```
AT-8000/8POE Local Management System
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 34. 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 an 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.

      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. 0 is the lowest priority queue and 3 is the highest. You can specify only one egress queue.

Configuring CoS

As explained in “QoS Overview” on page 134, 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 5 on page 135.

You can override the mappings at the port level by assigning a different 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.

Note
The switch does not alter the original priority level in tagged frames. The 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 Main Menu, type **A** to select **Advanced Switch Configuration**.

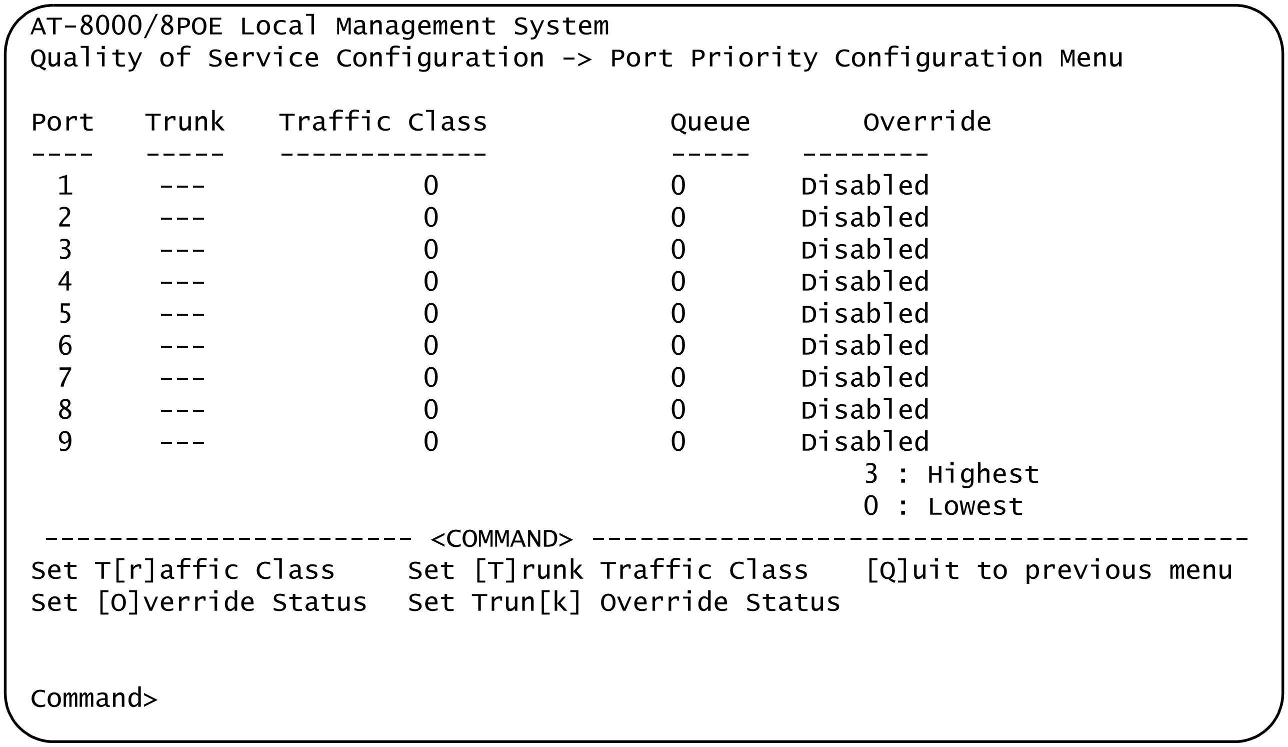
   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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 33 on page 137.

3. From the Quality of Service Configuration Menu, type **P** to select **Port Priority Configuration**.

   The Port Priority Configuration Menu is shown in Figure 35.



```
AT-8000/8POE Local Management System
Quality of Service Configuration -> Port Priority Configuration Menu

Port   Trunk   Traffic Class           Queue       Override
----   -----   -------------           -----   --------
  1     ---             0               0       Disabled
  2     ---             0               0       Disabled
  3     ---             0               0       Disabled
  4     ---             0               0       Disabled
  5     ---             0               0       Disabled
  6     ---             0               0       Disabled
  7     ---             0               0       Disabled
  8     ---             0               0       Disabled
  9     ---             0               0       Disabled
                                                    3 : Highest
                                                    0 : Lowest
 ----------------------- <COMMAND> -----------------------------------------
Set T[r]affic Class    Set [T]runk Traffic Class    [Q]uit to previous menu
Set [O]verride Status  Set Trun[k] Override Status


Command>
```

Figure 35. 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
The traffic class currently associated with the port.

Queue
Displays the number of the queue where untagged packets received on the port are stored on the egress queue.

Override
Displays whether the priority level in ingress tagged frames is being used or not. If No, the override is disabled and the port is using the priority levels contained within the frames to determine the egress queue. If Yes, the override is enabled and the tagged packets are stored in the egress queue specified in the Queue column.

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 that you want to configure. 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 egress queue where the ingress untagged frames received on the port or trunk are to be stored on the egress port. The range is 0 (lowest) to 3 (highest). For example, if you enter 3 for queue 3, then all ingress untagged packets that are received on the port will be stored in egress queue 3 on the egress port. The default is 0. (If you perform Step 7 and override the priority level in ingress tagged packets, this also applies to those packets as well.)

7. To configure a tagged port or trunk so that the switch ignores the priority tag in ingress tagged frames, 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 is 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 that you want to configure. 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 override or **D** to disable it.

Note
The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered.

The default for this parameter is disabled, meaning that the priority level of tagged frames is determined by the priority level specified in the frames themselves.

Chapter 11

IGMP Snooping

This chapter describes how to configure the OGMP snooping feature on the switch and includes the following sections:

IGMP Snooping Overview

The Internet Group Management Protocol (IGMP) enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node wanting to become a member of a 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 out 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 through the use of *Group-Source report* and *Group-Source leave* messages.

The IGMP snooping feature on the AT-8000/8POE Fast Ethernet switch supports IGMP versions 1 and 2. It enables the switch to monitor the flow of queries from a router and reports and leave messages from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping a switch would have to flood multicast packets out all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

The AT-8000/8POE Fast Ethernet switch maintains its 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.

By default, IGMP snooping is disabled on the switch.

Configuring IGMP

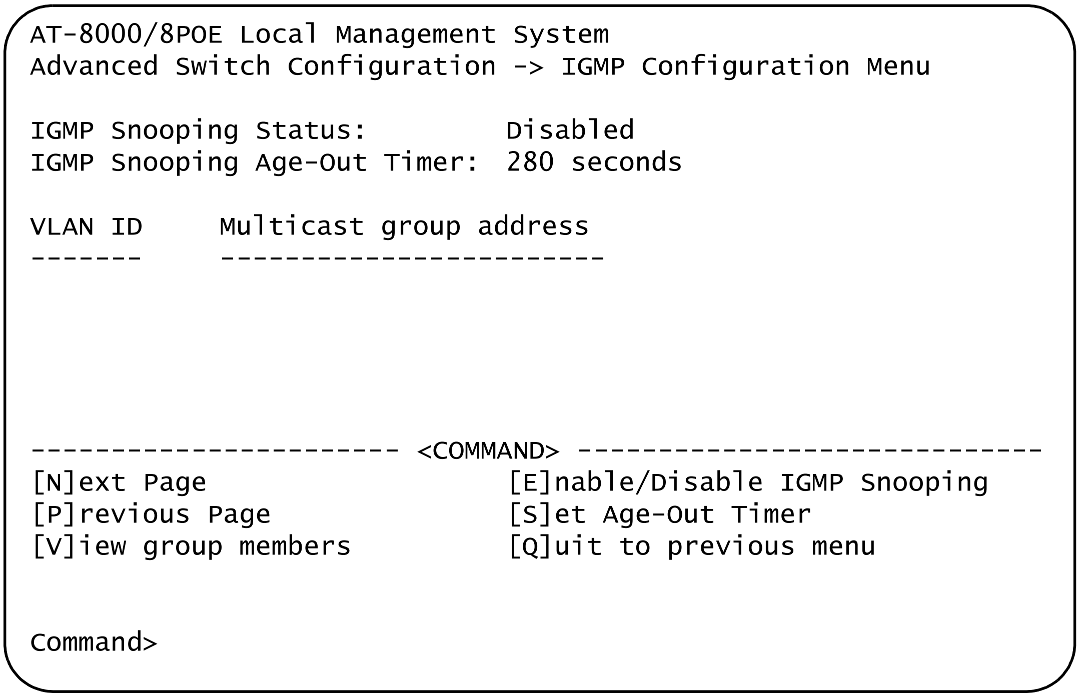
To configure IGMP, perform the following procedure:

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

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

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

   The IGMP Configuration Menu is shown in Figure 36.



```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> IGMP Configuration Menu

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

VLAN ID     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 36. IGMP Configuration Menu

3. Type **E** to select **Enable/Disable IGMP Snooping**.

   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.

5. If you are activating the feature, type **S** to Set Age-Out Timer.

   The following prompt is displayed:

   ```
   Enter age out time>
   ```

6. Specify the age-out time in seconds.

   The range is 280 to 420 seconds and the default is 280 seconds.

Viewing the Multicast Groups

To view the IGMP snooping multicast groups, 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 4 on page 32.

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

   The IGMP Configuration Menu is shown in Figure 36 on page 148.

3. Start y**our viewing application.**

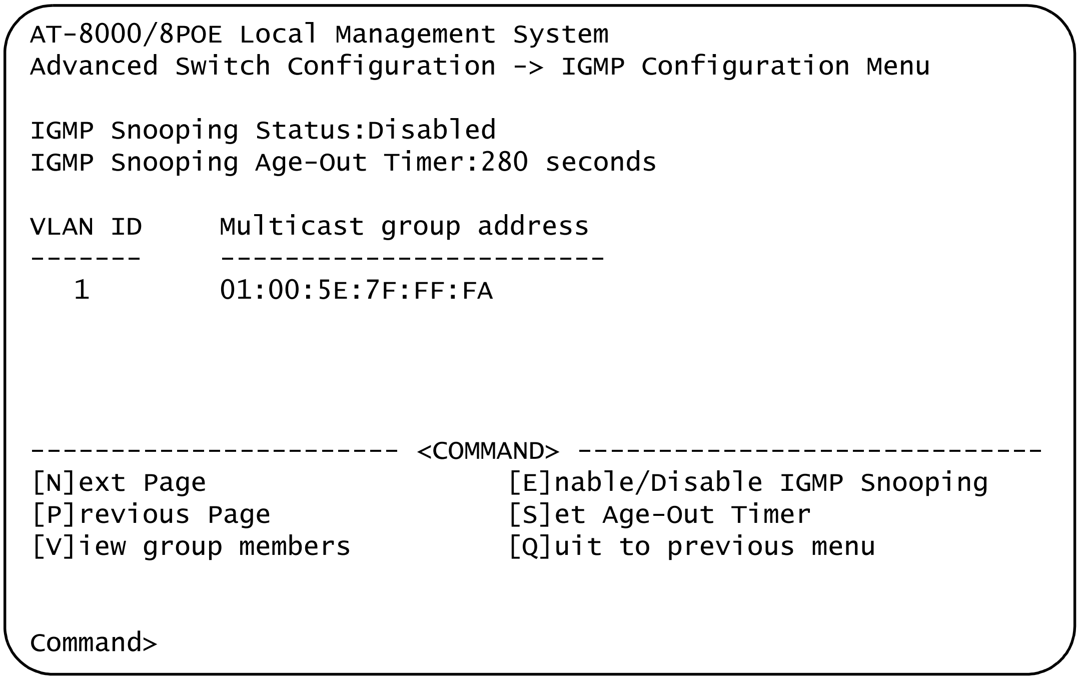
4. **Type V** to select **View group members**.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

5. Enter the VLAN ID number.

   The menu is updated to show the MAC address of the multicast group, as shown in Figure 37



```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> IGMP Configuration Menu

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

VLAN ID     Multicast group address
-------     ------------------------
   1        01:00:5E:7F:FF:FA




----------------------- <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>
```

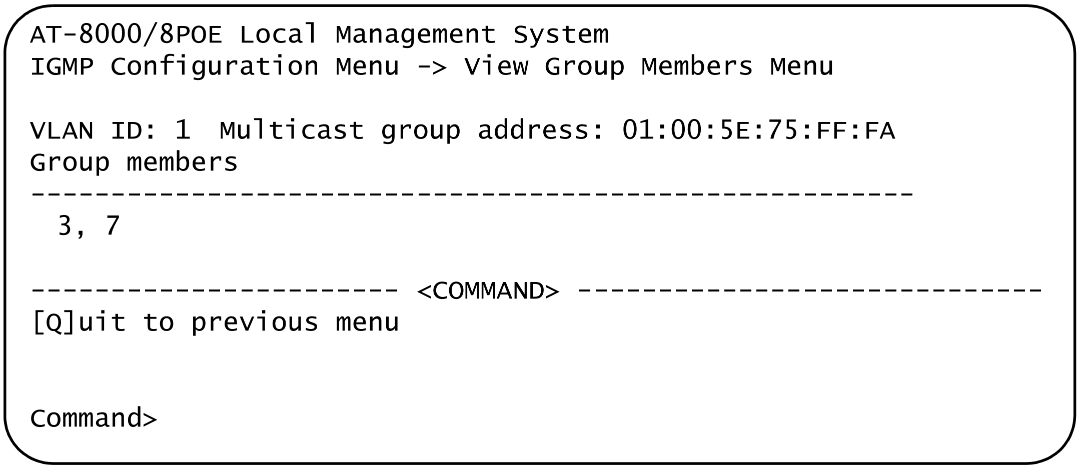
Figure 37. MAC Address DIsplayed on IGMP Configuration Menu

The following prompt is displayed:

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

6. Enter the MAC address as shown on the menu.

   The View Group Members Menu is shown in Figure 38.



```
AT-8000/8POE Local Management System
IGMP Configuration Menu -> View Group Members Menu

VLAN ID: 1  Multicast group address: 01:00:5E:75:FF:FA
Group members
-------------------------------------------------------
  3, 7

----------------------- <COMMAND> -----------------------------
[Q]uit to previous menu


Command>
```

Figure 38. View Group Members Menu

Chapter 12

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 AT-8000/8POE Fast Ethernet 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 6 lists the RSTP port costs with Auto-Detect.

Table 6. RSTP Auto-Detect Port Costs

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

Table 7 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 7. RSTP Auto-Detect Port Trunk Costs

Port Speed	No. of Ports/ Trunk	Port Cost
10/100	2	100,000
10/100	3	66,666
10/100	4	50,000

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 8 lists the values. The default value is **0**.

Table 8. 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-S81 management software. The interval is measured in seconds and the default is two seconds. Consequently, if an AT-8000/8POE Fast Ethernet 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 39 illustrates two AT-8000/8POE Fast Ethernet switch that have been connected with one data link. With the link operating in full-duplex, the ports are point-to-point ports.

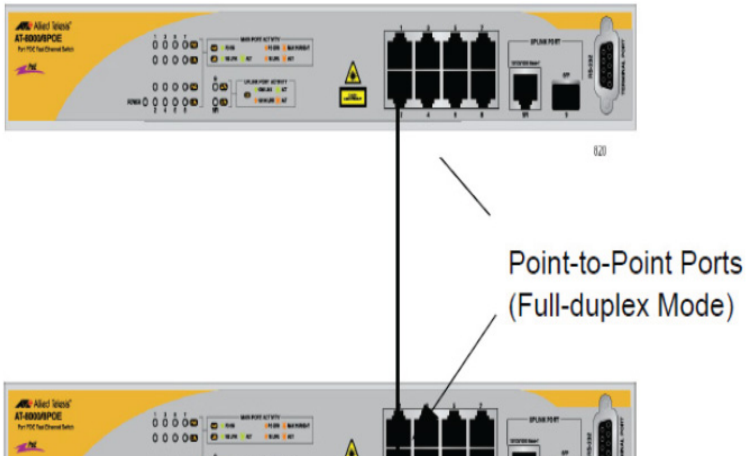


Figure 39. Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then you need to manually define the port as an edge port. The default setting for the edge port status is False. You must manually configure this setting for each port. There is no automatic mode for the edge port setting. Figure 40 illustrates an edge port on an AT-8000/8POE Fast Ethernet 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.

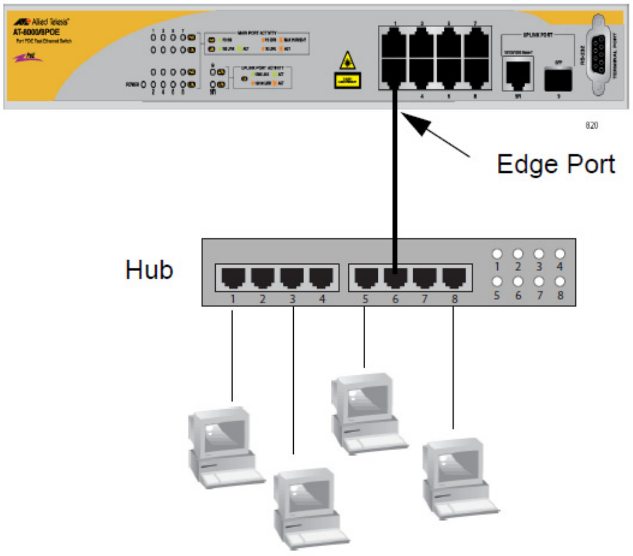


Figure 40. Edge Port

A port can be both a point-to-point and an edge port at the same time. Figure 41 illustrates a port functioning as both a point-to-point and edge port. You must manually configure the edge port status.

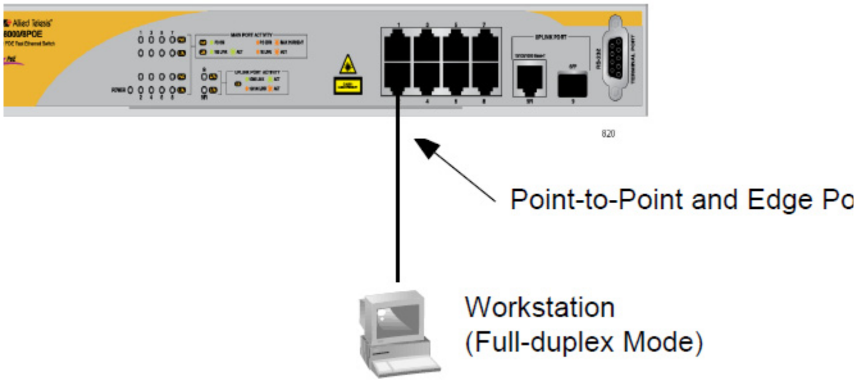


Figure 41. Point-to-Point and Edge Port

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-S81 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 42. Two VLANs, Sales and Production, span two AT-8000/8POE Fast Ethernet 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.

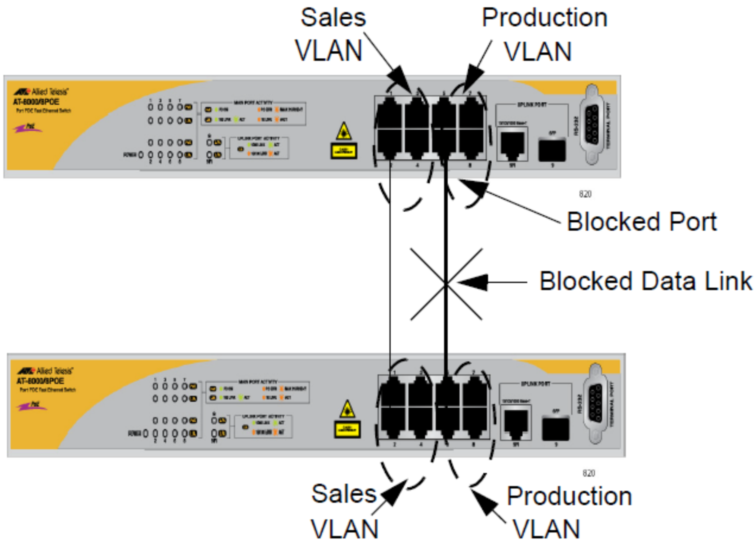


Figure 42. VLAN Fragmentation

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 9, “Virtual LANs and GVRP” on page 111.)

Enabling or Disabling RSTP

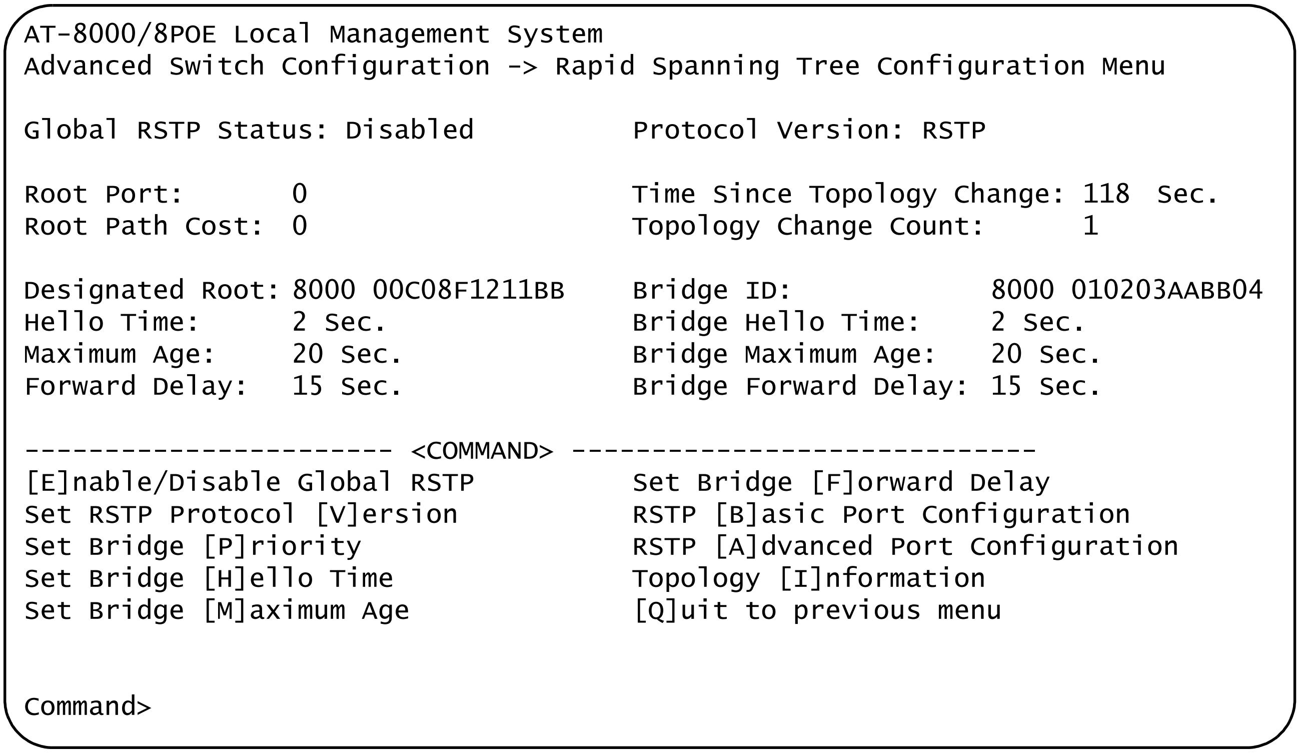
To enable or disable RSTP, perform the following procedure:

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 43.



```
AT-8000/8POE Local Management System
Advanced 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 43. 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 157. 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 43 on page 161.

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.
   ```

   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 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.

   The bridge priority is shown as the first field in the “Designated Root” and “Bridge ID” parameters.

4. 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. The range of this parameter is from 1 to 10 seconds. The default is 2 seconds.

5. Type a number for the bridge priority.

6. Type **M** to select **Set Bridge Maximum Age**.

   The following prompt is displayed:

   ```
   Enter bridge maximum age>
   ```

The bridge maximum age is the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 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.

7. Type a number for the bridge maximum age.

8. 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.

9. Type 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 43 on page 161.

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 169

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**.

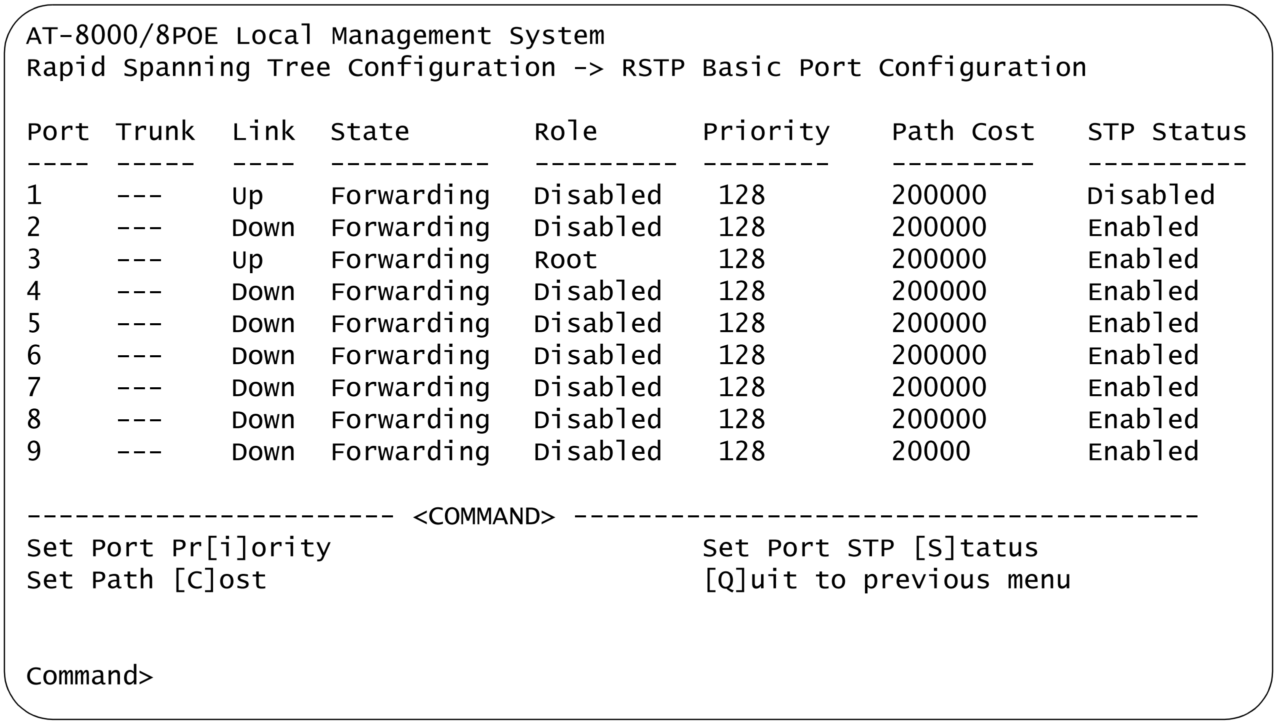
   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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 43 on page 161.

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 44.



```
AT-8000/8POE Local Management System
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

----------------------- <COMMAND> ---------------------------------------
Set Port Pr[i]ority                       Set Port STP [S]tatus
Set Path [C]ost                           [Q]uit to previous menu


Command>
```

Figure 44. 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 8 on page 157.

   > **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 8 on page 157.

   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 6 on page 156.

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**.

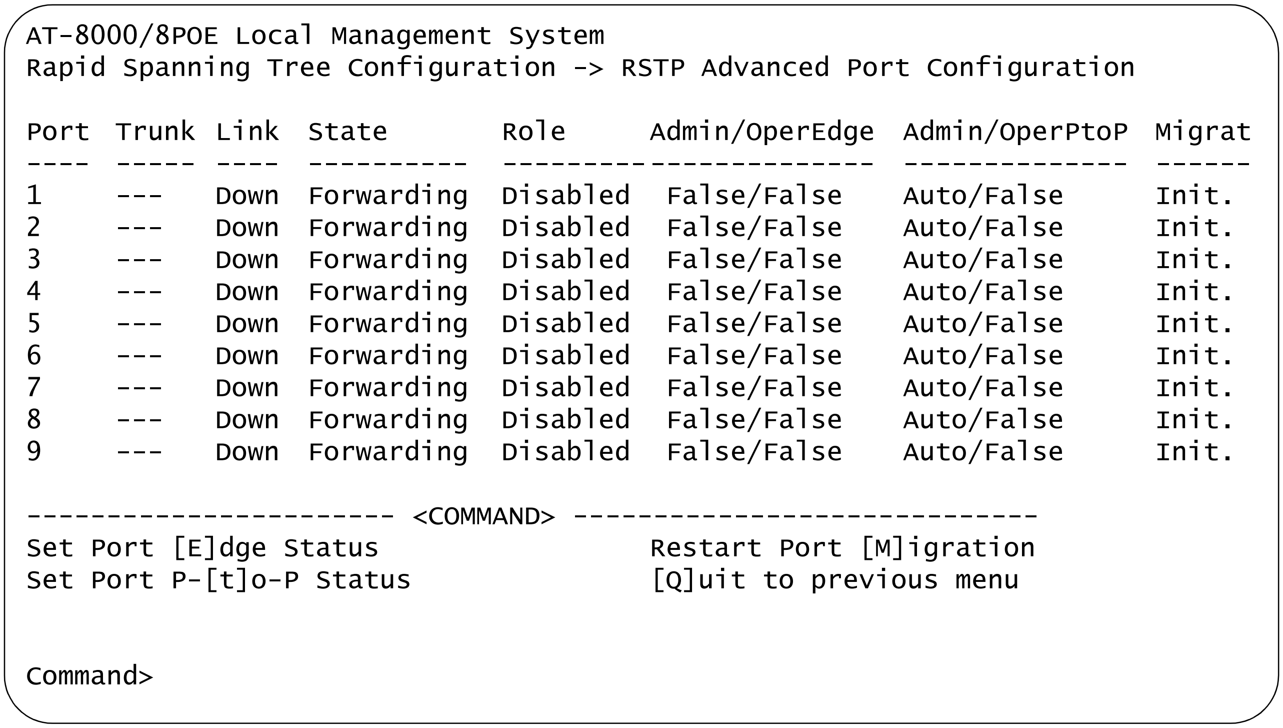
   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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 43 on page 161.

