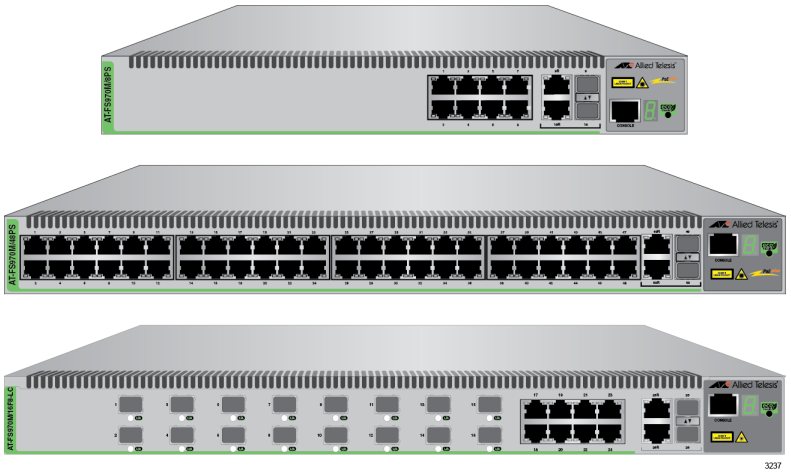
AT-FS970M Series

Fast Ethernet Switch

- AT-FS970M/8
- AT-FS970M/8PS
- AT-FS970M/8PS-E
- AT-FS970M/24C
- AT-FS970M/24PS
- AT-FS970M/48
- AT-FS970M/48PS
- AT-FS970M/16F8-LC



Management Software Web Interface User's Guide

AT-FS970M Series Version 2.3.1.0

613-001946 Rev. A

Copyright

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis, Inc.
3041 Orchard Parkway
San Jose, California 95134

Contents

Figures

Preface

This is the web interface user's guide for the AT-FS970M Series of Fast Ethernet switches. The instructions in this guide explain how to start a management session, use the web interface of the AlliedWare Plus™ Management Software, and configure the features of the switch.

For hardware installation instructions, refer to the *AT-FS970M Series Fast Ethernet Switches Installation Guide*.

This preface contains the following sections:

Caution

The software described in this document may contain certain encryption/security or cryptographic functionality and for exporting those products/software, USA export restrictions apply as per 15 C.F.R. Part 730-772 (particularly Part 740.17). At present, as per United States of America's export regulations our products/software cannot be exported to Cuba, Iran, North Korea, North Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please refer to export regulations of USA.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

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

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

Where to Find Web-based Guides

The installation and user guides for all of the Allied Telesis products are available for viewing in portable document format (PDF) from our web site at **www.alliedtelesis.com/support/documentation**.

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 product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis 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 Materials Authorization (RMA) request via our interactive support center.
- Documentation— View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- Software Downloads— Download the latest software releases for your managed products.

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

Chapter 1

AT-FS970M Series Version 2.3.1.0 Web Browser Interface

This chapter describes the types of management sessions using the AT-FS970M Series management software and the web interface manager accounts. See the following sections:

Management Sessions

The AT-FS970M Series switches provide two management interfaces: the web interface and Command Line Interface (CLI). This manual provides procedures that guide you through the web interface.

The initial management session of the switch can be from a management session, either through the web interface or the CLI. The switch is shipped from the factory with an IP address assigned and the web interface (HTTP service) enabled so that you can start the initial management session through the web interface. To start the initial web management session, see Chapter 2, “Starting a Management Session” on page 23.

The web interface allows access to a subset of the AlliedWare Plus features. For access to all of the AlliedWare Plus features, you must use the CLI.

Detailed feature descriptions are not provided in this guide. For thorough explanations of the features, see the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide.*

Web Manager Accounts

You must log on to manage the switch. This requires a valid username and password. The switch comes with one manager account with a username of "manager" and the default password of "friend." Both the username and password are case-sensitive. This account gives you access to all management modes and commands.

In the web interface, you can create two additional remote manager accounts. For instructions, see "Managing Local User Accounts" on page 52. The switch supports up to three manager sessions at one time.

Chapter 2

Starting a Management Session

This chapter describes how to start a management session using the AlliedWare Plus™ web interface as well as how to select fields, save your changes, and end a management session. See the following sections:

For additional information about the web server, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- Non-secure HTTP Web Browser Server
- Non-secure HTTP Web Browser Server Commands
- Secure HTTPS Web Browser Server
- Secure HTTPS Web Browser Server Commands
- Starting a Management Session

Non-secure HTTP and Secure HTTPS Modes

The switch has a web server so that you can remotely manage the switch over the network from a web browser on your PC. The server can operate in either plain-text HTTP mode or encrypted HTTPS mode. To access the switch through a web browser on your PC, either HTTP service or HTTPS service must be enabled.

HTTP Mode

Web browser management sessions of the switch conducted in the HTTP mode are non-secure because the packets exchanged by the server on the switch and your management workstation are sent in clear text, leaving the packets vulnerable to snooping.

The switch shipped from the factory is configured with HTTP service enabled.

HTTPS Mode

Web browser management sessions of the switch conducted in the HTTPS mode are protected against snooping because the packets exchanged between the switch and your management workstation are encrypted. Only the switch and the workstation are able to decipher the packets.

To access the switch in the HTTPS mode:

- The switch must have an HTTPS certificate.
- HTTPS service on the switch must be enabled.

> **Note**
> Either HTTPS or HTTP service can be enabled. To enable HTTPS service, HTTP must be disabled.

To configure the switch with an HTTPS certificate and enable HTTPS service, you must use the AlliedWare Plus™ Command Line Interface (CLI). See “Secure HTTPS Web Browser Server” chapter in *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide.*

Starting the Initial Web Management Session

This section explains how to start a management session for the first time using the AT-FS970M web interface. The switch shipped from the factory is configured with an IP address assigned and the web interface (HTTP service) enabled.