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 44 on page 167.



```
AT-8000/8POE Local Management System
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.

----------------------- <COMMAND> -----------------------------
Set Port [E]dge Status                Restart Port [M]igration
Set Port P-[t]o-P Status              [Q]uit to previous menu


Command>
```

Figure 45. 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 158.

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 158.

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 9.

Table 9. 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**.

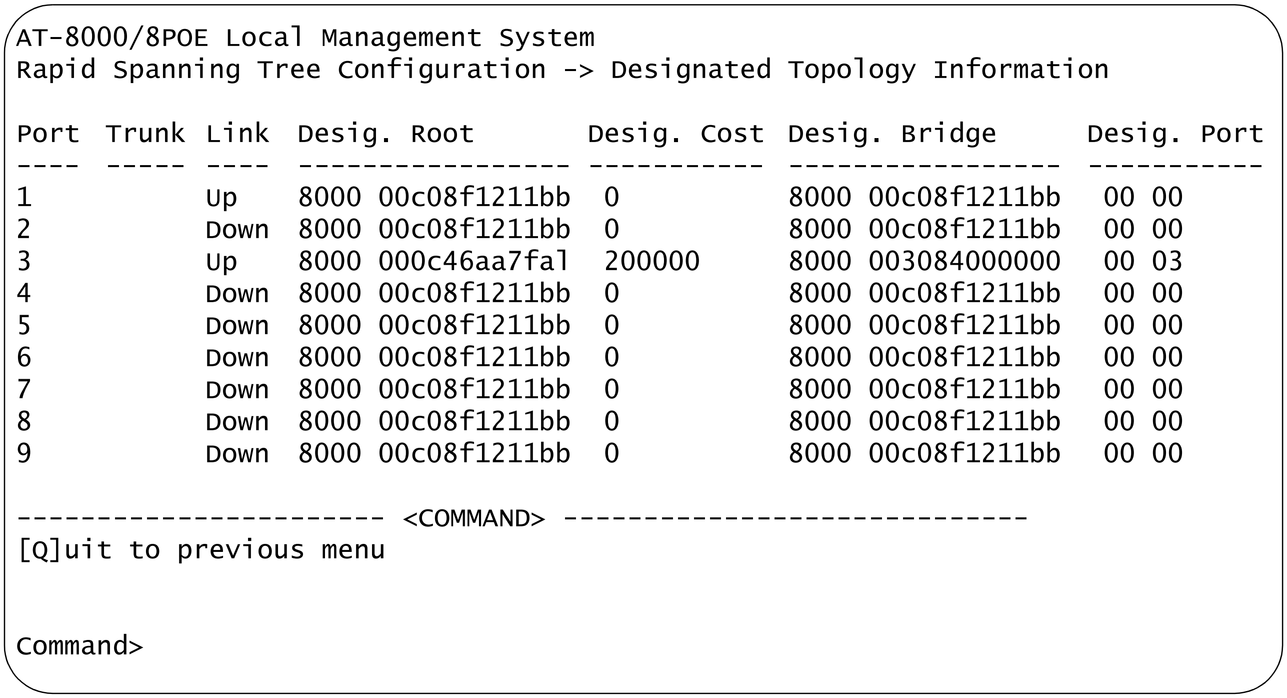
   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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 43 on page 161.

3. From the Rapid Spanning Tree Configuration Menu, type **I** to select **Topology Information**.

   The Topology Information menu is shown in Figure 44.



```
AT-8000/8POE Local Management System
Rapid Spanning Tree Configuration -> Designated Topology Information

Port  Trunk 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

----------------------- <COMMAND> -----------------------------
[Q]uit to previous menu


Command>
```

Figure 46. 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 to which the switch’s root port is actively connected.

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 root bridge to which the root port of the switch is actively connected.

Chapter 13

802.1x Network Access Control

This chapter contains information about and the procedure for configuring 802.1x Network Access Control. It includes the following sections:

802.1x Network Access Control Overview

802.1x 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 will 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 will be able to use the switch to access the network.

This feature must be used with the RADIUS authentication protocol and requires that there be 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-8000/8POE Fast Ethernet switch does not authenticate the usernames and passwords from the end users. Rather, the switch acts as an intermediary between a supplicant and the authentication server during the authentication process.

Authentication Process

Below is a brief overview of the authentication process that occurs between a supplicant, authenticator, and authentication server. For further details, refer to the IEEE 802.1x standard.

- ❐ 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-8000/8POE Fast Ethernet Switch 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 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 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 47 illustrates the concept of the authenticator port control settings.

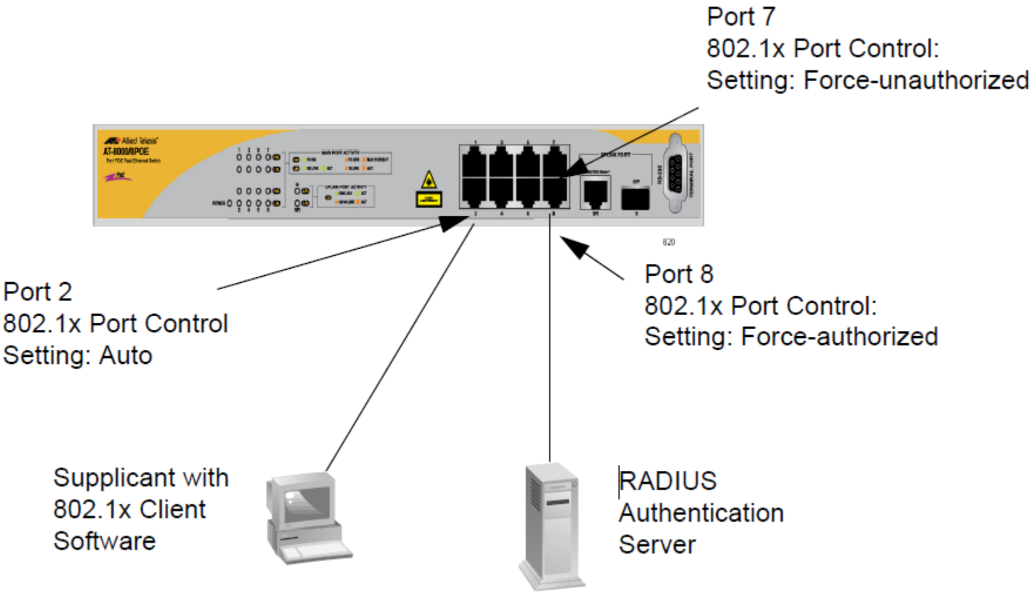


Figure 47. Example of the Authenticator Role

❐ 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 8 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 7 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 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.

2. You need to install 802.1x client software on those workstations that are to be supplicants.

3. You must configure and activate the RADIUS client software in the AT-S81 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 14, “RADIUS Authentication Protocol” on page 189.

4. You must configure the authenticator port settings, as explained in “Configuring 802.1x Network Access Control” on page 183 in this chapter.

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-8000/8POE Fast Ethernet 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 on those 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 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 48 on page 182.

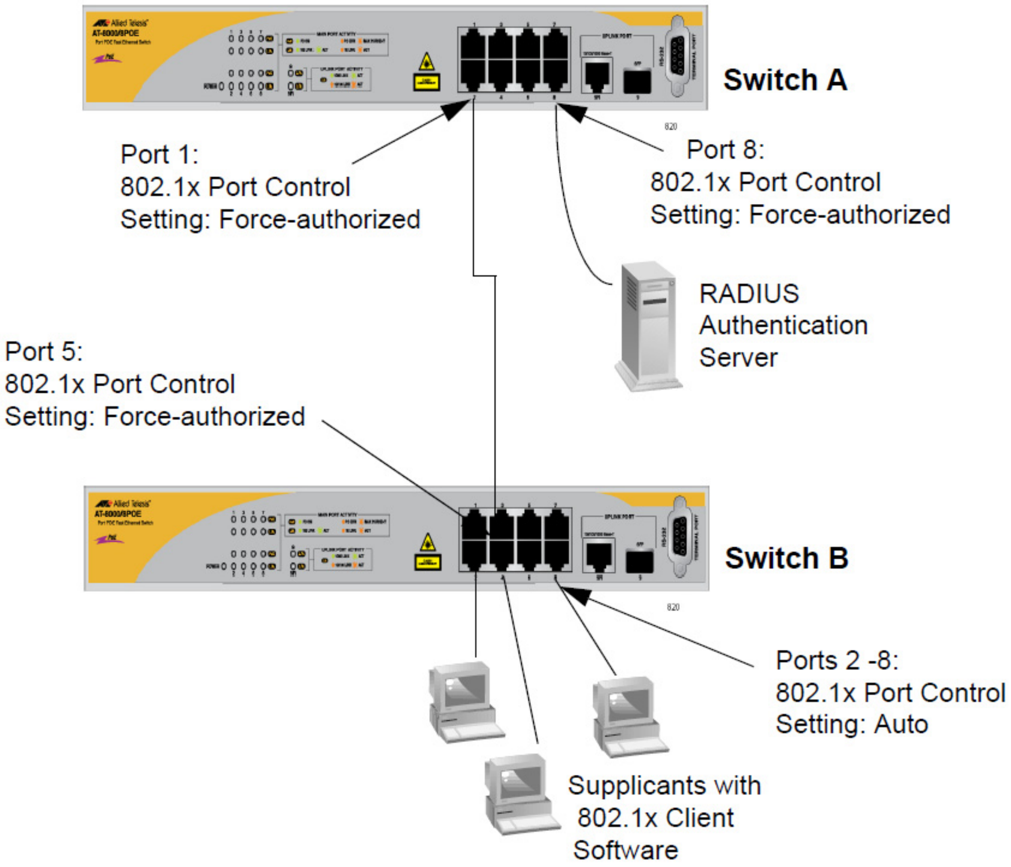


Figure 48. Authentication Across Multiple Switches

Configuring 802.1x Network Access Control

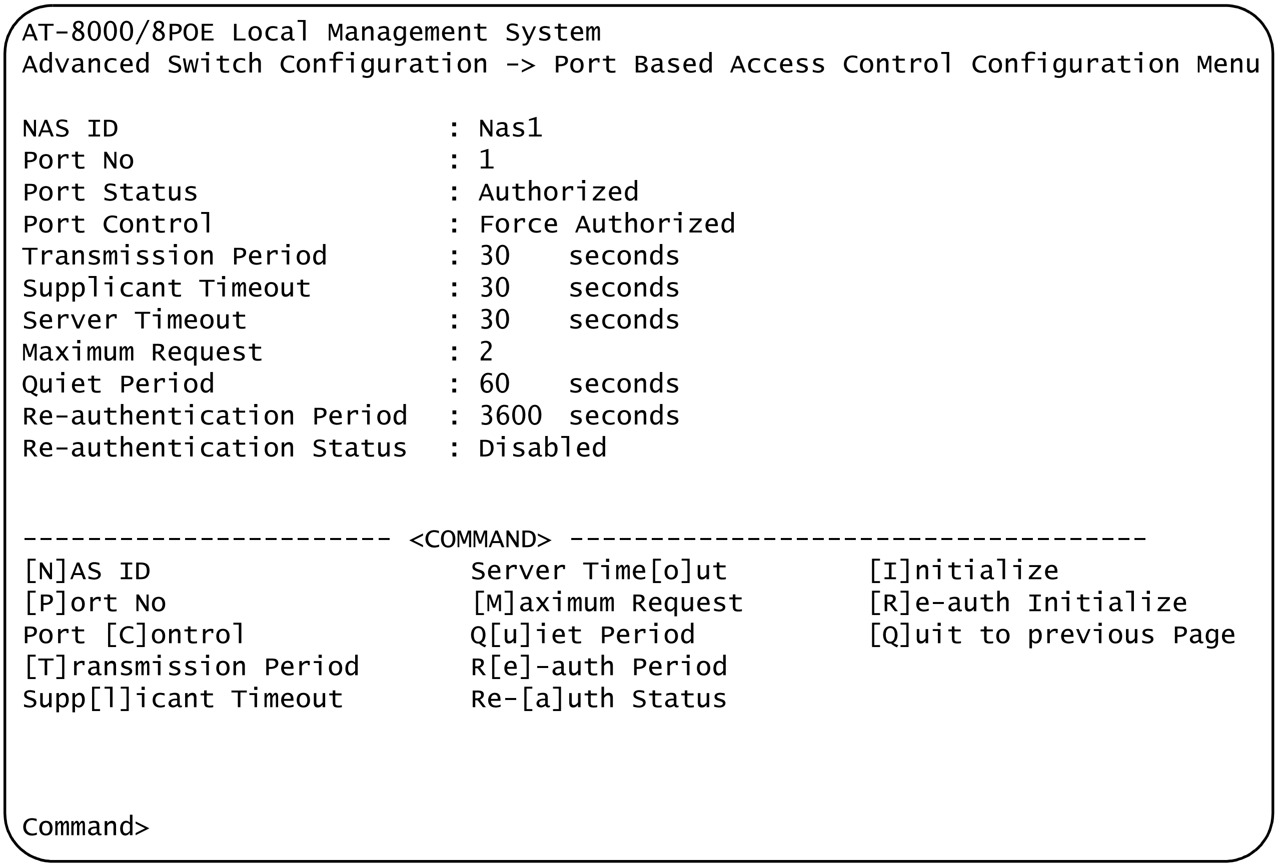
To configure 802.1x network access control, perform the following procedure:

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

   The Advanced Switch Configuration Menu is shown in Figure 21 on page 87.

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 49.



```
AT-8000/8POE Local Management System
Advanced Switch Configuration -> Port Based Access Control Configuration Menu

NAS ID                     : Nas1
Port No                    : 1
Port Status                : Authorized
Port Control               : Force Authorized
Transmission Period        : 30   seconds
Supplicant Timeout         : 30   seconds
Server Timeout             : 30   seconds
Maximum Request            : 2
Quiet Period               : 60   seconds
Re-authentication Period   : 3600  seconds
Re-authentication Status   : Disabled


----------------------- <COMMAND> ------------------------------------
[N]AS ID                    Server Time[o]ut        [I]nitialize
[P]ort No                   [M]aximum Request       [R]e-auth Initialize
Port [C]ontrol              Q[u]iet Period          [Q]uit to previous Page
[T]ransmission Period       R[e]-auth Period
Supp[l]icant Timeout        Re-[a]uth Status



Command>
```

Figure 49. 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. Type **N** to select 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.

   The following prompt is displayed:

   ```
   Enter NAS ID >
   ```

6. Type a name for the NAS ID.

   Note
   Port Status displays the current 802.1 status of the port as either authorized or unauthorized. This is not an adjustable parameter.

7. To configure the port control type, do the following:

   a. Type **C** to select **Port Control**.

      The following prompt is displayed:

      ```
      Select authenticator port control (A/U/F) >
      ```

      The options are:

      A (Auto) - Enables 802.1x 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 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.

b. Type **A**, **U**, or **F**.

8. To configure the transmission period, do the following:

a. Type **T** to select **Transmission Period**.

The following prompt is displayed:

```
Enter transmission period >
```

This parameter 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.

b. Type a number for the transmission period.

9. To set the supplicant timeout, do the following:

a. Type **L** to select **Supplicant Timeout**.

The following prompt is displayed:

```
Enter supplicant timeout value >
```

This parameter sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

b. Type a number for the supplicant timeout.

10. To set the server timeout, do the following:

a. Type **O** to select **Server Timeout**.

The following prompt is displayed:

```
Enter transmission period >
```

This parameter sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

b. Type a number for the server timeout.

11. To set the maximum number of requests, do the following:

a. Type **M** to select **Maximum Request**.

The following prompt is displayed:

Enter maximum request count >

This parameter 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.

b. Type a number for the maximum request count.

12. To configure the quiet period, do the following:

    a. Type **U** to select **Quiet Period**.

    The following prompt is displayed:

    ```
    Enter quiet period >
    ```

    This parameter 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.

    b. Enter a number for the quiet period.

13. To configure the reauthentication period, do the following:

    a. Type **E** to select **Re-Auth Period**.

    The following prompt is displayed:

    ```
    Enter re-authentication period >
    ```

    This parameter specifies the time period between periodic reauthentication of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

    b. Enter a number for the re-authentication period.

14. To enable or disable reauthentication, do the following:

    a. Type **A** to select **Re-Auth Status**.

    The following prompt is displayed:

    ```
    Enable or Disable re-authentication? (E/D) >
    ```

    This parameter specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

    b. Type **E** to enable reauthentication or **D** to disable reauthentication.

15. 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**.

       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.

16. If the port control setting is Auto and you want the node connected to the port to reauthenticate with the RADIUS server, do the following:

    a. Type **R** to select **Re-auth Initialize**.

       The following prompt is displayed:

       ```
       Initialize re-authentication? (Y/N)>
       ```

    b. Typing **Y** returns the port to the unauthenticated state and the re-authentication period to zero. The user must enter a valid username and password to continue to use the switch port. Typing **N** cancels the reauthentication.

Chapter 14

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 network access control to control who can forward packets through the switch. Sections in the chapter include:

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-S81 management software comes with RADIUS client software. You can use the client software together with 802.1x network access control, described in Chapter 13, “802.1x Network Access Control” on page 175, to control which end users and end nodes can send packets through the switch.

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 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-S81 management software and configure the settings. This is explained in “Configuring the RADIUS Server” on page 192. By default, authentication protocol is disabled.

Note

For more information on the RADIUS authentication protocol, refer to the RFC 2865 standard.

Configuring the RADIUS Server

To configure the RADIUS client, perform the following procedure:

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

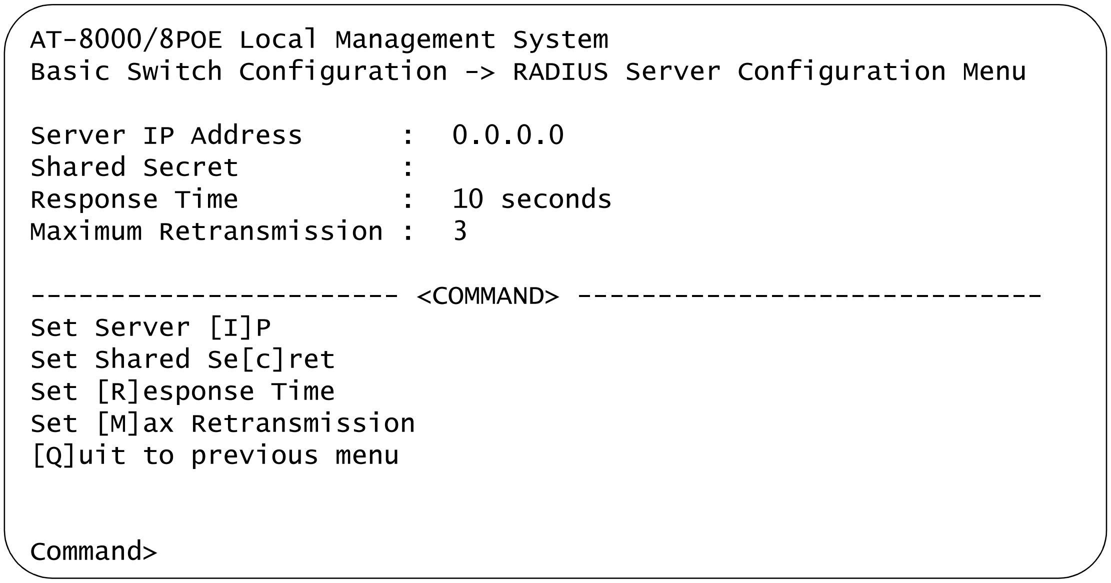
   The Basic Switch Configuration Menu is shown in Figure 4 on page 32.

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 38.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 50.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> RADIUS Server Configuration Menu

Server IP Address      :  0.0.0.0
Shared Secret          :
Response Time          :  10 seconds
Maximum Retransmission :  3

----------------------- <COMMAND> -----------------------------
Set Server [I]P
Set Shared Se[c]ret
Set [R]esponse Time
Set [M]ax Retransmission
[Q]uit to previous menu


Command>
```

Figure 50. RADIUS Server Configuration Menu

4. To set the RADIUS server's IP address, do the following:

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

      The following prompt is displayed:

      ```
      Enter IP address for RADIUS server>
      ```

   b. Enter the IP address of the RADIUS server.

5. To configure the shared secret, do the following:

   a. Type **C** to select **Shared Secret**.

The following prompt is displayed:

```
Enter secret string for server>
```

b. Enter the encryption key of the RADIUS server.

6. To set the response time, do the following:

a. Type **R** to select **Set Response Time**.

The following prompt is displayed:

```
Enter response time>
```

b. Enter the amount of time in seconds the switch should wait for a response from the RADIUS server. The range is 1 to 120 seconds. The default is 10 seconds.

7. To configure the maximum retransmissions, do the following:

a. Type **M** to select **Max Retransmission**.

The following prompt is displayed:

```
Enter maximum retransmissions>
```

b. Enter the number of times the switch should retransmit to the RADIUS server in the event that the server does not respond. The range is 1 to 254. The default is 3.

Displaying the RADIUS Server 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 38.

3. Type **R** to select **RADIUS Server Configuration**.

   The RADIUS Server Configuration Menu is shown in Figure 50 on page 192. The top of the menu shows the current RADIUS server configuration.

Chapter 15

Broadcast Storm Control

This chapter describes how to configure the broadcast storm control feature on the switch and includes the following sections:

Broadcast Storm Control Overview

The broadcast storm control feature limits the number of broadcast frames forwarded by the switch. The feature can help improve network performance in situations where broadcast frames are consuming a significant portion of network bandwidth, to a degree where the remaining bandwidth is insufficient for efficiently carrying the unicast and multicast frames.

This feature can also protect your network from broadcast storms. Broadcast storms commonly occur when an Ethernet network topology contains a loop and where the Spanning Tree Protocol is not implemented. Ethernet frames become caught in repeating cycles that needlessly consume network bandwidth.

The default setting for this feature is disabled. In the default setting, the switch forwards all ingress broadcast frames, provided that ports are not over-subscribed.

When you enable the feature, you are given three threshold levels from which to choose. The levels prescribe the maximum number of ingress broadcast frames the switch will accept per second. Broadcast frames that exceed the limit are discarded. The level are:

- High: 3000 broadcast packets per second
- Medium: 500 broadcast packets per second
- Low: 100 broadcast packets per second

For example, activating the feature and selecting Medium as the threshold means that the switch accepts up to a maximum of 500 ingress broadcast packets per second and discards those broadcast packets that exceed the limit.

Configuring Broadcast Storm Control

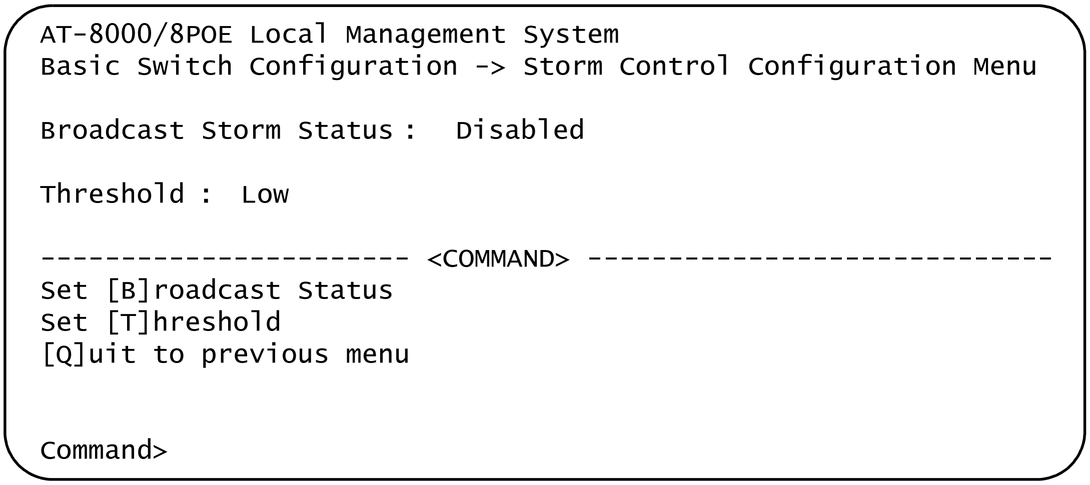
To configure the broadcast storm control feature, perform the following procedure:

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 **C** to select **Storm Control Configuration**.

   The Storm Control Configuration Menu is shown in Figure 51.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> Storm Control Configuration Menu

Broadcast Storm Status :  Disabled

Threshold :  Low

----------------------- <COMMAND> -----------------------------
Set [B]roadcast Status
Set [T]hreshold
[Q]uit to previous menu


Command>
```

Figure 51. Storm Control Configuration Menu

3. Type **B** to select **Broadcast Storm Status**.

   The following prompt is displayed:

   ```
   Enable or Disable broadcast storm control (E/D)>
   ```

4. Type **E** to enable broadcast storm control or **D** to disable broadcast storm control.

5. If you are activating the feature, type **T** to select Threshold.

   The following prompt is displayed:

   ```
   Enter threshold level>
   ```

6. Specify the broadcast threshold. Choices are:

   ❒ **H -** High (3000 broadcast packets per second)

   ❒ **M -** Medium (500 broadcast packets per second)

- **L** - Low (100 broadcast packets per second)

Chapter 16

MAC Address Tables

This chapter contains the procedures for viewing the MAC address table and contains the following sections:

MAC Address Overview

Each hardware device that you connect to your Ethernet network has a unique MAC address assigned to it by the device's manufacturer. For example, every network interface card (NIC) that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The switch contains a MAC address table with a storage capacity of up to 16,000 entries. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned.

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

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

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

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Because both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

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

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

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *age-out time*. The default value is 300 seconds (5 minutes) and the range is 15 to 3000 seconds. For instructions on changing the aging timer, refer to "Setting the Age-Out Time" on page 206.

Displaying the MAC Address Tables

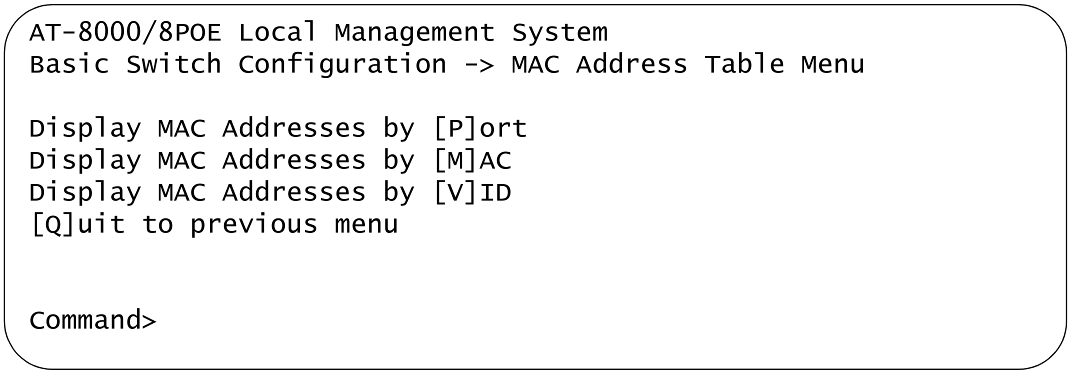
To display the MAC address tables, perform the following procedure:

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 **M** to select **MAC Address Table Menu**.