The switch and your PC must be directly connected through a twisted-pair cable, and the IP addresses of the switch and your PC must be members of the same network. Because the switch is shipped from the factory with the IP address 169.254.1.1 and the subnet mask 16, you must assign your PC an IP address in the 169.254.0.0/16 network, except 169.254.1.1. In addition, your PC must have a web browser, such as Windows Internet Explorer, installed.

There are two ways to assign an IP address to your PC:

- Manually assign any IP address in the 169.254.0.0/16 network (except 169.254.1.1) to your PC.
- Disconnect your PC from a network and let your PC automatically set an IP address in the 169.254.0.0/16 network. When a PC is disconnected from a network and no longer connected to a DHCP server, Windows assigns a random IP address in the 169.254.0.0/16 network to the PC.

Note
Deleting the boot.cfg file and restarting the switch restores the switch to its default configuration with HTTP service disabled and no IP address assigned.

To start a web management session when the switch has lost the factory default settings, you must use the Command Line Interface (CLI) to assign an IP address and enable HTTP or HTTPS service. For more information about enabling HTTP or HTTPS service and assigning an management IP address, see "Starting a Web Management Session" on page 32."

To start a web management session using a PC with an IP address in the 169.254.0.0/16 network, perform the following procedure:

1. Connect an RJ-45 plug on a straight-through twisted-pair cable to an Ethernet port on the switch.
2. Connect the other RJ-45 plug on the straight-through twisted-pair cable to an Ethernet port on the PC network interface card (NIC).

3. Open a web browser on the PC and enter the following:

   http://169.254.1.1

   The AT-FS970M Login page is displayed as shown in Figure 1.

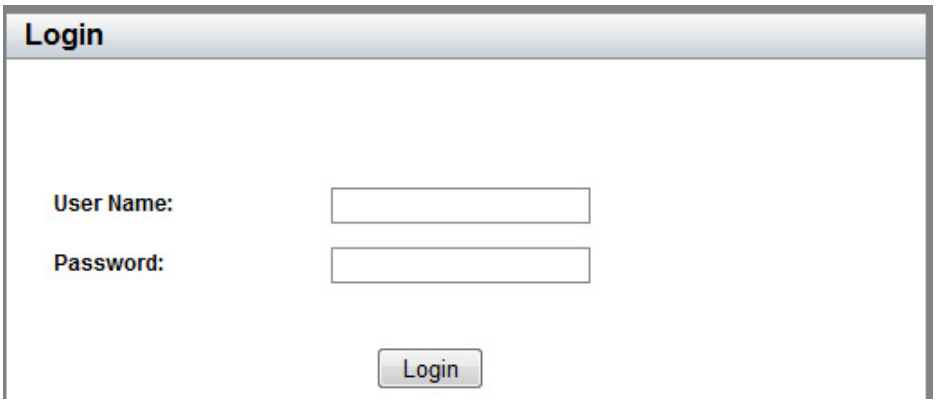


Figure 1. Login Page

Logging onto the Switch

Once you start the web interface, the AT-FS970M Login page is displayed.

Enter "manager" in the User Name field and "friend" in the Password field as shown in Figure 2. Then click the **Login** button.

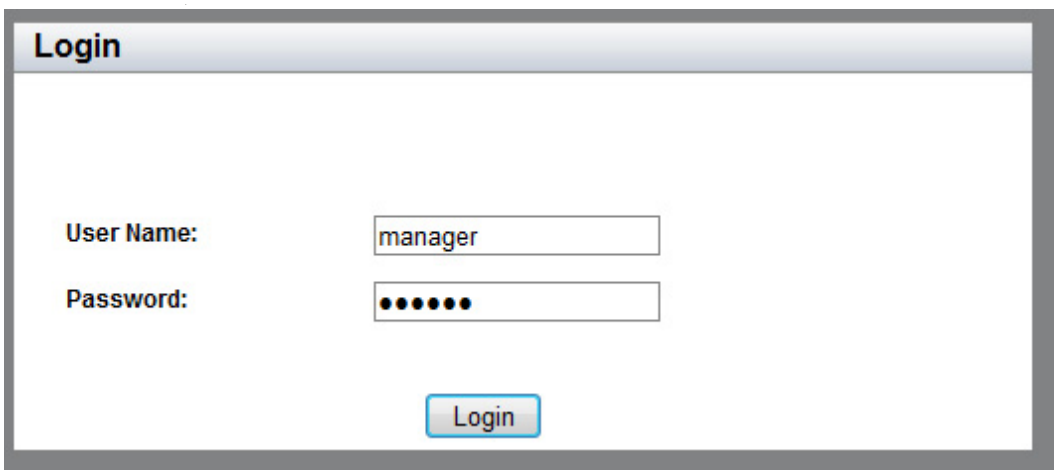


Figure 2. Login Page with Entries

The Dashboard page is displayed. See Figure 3 on page 28. The Dashboard page is the home page of the switch.

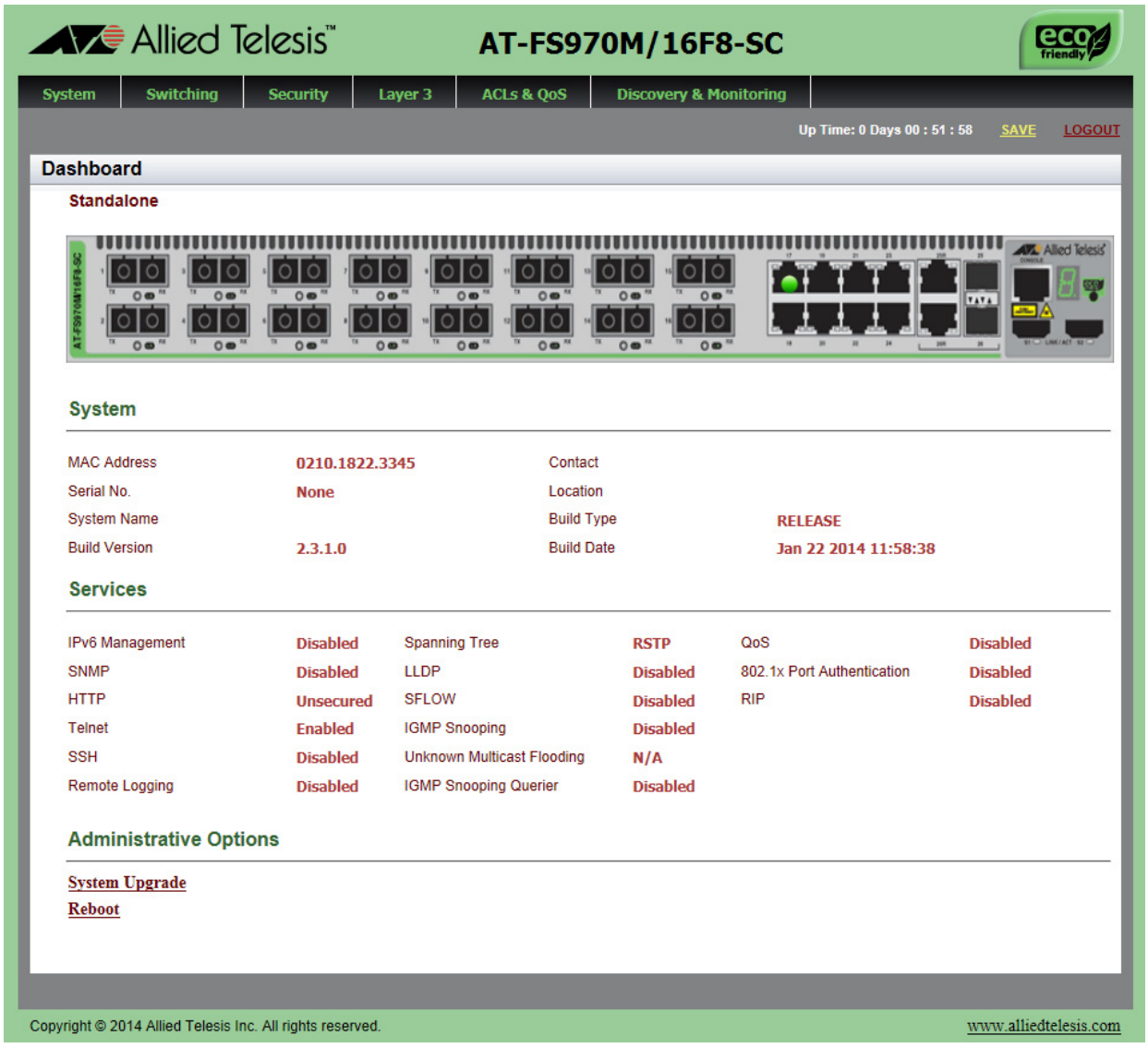


Figure 3. Dashboard Page

The following fields are displayed:

- **Up Time**— Length of time since the switch was last reset or power cycled in days, hours, minutes and seconds.

Note
Up Time is displayed on the top-right corner of the screen.

The System section displays the following information:

- **MAC Address**— MAC address of the switch.
- **Serial No.**— Unique serial number of the switch.

- **System Name**— Name of the switch. To specify this field, see "Setting the Switch Information" on page 48.
- **Version**— Software version number of the Management Software.
- **Contact**— Contact person for the switch. To specify this field, see "Setting the Switch Information" on page 48.
- **Location**—Location of the switch. To specify this field, see "Setting the Switch Information" on page 48.

The Services section displays the following information:

- **IPv6 Management**— Indicates if IPv6 Management is enabled or disabled on the switch.
- **SNMP**— SNMP setting of the switch.
- **HTTP**— HTTP setting of the switch.
- **Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- **SSH**— Indicates if SSH is enabled or disabled on the switch.
- **Remote Logging**— Indicates if the remote logging is enabled or disabled on the switch.
- **Spanning Tree**— Indicates if STP, RSTP, or MSTP is enabled on the switch. The default setting is "RSTP."
- **QoS**— Indicates if QoS is enabled or disabled on the switch.
- **LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- **sFLOW**— Indicates if sFlow is enabled or disabled on the switch.
- **IGMP Snooping**— Indicates if IGMP Snooping is enabled or disabled on the switch.
- **IGMP Snooping Querier**— Indicates if IGMP Snooping Querier is enabled or disabled on the switch.
- **802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- **RIP**— Indicates if RIP is enabled or disabled on the switch.

The Administration Options section displays the following information:

- **System Upgrade**— Select this field to upgrade your system software. See "Upgrading the Software" on page 58.
- **Reboot**— Select this field to reboot the switch. For instructions, see "Rebooting a Switch" on page 57.

What to Configure First

Here are a few suggestions on what to configure during your initial management session on the switch through the web interface. The initial management session can be performed through the Command Line Interface (CLI) as well as the web interface. For instructions on how to start a local management session through the CLI, refer to the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide*.

Changing the Login Password

To protect the switch from unauthorized access, change the password of the manager account. For instructions, see "Changing a User Password" on page 53.

Note
Write down the new password and keep it in a safe and secure location. If you forget the manager password, you cannot manage the switch if there are no other management accounts on the unit. In this case, contact Allied Telesis Technical Support for assistance.

For instructions on how to create additional management accounts, see "Adding a New User Account" on page 52.

Assigning a Name to the Switch

The switch is easier to identify if you assign it a name. The switch's name is displayed on the Dashboard page. To change the name of the switch, see "Setting the Switch Information" on page 48.

A name can be up to 39 alphanumeric characters. Special characters, except spaces and quotation marks, are allowed.