   The MAC Address Table menu is shown in Figure 52.



```
AT-8000/8POE Local Management System
Basic Switch Configuration -> MAC Address Table Menu

Display MAC Addresses by [P]ort
Display MAC Addresses by [M]AC
Display MAC Addresses by [V]ID
[Q]uit to previous menu


Command>
```

Figure 52. MAC Address Table Menu

Displaying the MAC Addresses by Port Number

To display the MAC addresses learned on a specific port, perform the following procedure:

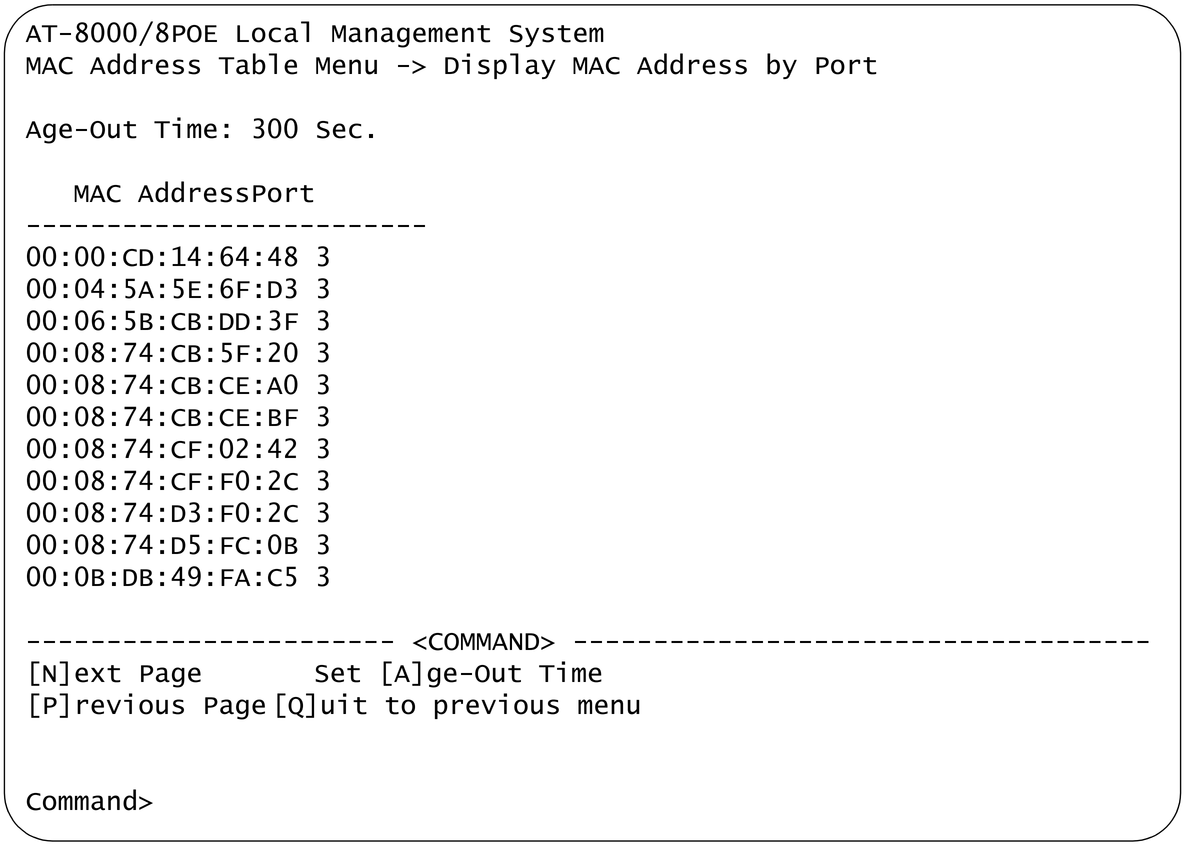
1. From the MAC Address Table menu, type **P** to select **Display MAC Addresses by Port**.

   The following prompt is displayed:

   ```
   Enter port number >
   ```

2. Type a number for the port.

   The Display MAC Addresses by Port menu is shown in Figure 53 on page 203.



```
AT-8000/8POE Local Management System
MAC Address Table Menu -> Display MAC Address by Port

Age-Out Time: 300 Sec.

   MAC AddressPort
-------------------------
00:00:CD:14:64:48 3
00:04:5A:5E:6F:D3 3
00:06:5B:CB:DD:3F 3
00:08:74:CB:5F:20 3
00:08:74:CB:CE:A0 3
00:08:74:CB:CE:BF 3
00:08:74:CF:02:42 3
00:08:74:CF:F0:2C 3
00:08:74:D3:F0:2C 3
00:08:74:D5:FC:0B 3
00:0B:DB:49:FA:C5 3

----------------------- <COMMAND> -----------------------------------
[N]ext Page       Set [A]ge-Out Time
[P]revious Page [Q]uit to previous menu


Command>
```

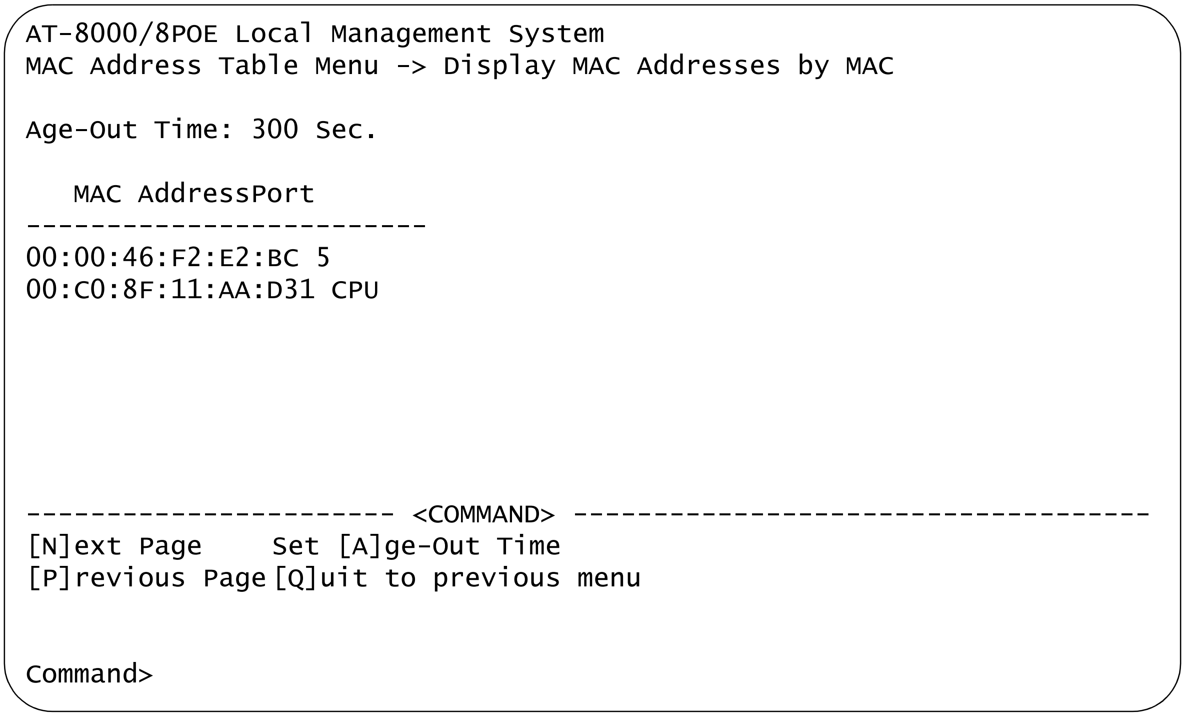
Figure 53. Display MAC Addresses by Port Menu

Displaying the MAC Addresses by MAC

To display all MAC addresses in alphanumeric order, perform the following procedure:

1. From the MAC Address Table menu, type **M** to select **Display MAC Addresses by MAC**.

   The Display MAC Addresses by MAC menu is shown in Figure 54 on page 204.



```
AT-8000/8POE Local Management System
MAC Address Table Menu -> Display MAC Addresses by MAC

Age-Out Time: 300 Sec.

   MAC AddressPort
-------------------------
00:00:46:F2:E2:BC 5
00:C0:8F:11:AA:D31 CPU







----------------------- <COMMAND> ------------------------------------
[N]ext Page    Set [A]ge-Out Time
[P]revious Page[Q]uit to previous menu


Command>
```

Figure 54. Display MAC Addresses by Port Menu

Displaying the MAC Addresses by VLAN ID

To display the MAC addresses learned on the port of a particular VLAN, perform the following procedure:

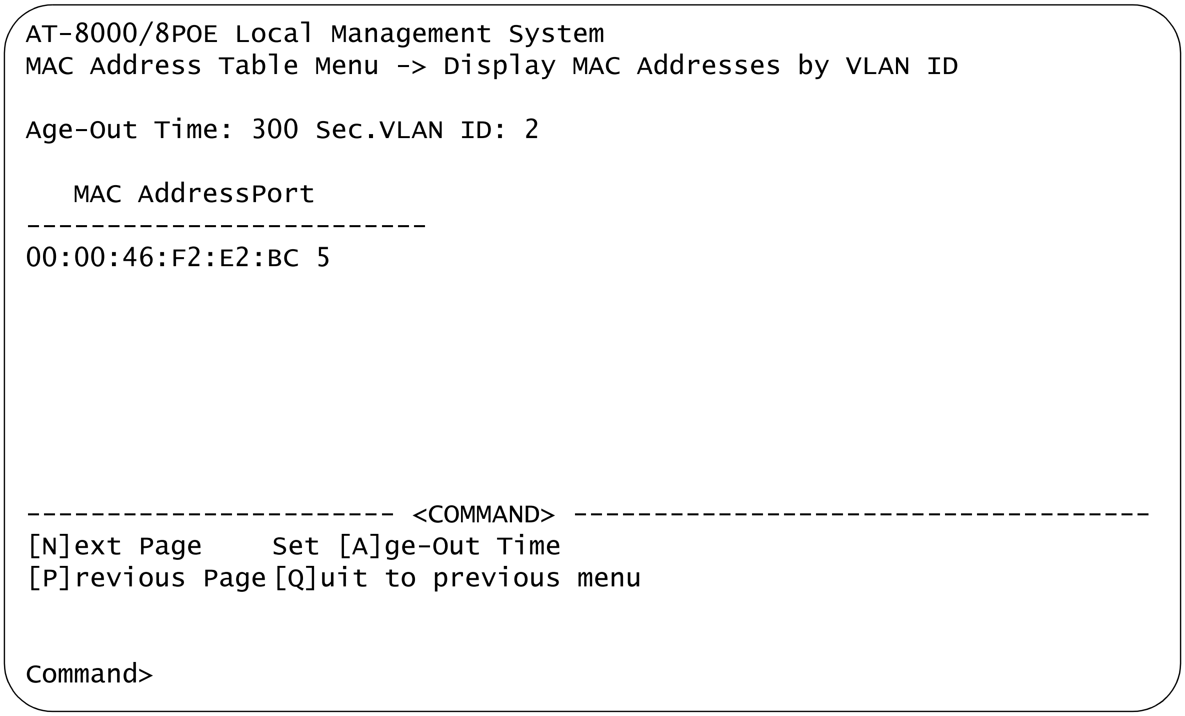
1. From the MAC Address Table menu, type **V** to select **Display MAC Addresses by VID**.

   The following prompt is displayed:

   ```
   Enter VLAN ID >
   ```

2. Enter a number for the VLAN ID.

   The Display MAC Addresses by VLAN ID menu is shown in Figure 53 on page 203.



```
AT-8000/8POE Local Management System
MAC Address Table Menu -> Display MAC Addresses by VLAN ID

Age-Out Time: 300 Sec.VLAN ID: 2

   MAC AddressPort
-------------------------
00:00:46:F2:E2:BC 5







----------------------- <COMMAND> ------------------------------------
[N]ext Page     Set [A]ge-Out Time
[P]revious Page [Q]uit to previous menu


Command>
```

Figure 55. Display MAC Addresses by VLAN ID Menu

Setting the Age-Out Time

The switch uses the age-out time to delete inactive MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default for the age-out time is 300 seconds (5 minutes).

To adjust the age-out time, perform the following procedure:

1. From the MAC Address Table menu, select one of the MAC address display options.
2. On the MAC address display menu, type **A** to select **Set Age-Out Time**.

   The following prompt is displayed:

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

   The range is 15 to 3000 seconds.
3. Enter a new number for the age-out time.

Chapter 17

Working With System Files

The procedures in this chapter explain how to work with system files on the AT+8000/8POE Fast Ethernet switch, including software image files and the system configuration file.

The procedures include:

❒ “Downloading a New Management Software Image Using TFTP” on page 208

> **Note**
> For information on how to obtain new releases of the AT-S81 management software, refer to “Contacting Allied Telesis” on page 15.

❒ “Uploading or Downloading the Configuration File” on page 211

Downloading a New Management Software Image Using TFTP

Before downloading a new version of the AT-S81 management software onto the switch, note the following:

- ❒ The current configuration of a switch is retained when a new AT-S81 software image is installed. To return a switch to its default configuration values, refer to "Returning the AT-S81 Management Software to the Factory Default Values" on page 59.
- ❒ Your network must have a node with TFTP server software.
- ❒ You must store the new AT-S81 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, stored it on the TFTP server, and specified a path to the new software in the TFTP configuration.

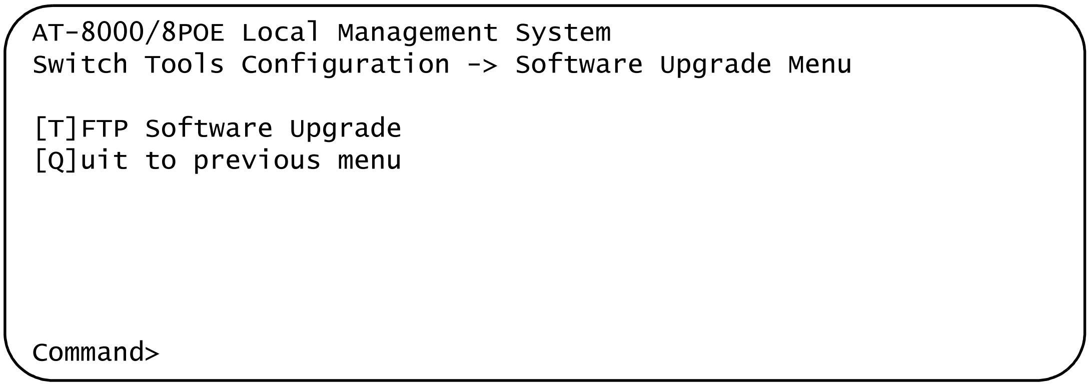
To download the AT-S81 image software onto the switch, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

2. From the Switch Tools Menu, type **U** to select **Software Upgrade**.

   The Software Upgrade Menu is shown in Figure 56 on page 209.

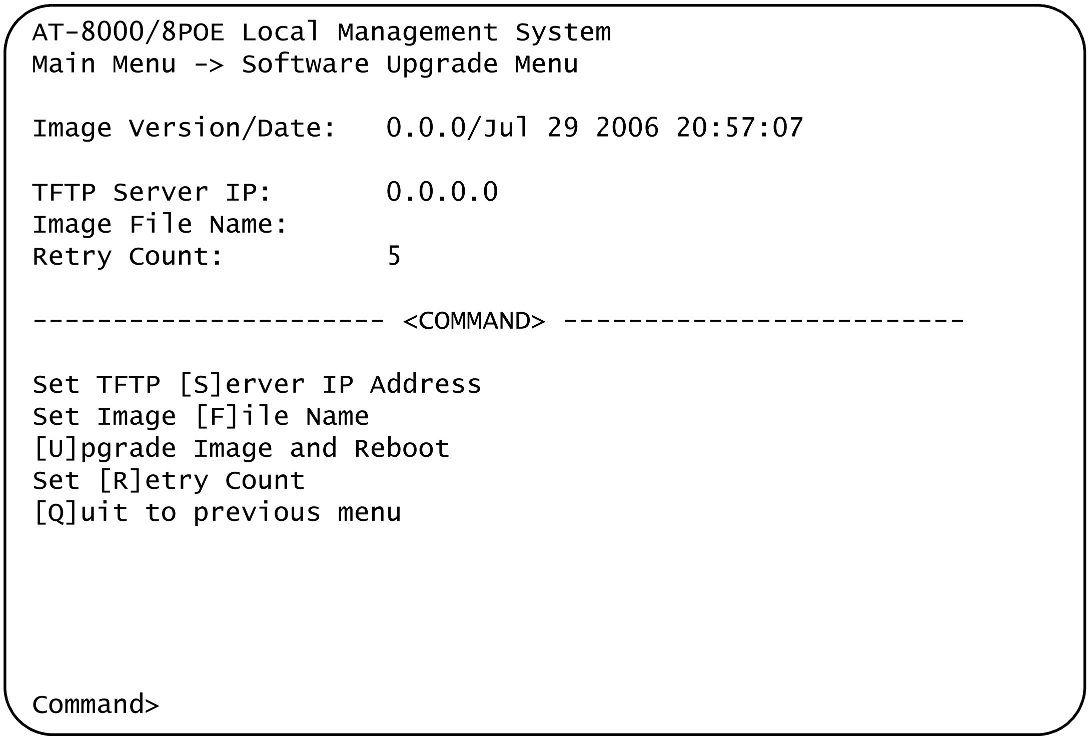


```
AT-8000/8POE Local Management System
Switch Tools Configuration -> Software Upgrade Menu

[T]FTP Software Upgrade
[Q]uit to previous menu






Command>
```

Figure 56. Software Upgrade Menu (1 of 2)

3. Type **T** to select **TFTP Upgrade**.

   The Software Upgrade Menu (2 of 2) is shown in Figure 57.



```
AT-8000/8POE Local Management System
Main Menu -> Software Upgrade Menu

Image Version/Date:   0.0.0/Jul 29 2006 20:57:07

TFTP Server IP:       0.0.0.0
Image File Name:
Retry Count:          5

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

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image and Reboot
Set [R]etry Count
[Q]uit to previous menu






Command>
```

Figure 57. 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. Enter the IP address of the TFTP server.

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-S81 image file on the TFTP server.

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.

    Note
    Do not interrupt the file download and reboot processes.

Uploading or Downloading the Configuration File

The procedure in this section allows you to download a different configuration file onto the switch from a TFTP server, or upload the file to a TFTP server. To return a switch to its default configuration values, refer to "Returning the AT-S81 Management Software to the Factory Default Values" on page 59.

- ❐ Before downloading a configuration file onto the switch, note the following:
- ❐ Your network must have a node with TFTP server software.
- ❐ You must store the new configuration file on the TFTP server.
- ❐ You should start the TFTP server software before you begin the procedure.
- ❐ The switch where you are downloading the configuration 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.
- ❐ When you download a new configuration file onto the switch, the new file overrides the current file and the current file is lost unless you uploaded it to a TFTP server before you replaced it.

Note
The configuration file contains only those settings that have been changed since the switch was last reset to the default settings.

Uploading the Configuration File

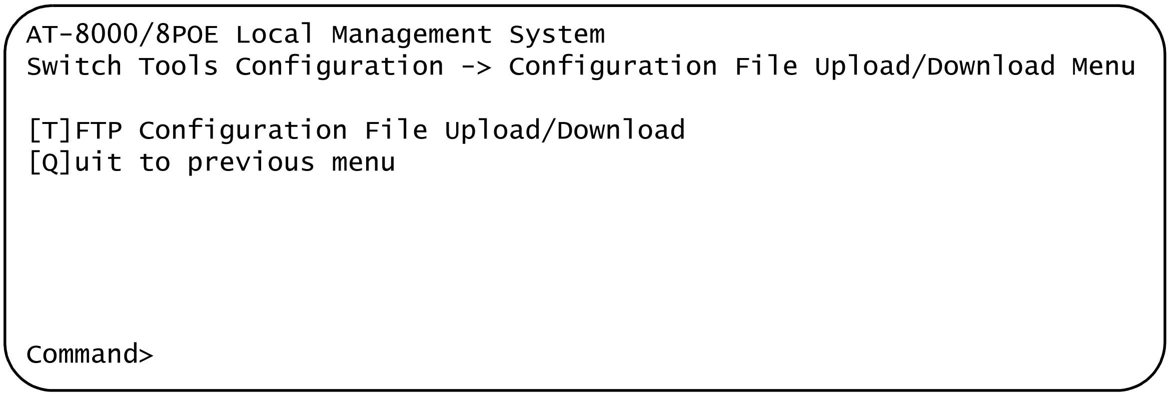
To upload the switch's configuration file onto a TFTP server, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

2. From the Switch Tools Menu, type **C** to select **Configuration File Upload/Download**.

   The Configuration File Upload/Download Menu is shown in Figure 58 on page 212.

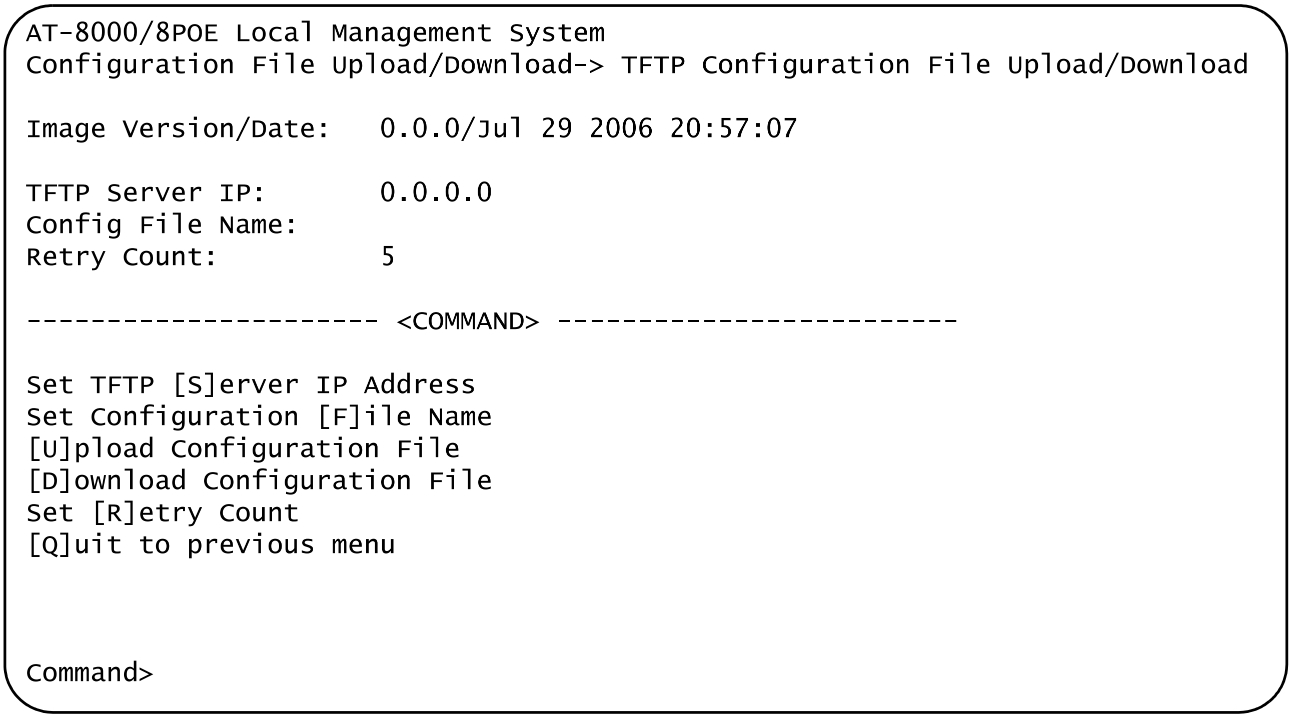


```
AT-8000/8POE Local Management System
Switch Tools Configuration -> Configuration File Upload/Download Menu

[T]FTP Configuration File Upload/Download
[Q]uit to previous menu




Command>
```

Figure 58. Configuration File Upload/Download Menu

3. From the Configuration File Upload/Download Menu, type **T** to select **TFTP Configuration File Upload/Download**.

   The TFTP Configuration File Upload/Download Menu is shown in Figure 59.



```
AT-8000/8POE Local Management System
Configuration File Upload/Download-> TFTP Configuration File Upload/Download

Image Version/Date:   0.0.0/Jul 29 2006 20:57:07

TFTP Server IP:       0.0.0.0
Config File Name:
Retry Count:          5

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

Set TFTP [S]erver IP Address
Set Configuration [F]ile Name
[U]pload Configuration File
[D]ownload Configuration File
Set [R]etry Count
[Q]uit to previous menu



Command>
```

Figure 59. TFTP Configuration File Upload/Download Menu

4. Type **S** to select **Set TFTP Server IP Address**.

   The following prompt is displayed:

   ```
   Enter IP address of TFTP server:
   ```

5. Enter the IP address of the TFTP server.

6. Type **F** to select **Set Configuration File Name**.

   The following prompt is displayed:

   ```
   Enter file name>
   ```

7. Enter a name for the configuration file.

   > **Note**
   > There is no default name for the configuration file.

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 upload process. The range is 1 to 20. The default is 5 times.

10. To begin the upload, type **U** to select **Upload Configuration File**.

    The following prompt is displayed:

    ```
    Upload file? (Y/N)>
    ```

11. Type **Y** for yes to begin the uploading or **N** for no to cancel the procedure.

Downloading a Configuration File

To download a configuration file onto the switch from a TFTP server, perform the following procedure:

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

   The Switch Tools Configuration Menu is shown in Figure 11 on page 50.

2. From the Switch Tools Menu, type **C** to select **Configuration File Upload/Download**.

   The Configuration File Upload/Download Menu is shown in Figure 58 on page 212.

3. From the Configuration File Upload/Download Menu, type **T** to select **TFTP Configuration File Upload/Download**.

   The TFTP Configuration File Upload/Download Menu is shown in Figure 59 on page 212.

4. Type **S** to select **Set TFTP Server IP Address**.

   The following prompt is displayed:

   ```
   Enter IP address of TFTP server:
   ```

5. Enter the IP address of the TFTP server.

6. Type **F** to select **Set Configuration File Name**.

   The following prompt is displayed:

   ```
   Enter file name>
   ```

7. Enter the file name of the configuration file on the TFTP server.

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 **D** to select **Download Configuration File**.

    The following prompt is displayed:

    ```
    Download file? (Y/N)>
    ```

11. Type **Y** for yes to begin the downloading or **N** for no to cancel the procedure.

    After the downloading is complete, reset the switch to implement the new settings.

Section II

Using the Web Browser Interface

The chapters in this section provide information and procedures for using the web browser interface in the AT-S81 management software. The chapters include:

Note
The menus interface is described in Section I, “Using the Menus Interface” on page 17, and the command line interface is described in Section III, “Using the Command Line Interface” on page 329.

Chapter 18
Starting a Web Browser Management Session

This chapter contains the procedures for starting, using, and quitting a web browser management session on an AT-8000/8POE Fast Ethernet switch. Sections in the chapter include:

Establishing a Remote Connection to Use the Web Browser Interface

In order for you to manage a switch using the web browser interface, the switch must have an IP address and subnet mask. 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
Enhanced stacking, a feature of other Allied Telesis Layer 2 and Layer 2+ managed switches, is not supported by the AT-9000/24 Gigabit Ethenet and AT-8000/8POE Fast Ethernet switches.

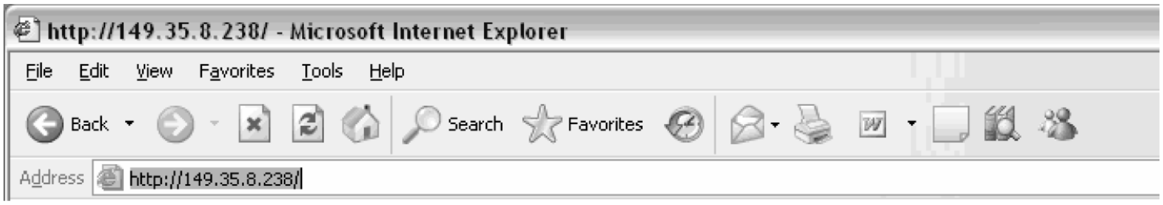
Note
The remote management station must be a member of the switch’s Default VLAN. The switch responds and processes management packets only if they are received on an untagged port of the Default VLAN.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note
If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser’s network options not to use proxies. Consult your web browser’s documentation on how to configure the switch’s web browser to not use proxies.

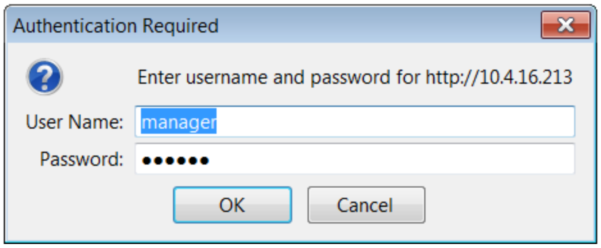
2. In the URL field of the browser, enter the IP address of the switch to be managed.



http://149.35.8.238/

Figure 60. Entering a Switch’s IP Address in the URL Field

The AT-S81 management software displays the login dialog box, shown in Figure 61.