Changing a Management IP Address

The switch shipped from the factory has the IP address 169.254.1.1 assigned. You must change the factory default IP address to an address in your network. To change the IP address, see "Changing an IPv4 Address" on page 220. Also, remember to change the IP address of your PC.

Note
When you change the management IP address of the switch, you lose the connection to the switch. After you change the IP address of your PC, start a management session again by opening a web browser on the PC and entering the new IP address of the switch.

Here are the requirements:

- You can assign one IPv4 address per VLAN.
- The switch can have up to 256 IPv4 addresses.

- The management IPv4 address can be any IPv4 address assigned on the switch.
- The switch can have only one IPv6 address.
- Your PC must have an IP address that belongs to the network where the management IP address belongs, or have access to the network where the management IP address belongs.

Setting System Time

To set the system time, either manually or with an NTP server, see "Setting the System Date and Time" on page 40.

Starting a Web Management Session

This section provides how to start a web management session when the switch does not have the factory default configuration.

To log onto the switch through the web interface, enter the IP address of the switch on the web browser, such as Windows Internet Explorer, on the PC or laptop that can access the switch. If the web interface comes up, you can skip the rest of this section and continue a web management session. If the web interface does not come up, you must configure the switch using the Command Line Interface (CLI).

Note
For more information about how to start the Command Line Interface (CLI), see the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide.*

There are some cases in which you must configure the switch using the CLI to start a web management session:

- The switch does not have an IP address assigned, or you do not know the IP address of the switch.
- HTTP service on the switch is disabled.
- You want to access the switch in the HTTPS mode.

When You Do Not Know the IP Address of the Switch

If the switch has no IP address assigned, or you do not know the IP address of the switch, perform the following steps:

1. "Logging onto the CLI through the Console Port" on page 33.
2. "Checking for the IP Addresses of the Switch in the CLI" on page 34.
3. If the switch does not have any IP address assigned, "Adding an IP Address to the Switch in the CLI" on page 34.
4. "Checking the Status of HTTP and HTTPS Services in the CLI" on page 34.
5. "Enabling HTTP or HTTPS Service in the CLI" on page 35.
6. "Saving your Changes in the CLI" on page 36.

When the Switch Does Not Display the Login Page

When the switch does not display the web interface, even though you enter the IP address of the switch on the web browser, you must enable HTTP or HTTPS service on the switch through the CLI by performing the following steps:

1. "Logging onto the CLI through the Console Port" on page 33.

   Or

   Log onto the CLI using the Telnet or SSH protocol.

   Note
   To start a Telnet or SSH management session, see the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide.*

2. "Checking the Status of HTTP and HTTPS Services in the CLI" on page 34.
3. "Enabling HTTP or HTTPS Service in the CLI" on page 35.
4. "Saving your Changes in the CLI" on page 36.

Logging onto the CLI through the Console Port

To log onto the CLI through the console port on the switch, perform the following procedure:

1. Connect the RJ-45 connector on the management cable to the console port on the switch.
2. Connect the other end of the cable to an RS-232 port on a terminal or a PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
   - Baud rate: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
4. Press Enter.

   You are prompted for a username and password.

5. Enter a username and password. If this is the initial management session of the switch, enter "manager" as the username and "friend" as the password. The username and password are case-sensitive.

The local management session is started when the AlliedWare Plus™ command line prompt is displayed as shown in Figure 4.

```
awplus>
```

Figure 4. AlliedWare Plus™ Command Line Prompt

Checking for the IP Addresses of the Switch in the CLI

To check for IP addresses assigned to the switch, enter the following commands:

```
awplus> enable

awplus# show ip interface
```

For a display of this command, see Figure 5.

```
awplus# show ip interface

Interface     IP-Address        Status        Protocol
  vlan1-0     192.168.1.3/24  admin up        running
```

Figure 5. Displaying the IP Address

Adding an IP Address to the Switch in the CLI

When the switch does not have an IP address, assign an IP address and subnet mask to the switch. The following example assigns the IP address 192.168.1.2. and the subnet mask 24 to VLAN 1:

```
awplus> enable

awplus# configure terminal

awplus(config)# interface vlan1

awplus(config-if)# ip address 192.168.1.2/24

awplus(config-if)#
```

Checking the Status of HTTP and HTTPS Services in the CLI

To check if HTTP service is enabled, enter the following commands:

```
awplus> enable

awplus# show ip http
```

Figure 6 on page 35 shows an example of the command output.

```
awplus# show ip http

HTTP server disabled.
```

Figure 6. Displaying the Status of HTTP Service

To check whether HTTPS service is enabled, enter the following commands:

```
awplus> enable

awplus# show ip https
```

Figure 7 shows an example of the command output.

```
HTTPS server enabled. Port: 443
Certificate 1 is active
Issued by: self-signed
```

Figure 7. Displaying the Status of HTTPS Service

Note
HTTPS and HTTP services cannot be enabled at the same time. For example, when HTTP is enabled, HTTPS is disabled.

Enabling HTTP or HTTPS Service in the CLI

To enable HTTP service on the switch, enter the following commands:

```
awplus# configure terminal

awplus(config)# service http

awplus(config)# exit

awplus#
```

To enable HTTPS, the switch must have a certificate. To configure the web server in the HTTPS mode, see the "Secure HTTPS Web Browser Server" chapter in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide.*

Saving your Changes in the CLI

Save your changes to the startup configuration file by entering the following commands:

```
awplus# copy running-config startup-config
```

Or

```
awplus# write
```

Saving Your Changes

The changes you have made are temporarily stored in the running configuration file. When you reboot the switch, the information in the running configuration file is lost. To save your changes after you reboot the switch, do the following:

1. Click **SAVE**.

   Figure 8 shows the **SAVE** at the upper right corner of the web page. Clicking **SAVE** saves the changes to the startup configuration file.