Authentication Required

Enter username and password for http://10.4.16.213

User Name: manager

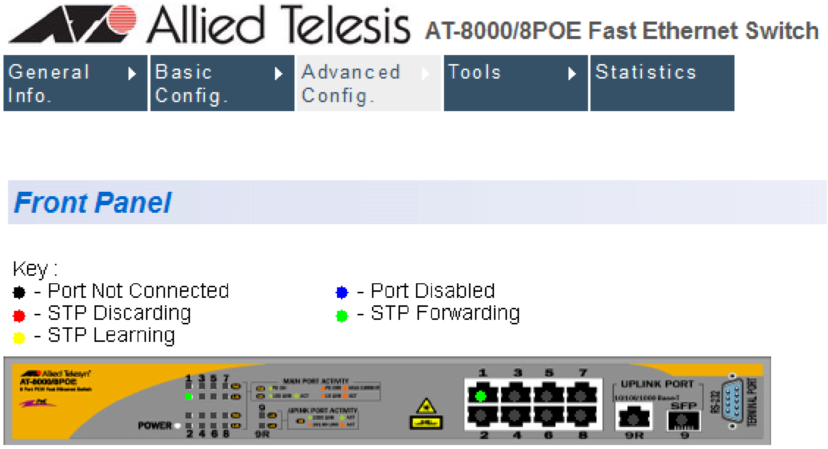
Password: ••••••

Figure 61. AT-S81 Login Dialog Box

3. Enter the AT-S81 management login user name and password. The default user name is “manager” and the default password is “friend.” The login name and password are case-sensitive.

   To change the user name and password, refer to “Configuring System Administration Information” on page 227.

   The AT-S81 management software displays the home page. The window contains an image of the front of the switch. Ports that have a link to an end node are green. Ports without a link are grey. An example of the home page is shown in Figure 62.



Key :

● - Port Not Connected
🔴 - STP Discarding
🟡 - STP Learning
🔵 - Port Disabled
🟢 - STP Forwarding

Figure 62. Home Page for the AT-8000/8POE

The main menu is on the top of the home page. It consists of the following selections:

- General Info.
- Basic Config.
- Advanced Config.
- Tools
- Statistics

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 19

Basic Switch Parameters

This chapter contains the following sections:

Configuring an IP Address, Subnet Mask and Gateway Address

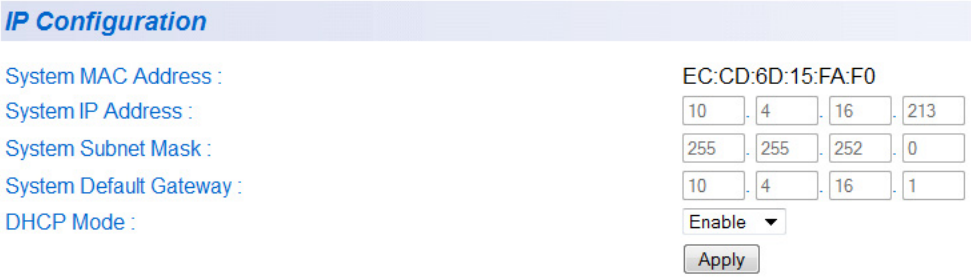
This procedure explains how to change the IP address, subnet mask, and gateway address of the switch. Before performing the procedure, note the following:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device using the web browser interface.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to “Enabling and Disabling the DHCP Client” on page 226.
- You must use the menus interface to manually assign an IP address to the switch, as described in “Configuring an IP Address, Subnet Mask and Gateway Address” on page 224.

To change the switch’s IP configuration, perform the following procedure:

1. From the Basic Config menu, select **IP Config**.

   The IP Configuration page opens, as shown in Figure 63.



IP Configuration

System MAC Address : EC:CD:6D:15:FA:F0
System IP Address : 10 . 4 . 16 . 213
System Subnet Mask : 255 . 255 . 252 . 0
System Default Gateway : 10 . 4 . 16 . 1
DHCP Mode : Enable

Figure 63. IP Configuration Page

2. 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 226.

3. 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 60 on page 218.

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:

- An IP address and subnet mask are not required for normal network operations of the switch. Values for these parameters are only required if you want to remotely manage the device with a web browser.
- A gateway address is only required if you want to remotely manage the device from a remote management station that is separated from the switch by a router.
- The DHCP client is disabled by default on the switch.
- The DHCP client does not support BOOTP.
- You must assign an IP address initially 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 Basic Config menu, select **IP Config**.

   The IP Configuration page is shown in Figure 63 on page 224.

2. For the **DHCP Mode**, select **Enable** or **Disable**.

3. 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 with its new IP address.

> **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.

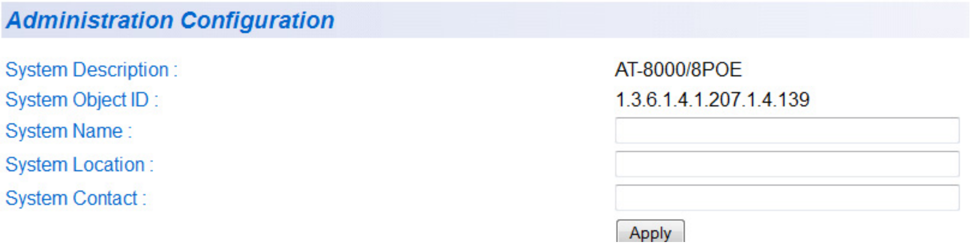
Configuring System Administration Information

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 Basic Config menu, select **Admin. Config.**

   The Administration Configuration page opens, as shown in Figure 64.



Administration Configuration

System Description : AT-8000/8POE

System Object ID : 1.3.6.1.4.1.207.1.4.139

System Name :

System Location :

System Contact :

Figure 64. Administration Configuration Page

2. 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 that you assign a name to the switch. A name can help you identify the switch when you manage it 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.

3. Click **Apply**.

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:

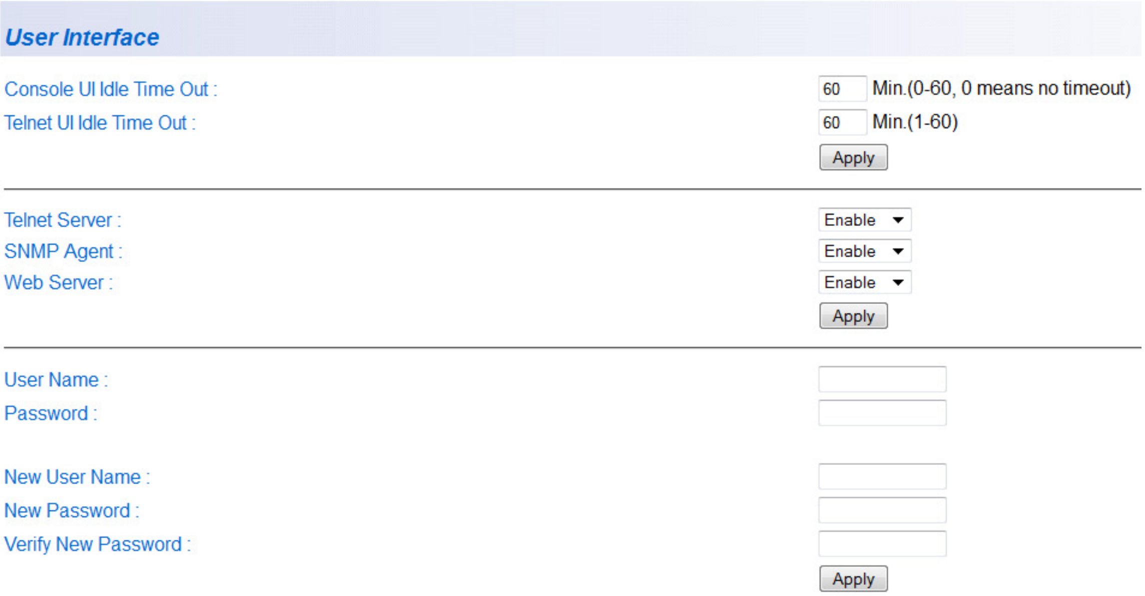
- ❒ Change the console timer, used to automatically end inactive local management sessions.
- ❒ Change the AT-S81 management login user name and password.
- ❒ Enable and disable the web server, used to manage the switch from a remote management station with a web browser.

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

1. From the Basic Config menu, select **User Interface** > **User Interface**.

   The other selection on this menu, RADIUS, is described in Chapter 30, "RADIUS Authentication Protocol" on page 311.

   The User Interface page opens, as shown in Figure 65.



User Interface

Console UI Idle Time Out : 60 Min.(0-60, 0 means no timeout)
Telnet UI Idle Time Out : 60 Min.(1-60)

Telnet Server : Enable
SNMP Agent : Enable
Web Server : Enable

User Name :
Password :

New User Name :
New Password :
Verify New Password :

Figure 65. User Interface Page

The User Interface page has three parts:

- ❒ Console and Telnet UI Idle Time Out settings
- ❒ Server and SNMP settings
- ❒ User name and password settings

Note
For information about the SNMP Agent selection, refer to “Enabling or Disabling the SNMP Agent” on page 256.

2. To configure the console UI time out parameters, do the following:

   a. In the **Console UI Time Out** field, enter a new value.

      The range is 0 to 60 minutes. The default is 5 minutes. A timeout value of 0 causes the console connection to never times 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**.

3. To configure the Telnet UI timeout value, do the following:

   a. In the **Telnet UI Time Out** field, enter a new value.

      The Telnet idle time out parameter specifies the length of time that a remote Telnet management session can be inactive before the management software automatically ends it.

4. To change the user settings, do the following:

   a. Enter the existing name and password in the **User Name** and **Password** fields. The default name and password are both “manager”. The login name and password are case sensitive.

   b. Click the **New User Name** field and enter a new user name or, if you do not want to change the login name, enter the current name. Leaving this field empty deletes the current login name without assigning a new one. The name can be from 0 to 12 characters. Spaces are allowed. The login name is case sensitive.

c. Click the **New Password** field and enter a new login password or, if you do not want to change the password, enter the current password. 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. Leaving this field empty deletes the current password without assigning a new one.

d. Click the **Verify New Password** field and enter the same password entered in the previous step.

e. Click **Apply**.

Enabling or Disabling the Web Server

To enable or disable the web server, perform the following procedure:

1. From the Basic Config menu, select **User Interface** > **User Interface**.

   The User Interface page is shown in Figure 65 on page 229.

2. For the **Web Server** parameter, 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 server automatically ends your remote management session.

3. Click **Apply**.

Enabling or Disabling the Telnet Server

To enable or disable the Telnet server, perform the following procedure:

1. From the Basic Config menu, select **User Interface** > **User Interface**.

   The User Interface page is shown in Figure 65 on page 229.

2. For the **Telnet Server** parameter, choose **Enable** or **Disable** from the list.

   The default is Enable. When you enable this parameter, a Telnet connection to the switch is available.

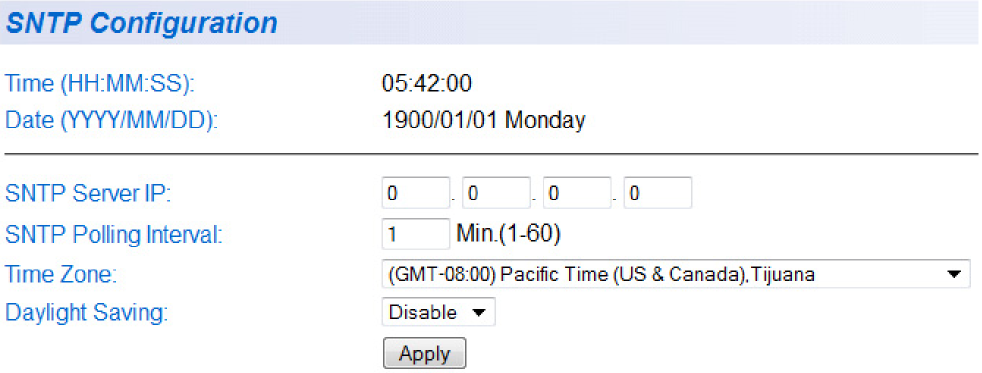
3. Click **Apply**.

Configuring SNTP

To configure SNTP, perform the following procedure:

1. From the Basic Configuration menu, select **SNTP Configuration**.

   The SNTP Configuration page opens, as shown in Figure 66.



SNTP Configuration

Time (HH:MM:SS): 05:42:00

Date (YYYY/MM/DD): 1900/01/01 Monday

SNTP Server IP: 0 . 0 . 0 . 0

SNTP Polling Interval: 1 Min.(1-60)

Time Zone: (GMT-08:00) Pacific Time (US & Canada),Tijuana

Daylight Saving: Disable

Figure 66. SNTP Configuration Page

2. In the **SNTP Server IP** field, type the IP address for the SNTP server you want to use.

3. In the **Set SNTP Interval** field, type a number to specify the number of minutes between occurrences of polling the SNTP server. The range is 1 to 60 minutes and the default is 1 minute.

4. To set the time zone, select one from the **Time Zone** list.

5. For **Daylight Saving** (if it applies to the time zone you chose), choose one of the following from the list:

   Disabled - To disable daylight saving time.

   Enabled - To enable daylight saving time.

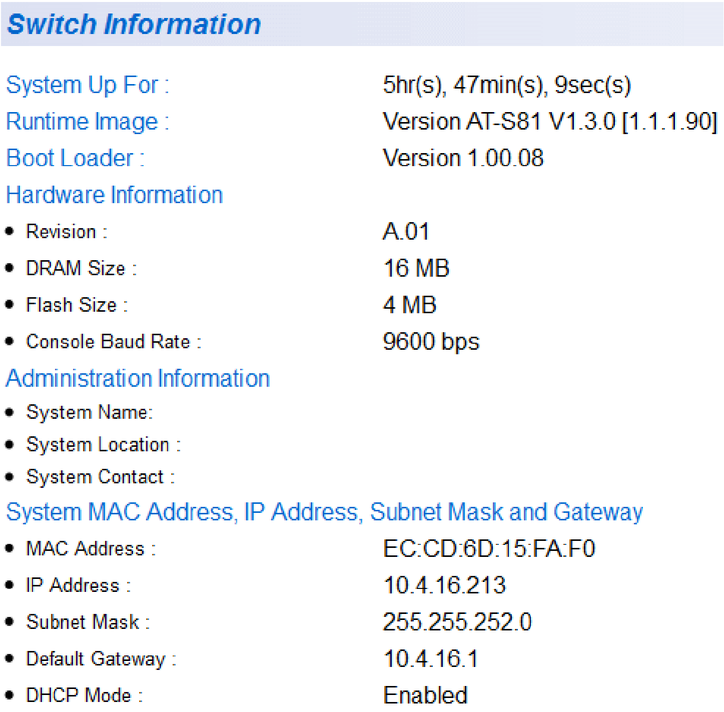
6. Click **Apply**.

Viewing System Information

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

1. From General Info. menu, select **Switch Information**.

   The Switch Information page opens, as shown in Figure 67.



Switch Information

System Up For :	5hr(s), 47min(s), 9sec(s)
Runtime Image :	Version AT-S81 V1.3.0 [1.1.1.90]
Boot Loader :	Version 1.00.08
Hardware Information	
• Revision :	A.01
• DRAM Size :	16 MB
• Flash Size :	4 MB
• Console Baud Rate :	9600 bps
Administration Information	
• System Name:	
• System Location :	
• System Contact :	
System MAC Address, IP Address, Subnet Mask and Gateway	
• MAC Address :	EC:CD:6D:15:FA:F0
• IP Address :	10.4.16.213
• Subnet Mask :	255.255.252.0
• Default Gateway :	10.4.16.1
• DHCP Mode :	Enabled

Figure 67. 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. You cannot change this setting.

Administration Information Section:

System Name
The name assigned to the switch. To give the switch a name, refer to "Configuring System Administration Information" on page 227.

System Location
The location of the switch. To specify the location, refer to "Configuring System Administration Information" on page 227.

System Contact
The contact person responsible for managing the switch. To specify the name of a contact, refer to "Configuring System Administration Information" on page 227.

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 224 to manually assign an IP address or "Enabling and Disabling the DHCP Client" on page 226 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 224 to manually assign a subnet mask or "Enabling and Disabling the DHCP Client" on page 226 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 224 to manually assign a gateway address or "Enabling and Disabling the DHCP Client" on page 226 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 226.

Rebooting a Switch

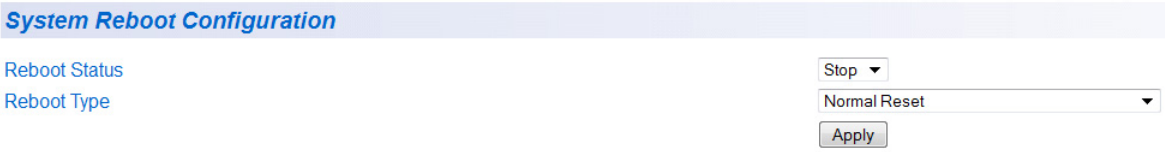
This procedure reboots the switch and reloads the AT-S81 management software from flash memory. You might reboot the device if you believe it is experiencing a problem. Rebooting the device does not change any of the device's parameter settings.

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 menu, select **System Reboot**.

   The System Reboot Configuration page opens, as shown in Figure 68.



System Reboot Configuration

Reboot Status: Stop

Reboot Type: Normal Reset

Figure 68. System Reboot Configuration Page

2. For the Reboot Type, select **Normal Reset**. This is the default setting.

Note
The two other Reboot Type options, Reset to Factory Default and **Reset to Factory Default Except IP Address**, are described in "Returning the AT-S81 Management Software to the Factory Default Values" on page 244.

3. For the Reboot Status, select **Start** to start the reboot.

4. Click **Apply**.

   The switch immediately begins to reload the AT-S81 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

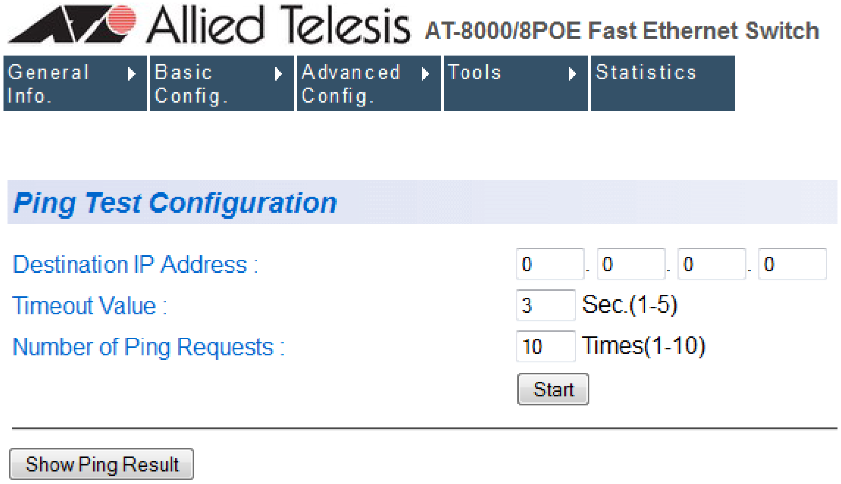
This procedure instructs the switch to ping a node on your network. This procedure is useful in determining whether an active link exists between the switch and another network device. Note the following before performing the procedure:

- The switch where you are initiating the ping must have an IP address.
- The device you are pinging must be a member of the Default VLAN. This means that the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

To ping a network device, perform the following procedure:

1. From the Tools menu, select **Ping**.

   The Ping Test Configuration page opens, as shown in Figure 69.



Ping Test Configuration

Destination IP Address : 0 . 0 . 0 . 0

Timeout Value : 3 Sec.(1-5)

Number of Ping Requests : 10 Times(1-10)

Figure 69. Ping Test Configuration Page

2. Configure the following parameters:

   Destination IP Address
   The IP address of the node you want to ping.

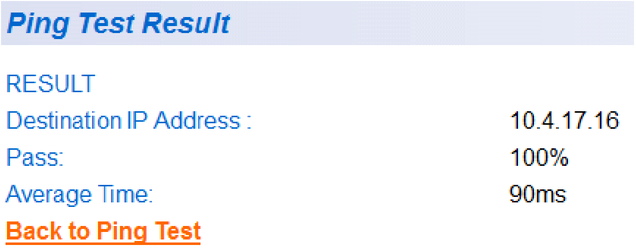
   Timeout Value
   Specifies the length of time in seconds the switch waits for a response before assuming that a ping has failed. The default is 3 seconds.

   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 70.



Ping Test Result

RESULT

Destination IP Address :	10.4.17.16
Pass:	100%
Average Time:	90ms

Back to Ping Test

Figure 70. Ping Test Results Page

5. Click **Back to Ping Test** to return to the Ping Test Configuration page.

Working with the System Log

The system log displays system-level events in the switch, such as logging in to the management software. You can view the system log locally, or send the system log file to a remote location. This section contains the following procedures:

- “Viewing the System Log,” next
- “Sending the System Log to a Remote Server” on page 243

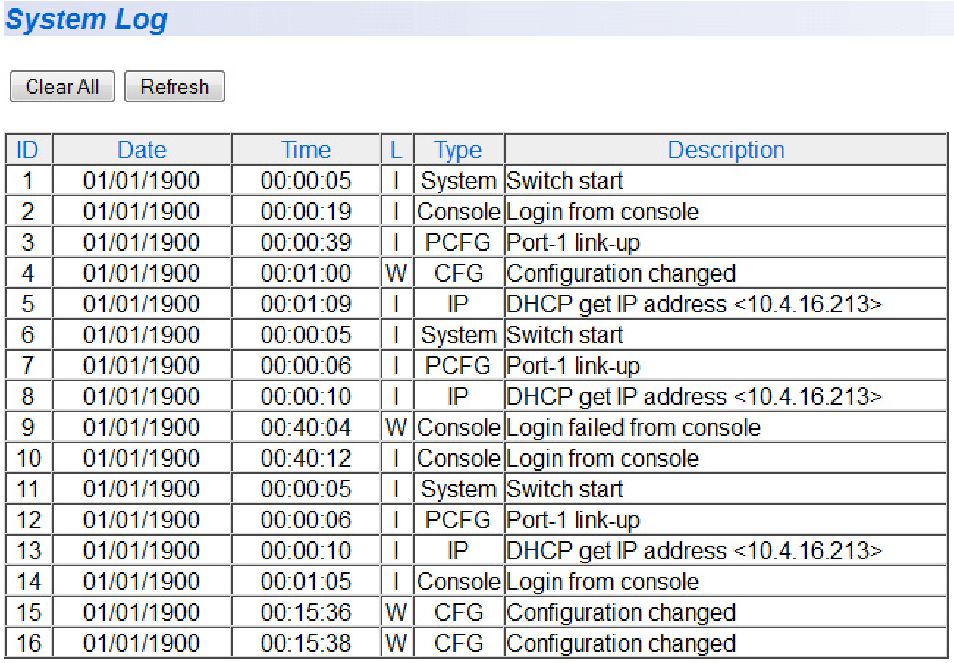
Viewing the System Log

The system log displays system-level events in the switch, such as logging in to the management software.

To view the system log, perform the following procedure:

1. From the Tools menu, select **System Log**.

   The System Log page opens, as shown in Figure 71.



ID	Date	Time	L	Type	Description
1	01/01/1900	00:00:05	I	System	Switch start
2	01/01/1900	00:00:19	I	Console	Login from console
3	01/01/1900	00:00:39	I	PCFG	Port-1 link-up
4	01/01/1900	00:01:00	W	CFG	Configuration changed
5	01/01/1900	00:01:09	I	IP	DHCP get IP address <10.4.16.213>
6	01/01/1900	00:00:05	I	System	Switch start
7	01/01/1900	00:00:06	I	PCFG	Port-1 link-up
8	01/01/1900	00:00:10	I	IP	DHCP get IP address <10.4.16.213>
9	01/01/1900	00:40:04	W	Console	Login failed from console
10	01/01/1900	00:40:12	I	Console	Login from console
11	01/01/1900	00:00:05	I	System	Switch start
12	01/01/1900	00:00:06	I	PCFG	Port-1 link-up
13	01/01/1900	00:00:10	I	IP	DHCP get IP address <10.4.16.213>
14	01/01/1900	00:01:05	I	Console	Login from console
15	01/01/1900	00:15:36	W	CFG	Configuration changed
16	01/01/1900	00:15:38	W	CFG	Configuration changed

Figure 71. System Log Page

The System Log page contains a table that displays the following information:

ID
An indentifying number for the event.

Date
The date that the event occurred.

Time
The time that the event occurred.

Note
When you enable the SNTP protocol, switch startup events show the default system date until SNTP polls for the current date and time.

L
Severity level of the event. The severity levels are:

(I)nformation - Useful information that you can ignore during normal operation.

W)arning - An issue that may require a manager’s attention.

(E)rror - Switch operation is severely impaired.

Type
The type provides more information about the event. The possible types are:

802.1X - An 802.1X event.

CFG - Configuration event.

CLI - CLI login.

Console - A console login by a user.

IP - Change to the IP information.

CFG - Port configuration.

PoE - PoE configuration or event.

SNTP - SNTP configuration.

STP - Spanning tree.

SwUpg - Software upgrade.

System - General system event.

Telnet - Access via Telnet.

Description
A description of the event.

2. To remove the current log entries, click **Clear All**. To refresh the log, click **Refresh**.

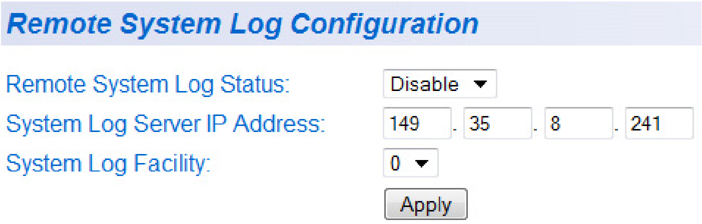
Sending the System Log to a Remote Server

The syslog protocol allows you to collect messages and events produced by a wide variety of network equipment in a single place. For instance, instead of viewing the event logs of several separate AT-8000/8POE Fast Ethernet switches, you can have those events sent to a single syslog server on your network. The destination for the events is referred to as a facility.

To send the system events to a syslog server, perform the following procedure:

1. From the Tools menu, select **Remote System Log**.

   The Remote System Log page opens, as shown in Figure 72.



Remote System Log Configuration

Remote System Log Status: Disable

System Log Server IP Address: 149 . 35 . 8 . 241

System Log Facility: 0

Figure 72. Remote System Log Page

2. Configure the following parameters:

   System Log Server IP Address
   The IP address of the server where you want to store the system log.

   System Log Facility
   Select a number for the system log facility on the server, from 0 through 7.

3. For the **Remote System Log Status** parameter, choose one of the following from the list:

   Disabled - To disable remote system logging.

   Enabled - To enable remote system logging.

4. Click **Apply**.

Returning the AT-S81 Management Software to the Factory Default Values

This procedure returns all AT-S81 management software parameters to their default values and deletes all tagged and VLANs on the switch. The AT-S81 management software default values are listed in Appendix A, “AT-8000/POE Default Settings” on page 345.

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-S81 management software to the default settings, perform the following procedure:

1. From the Tools menu, select **System Reboot**.

   The System Reboot Configuration page is shown in Figure 68 on page 238.

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 20

Port Configuration

The sections in this chapter explain the two methods to viewing and changing the parameter settings of the individual ports on the switch. The first method shows how to use the Port Configuration page to view and configure multiple ports at one time. The second is typically used to configure just one port at a time. There is also a section for viewing port statistics. The sections are:

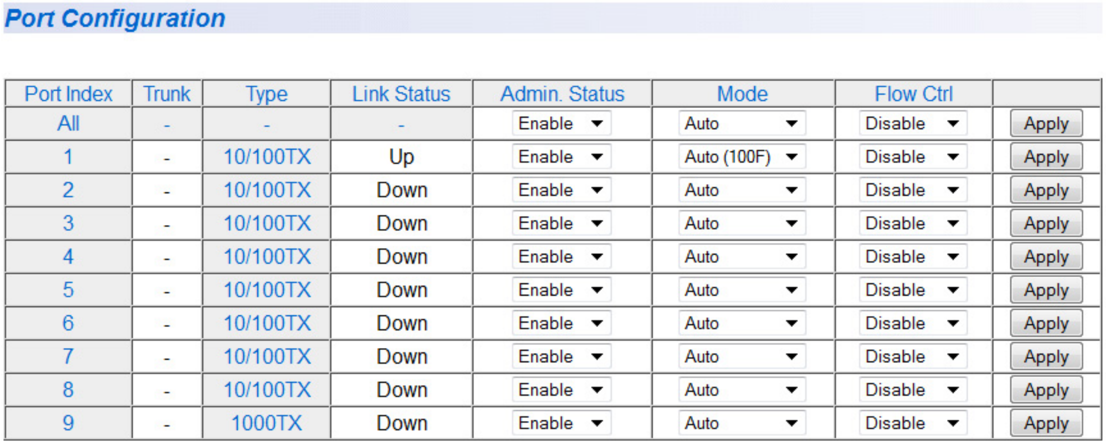
Viewing and Configuring Multiple Ports

This procedure allows you to configure the ports on the switch using the Port Configuration 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 Basic Config menu, select **Port Config**.

   The Port Configuration page opens, as shown in Figure 73. The page lists all the ports on the switch and their current settings.



Port Configuration

Port Index	Trunk	Type	Link Status	Admin. Status	Mode	Flow Ctrl	
All	-	-	-	Enable	Auto	Disable	Apply
1	-	10/100TX	Up	Enable	Auto (100F)	Disable	Apply
2	-	10/100TX	Down	Enable	Auto	Disable	Apply
3	-	10/100TX	Down	Enable	Auto	Disable	Apply
4	-	10/100TX	Down	Enable	Auto	Disable	Apply
5	-	10/100TX	Down	Enable	Auto	Disable	Apply
6	-	10/100TX	Down	Enable	Auto	Disable	Apply
7	-	10/100TX	Down	Enable	Auto	Disable	Apply
8	-	10/100TX	Down	Enable	Auto	Disable	Apply
9	-	1000TX	Down	Enable	Auto	Disable	Apply

Figure 73. Port Configuration Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are:

   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 22, “Port Trunking” on page 261.

   Type
   The port type. The port type is 10/100TX for 10/100Base-T twisted pair ports and 1000Base-F for the SFP fiber port.

   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 - A valid link is not established on the port.

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, "100F") after a port establishes a link with an end node.

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

Flow Ctrl

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.

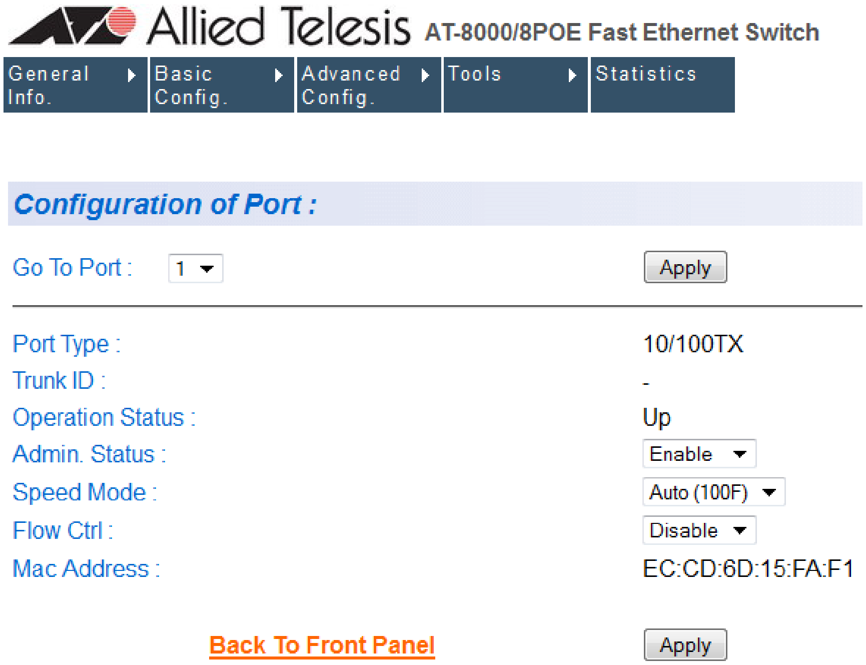
Viewing and Configuring a Single Port

The procedure in this section allows you to view or configure the parameter settings of *one* port on the switch. To view and configure the parameter settings for more than one port at a time, refer to "Viewing and Configuring Multiple Ports" on page 246.

To view or configure the parameter settings of a single port, perform the following procedure:

1. On the home page, in the front panel image, click the port that you want to configure.

   A sample Configuration of Port page is shown in Figure 74.



Configuration of Port :

Go To Port : 1

Port Type :	10/100TX
Trunk ID :	-
Operation Status :	Up
Admin. Status :	Enable
Speed Mode :	Auto (100F)
Flow Ctrl :	Disable
Mac Address :	EC:CD:6D:15:FA:F1

Figure 74. Configuration of Port Page

2. Adjust the following port settings as needed. Not all parameters are adjustable.

   Port Type
   The port type. The port type is 1000TX for 10/100/1000Base-T twisted pair ports and 1000BaseF for an optional SFP fiber optic port.

   Trunk ID
   The trunk group number. A number in this column indicates that the port is a member of a port trunk. For information about configuring a trunk, refer to Chapter 22, "Port Trunking" on page 261.

Operation Status
The status of the link between the port and the end node connected to the port. You must use the Port Configuration page to configure this parameter. For information, refer to “Viewing and Configuring Multiple Ports” on page 246.

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, “100F”) after a port establishes a link with an end node.

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 you select 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.

- ❒ Allied Telesis does not recommend manually setting a 10/100/1000Base-T twisted pair port to either 1000 Mbps full duplex or 1000 Mbps half duplex. For 1000 Mbps operation, Allied Telesis recommends setting the port to Auto-Negotiation.
- ❒ The only valid setting for an optional SFP port is Auto-Negotiation.

Flow Ctrl
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 uses flow control. This is the default setting for all ports on the switch.

Disabled - The port does not use flow control.

MAC Address
The port's MAC address. You cannot change this setting.

3. Click **Apply**.
4. To view or configure the parameter settings on another port, click **Go to Port** and select the port from the list,
5. Repeat step 2 in this procedure to configure the settings
6. Click **Apply**.

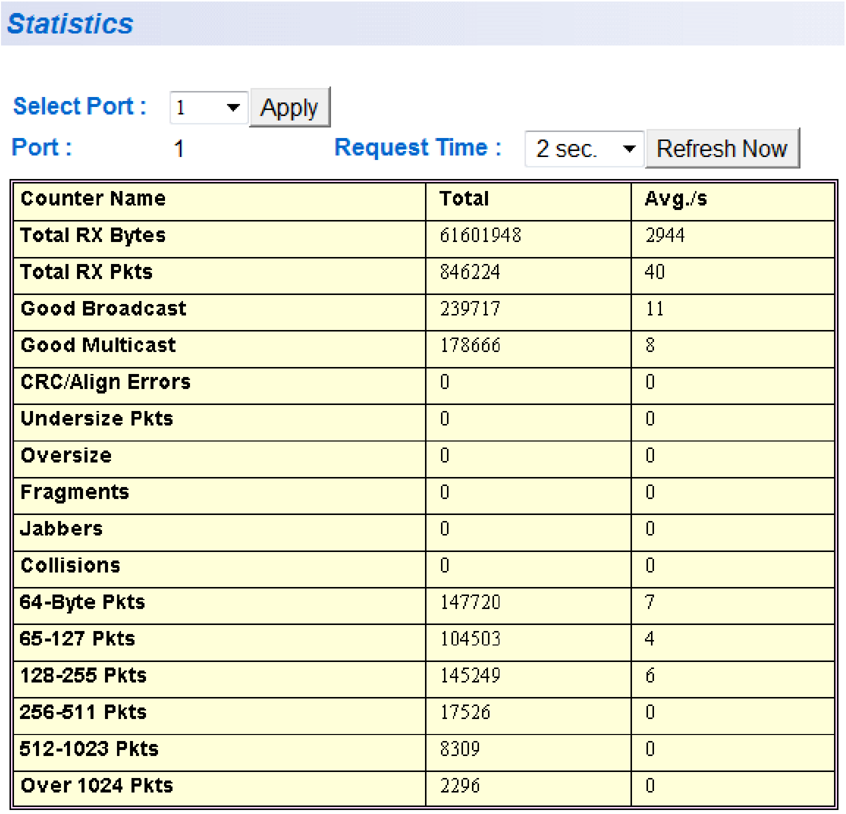
To return to the front panel page, click **Return To Front Panel**.

Displaying Port Statistics

To display port statistics, perform the following procedure:

1. From the Main Menu, select **Statistics**.

   The Statistics page opens, as shown in Figure 75.



Statistics

Select Port : 1 Apply

Port : 1 Request Time : 2 sec. Refresh Now

Counter Name	Total	Avg./s
Total RX Bytes	61601948	2944
Total RX Pkts	846224	40
Good Broadcast	239717	11
Good Multicast	178666	8
CRC/Align Errors	0	0
Undersize Pkts	0	0
Oversize	0	0
Fragments	0	0
Jabbers	0	0
Collisions	0	0
64-Byte Pkts	147720	7
65-127 Pkts	104503	4
128-255 Pkts	145249	6
256-511 Pkts	17526	0
512-1023 Pkts	8309	0
Over 1024 Pkts	2296	0

Figure 75. Statistics Page

2. To view statistics for a port, select a port from the Select Port list and click **Apply**.

   The statistics are displayed in a table that contains the following items of information:

   Total RX Bytes
   Number of bytes received on the port.

   Total RX Pkts
   Number of packets received on the port.

   Good Broadcast
   Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Pkts
Number of packets that were less than the minimum length specified by IEEE 902.3 (64 bytes including the CRC) received on the port.

Oversize Pkts
Number of packets that exceeded the maximum length specified by IEEE 902.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
Number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1024-1522 Pkts
Number of 1024- to 1522-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.

3. To modify how frequently the statistics are updated, from the Request Time list, select the desired time and click **Refresh Now**. The default is every two seconds. (You can click Refresh Now at any time to update the page.)

Chapter 21

SNMP

This chapter contains the following procedures for working with the Simple Network Management Protocol (SNMP):

- ❐ “Enabling or Disabling the SNMP Agent” on page 256
- ❐ “Changing the Default SNMP Community Names” on page 257
- ❐ “Working with Trap Receivers” on page 258

Note
For background information on SNMP, refer to “SNMP Overview” on page 72.

Enabling or Disabling the SNMP Agent

To enable or disable the SNMP agent, perform the following procedure:

1. From the Basic Config menu, select **User Interface**.

2. From the User Interface menu, select **User Interface**.

   The User Interface page is shown in Figure 65 on page 229.

3. For the **SNMP Agent** parameter, choose **Enable** or **Disable** from the list.

   The default is Enable. When you enable this parameter, SNMP access is allowed.

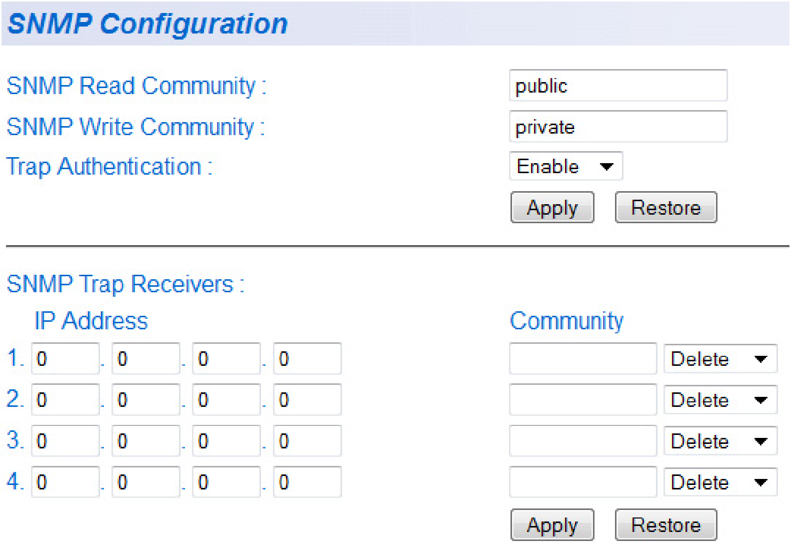
4. Click **Apply**.

Changing the Default SNMP Community Names

To configure the SNMP settings, perform the following procedure:

1. From the Basic Config menu, select **SNMP Config**.

   The SNMP Configuration page opens, as shown in Figure 76.



SNMP Configuration

SNMP Read Community : public

SNMP Write Community : private

Trap Authentication : Enable

SNMP Trap Receivers :

	IP Address	Community	
1.	0 . 0 . 0 . 0		Delete
2.	0 . 0 . 0 . 0		Delete
3.	0 . 0 . 0 . 0		Delete
4.	0 . 0 . 0 . 0		Delete

Figure 76. SNMP Configuration Page

2. Click the **SNMP Read Community** field and type the name of the read community.

   The default is “public.”

3. Click the **SNMP Write Community** field and type the name of the write community.

   The default is “private.”

4. To set **Trap Authentication** for that community string, select Enable or Disable from the list.

5. Click **Apply**.

Working with Trap Receivers

This section contains the following procedures:

- "Adding and Enabling a Trap Receiver," next
- "Disabling a Trap Receiver" on page 258
- "Deleting a Trap Receiver" on page 258

Adding and Enabling a Trap Receiver

To add and enable a trap receiver, perform the following procedure:

1. From the Basic Config menu, select **SNMP Config**.

   The SNMP Configuration page is shown in Figure 76 on page 257.

2. In the bottom half of the page, enter the IP address for each trap receiver.

3. Enter the community string to associate with that trap receiver.

4. Select **Enable** from the list.

5. Click **Apply**.

Disabling a Trap Receiver

To disable a trap receiver, perform the following procedure:

1. From the Basic Config menu, select **SNMP Config**.

   The SNMP Configuration page is shown in Figure 76 on page 257.

2. To the right of the trap receiver you want to disable, select **Disable** from the list.

3. Click **Apply**.

Deleting a Trap Receiver

To delete a trap receiver, perform the following procedure:

1. From the Basic Config menu, select **SNMP Config**.

   The SNMP Configuration page is shown in Figure 76 on page 257.

2. To the right of the trap receiver you want to disable, select **Delete** from the list.

3. Click **Apply**.

Restoring the Trap Receivers

To restore the trap receivers, perform the following procedure:

1. From the Basic Config menu, select **SNMP Config**.

The SNMP Configuration page is shown in Figure 76 on page 257.

2. Click **Restore**.

Chapter 22

Port Trunking

This chapter contains the following procedures for working with port trunking:

- ❒ “Setting Up a Port Trunk” on page 262
- ❒ “Setting Up an LACP Trunk” on page 265

Note
For background information on trunking, refer to “Port Trunking Overview” on page 82.

Setting Up a Port Trunk

This section contains the following procedures for working with port trunks:

- “Creating a Port Trunk” on page 262
- “Modifying a Port Trunk” on page 263
- “Enabling or Disabling a Port Trunk” on page 264

Creating a Port Trunk

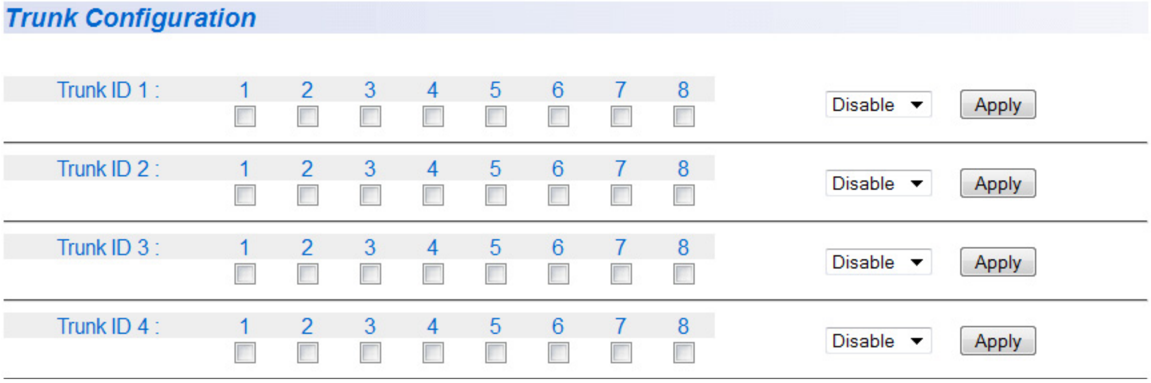
This procedure explains how to configure a port trunk.

> **Note**
> Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely affect the operation of your network.

To create a port trunk, perform the following procedure:

1. From the Advanced Config menu, select **Trunk Config**.

   The Trunk Configuration page opens, as shown in Figure 77.



Trunk Configuration

	1	2	3	4	5	6	7	8		
Trunk ID 1 :	□	□	□	□	□	□	□	□	Disable ▾	Apply
Trunk ID 2 :	□	□	□	□	□	□	□	□	Disable ▾	Apply
Trunk ID 3 :	□	□	□	□	□	□	□	□	Disable ▾	Apply
Trunk ID 4 :	□	□	□	□	□	□	□	□	Disable ▾	Apply

Figure 77. Trunk Configuration 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.

2. In any one of the unused **Trunk ID** rows, click the check box next to 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.

3. Change the status of the trunk from **Disable** to **Enable**.

4. Click **Apply**.

   The trunk is now operational on the switch.

5. 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.

> **Note**
> You should disconnect the cables from the ports of the trunk on the switch before modifying it. Adding or removing ports from a trunk without first disconnecting the cables can create loops in your network topology, which can cause broadcast storms and poor network performance.

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

1. From the Advanced Config menu, select **Trunk Config**.

   The Trunk Configuration page is shown in Figure 77.

2. On the row that corresponds to the trunk you want to modify, from the list, select **Disable**.

> **Note**
> Allied Telesis recommends disabling a port trunk before adding or removing ports.

3. Click **Apply**.

4. To add or remove a port from a trunk, click the check 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.

5. On the row that corresponds to the trunk you want to modify, from the list, select **Enable**.

6. Click **Apply**.

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

Enabling or 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.

Note
If you are disabling a port trunk, be sure to first disconnect all cables from the ports of the trunk. Leaving the cables connected can create loops in your network topology because the ports of a disabled port trunk function as normal network ports, forwarding individual network traffic.

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

1. From the Advanced Config menu, select **Trunk Config**.

   The Trunk Configuration page is shown in Figure 77.

2. On the row that corresponds to the trunk you want to modify, from the list, select **Enable** or **Disable**.

3. Click **Apply**.

Setting Up an LACP Trunk

This section contains the following procedures:

- ❒ “Creating an LACP Trunk,” next
- ❒ “Configuring the LACP Port Priority” on page 266
- ❒ “Viewing the LACP Group Settings” on page 267
- ❒ “Disabling an LACP Trunk” on page 267

Note
Create the trunk before you make it an LACP trunk. For more information, see “Setting Up a Port Trunk” on page 262.

Creating an LACP Trunk

To create an LACP trunk, perform the following procedure:

1. From the Advanced Config menu, select **Trunk Config** > **Trunk Config**.

   The Trunk Configuration page is shown in Figure 77.

2. On the row that corresponds to the trunk you want to enable as an LACP trunk, from the list, choose one of the following settings:

   Active - LACP Active: Ports are in an active negotiation state.

   Passive - LACP Passive: Ports are in a passive state where the port negotiates a bundle by exchanging LACP packets to the peer only if the far end initiates it.

   Note
   LACP must be enabled at both ends of the link to be operational.

3. Click **Apply**.

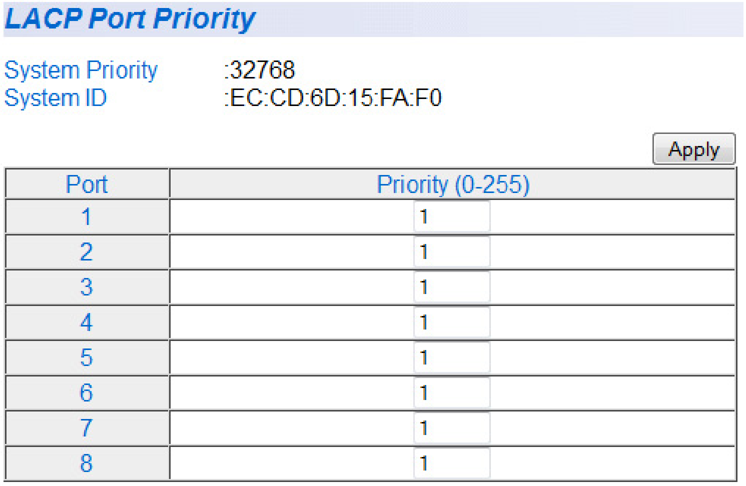
Configuring the LACP Port Priority

LACP port priority determines which port is the backup port to another port when the link to that port is down. The port with the lowest value has the highest value, and is selected to join the link aggregation group first.

To configure the LACP port priority, perform the following procedure:

1. From the Advanced Config menu, select **Trunk Config** > **Port Priority Config**.

   The LACP Port Priority page opens, as shown in Figure 78.



LACP Port Priority

System Priority :32768
System ID :EC:CD:6D:15:FA:F0

Port	Priority (0-255)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

Figure 78. LACP Port Priority Page

2. For each port, enter a priority in the priority column. The range is 0 to 255, and the default is 1.

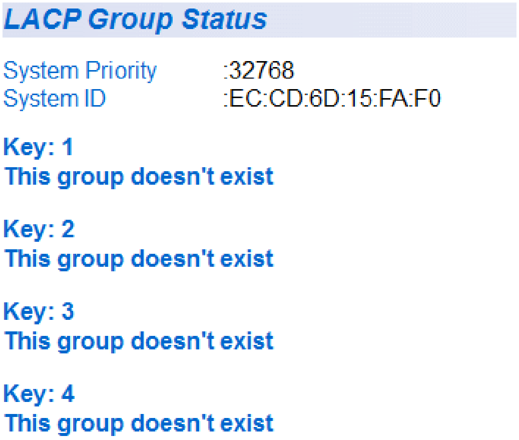
3. Click **Apply**.

Viewing the LACP Group Settings

To view the LACP group settings, perform the following procedure:

1. From the Advanced Config menu, select **Trunk Config** > **LACP Group Status**.

   The LACP Group Status page opens, as shown in Figure 79.



LACP Group Status

System Priority :32768
System ID :EC:CD:6D:15:FA:F0

Key: 1
This group doesn't exist

Key: 2
This group doesn't exist

Key: 3
This group doesn't exist

Key: 4
This group doesn't exist

Figure 79. LACP Group Status Page

The LACP Group Status page displays the following information about each LACP group:

System Priority
The system priority as defined by IEE 802.3ad. You cannot change this.

System ID
The MAC address of the system.

Key
The key for this trunk group.

The menu also contains a table that displays the following information:

Aggregator
The port that is operating as the aggregator.

Attached Port List
The ports assigned to the aggregator.

Disabling an LACP Trunk

To disable an LACP trunk, perform the following procedure:

1. From the Advanced Config menu, select **Trunk Config** > **Trunk Config**.

   The Trunk Configuration page is shown in Figure 77.

2. On the row that corresponds to the trunk you want to disable as an LACP trunk, from the list, choose **Disabled**.

3. Click **Apply**.

Chapter 23
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 270
- ❐ “Disabling Port Mirroring” on page 271

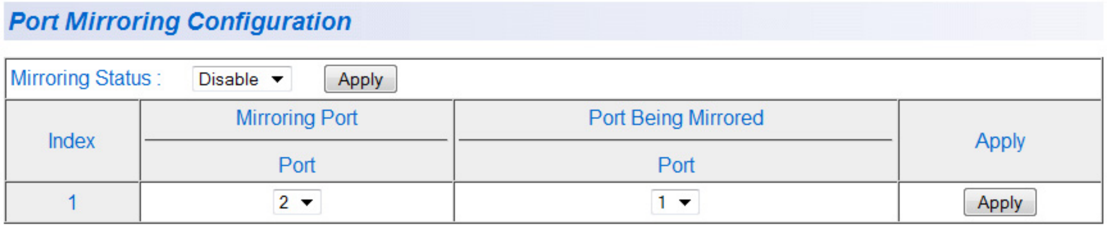
Note
For background information on port mirroring, refer to “Port Mirroring Overview” on page 98.

Configuring Port Mirroring

To set up port mirroring, perform the following procedure:

1. From the Advanced Config menu, select **Port Mirroring**.

   The Port Mirroring page opens, as shown in Figure 80.



Port Mirroring Configuration

Mirroring Status : Disable ▼ Apply

Index	Mirroring Port	Port Being Mirrored	Apply
	Port	Port	
1	2 ▼	1 ▼	Apply

Figure 80. Port Mirroring Page

2. In the Mirroring Port section, select the port where the network analyzer is connected.

3. In the Port Being Mirrored section, select the port whose ingress and egress traffic you want to monitor. You can select only one port.

4. Click **Apply**.

5. From the Mirroring Status list, select **Enable** and 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 Advanced Config menu, select **Port Mirroring**.

   The Port Mirroring page is shown in Figure 80 on page 270.

2. From the Mirroring Status list, select **Disable** and click **Apply**.

   Port mirroring is immediately disabled on the switch. You can now use the mirroring port for regular network operations.

Chapter 24

Power Over Ethernet

This chapter contains the following procedure for working with Power Over Ethernet (PoE):

❒ "Configuring PoE" on page 274

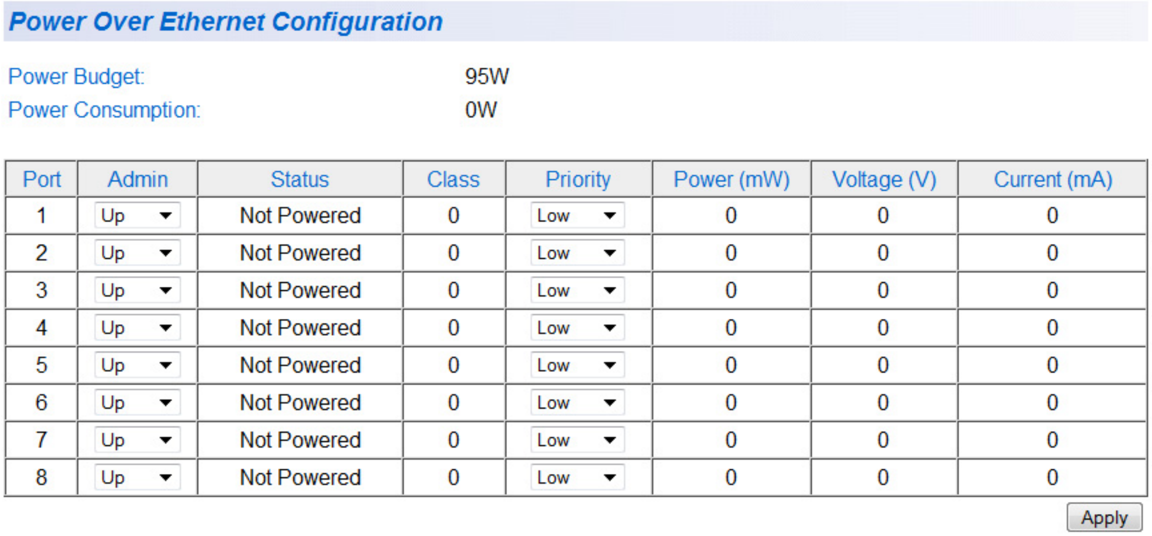
Note
For background information on PoE, refer to "PoE Overview" on page 104.

Configuring PoE

To configure the PoE settings, perform the following procedure:

1. From the Advanced Config menu, select **Power Over Ethernet**.

   The Power Over Ethernet Configuration page opens, as shown in Figure 81.



Power Over Ethernet Configuration

Power Budget:	95W
Power Consumption:	0W

Port	Admin	Status	Class	Priority	Power (mW)	Voltage (V)	Current (mA)
1	Up	Not Powered	0	Low	0	0	0
2	Up	Not Powered	0	Low	0	0	0
3	Up	Not Powered	0	Low	0	0	0
4	Up	Not Powered	0	Low	0	0	0
5	Up	Not Powered	0	Low	0	0	0
6	Up	Not Powered	0	Low	0	0	0
7	Up	Not Powered	0	Low	0	0	0
8	Up	Not Powered	0	Low	0	0	0

Figure 81. Power Over Ethernet Configuration Page

The Power Over Ethernet Configuration page displays information about the PoE status of each port and also allows you to configure the port's status and priority. The table includes the following items of information:

Admin
The status of the port, either up or down. To change the Admin selection, refer to "Changing the PoE Port's Admin Setting" on page 275.

Status
Whether a PoE device is being powered or not by that port. "Powered" means that the port is providing power to a powered device. "Not Powered" indicates that the device is not a powered device or that no device is connected to the port. You cannot alter this setting.

Class
The IEEE 802.3af class of the device. You cannot change this setting. For more information, refer to "PoE Device Classes" on page 105.