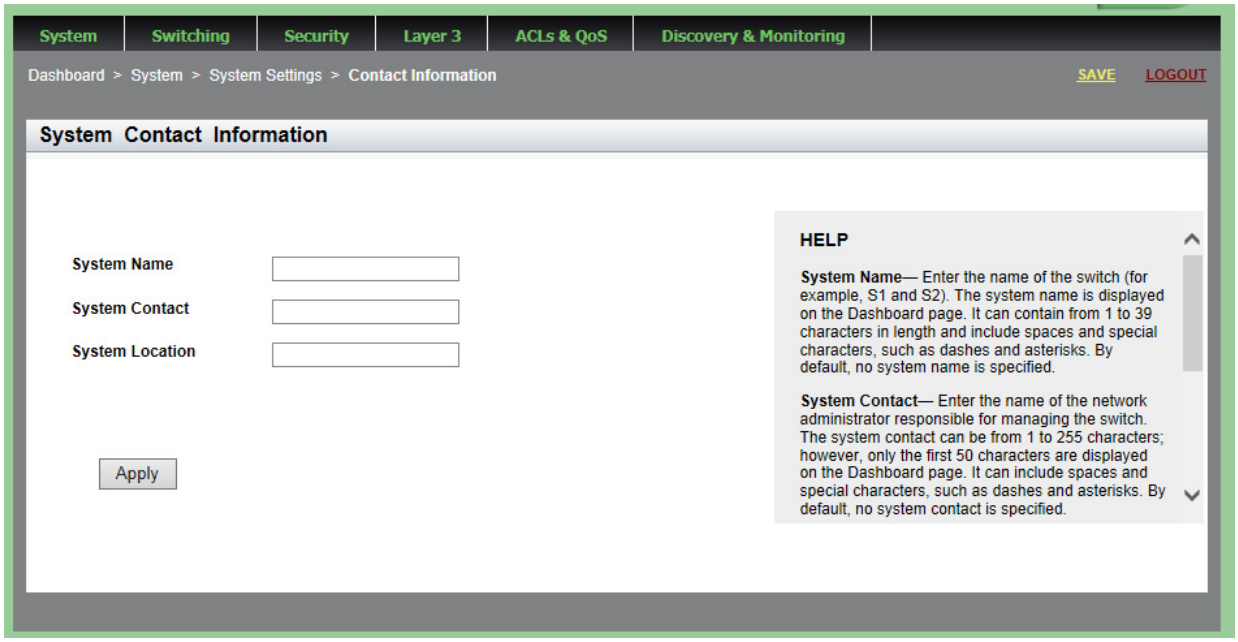


Figure 8. System Contact Information Page

Ending a Web Management Session

To end a web management session, select **LOGOUT** at the top of the web page. For an example, see the System Contact Information page in Figure 8 on page 37.

Chapter 3

Basic Switch Parameters

This chapter describes how to set up basic switch operations. See the following sections:

For additional information about basic port settings, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Basic Switch Management
- ❒ Basic Switch Management Commands

Setting the System Date and Time

This procedure explains how to set the switch's date and time. Setting the date and time is important if you plan to view the events in the switch's event log or on a syslog server. The correct date and time are also important if the management software sends traps to a management workstation or if you plan to create a self-signed SSL certificate. Events, traps, and self-signed certificates should contain the date and time of when they occurred or, in the case of certificates, when they were created.

There are two ways to set the switch's date and time. One method is to set it manually. This method is not recommended because the date and time are lost if you reboot the switch.

The second method uses the Simple Network Time Protocol (SNTP). The AlliedWare Plus™ Management Software comes with the client version of this protocol. You can configure the management software to obtain the current date and time from a Network Time Protocol (NTP) or SNTP server located on your network or the Internet.

SNTP is a simplified version of the NTP and uses the same packet structure as NTP. The SNTP client software in the management software is interoperable with NTP servers.

Note
In order for the management software on the switch to communicate with an SNTP or NTP server, there must be an interface on the local subnet from where the switch is able to reach the server. The switch uses the IP address of the interface as its source address when sending packets to the server.

Note
The default system time on the switch is midnight, January 1, 2000.

Choose from the following procedures:

- "Configuring an SNTP or NTP Server" on page 40
- "Setting System Time Manually" on page 43

Configuring an SNTP or NTP Server

To configure SNTP or NTP server, do the following:

1. Hover the cursor over the **System** tab.
2. From the System tab, select **System Settings**.

   The System Settings Tab is displayed in Figure 9 on page 41.

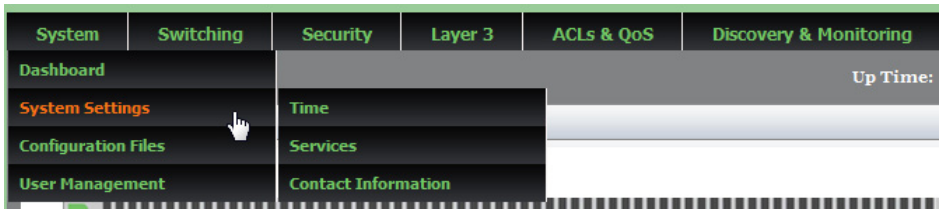


Figure 9. System Settings Tab

3. From the System tab, hover over **System Settings**.
4. Move the cursor to the right and select **Time**.

   The System Time Settings page is displayed. See Figure 10.