Priority
The port's priority for receiving power from the switch. For more

information about port priority, refer to “Port Prioritization for Power Allocation” on page 105. To set the priority, refer to “Setting the PoE Port's Priority” on page 275.

Power (mW)
The amount of power being delivered to the device, in Milliwatts.

Voltage (V)
The amount of voltage being delivered to the device, in Volts.

Current (mA)
The amount of current being delivered to the device, in Milliamps.

Changing the PoE Port's Admin Setting

To change a port's admin setting from up (online) to down (offline), perform the following procedure:

1. Next to the port you whose status you want to change, select **Up** or **Down** from the Admin list.

2. Click **Apply**.

Setting the PoE Port's Priority

The priority defines which port and its attached PoE powered device should receive priority for the available power over other PoE devices. For more information about port priority, refer to “Port Prioritization for Power Allocation” on page 105.

To select the priority for each port, perform the following procedure:

1. From the Priority list, select one of the following:

   Low - To change the port priority to low. This is the default.

   High - To change the port priority to high.

   Critical - To change the port priority to critical, so that this device continues to receive power even if others do not.

2. Click **Apply**.

Chapter 25
Virtual LANs

This chapter contains the procedures for creating, modifying, and deleting and tagged Virtual Local Area Networks (VLANs) from a web browser management session. This chapter contains the following sections:

Note
For background information, refer to “VLAN Overview” on page 114.

Creating a VLAN

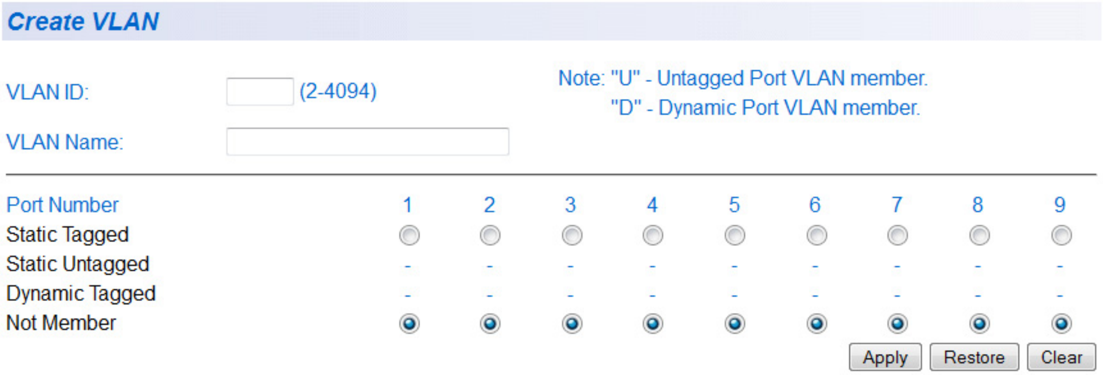
This section contains the procedure for creating a new or tagged VLAN. This procedure assigns the VLAN a name, a VID number, and the untagged and tagged member ports.

After performing this procedure, the PVID values of the untagged ports of the VLAN must be adjusted to match the virtual LAN's VID number. In order for a port to be considered an untagged member of a VLAN, its PVID value must be changed to match the VID of the virtual LAN. This procedure is found in “Configuring the PVID of Untagged Ports” on page 280.

To configure a VLAN, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Config** > **Create VLAN**.

   The Create VLAN page opens, as shown in Figure 82.



Create VLAN

VLAN ID: (2-4094)

VLAN Name:

Note: "U" - Untagged Port VLAN member.
"D" - Dynamic Port VLAN member.

Port Number	1	2	3	4	5	6	7	8	9
Static Tagged	○	○	○	○	○	○	○	○	○
Static Untagged	-	-	-	-	-	-	-	-	-
Dynamic Tagged	-	-	-	-	-	-	-	-	-
Not Member	●	●	●	●	●	●	●	●	●

Figure 82. Create VLAN Page

2. In the **VLAN ID** field, enter a VLAN ID for the new VLAN. The range is 2 to 4094.

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

3. In the **VLAN Name** field, enter a name for the VLAN.

   The name can contain up to 32 characters including spaces but not including special characters such as asterisks (*) or exclamation points (!).

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

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

4. In the **Static Tagged** row, click the buttons of those ports on the switch that are to be tagged or untagged members of the new VLAN.

   While you might assume that the **Static Tagged** row is only used to specify tagged ports of the VLAN, you should use it to specify the untagged ports of a new VLAN as well.

5. Click **Apply** to create the new VLAN.

   The switch creates the VLAN. However, the page does not change. It continues to display the VLAN just created.

6. To create another new VLAN, click **Clear** or repeat this procedure.

7. If the new VLAN contains untagged ports, perform the next procedure, “Configuring the PVID of Untagged Ports” on page 280, to change the PVID of the untagged ports to match the virtual LAN’s VID.

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 is an untagged member of the VLAN whose VID value matches its PVID. A port can be an untagged member of only one VLAN at a time.

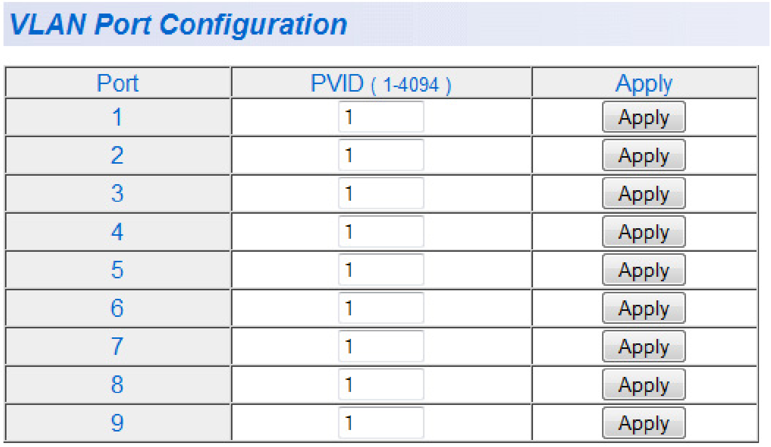
The ports of a new VLAN are initially designated as tagged ports. Their PVID values retain their previous settings when they are assigned to a new VLAN. If you want the ports to function as untagged members of a new VLAN, you must change their PVID values to match the VID of the VLAN, as explained in this 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 adjust the PVID value of a port, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Config. > VLAN Port Config**.

   The VLAN Port Configuration page opens, as shown in Figure 83.



VLAN Port Configuration

Port	PVID (1-4094)	Apply
1	1	Apply
2	1	Apply
3	1	Apply
4	1	Apply
5	1	Apply
6	1	Apply
7	1	Apply
8	1	Apply
9	1	Apply

Figure 83. PVID Page

2. Click the **PVID** field of the port whose value you want to change and enter the new PVID value for the port. The PVID must be equal to the VID of the VLAN where you want the port to be an untagged member.

   For example, to make Port 10 an untagged member of a VLAN that has a VID of 12, you would change its PVID to 12.

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.

3. Click **Apply**.

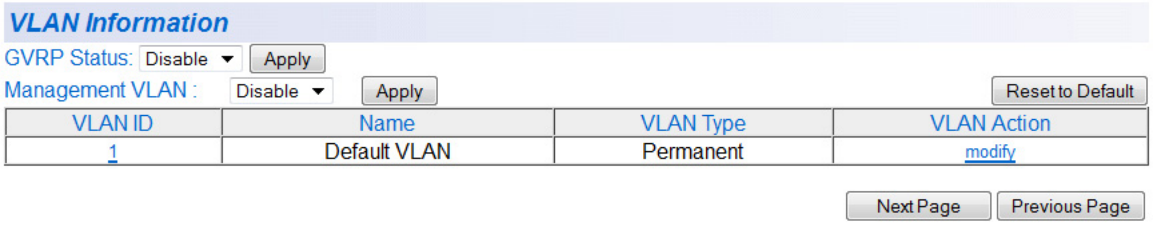
4. Repeat steps 2 and 3 to change the PVID values of other ports.

Displaying the VLANs

To display the VLANs, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Config.** > **VLAN Info**.

   The VLAN Information page opens, as shown in Figure 84.



VLAN Information

GVRP Status: Disable

Management VLAN : Disable

VLAN ID	Name	VLAN Type	VLAN Action
1	Default VLAN	Permanent	modify

Figure 84. VLAN Information Page

   For **GVRP Status**, see See “Enabling or Disabling GVRP” on page 289.

   For **Management VLAN**, see See “Restricting Management VLAN Access” on page 284.

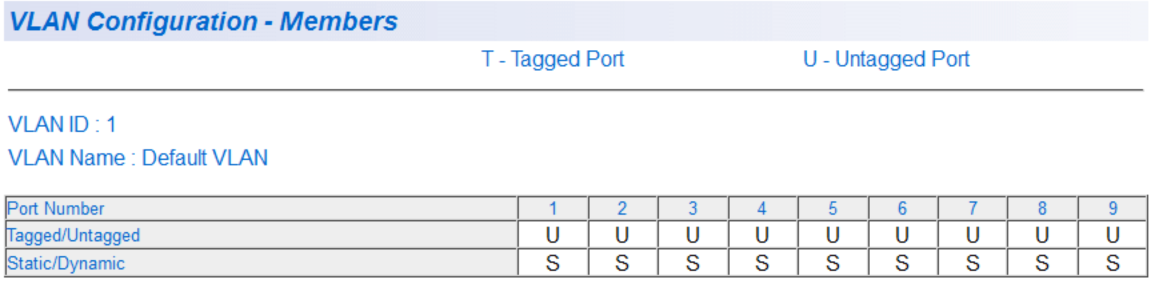
2. The **VLAN Information** page provides the following columns of information:

   VLAN ID
   The VLAN ID number.

   Name
   The VLAN’s name.

   VLAN Type
   The VLAN type as either permanent or static. The Default VLAN is permanent and all other VLANs are static.

3. To view the ports or members of a VLAN, click on the VLAN ID number to view the **VLAN Configuration - Members** page. An example of this page is shown in Figure 85 on page 283.



VLAN Configuration - Members

T - Tagged Port U - Untagged Port

VLAN ID : 1

VLAN Name : Default VLAN

Port Number	1	2	3	4	5	6	7	8	9
Tagged/Untagged	U	U	U	U	U	U	U	U	U
Static/Dynamic	S	S	S	S	S	S	S	S	S

Figure 85. VLAN Configuration - Members Page

Untagged ports of the VLAN are indicated with a “U” and tagged ports with a “T”.

Restricting Management VLAN Access

Management access can be restricted to the default vlan (VLAN 1) or made available on any VLAN. This feature is activated when you select ENABLE in the Management VLAN field. If this field is set to DISABLED, the management access is available on any VLAN.

1. From the Advanced Config menu, select **VLAN Config.** > **VLAN Info**.

   The **VLAN Information** page opens, as shown in Figure 84 on page 282.

2. In the **Management VLAN** field, select **Enable** to restrict the management access in the default vlan (VLAN 1) only or **Disable** to allow management access on any vlan.

3. Click **Apply**.

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 an existing VLAN.
- You cannot add an untagged port to a VLAN using this procedure. That function requires changing a port's VID value, as explained in "Configuring the PVID of Untagged Ports" on page 280
- You cannot remove an untagged port from a VLAN using 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 280.

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

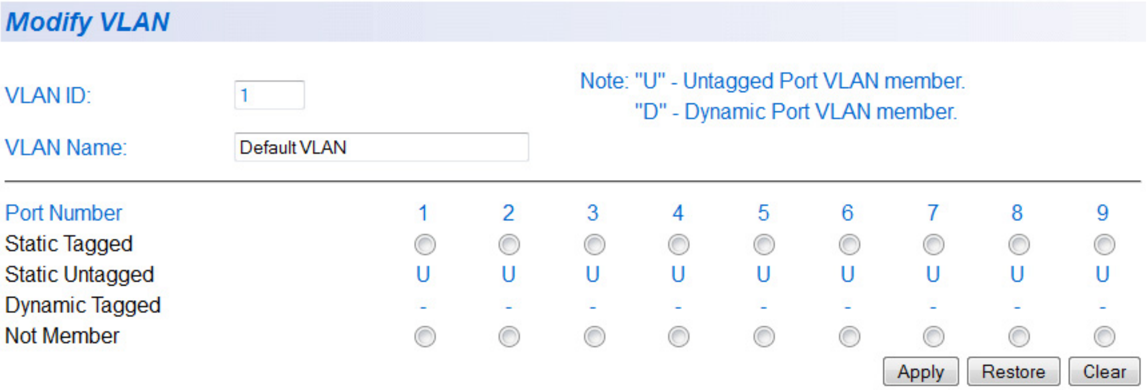
1. From the Advanced Config menu, select **VLAN Config.** > **VLAN Info**.

   The VLAN Information page is shown in Figure 84 on page 282.

   Use the **Next Page** and **Previous Page** buttons to scroll through the list of VLANs.

2. In the **VLAN Action** column, click **Modify** next to the VLAN you want to modify.

   The Modify VLAN page opens, as shown in Figure 86.



Modify VLAN

VLAN ID: 1

VLAN Name: Default VLAN

Note: "U" - Untagged Port VLAN member.
"D" - Dynamic Port VLAN member.

Port Number	1	2	3	4	5	6	7	8	9
Static Tagged	○	○	○	○	○	○	○	○	○
Static Untagged	U	U	U	U	U	U	U	U	U
Dynamic Tagged	-	-	-	-	-	-	-	-	-
Not Member	○	○	○	○	○	○	○	○	○

Figure 86. Modify VLAN Page

3. To change the VLAN’s name, click the **VLAN Name** field and enter the new name.

   The name can contain up to 32 characters including spaces but not including special characters such as asterisks (*) or exclamation points (!).

4. To add a new tagged port to the VLAN, click the button in the **Static Tagged** row of the port to be added as a tagged port.

5. To remove a tagged port from the VLAN, click the button in the **Not Member** row of the port to be removed.

   If you make changes to the VLAN that you want to cancel, click **Restore**. If you want to clear the current name and all tagged port assignments from the VLAN prior to assigning it a new name and new tagged ports, click **Clear**.

6. After you have made the desired changes, click **Apply**.

   The changes are implemented on the VLAN. The current VLAN window remains on the screen. You can make additional changes to the VLAN or you can repeat this procedure to modify other VLANs.

Deleting a VLAN

To delete a VLAN, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Info**.

   The VLAN Information page is shown in Figure 84 on page 282.

2. In the VLAN Action column, click **Delete** next to the VLAN you want to delete.

   A confirmation prompt is displayed.

3. 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.

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

Deleting All VLANs

The following procedure for deletes **all** VLANs, except the Default_VLAN, on a switch. To delete selected VLANs, refer to “Deleting a VLAN” on page 287.

To reset to the default VLAN, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Info**.

   The VLAN Information page is shown in Figure 84 on page 282.

2. Click **Reset to Default**.

   The following prompt is displayed:

   ```
   Reset VLAN configuration to default?
   ```

3. Click **OK** to continue or click **Cancel** to stop the changes.

   The VLAN Information page is redisplayed with ALL VLANs, except the default, deleted.

Enabling or Disabling GVRP

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information. For more information about GVRP, refer to "GVRP" on page 131.

To enable or disable GVRP, perform the following procedure:

1. From the Advanced Config menu, select **VLAN Config.** > **VLAN Info.**

   The VLAN Information page is shown in Figure 84 on page 282.

2. From the GVRP Status list, choose **Enable** or **Disable**.

3. Click **Apply**.

Chapter 26

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 292
- ❐ “Configuring CoS” on page 293

Note
For background information on QoS, refer to “QoS Overview” on page 134

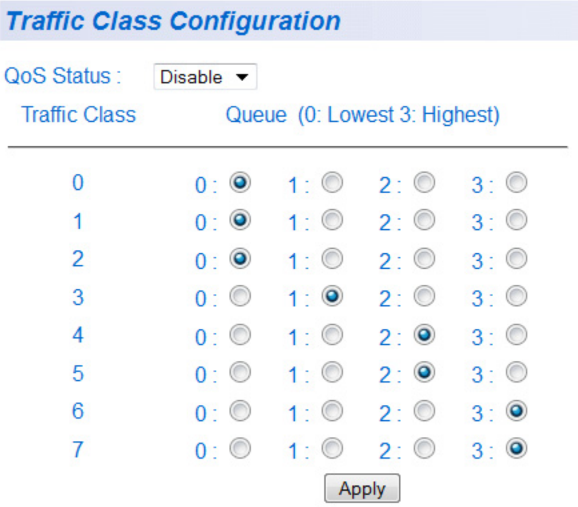
Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, as shown in Table 5 on page 135. 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 Advanced Config menu, select **QoS Config** > **Traffic Class**.

   The Traffic Class Configuration page opens, as shown in Figure 87.



Traffic Class Configuration

QoS Status : Disable ▾

Traffic Class	Queue (0: Lowest 3: Highest)			
0	0 : ●	1 : ○	2 : ○	3 : ○
1	0 : ●	1 : ○	2 : ○	3 : ○
2	0 : ●	1 : ○	2 : ○	3 : ○
3	0 : ○	1 : ●	2 : ○	3 : ○
4	0 : ○	1 : ○	2 : ●	3 : ○
5	0 : ○	1 : ○	2 : ●	3 : ○
6	0 : ○	1 : ○	2 : ○	3 : ●
7	0 : ○	1 : ○	2 : ○	3 : ●

Figure 87. Traffic Class Configuration Page

2. To enable or disable QoS, select **Enable** or **Disable** from the QoS Status list. The default is disabled.

3. 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, you would click the button for queue 3 in the priority 4 row.

4. 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 134, 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 5 on page 135.

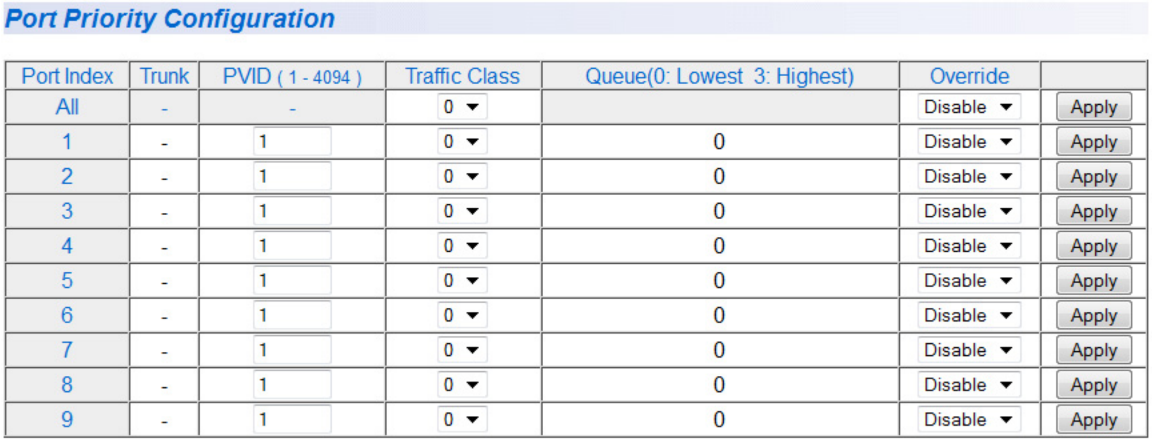
You can override the mappings at the port level by assigning a new default egress queue to a port. Note that this assignment is made on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port. For example, you can configure 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 Advanced Config menu, select **QoS Config** > **Port Priority**.

   The Port Priority Configuration page opens, as shown in Figure 88.



Port Priority Configuration

Port Index	Trunk	PVID (1 - 4094)	Traffic Class	Queue(0: Lowest 3: Highest)	Override	
All	-	-	0		Disable	Apply
1	-	1	0	0	Disable	Apply
2	-	1	0	0	Disable	Apply
3	-	1	0	0	Disable	Apply
4	-	1	0	0	Disable	Apply
5	-	1	0	0	Disable	Apply
6	-	1	0	0	Disable	Apply
7	-	1	0	0	Disable	Apply
8	-	1	0	0	Disable	Apply
9	-	1	0	0	Disable	Apply

Figure 88. Port Priority Configuration Page

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
Enter the traffic class's current egress priority.

Queue
Displays the number of the queue where untagged packets received on the port are stored on the egress queue.

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.

2. To change the egress queue where ingress untagged frames received on a port are to be stored on the egress port, refer to Table 5 on page 135. 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.

3. 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.

4. 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 27
IGMP

This chapter contains the following procedures for working with the Internet Group Management Protocol (IGMP):

- "Configuring IGMP" on page 296

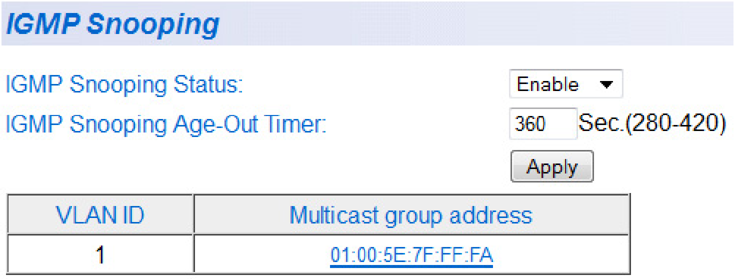
Note
For background information on IGMP, refer to "IGMP Snooping Overview" on page 146.

Configuring IGMP

To configure the IGMP settings, perform the following procedure:

1. From the Advanced Config menu, select **IGMP Snooping**.

   The IGMP Snooping page opens, as shown in Figure 89.



IGMP Snooping

IGMP Snooping Status: Enable

IGMP Snooping Age-Out Timer: 360 Sec.(280-420)

VLAN ID	Multicast group address
1	01:00:5E:7F:FF:FA

Figure 89. IGMP Snooping Page

2. To enable or disable IGMP, select **Enable** or **Disable** from the IGMP Snooping Status list.

3. To set the age-out timer, type a number in the IGMP Snooping Age-Out Timer field.

   The range is 280 to 420 seconds and the default is 360 seconds.

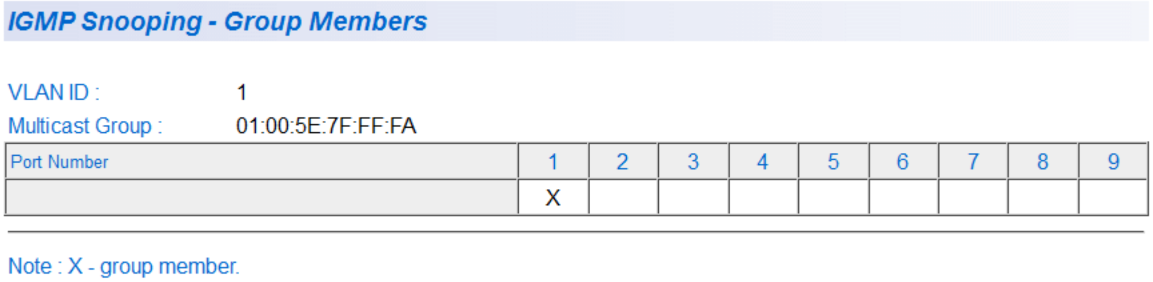
Viewing the Multicast Group Members

1. From the Advanced Config menu, select **IGMP Snooping**.

   The IGMP Snooping page is shown in Figure 89 on page 296.

2. Click on the Mac address in the **Multicast group address** column that you want to view.

   The IGMP Snooping - Group Members page opens, as shown in Figure 90.



IGMP Snooping - Group Members

VLAN ID : 1

Multicast Group : 01:00:5E:7F:FF:FA

Port Number	1	2	3	4	5	6	7	8	9
	X								

Note : X - group member.

Figure 90. IGMP Snooping - Group Members Page

Chapter 28
RSTP

This chapter contains the following procedures for working with the Remote Spanning Tree Protocol (RSTP):

- “Basic RSTP Configuration” on page 301
- “Configuring RSTP Port Settings” on page 303
- “Viewing the RSTP Topology” on page 306

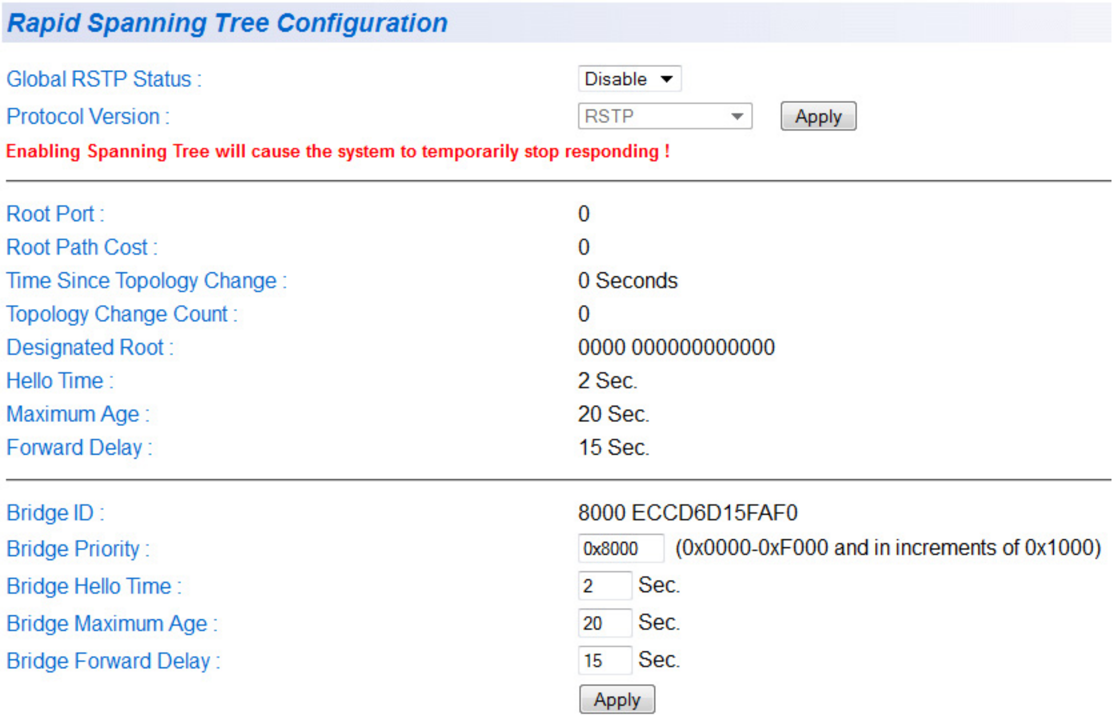
Note
For background information on RSTP, refer to “RSTP Overview” on page 154.

Enabling or Disabling RSTP and STP Compatibility

To enable or disable RSTP globally for all ports, and set the STP compatibility, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** > **RSTP Config**.

   The Rapid Spanning Tree Configuration page opens, as shown in Figure 91.



Rapid Spanning Tree Configuration

Global RSTP Status : Disable

Protocol Version : RSTP

Enabling Spanning Tree will cause the system to temporarily stop responding !

Root Port : 0

Root Path Cost : 0

Time Since Topology Change : 0 Seconds

Topology Change Count : 0

Designated Root : 0000 000000000000

Hello Time : 2 Sec.

Maximum Age : 20 Sec.

Forward Delay : 15 Sec.

Bridge ID : 8000 ECCD6D15FAF0

Bridge Priority : 0x8000 (0x0000-0xF000 and in increments of 0x1000)

Bridge Hello Time : 2 Sec.

Bridge Maximum Age : 20 Sec.

Bridge Forward Delay : 15 Sec.

Figure 91. Rapid Spanning Tree Configuration Page

2. From the **Global RSTP Status** list, choose one of the following:

   Enable - Enables RSTP.

   Disable - Disables RSTP.

3. From the **Protocol Version** list, choose one of the following:

   STP - Makes the ports STP compatible.

   RSTP - Makes the ports operate only in RSTP mode.

4. Click **Apply**.

Basic RSTP Configuration

To configure the RSTP settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** > **RSTP Config**.

   The Rapid Spanning Tree Configuration page is shown in Figure 91 on page 300.

   The RSTP Configuration page 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 157. 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 and 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.

Configuring RSTP Port Settings

This section contains the following topics:

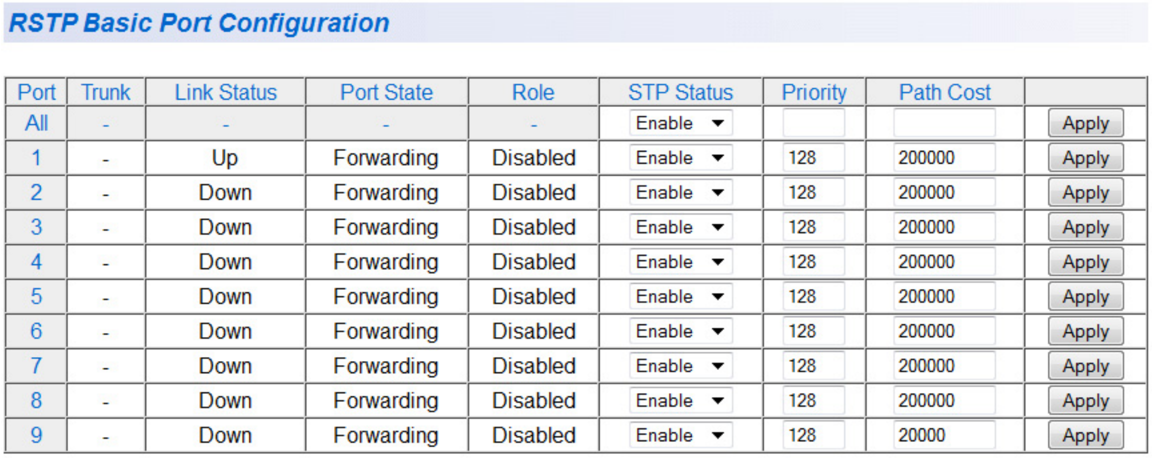
- "Configuring the Basic RSTP Port Settings," next
- "Configuring the Advanced RSTP Port Settings" on page 304

Configuring the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** > **RSTP Basic Port Config**.

   The RSTP Basic Port Configuration page opens, as shown in Figure 92.



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	-	Down	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	20000	Apply

Figure 92. RSTP Basic Port Configuration Page

2. In the **STP Status** column for the port you want to configure, select either **Enable** or **Disable** for the STP status.

3. 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 156.

4. 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 155.

5. Click **Apply**.

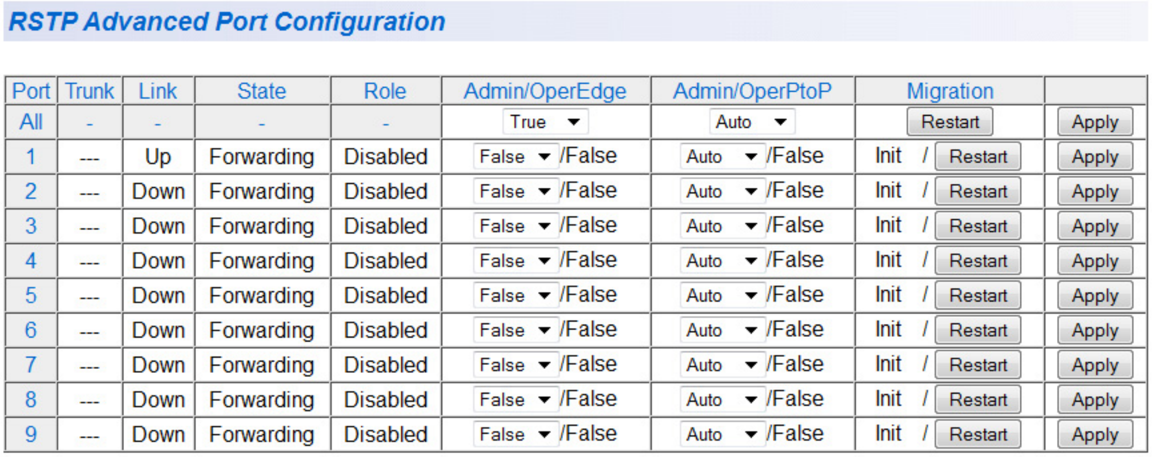
6. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: STP Status, Priority, and Path Cost. Click **Apply**.

Configuring the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** > **RSTP Adv. Port Config**.

   The RSTP Advanced Port Configuration page opens, as shown in Figure 93.



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	---	Down	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

Figure 93. RSTP Advanced Port Configuration Page

2. 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.

3. In the **Admin/OperPtoP** column for the port you want to configure, choose a setting based on the information in Table 10.

Table 10. 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

4. In the Migration column for the port you want to configure, click **Restart** to reset the port.

5. Click **Apply**.

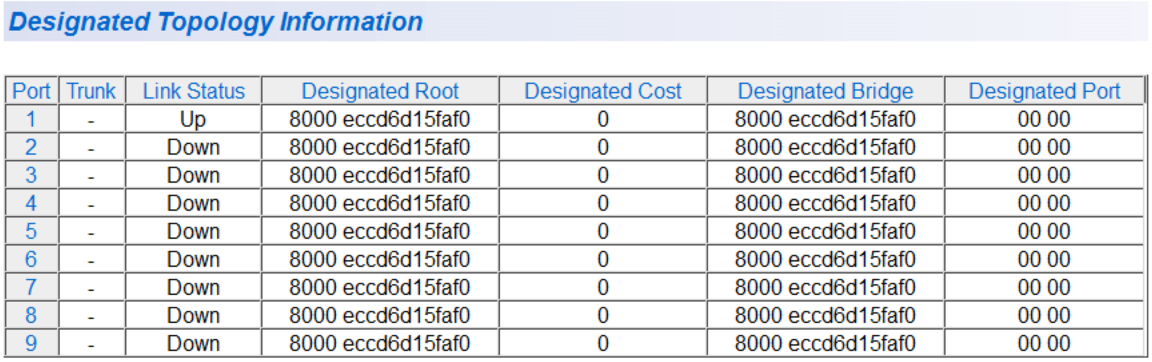
6. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: Admin/OperEdge, Admin/OperPtoP, and Migration. Click **Apply**.

Viewing the RSTP Topology

To view the current RSTP topology, perform the following procedure:

1. From the Basic Config menu, select **Rapid Spanning Tree** > **RSTP Topology**.

   The Designated Topology Information page opens, as shown in Figure 94.



Designated Topology Information

Port	Trunk	Link Status	Designated Root	Designated Cost	Designated Bridge	Designated Port
1	-	Up	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
2	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
3	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
4	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
5	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
6	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
7	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
8	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00
9	-	Down	8000 eccd6d15faf0	0	8000 eccd6d15faf0	00 00

Figure 94. Designated Topology Information Page

This page displays the following information about the ports:

Trunk
The trunk of which the port is a member.

Link Status
Whether the link on the port is up or down.

Designated Root
The designated root bridge to which the switch's root port is actively connected.

Designated Cost
The sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Designated Bridge
An adjacent bridge to which the root port of the switch is actively connected.

Designated Port
The root bridge to which the root port of the switch is actively connected.

Chapter 29

802.1x Network Access Control

This chapter contains the procedure for configuring 802.1x network access control:

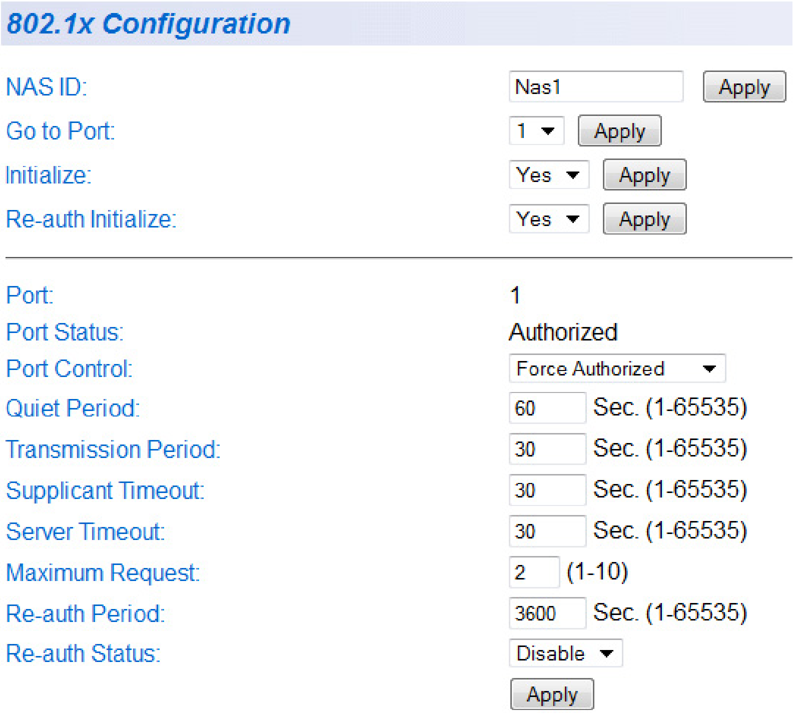
Note
For background information, refer to “802.1x Network Access Control Overview” on page 176.

Configuring 802.1x Network Access Control

To configure 802.1x network access control, perform the following procedure:

1. From the Advanced Config menu, select **802.1x**.

   The 802.1x Configuration page opens, as shown in Figure 95.



802.1x Configuration

NAS ID: Nas1

Go to Port: 1

Initialize: Yes

Re-auth Initialize: Yes

Port: 1

Port Status: Authorized

Port Control: Force Authorized

Quiet Period: 60 Sec. (1-65535)

Transmission Period: 30 Sec. (1-65535)

Supplicant Timeout: 30 Sec. (1-65535)

Server Timeout: 30 Sec. (1-65535)

Maximum Request: 2 (1-10)

Re-auth Period: 3600 Sec. (1-65535)

Re-auth Status: Disable

Figure 95. 802.1x Configuration Page

Note
The Initialize and Re-auth Initialize parameters are described in Steps 5 and 6, respectively.

2. To select a port, do the following:

   a. Click on the **Go To Port** field and select the port you want to configure from the list. You can configure only one port at a time.

   b. Click **Apply**.

   The current settings for the selected port are displayed.

3. Configure the following parameters as needed:

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. You cannot adjust this parameter.

Port Control

Sets the 802.1x port control setting. The possible settings are:

> Auto - Enables 802.1x 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 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

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.

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.

Supplicant Timeout

Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Server Timeout

Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 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-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.

4. When you are finished configuring the parameters, click **Apply**.

5. 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**.

6. 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 30

RADIUS Authentication Protocol

This chapter explains how to configure the RADIUS client on the switch. You can use the RADIUS client with 802.1x network access control to control who can forward packets through the switch. The chapter contains the following section:

❒ “Configuring the RADIUS Client” on page 312

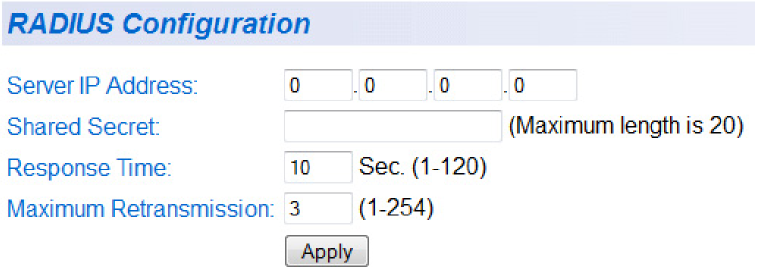
Note
For background information, refer to “802.1x Network Access Control Overview” on page 176 and “RADIUS Overview” on page 190.

Configuring the RADIUS Client

To configure the RADIUS client, perform the following procedure:

1. From the Basic Config menu, select **User Interface** > **RADIUS Config**.

   The RADIUS Configuration page opens, as shown in Figure 96.



RADIUS Configuration

Server IP Address: 0 . 0 . 0 . 0

Shared Secret: (Maximum length is 20)

Response Time: 10 Sec. (1-120)

Maximum Retransmission: 3 (1-254)

Figure 96. RADIUS Configuration Page

2. Enter the RADIUS server’s IP address in the **Server IP Address** field.

3. To specify the server’s encryption key, enter the encryption key in the **Shared Secret** field.

4. To change the response time setting, enter a value in the **Response Time** field.

   The response time is the amount of time in seconds the switch waits for a response from the RADIUS server. The range is 1 to 120 seconds. The default is 10 seconds.

5. To change the maximum retransmissions setting, enter a new value in the **Maximum Retransmissions** field.

   This parameter specifies the number of times the switch should retransmit to the RADIUS in the event the server does not respond. The range is 1 to 254. The default is 3.

6. Click **Apply** to save your changes.

Chapter 31

Broadcast Storm Control

This chapter contains the procedure for configuring the broadcast storm control feature on the switch:

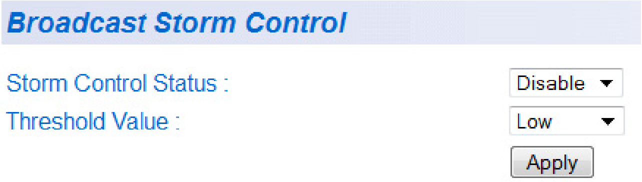
Note
For background information on broadcast storm control, refer to “Broadcast Storm Control Overview” on page 196.

Configuring Broadcast Storm Control

To configure the broadcast storm control feature, perform the following procedure:

1. From the Basic Config menu, select **Storm Control**.

   The Broadcast Storm Control page opens, as shown in Figure 97.



Broadcast Storm Control

Storm Control Status : Disable

Threshold Value : Low

Figure 97. Broadcast Storm Control Page

2. From the Storm Control Status list, select **Enable** to activate the feature or **Disable** to deactivate it. The default setting is disabled.

3. If you are activating the feature, from the Threshold Value list select the desired threshold. Possible values are:

   - **High** - 3000 broadcast packets per second
   - **Medium** - 500 broadcast packets per second
   - **Low** - 100 broadcast packets per second

4. Click **Apply**.

Chapter 32

MAC Address Tables

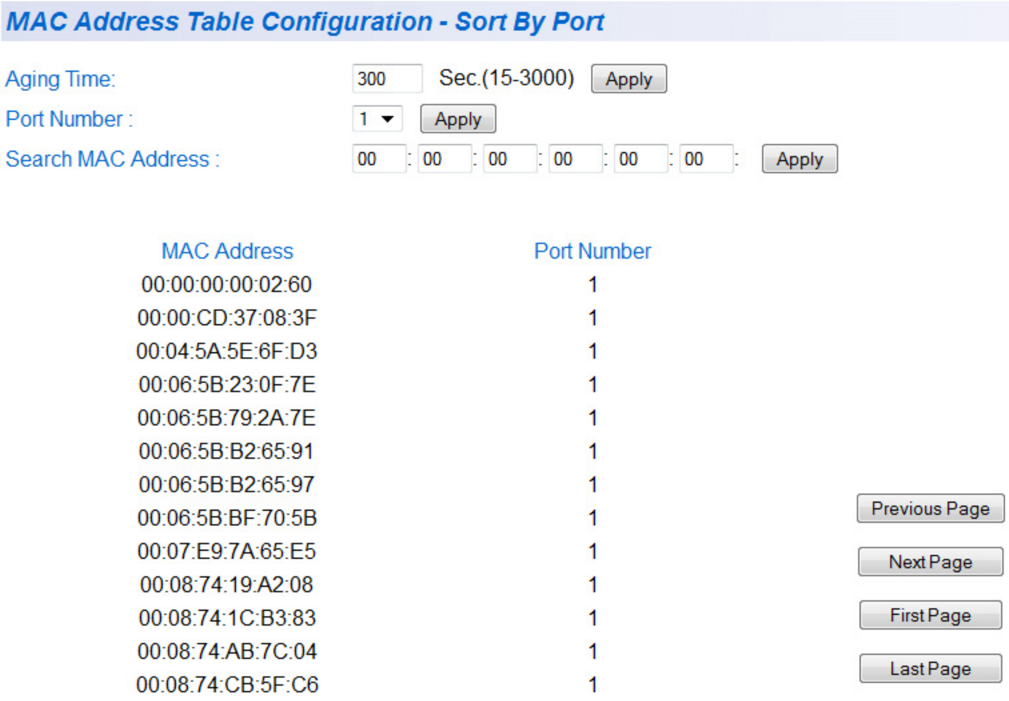
This chapter contains the procedures for viewing the MAC address table and contains the following sections:

Displaying the MAC Address Tables

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

1. From the Basic Config. menu, select **MAC Address Table** > **Sort by Port**.

   The MAC Address by Port page opens, as shown Figure 98.



MAC Address Table Configuration - Sort By Port

Aging Time: 300 Sec.(15-3000) Apply

Port Number : 1 Apply

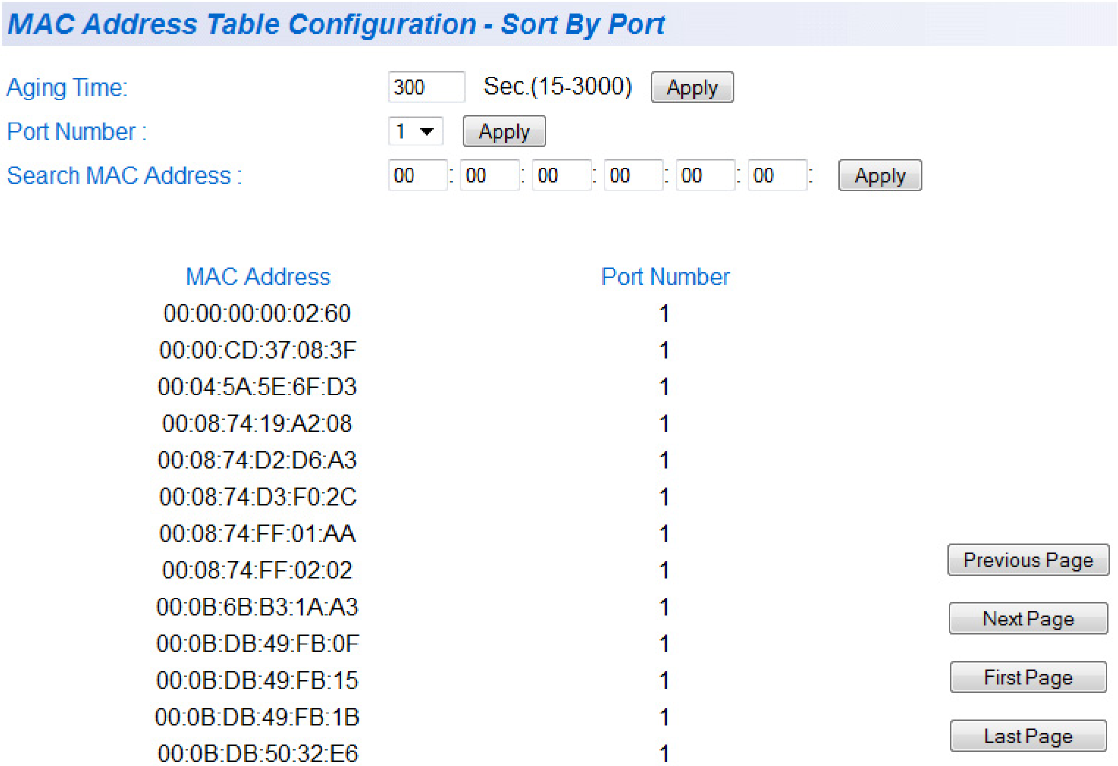
Search MAC Address : 00 : 00 : 00 : 00 : 00 : 00 : Apply

MAC Address	Port Number
00:00:00:00:02:60	1
00:00:CD:37:08:3F	1
00:04:5A:5E:6F:D3	1
00:06:5B:23:0F:7E	1
00:06:5B:79:2A:7E	1
00:06:5B:B2:65:91	1
00:06:5B:B2:65:97	1
00:06:5B:BF:70:5B	1
00:07:E9:7A:65:E5	1
00:08:74:19:A2:08	1
00:08:74:1C:B3:83	1
00:08:74:AB:7C:04	1
00:08:74:CB:5F:C6	1

Figure 98. MAC Address by Port Page

2. From the **Port Number** list, select the port and click **Apply**.

   The list of MAC addresses for that port is displayed, as shown in Figure 99 on page 317.



MAC Address Table Configuration - Sort By Port

Aging Time: 300 Sec.(15-3000)

Port Number : 1

Search MAC Address : 00 : 00 : 00 : 00 : 00 : 00 :

MAC Address	Port Number
00:00:00:00:02:60	1
00:00:CD:37:08:3F	1
00:04:5A:5E:6F:D3	1
00:08:74:19:A2:08	1
00:08:74:D2:D6:A3	1
00:08:74:D3:F0:2C	1
00:08:74:FF:01:AA	1
00:08:74:FF:02:02	1
00:0B:6B:B3:1A:A3	1
00:0B:DB:49:FB:0F	1
00:0B:DB:49:FB:15	1
00:0B:DB:49:FB:1B	1
00:0B:DB:50:32:E6	1

Figure 99. MAC Address Table by Port Page

3. To locate a specific MAC address, in the **Search MAC Address** field, enter the MAC address you want to search for and click **Apply**.

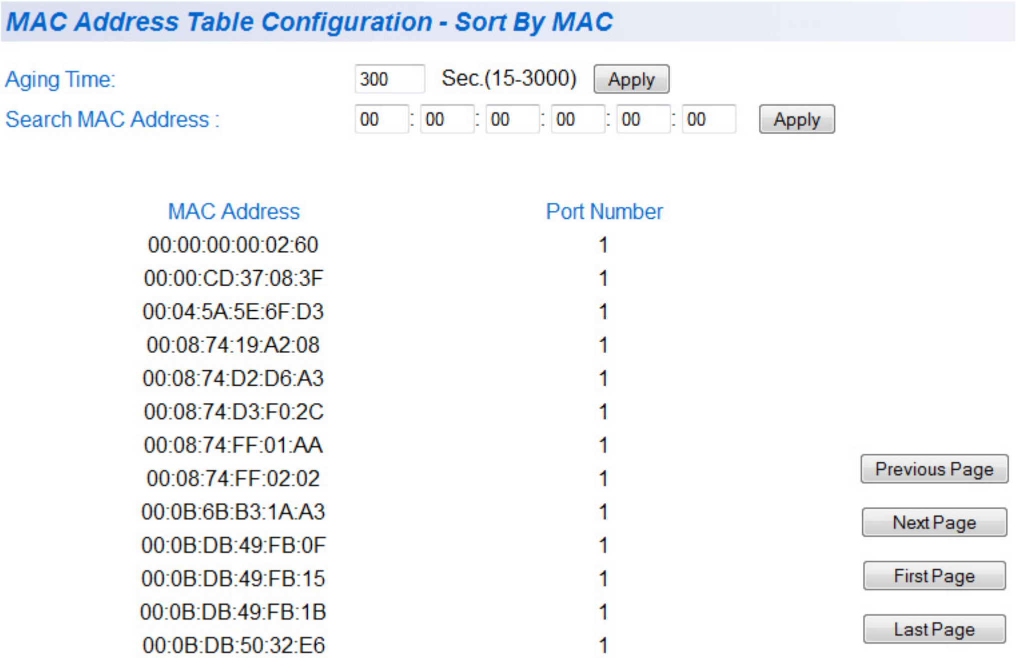
   If the MAC address exists in the MAC address table, a message is displayed stating the MAC address and its associated port number. If the MAC address does not exist, a “Not Found” message is displayed.

Displaying the MAC Addresses by MAC

To display the MAC addresses in alphanumeric order, perform the following procedure.

1. From the Basic Config. menu, select **MAC Address Table** > **Sort by MAC**.

   The MAC Address by MAC page opens, as shown in Figure 100.



MAC Address Table Configuration - Sort By MAC

Aging Time: 300 Sec.(15-3000) Apply

Search MAC Address : 00 : 00 : 00 : 00 : 00 : 00 Apply

MAC Address	Port Number
00:00:00:00:02:60	1
00:00:CD:37:08:3F	1
00:04:5A:5E:6F:D3	1
00:08:74:19:A2:08	1
00:08:74:D2:D6:A3	1
00:08:74:D3:F0:2C	1
00:08:74:FF:01:AA	1
00:08:74:FF:02:02	1
00:0B:6B:B3:1A:A3	1
00:0B:DB:49:FB:0F	1
00:0B:DB:49:FB:15	1
00:0B:DB:49:FB:1B	1
00:0B:DB:50:32:E6	1

Figure 100. MAC Address by MAC Page

2. To locate a specific MAC address, in the **Search MAC Address** field, enter the MAC address you want to search for and click **Apply**.

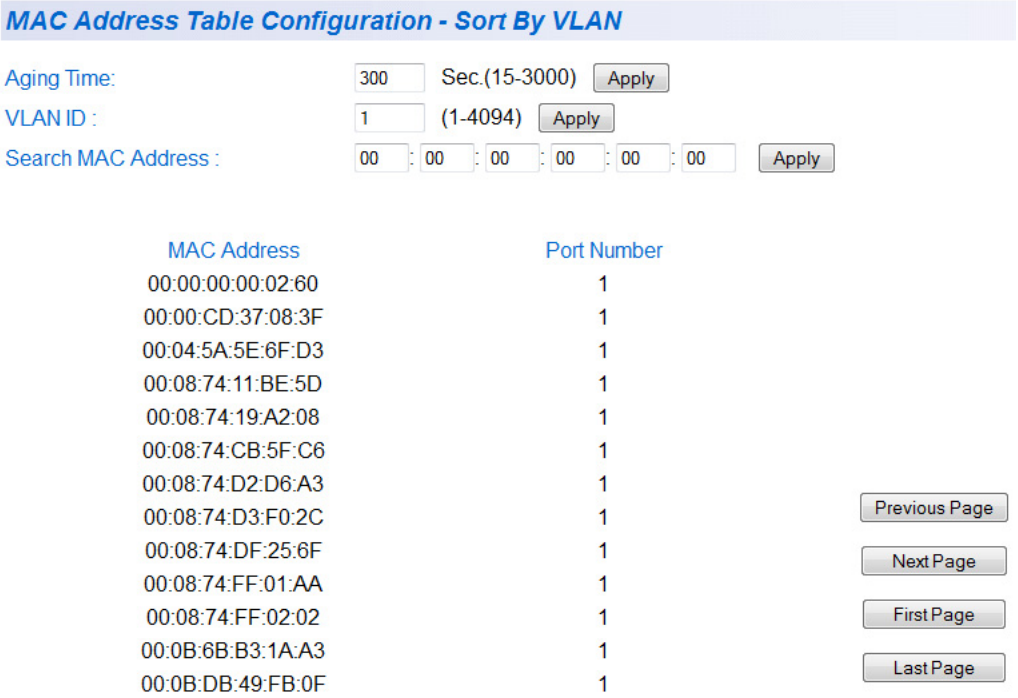
   If the MAC address exists in the MAC address table, a message is displayed stating the MAC address and its associated port number. If the MAC address does not exist, a “Not Found” message is displayed.

Displaying the MAC Addresses by VLAN ID

To display the MAC addresses associated with a particular VLAN ID, perform the following procedure:

1. From the Basic Config. menu, select **MAC Address Table** > **Sort by VLAN**.

   The **Sort by VLAN** page is displayed, as shown in Figure 101, with information for the default VLAN, VLAN ID 1.



MAC Address Table Configuration - Sort By VLAN

Aging Time: 300 Sec.(15-3000)

VLAN ID : 1 (1-4094)

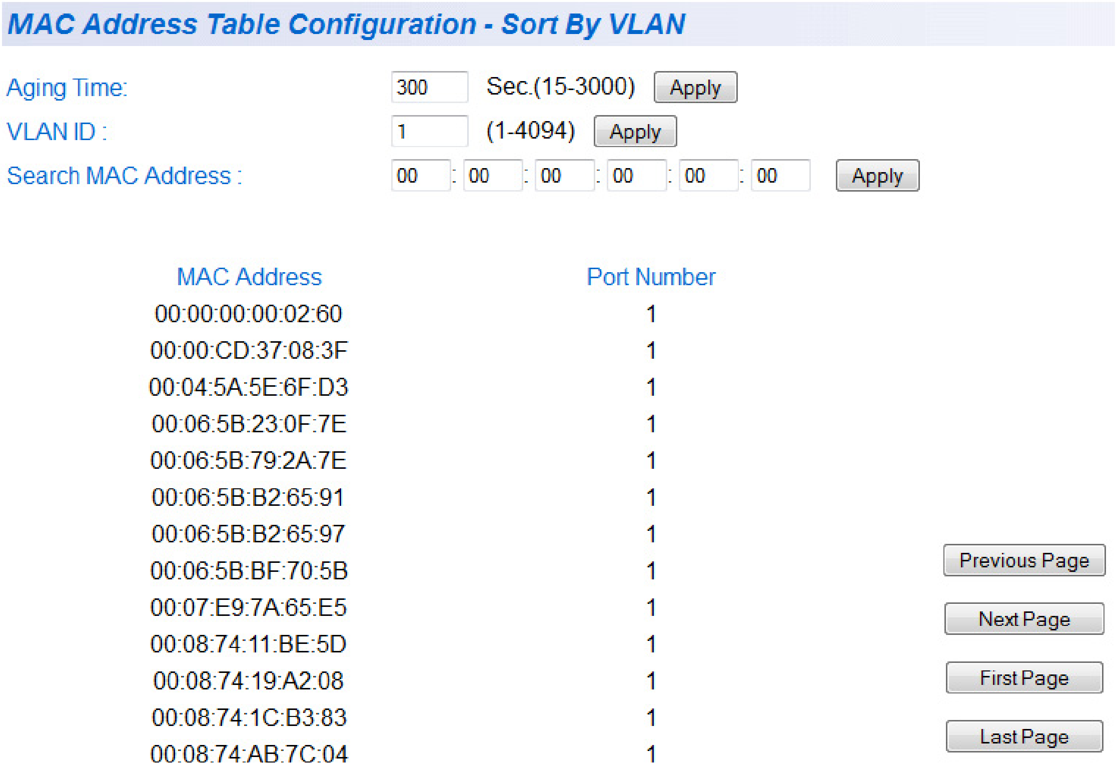
Search MAC Address : 00 : 00 : 00 : 00 : 00 : 00

MAC Address	Port Number
00:00:00:00:02:60	1
00:00:CD:37:08:3F	1
00:04:5A:5E:6F:D3	1
00:08:74:11:BE:5D	1
00:08:74:19:A2:08	1
00:08:74:CB:5F:C6	1
00:08:74:D2:D6:A3	1
00:08:74:D3:F0:2C	1
00:08:74:DF:25:6F	1
00:08:74:FF:01:AA	1
00:08:74:FF:02:02	1
00:0B:6B:B3:1A:A3	1
00:0B:DB:49:FB:0F	1

Figure 101. MAC Addresses by VLAN Page

2. In the **VLAN ID** field, enter the VLAN ID for the VLAN you want to search and click **Apply**.

   The page is redisplayed to show the MAC addresses associated with that VLAN, as shown in Figure 102 on page 320.