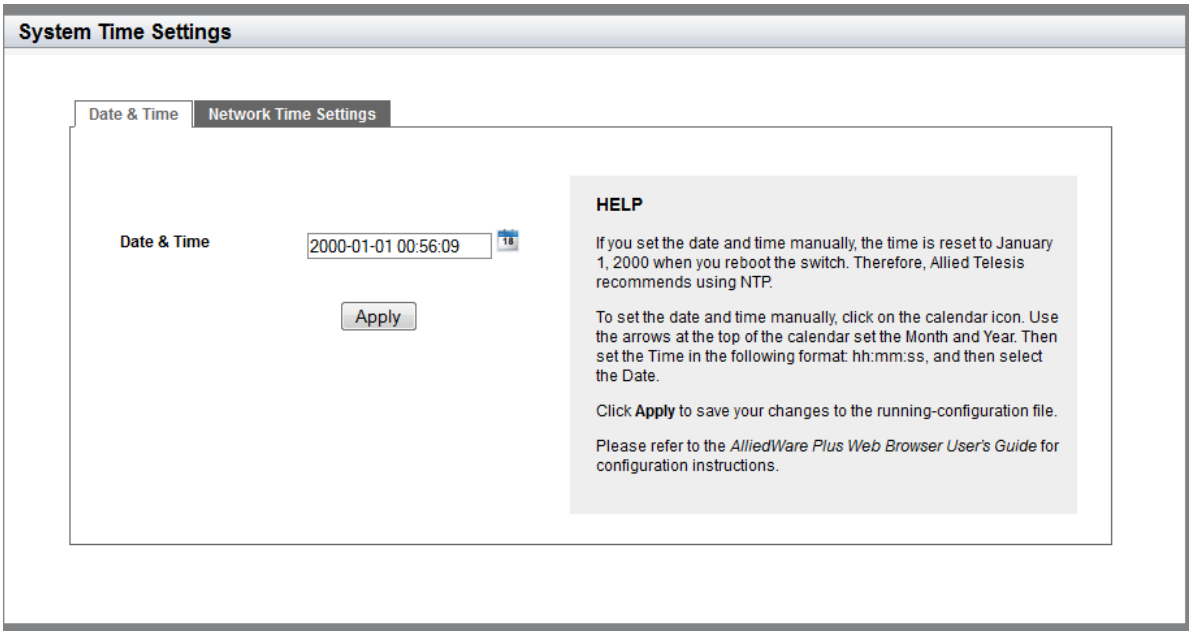


Figure 10. System Time Settings Page

5. Select the Network Time Settings tab.

   The Network Time Settings page is displayed. See Figure 11 on page 42.

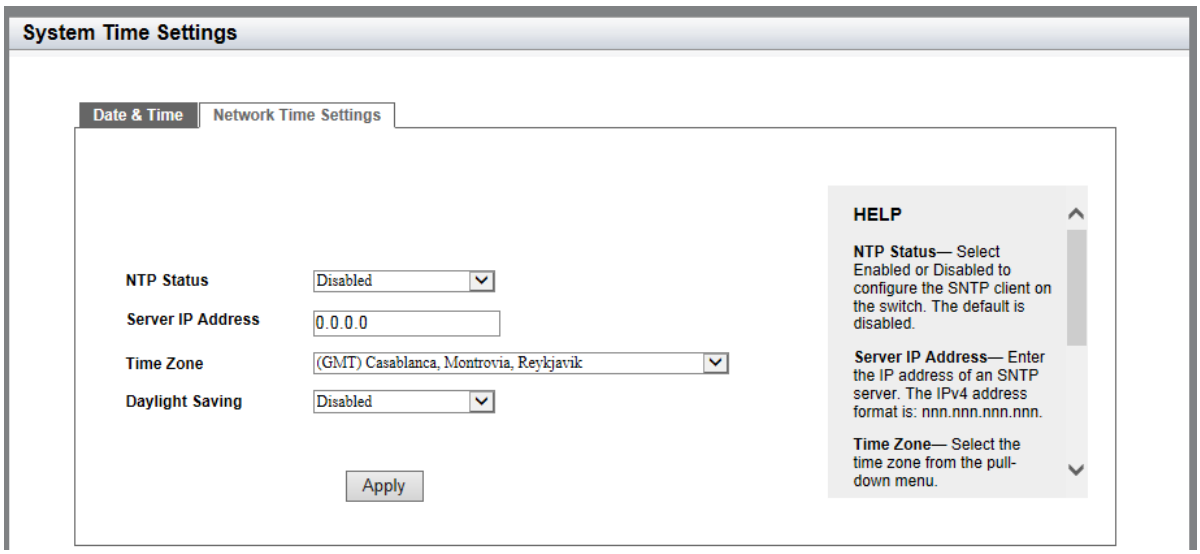


Figure 11. System Time Settings Page with Network Time Settings Tab

6. To configure the switch to obtain its date and time from an SNTP or NTP server on your network or the Internet, specify the following fields:

   - **NTP Status**— Select Enabled or Disabled to configure the SNTP client on the switch. The default is disabled.
   - **Server IP Address**— Specify the IPv4 address of an SNTP or NTP server.

     The IPv4 format is: xxx.xxx.xxx.xxx where xxx is a decimal number from 0 to 255.

     Note
     If the local interface on the switch is obtaining its IP address and subnet mask from a DHCP server, you can configure the server to provide the interface with an IP address of an NTP or SNTP server. If you configured the server to provide this address, then you do not need to enter it here.

   - **Time Zone**— Select the time zone as a measurement of Greenwich Mean Time (GMT) which is the default setting. Use the pull-down menu to select the other time zones.
   - **Daylight Saving**— Enable or disable the system's adjustment for daylight savings time. The default is disabled.

Note
The switch does not set daylight saving time (DST) automatically. If the switch is in a locale that uses DST, you must remember to enable this in March when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, this option should be set to disabled all the time.

7. Click **Apply**.

   If you enabled the SNTP client, the switch immediately polls the SNTP or SNTP server for the current date and time. (When SNTP is enabled, the switch automatically polls the server whenever a change is made to any of the fields on this page.)

8. Click **SAVE** to save your changes to the startup configuration file.

Setting System Time Manually

To set the system time manually, do the following:

1. Hover the cursor over the **System** tab.
2. From the System tab, hover over **System Settings**.

   The System Settings Tab is displayed in Figure 9 on page 41.

3. Move the cursor to the right and click **Time**.

   The System Time Settings page is displayed. See Figure 10 on page 41.