MAC Address Table Configuration - Sort By VLAN

Aging Time: 300 Sec.(15-3000)

VLAN ID : 1 (1-4094)

Search MAC Address : 00 : 00 : 00 : 00 : 00 : 00

MAC Address	Port Number
00:00:00:00:02:60	1
00:00:CD:37:08:3F	1
00:04:5A:5E:6F:D3	1
00:06:5B:23:0F:7E	1
00:06:5B:79:2A:7E	1
00:06:5B:B2:65:91	1
00:06:5B:B2:65:97	1
00:06:5B:BF:70:5B	1
00:07:E9:7A:65:E5	1
00:08:74:11:BE:5D	1
00:08:74:19:A2:08	1
00:08:74:1C:B3:83	1
00:08:74:AB:7C:04	1

Figure 102. MAC Addresses by VLAN Page

3. To locate a specific MAC address, in the **Search MAC Address** field, enter the MAC address you want to search for and click **Apply**.

   If the MAC address exists in the MAC address table, a message is displayed stating the MAC address and its associated port number. If the MAC address does not exist, a “Not Found” message is displayed.

Setting the Aging Time

To set the aging time, perform the following procedure:

1. From the Basic Config. menu, select **MAC Address Table** and one of MAC address table display options.

2. On the MAC address display page, for the aging time, type a number and click **Apply**.

   The default is 300 seconds (5 minutes) and the range is 15 to 3000 seconds.

Chapter 33

Working With System Files

The procedures in this chapter include:

- "Downloading a New Management Software Image Using TFTP" on page 324

> **Note**
> For information on how to obtain new releases of the AT-S81 management software, refer to "Contacting Allied Telesis" on page 15.

- "Uploading or Downloading the Configuration File" on page 326

Downloading a New Management Software Image Using TFTP

Before downloading a new version of the AT-S81 management software onto the switch, note the following:

- The current configuration of a switch is retained when a new AT-S81 software image is installed. To return a switch to its default configuration values, refer to "Returning the AT-S81 Management Software to the Factory Default Values" on page 59.
- Your network must have a node with TFTP server software.
- You must store the new AT-S81 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-S81 image software onto the switch, perform the following procedure:

1. From the Tools menu, select **Image Upgrade**.

   The Image Upgrade page opens, as shown in Figure 103.

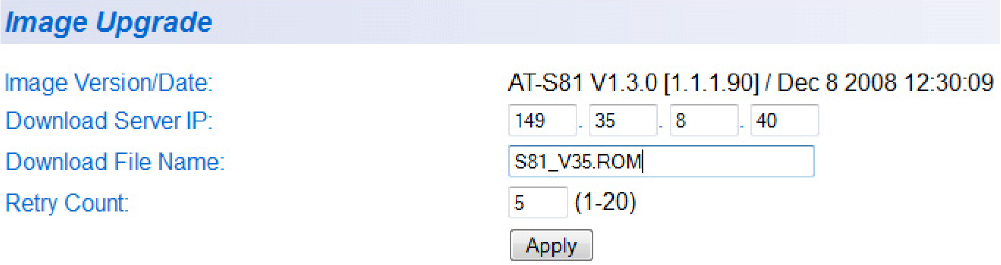


Image Upgrade

Image Version/Date:	AT-S81 V1.3.0 [1.1.1.90] / Dec 8 2008 12:30:09
Download Server IP:	149 . 35 . 8 . 40
Download File Name:	S81_V35.ROM
Retry Count:	5 (1-20)

Figure 103. Image Upgrade Page

   The Image/Version Date shows the current version and date of software installed on the switch.

2. In the **Download Server IP** field, enter The IP address of the TFTP server from which you are downloading the new software.

3. In the **Download File Name** field, enter the name of the AT-S81 file you are downloading.

4. In the **Retry Count** field, 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.

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.

Uploading or Downloading the Configuration File

The procedure in this section allows you to download a different configuration file onto the switch from a TFTP server, or upload the file to a TFTP server. To return a switch to its default configuration values, refer to “Returning the AT-S81 Management Software to the Factory Default Values” on page 244.

> **Note**
> The configuration file contains only those settings that have been changed since the switch was last reset to the default settings.

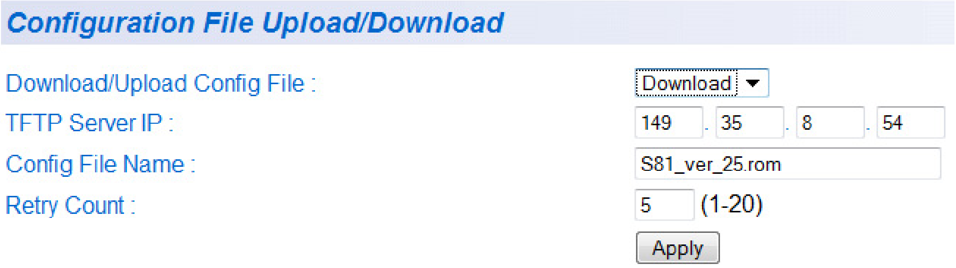
Before downloading a configuration file onto the switch, note the following:

- ❐ Your network must have a node with TFTP server software.
- ❐ You must store the new configuration file on the TFTP server.
- ❐ You should start the TFTP server software before you begin the download procedure.
- ❐ The switch where you are downloading the configuration 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.
- ❐ When you download a new configuration file onto the switch, the new file overrides the current file and the current file is lost unless you uploaded it to a TFTP server before you replaced it.

To download or upload a configuration file, perform the following procedure:

1. From the Tools menu, select **Config. File Upload/Download**.

   The Configuration File Upload/Download page opens, as shown in Figure 104.



Configuration File Upload/Download

Download/Upload Config File : Download

TFTP Server IP : 149 . 35 . 8 . 54

Config File Name : S81_ver_25.rom

Retry Count : 5 (1-20)

Figure 104. Configuration File Upload/Download Page

2. From the Download/Upload Config File list, choose **Upload** to upload a file to the TFTP server, or **Download** to download the configuration file from the TFTP server to the switch.

3. Change the following parameters as necessary:

   TFTP Server IP
   The IP address of the TFTP server.

   Config File Name
   The name of the configuration file. There is no default name for the configuration file.

   Retry Count
   The number of times you want the switch to retry in the event a problem occurs during the upload or download process. The range is 1 to 20, and the default is 5 times.

4. Click **Apply**.

   The following message is displayed:

   ```
   Are you sure you want to Upload/Download the new
   configuration file?
   ```

5. Click **OK** to continue, or **Cancel** to stop the process.

Section III

Using the Command Line Interface

The chapter in this section provides information for using the command line interface in the AT-S81 management software.

Note
The menus interface is described in Section I, “Using the Menus Interface” on page 17, and the web browser interface is described in Section II, “Using the Web Browser Interface” on page 215.

Chapter 32

Getting Started with the Command Line Interface

This chapter describes the command modes of the AT-S81 management software command line interface and how to access them. This chapter includes the following sections:

CLI Command Modes Introduction

The Command Line interface in the AT-S81 software is accessible from the Main Menu. The commands offer the same functionality as the Menu interface. For instructions on how to access the command line interface, see “Starting the Command Line Interface” on page 342. This chapter describes the CLI command modes and how to access the command line interface. In addition, it provides command formatting information.

In the AT-S81 software, there is a hierarchy of commands which are called command modes. There are five command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- VLAN Configuration

When you enter the CLI interface, you access the User EXEC command mode automatically. This is the first command mode level and it allows you access to the basic switch commands. Each command mode contains a subset of commands that are available within that mode only. As a result, you enter commands according to which command mode you have accessed. For example, port-specific commands are available from the Interface Configuration mode.

You must access the first three command modes (User EXEC, Privilege EXEC, and Global Configuration modes) in the order that they are listed. You can access both the Interface Configuration and VLAN Configuration modes from the Global Configuration mode. The AT-S81 prompt changes to indicate which mode you are accessing.

To access the Privilege EXEC, Global Configuration, Interface, and VLAN Configuration modes, you must enter a specific command that permits entry to a new mode. Each time you change modes, the prompt changes to indicate the mode. See Table 11 on page 333 for information about the commands used to access the modes and their respective prompts. In addition, there are commands that allow you to move between the modes and return to the Main Menu. For example, typing the EXIT command when you are in the Interface Configuration mode returns you to the Global Configuration mode. From all the command modes, the LOGOUT command exits the command line interface and returns you to the Main Menu.

If you enter a command that is not accessible in a particular command mode, the software displays a “command not found” message. For example, you can enter the SHOW SNMP command from the Privileged

EXEC command mode, but you cannot enter this command from the VLAN Configuration mode.

Command Formatting Conventions

The following formatting conventions are used in this manual:

- `screen text font` - This font illustrates the format of a command and command examples.
- *`screen text font`* - Italicized screen text indicates a variable for you to enter.
- [ ] - Brackets indicate optional parameters.
- | - Vertical line separates parameter options for you to choose from.

See the following sections for a description of each command mode, including a list of the commands available from each mode.

- "User EXEC Command Mode" on page 334
- "Privileged EXEC Command Mode" on page 335
- "Global Configuration Command Mode" on page 335
- "Interface Configuration Command Mode" on page 338
- "VLAN Configuration Command Mode" on page 340

Table 11. Command Modes

Command Mode	Prompt	Enter and Exit Commands
User EXEC mode	Switch>	❒ Access this command mode by typing "C" at the Main Menu. This is the default command mode. ❒ Enter the LOGOUT or EXIT commands to quit the command mode and return to the Main Menu.
Privileged EXEC mode	Switch#	❒ Access this mode from the User EXEC mode with the ENABLE command. ❒ Enter the DISABLE or EXIT commands to return to the User EXEC mode. ❒ Enter the LOGOUT command to quit the command mode and return to the Main Menu.
Global Configuration mode	Switch(config)#	❒ Enter the CONFIGURE command to enter this mode from the Privileged EXEC mode. ❒ Enter the END or EXIT commands to return to the Privileged EXEC mode. ❒ Enter the LOGOUT command to quit the command mode and return to the Main Menu.

Table 11. Command Modes (Continued)

Command Mode	Prompt	Enter and Exit Commands
Interface Configuration	Switch(config-if)#	❐ From the Global Configuration mode, type: `interface Ethernet1/`*`port`* ❐ Enter the END or EXIT commands to return to the Global Configuration mode. ❐ Enter the LOGOUT command to quit the command mode and return to the Main Menu.
VLAN Configuration	Switch(config-vlan)#	❐ From the Global Configuration mode, type: `interface vlan`*`id`* ❐ Enter the END or EXIT commands to return to the Global Configuration mode. ❐ Enter the LOGOUT command to quit the command mode and return to the Main Menu.

User EXEC Command Mode

The User EXEC command mode is the default command mode that is available from the Main Menu. It permits access to basic commands. To access any of the other modes, you must first access the User EXEC mode. The commands in the User EXEC mode are accessible from any of the other modes with the exception of the ENABLE command which is only accessible from the User EXEC mode. The prompt changes to Switch> to indicate the User EXEC mode.

See Table 12 for a list of the commands that can be accessed from the User EXEC mode and a brief description of each command.

Table 12. User EXEC Command Mode Commands

Command	Definition
ENABLE	Changes mode from the User EXEC mode to the Privilege EXEC mode.
EXIT	Exits the User EXEC mode and returns you to the Main Menu.
LOGOUT	Exits the command line interface and returns you to the Main Menu.
MODE	Displays the available command modes.
PING	Pings a specified IP address to check connectivity to another system.

Privileged EXEC Command Mode

The commands in the Privileged EXEC command mode permit you to perform system level commands such as rebooting the system, copying configuration files, and clearing statistics. To access this mode, you must first access the User EXEC command mode. The prompt changes to Switch# to indicate the Privileged EXEC mode.

See Table 13 for a list of commands that can be access from the Privileged EXEC command mode.

Table 13. Privileged EXEC Command Mode Commands

Command	Description
CLEAR	Clears the interface (port) statistics counter.
CONFIGURE	Changes the mode to the Global Configuration Mode.
COPY	Uploads the configuration file to an image or configuration file.
DISABLE	Exits from the Privileged EXEC command mode to the User EXEC command mode.
EXIT	Exits from the Privileged EXEC command mode to the User EXEC command mode.
LOGOUT	Exits the command line interface and returns to the Main Menu.
MODE	Displays the available modes.
PING	Pings a specified IP address to check connectivity to another system.
REBOOT	Reboots the system.
SHOW	Displays running system information.

Global Configuration Command Mode

The Global Configuration command mode allows you to configure advanced system features such as broadcast storm control, SNMP, and STP. To access this mode, you must first access the User EXEC and the Privileged modes. The prompt changes to Switch(config)# to indicate the Interface Configuration mode.

See Table 14 for a list of commands that can be accessed from the Global Configuration mode.

Table 14. Global Configuration Command Mode Commands

Command	Description
BACK-PRESSURE	Sets the back pressure feature.
CONSOLE	Sets the console configuration.
DOT1X	Sets the 802.1x Port-based Network Access Control configuration.
END	Exits from the Global Configuration Command Mode to the Privileged EXEC Command Mode.
EXIT	Exits from the Global Configuration command mode to the Privileged EXEC command mode.
HOSTNAME	Sets the name of the system.
INTERFACE	Changes the command mode to the Interface Configuration command mode (you must also specify a port).
IP	Set the IP Address and IP related commands for the system.
LOGOUT	Exits the command line interface and returns to the Main Menu.
MLS	Sets the QoS feature.
MODE	Displays the available modes.
NO	Negates a command or sets its defaults.
PING	Pings a specified IP address to check connectivity to another system.
PRIORITY-QUEUE	Maps a CoS value to a priority value.
RADIUS-SERVER	Sets a RADIUS Server.
SNMP-SERVER	Sets the SNMP configuration in the system.
SPANNING-TRESS	Sets the STP features.
STORM-CONTROL	Sets the Broadcast Storm Control feature for the system.

Table 14. Global Configuration Command Mode Commands (Continued)

Command	Description
TELNET-SERVER	Sets the Telnet server.
TRUNK	Add ports to a trunk group.
USERNAME	Sets a system user name and password.

Interface Configuration Command Mode

The Interface Configuration command mode allows you to configure features that pertain to the ports on the system such as flow control, port mirroring, and duplex mode. To access this mode, you must first access the User EXEC, Privileged EXEC, and Global Configuration modes. From the Global Configuration mode, type:

interface ethernet1/*port*

You can specify a port or a range of ports. Separate a list of ports with commas or a dash. The prompt changes to Switch(config-if)# to indicate the Interface Configuration mode.

See the “Port Mirroring Example” on page 339 for a procedure that describes how to set the port mirroring in the Interface Configuration mode.

After you have accessed the Interface Configuration mode, the commands you enter apply to the ports specified in the Global Configuration mode. To perform port-specific commands on another group of ports, you must first exit the Interface Configuration mode and then specify the new ports in the Global Configuration mode before returning to the Interface Configuration mode.

For a list of commands that can be accessed from the Interface Configuration command mode, see Table 15.

Table 15. Interface Configuration Command Mode Commands

Commands	Description
DEFAULT-PRIORITY	Sets priority for a port.
DOT1X	Sets the 802.1 protocol configuration.
END	Exits from the Interface Configuration Command Mode to the Global Configuration Command Mode.
EXIT	Exits from the Interface Configuration Command Mode to the Global Configuration Command Mode.
FLOW-CTRL	Sets the parameters for the flow control feature.
GETPORT	Provided information about the ports.
LOGOUT	Exits the command line interface and returns to the Main Menu.
MODE	Displays the available modes.
NO	Negates a command or sets its defaults.
OVERRIDE	Enables the port override feature.

Table 15. Interface Configuration Command Mode Commands

Commands	Description
PING	Pings a specified IP address to check connectivity to another system.
PORT	Sets port mirroring parameters.
PVID	Sets the PVID.
SHUTDOWN	Disables a port.
SPANNING-TREE	Sets the parameters for the STP feature.
SPEED-DUPLEX	Sets the speed and duplex mode for a port.

Port Mirroring Example

To configure port 8 as the mirroring port and port 6 as the mirrored port you need to first access the Interface Configuration mode, specify the port, and then configure the port mirroring feature. Perform the following procedure.

1. From the User EXEC mode, enter:

   enable

   You now have access to the Privileged EXEC Configuration mode as indicated by the Switch(config)# prompt.

2. From the Privileged EXEC Configuration mode, enter:

   configure

   You now have access to the Global Configuration mode as indicated by the Switch(config)# prompt.

3. Access port 8 on the Interfa**ce Configuration mode:**

   interface Ethernet1/8

   You now have access to the Interface Configuration mode as indicated by the Switch(config-if)# prompt.

4. Enter the port mirroring command, making port 6 the mirrored port:

   Switch# **port mirror 6**

VLAN Configuration Command Mode

The VLAN Configuration command mode allows you to configure VLAN commands. To access this mode, you must first access the User EXEC, Privileged EXEC, and Global Configuration modes. From the Global Configuration command mode, type:

interface vlan*id*

The prompt changes to Switch(config-vlan)# to indicate the VLAN Configuration mode. Then enter VLAN commands.

After you have accessed the VLAN Configuration mode, the commands you enter apply to the VLAN specified in the Interface Configuration mode. To configure another VLAN, you must first exit the Interface Configuration mode and then specify the new VLAN ID in the Global Configuration mode before returning to the Interface Configuration mode.

See Table 16 for list of commands that can be accessed from the VLAN Configuration command mode.

Table 16. VLAN Configuration Command Mode Commands

Commands	Description
END	Exits from the VLAN Configuration mode to the Global Configuration mode.
EXIT	Exits from the VLAN Configuration mode to the Global Configuration mode.
GETVLAN	Displays VLAN ID information.
INTERFACE	Changes mode to the Interface Configuration command mode.
LOGOUT	Exits the command line interface and returns to the Main Menu.
MEMBER	Sets a static VLAN member.
MODE	Displays the available command modes.
NAME	Sets the VLAN name.
NO	Negates a command or sets its defaults.
PING	Pings a specified IP address to check connectivity to another system.

VLAN Example

To create a new VLAN with a VLAN ID of 2, access the Interface Configuration mode and specify the VLAN ID. Perform the following procedure.

1. From the User EXEC mode, enter:

   enable

   You now have access to the Privileged EXEC Configuration mode as indicated by the Switch(config)# prompt.

2. From the Privileged EXEC Configuration mode, enter:

   configure

   You now have access to the Global Configuration mode as indicated by the Switch(config)# prompt.

3. Create a VLAN with a VLAN ID of 2 by entering:

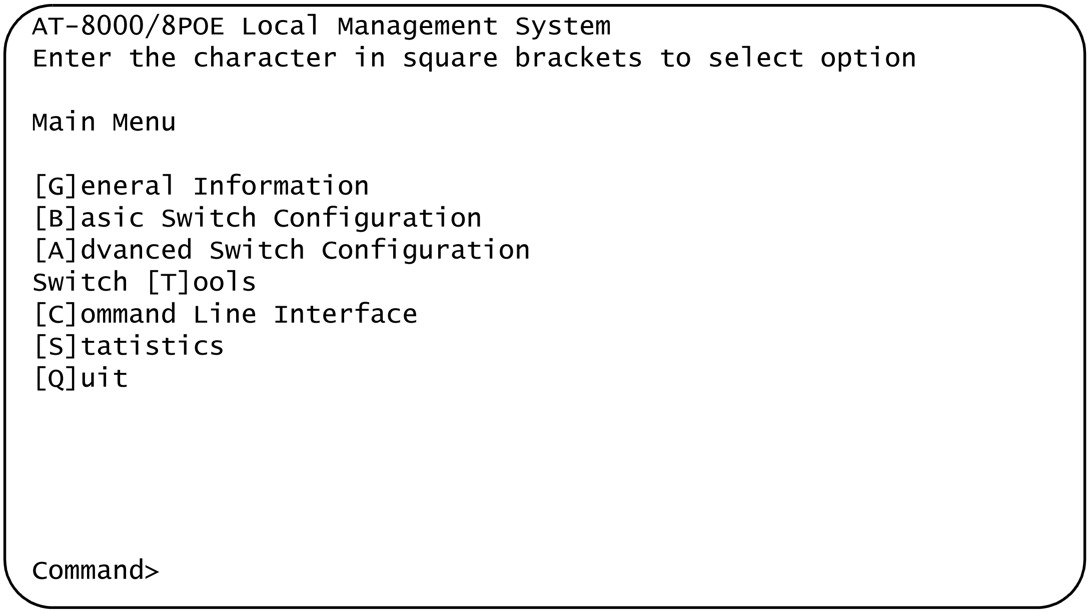
   interface vlan2

   You have created a VLAN with an ID of 2. You have access to the VLAN Configuration mode as indicated by the Switch(config-vlan)# prompt.

Starting the Command Line Interface

To start the command line interface, perform the following procedure:

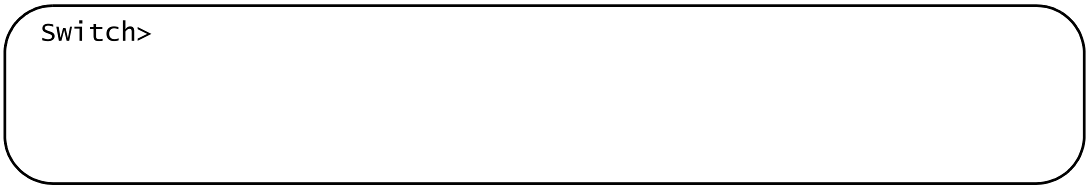
4. From the Main Menu (see Figure 105), type **C** to choose **Command Line Interface**.



```
AT-8000/8POE Local Management System
Enter the character in square brackets to select option

Main Menu

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





Command>
```

Figure 105. Main Menu

A command line prompt is displayed in Figure 106. The default switch name is “Switch>” and the arrow prompt indicates the user executive mode. After you name the switch with the HOSTNAME command, the new switch name replaces “Switch.” For example, if you rename the switch “San Jose, the prompt changes to “San Jose>.”



```
Switch>
```

Figure 106. Command Line Prompt, User Executive Mode

Command Formatting

The AT-S81 command line interface follows same formatting conventions for all of the command modes. There are command line interface features which apply to the general use of the command line and command syntax conventions which apply when entering the commands. See the following sections.

Command Line Interface Features

The following features are supported in the command line interface:

- **Command history** - Use the up and down arrow keys.
- **Context-specific help** - Press the question mark key, ?, to see a list of legal parameters or display all of the available commands for a particular command mode. There are two formatting options:

  command ? - List the keywords or arguments that are required by a particular command. A space between a command and a question mark is required.

  abbreviated command? - Provides a list of commands that begin with a particular character string. There is no space between the command and the question mark.
- **Keyword abbreviations** - Any keyword can be recognized by typing an unambiguous prefix, for example, type "sh" and the software responds with "show".
- **Tab key** - Pressing the Tab key fills in the rest of the keyword. For example, typing "di" and pressing the Tab key enters "disable" on the command line.

Command Line Syntax Conventions

The following table describes the conventions used in the command interface.

Table 17. Command Line Syntax Conventions

Convention	Description	Example
<string>	A string of alphanumeric characters	Switch-24
<int>	Integer	202
<ip>	IP address	192.168.0.1
<interface>	Port instance	Ethernet1/15

Table 17. Command Line Syntax Conventions (Continued)

<mask>	Subnet mask	255.255.240.0
<mac-add>	MAC address	00:02:15:af:2e:02
<sec>	Second	12
<min>	Minute	12
<port>	Port instance	Ethernet1/2 (stack-1,port-2)
<trunk ID>	Trunk group ID	4
<vlanID>	VLAN instance (including name and VLAN identifier)	vlan3
<port list>	A list of ports (separate entries with a comma or dash)	1,2,3,4-6,20-24
<traffic class>	Traffic class number	5

Appendix A
AT-8000/POE Default Settings

This appendix lists the AT-S81 factory default settings. It contains the following sections:

Basic Switch Default Settings

This section lists the default settings for basic switch parameters. The following topics are covered:

- ❐ “System Reboot Default Settings,” next
- ❐ “User Interface Configuration Default Settings” on page 346
- ❐ “Management Interface Default Settings” on page 346
- ❐ “Ping Default Settings” on page 347
- ❐ “System IP Configuration Default Settings” on page 347
- ❐ “System Administration Configuration Default Settings” on page 347

System Reboot Default Settings

The following table lists the system reboot default settings:

Setting	Default
Reboot Status	Stop
Reboot Type	Normal

User Interface Configuration Default Settings

The following table lists the user interface default settings.

Setting	Default
Console UI Idle Timeout	5 minutes
Telnet UI Idle Timeout	5 minutes
Telnet Server	Enabled
SNMP Agent	Disabled
Web Server	Enabled
User Name	Manager

Management Interface Default Settings

The following table lists the management interface default settings.

Setting	Default
Manager Username	manager
Manager Password	friend
Console Idle Timeoutl	5 minutes

Note
Login names and passwords are case sensitive.

Ping Default Settings

The following table lists the ping default settings.

Setting	Default
Target IP Address	0.0.0.0
Number of Requests	10
Timeout Value (sec.)	3

System IP Configuration Default Settings

The following table lists the system IP configuration default settings.

Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DHCP Mode	Disabled

System Administration Configuration Default Settings

The following table describes the system administration default settings.

Administration Setting	Default
Description	AT-8000/8POE
Name	None
Location	None
Contact	None

SNMP Default Settings

The following table describes the SNMP default settings.

Setting	Default
SNMP Status	Disabled
SNMP Read Community	public (Read only)
SNMP Write Community	private (Read|Write)
Trap Authentication	Enabled

Port Configuration Default Settings

The following table lists the port configuration default settings.

Port Configuration Setting	Default
Status	Enabled
Mode	Auto
Flow Ctrl	Enabled

Quality of Service

The following table lists the default mappings of IEEE 802.1p priority levels to egress port priority queues.

IEEE 802.1p Priority Level	Port Priority Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

IGMP Snooping Default Settings

The following table lists the IGMP Snooping default settings.

Setting	Default
IGMP Snooping Status	Disabled
IGMP Snooping Age-Out Timer	280 seconds
Maximum Multicast Groups	64
Multicast Router Ports Mode	Auto Detect

RSTP Default Settings

The following table describes the RSTP default settings.

Setting	Default
Global RSTP Status	Disabled
Hello Time	2 Sec.
Bridge Forwarding	15
Maximum Age	20 Sec.
Forward Delay	15 Sec.
Hello Time	2 Sec.
Bridge Maximum Age	20 Sec.
Bridge Forward Delay	15 Sec.

802.1x Network Access Control Default Settings

The following table describes the access control default settings per port.

Settings	Default
NAS ID	Nas1
Port Status	Authorized
Port Role	None
Port Control	Force Authorized
Transmission Period	30 seconds
Supplicant Timeout	30 seconds
Server Timeout	30 seconds
Maximum Request	2
Quiet Period	60 seconds
Re-authentication Period	3600 seconds
Re-authentication Status	Disabled

RADIUS Server Default Settings

The following table lists the default settings for the RADIUS server.

Settings	Default
Server IP Address	0.0.0.0
Response Time	10 seconds
Maximum Retransmissions	3

Broadcast Storm Control Default Settings

The following table lists the default settings for broadcast storm control.

Settings	Default
Broadcast Storm Status	Disabled
Threshold	Low

Index