4. You have two ways to set the date and time in the **Date & Time** field. Use either Step 5 or Step 6.
5. Type in the time and date in the following format:

   yyyy-dd-mm hh:mm:ss

6. Select the calendar icon next to the **Date & Time** field.

   The Calendar page is displayed. See Figure 12 on page 44.

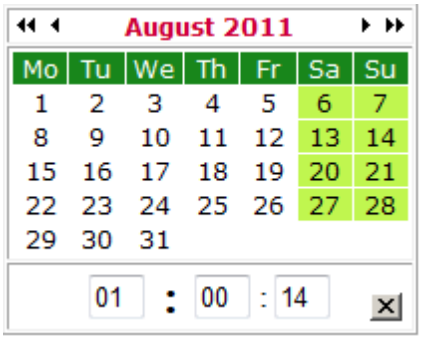


Figure 12. Calendar Page

a. Use the arrows at the top of the Calendar to select the month and year.

b. Set the time of day using the following format:

   hh:mm:ss

c. Click on the day of the month.

7. Click **Apply**.

8. Click **SAVE** to save your changes to the startup configuration file.

Configuring a Telnet or SSH Server

The AT-FS970M web browser interface allows you to configure the switch as a Telnet or SSH server.

You can use the web browser interface to enable a Telnet server, but not as a Telnet client. The Telnet client is only supported from the Command Line Interface (CLI). For information about how to use a Telnet client, see the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide*.

To enable an SSH server in the web interface, you must first create an encryption key in the CLI interface. Then you can enable the SSH server in the web interface.

To enable Telnet or SSH server on the switch, do the following:

1. From the home page, hover the cursor over the **System** tab.
2. From the System tab, hover over System Settings.

   The System Settings tab is displayed. See Figure 9 on page 41.
3. Move the cursor to the right and select **Services** from the drop-down menu.

   The System Services page is displayed. See Figure 13.

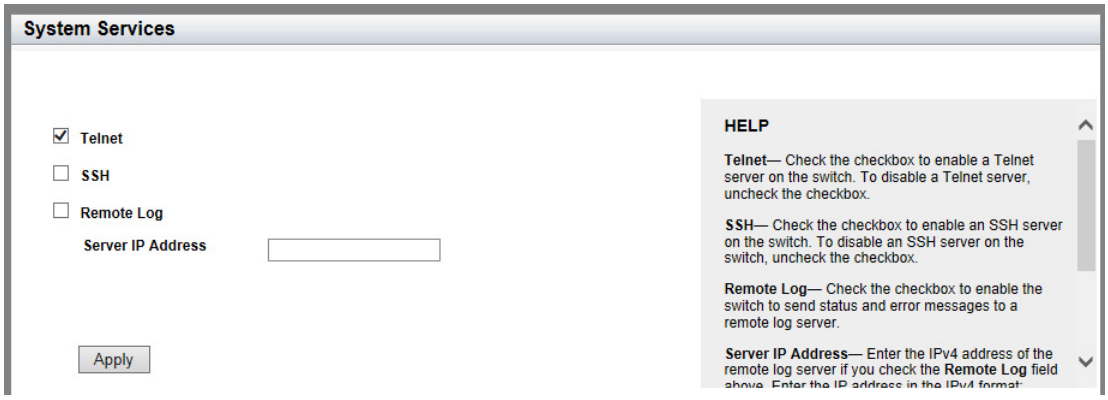


Figure 13. System Services Page

4. Specify the following fields as necessary:
   - **Telnet**— Check the checkbox to enable the Telnet server on the switch. To disable the server on the switch, uncheck the checkbox.
   - **SSH**— Check the checkbox to enable the SSH server on the switch. To disable the server on the switch, uncheck the checkbox.

Note
Both the Remote Log and Server IP Address fields are used only to set a remote log server. For information on these fields, see “Configuring a Remote Log Server” on page 47.

- **Remote Log**— Check the checkbox to enable the switch to send status and error messages to a remote log server. To disable the switch to send messages to a remote log server, uncheck the checkbox.
- **Server IP Address**— Enter the IPv4 address of the remote log server if you check the Remote Log checkbox above. Enter the IP address in the IPv4 format: nnn.nnn.nnn.nnn.

5. Click **Apply.**
6. Click **SAVE** to save your changes to the startup configuration file.

Configuring a Remote Log Server

You can use the AT-FS970M web browser interface to enable logging to a remote log server, which is part of the Syslog feature. However, you must use the CLI to view or clear the event log. For information about the Syslog features, see the SysLog chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide*.

To activate remote logging on the switch, do the following:

1. Hover the cursor over the **System** tab.
2. From the System tab, hover over System Settings.

   The System Settings tab is displayed. See Figure 9 on page 41.
3. Move the cursor to the right and select **Services**.

   The System Services page is displayed. See Figure 13 on page 45.
4. Specify the following fields:
   - **Remote Log**— Check the checkbox to enable the switch to send status and error messages to a remote log server. To disable the switch from sending messages to a remote log server, uncheck the checkbox.
   - **Server IP Address**— Enter the IPv4 address of the remote log server in the IPv4 format: nnn.nnn.nnn.nnn.
5. Click **Apply.**
6. Click **SAVE** to save your changes to the startup configuration file.

Setting the Switch Information

This procedure allows you to set information about the switch, such as a switch name, contact person, and location. Assigning a name to the switch helps you identify your switches when you manage them and avoid performing a configuration procedure on the wrong switch.

To assign a name, contact person, and location to the switch, perform the following procedure:

1. From the home page, hover the cursor over the **System tab**.
2. From the System tab, hover over **System Settings**.

   The System Setting tab is displayed. See Figure 9 on page 41.
3. Move the cursor to the right and select **Contact Information**.

   The System Contact Information page is displayed. See Figure 14.

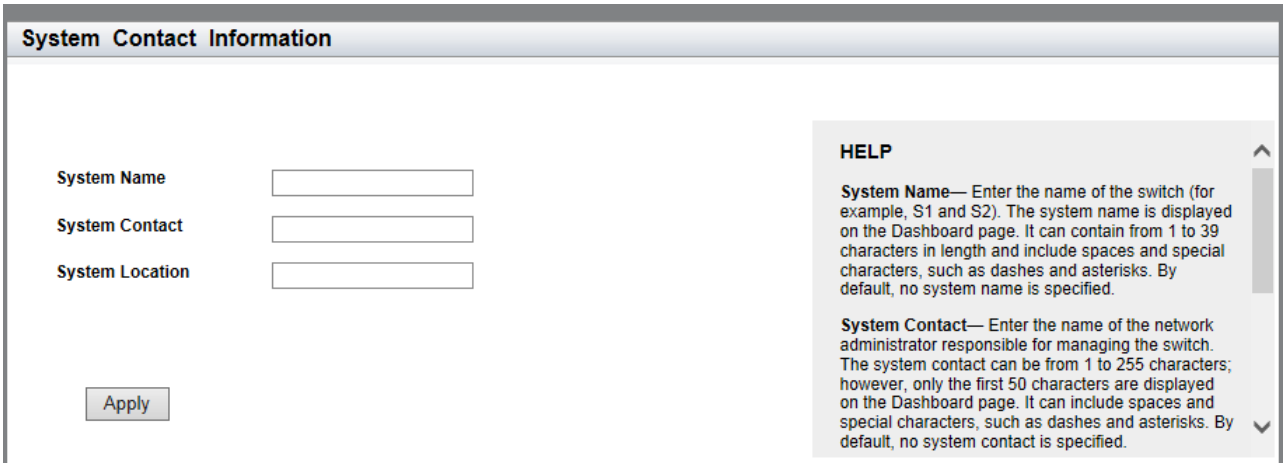


Figure 14. System Contact Information Page

Specify the following fields as necessary:

- **System Name**— Enter a name for the switch, for example, S1 or Switch2. The name is displayed on the Dashboard page. See Figure 3 on page 28. The name can be from 1 to 39 characters in length. Special characters, except spaces and quotation marks, are allowed. By default, no system name is specified. This field is optional.
- **System Contact —** Enter the name of a network administrator responsible for managing the switch. The name can be from 1 to 255 characters; however, only the first 50 characters are displayed on the Dashboard page. Spaces and special characters, such as dashes and asterisks are allowed. By default, no system contact is specified. This field is optional.
- **System Location—** Enter the location of the switch, (for example, 4th Floor - room 402B). The location can be from 1 to 255 characters; however, only the first 50 characters are displayed on the Dashboard page. Spaces and special characters, such as dashes and asterisks, are allowed. By default, no system location is specified. This field is optional.

4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Managing the Configuration File

Within the web browser interface, you can upload a configuration file onto the switch, download a configuration file from the switch, delete a configuration file, and save your changes to the current configuration file. However, to create a new configuration file, you need to access the switch through the CLI.

See the following procedures:

- “Displaying the Configuration Files” on page 50
- “Setting the Active Configuration File” on page 51
- “Downloading a Configuration File onto Your PC” on page 51

Displaying the Configuration Files

To display a list of the configuration files on the switch, do the following:

1. From the Dashboard page, hover the cursor over the **System** tab.
2. From the System tab drop-down menu, select **Configuration Files** from the pull-down menu.

   For an example of the Configuration Files page, see Figure 15.

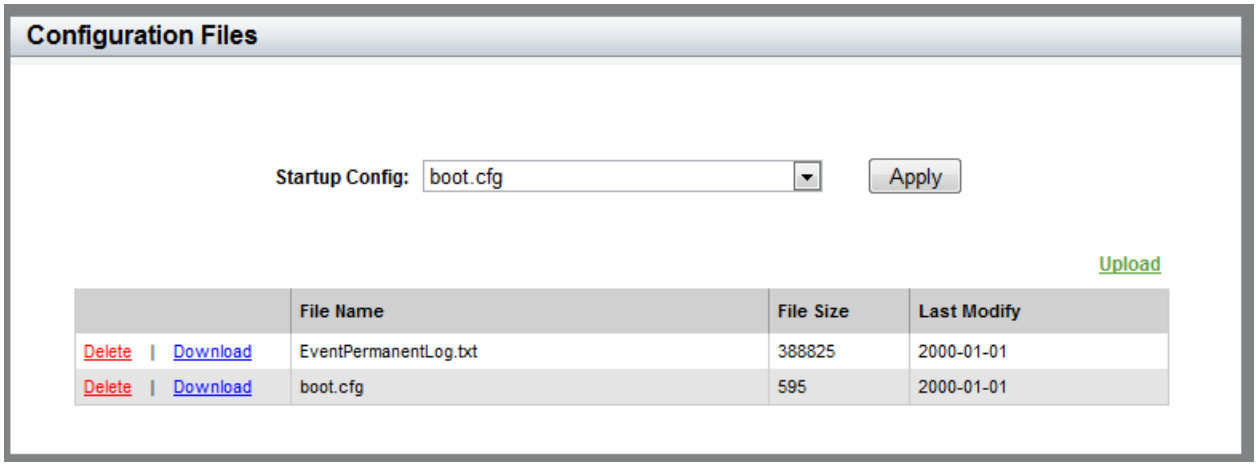


Figure 15. Configuration Files Page

The following fields are displayed:

- **Startup Config**— Name of the active boot configuration file, which for the switch of the example is “boot.cfg.”
- **File Name**— Name of the file.
- **File Size**— File size in bytes.

- **Last Modify**— Date the configuration file was last modified. The format is year, month, date.

Setting the Active Configuration File

To specify a file as the startup configuration file, do the following:

1. Use the pull-down menu to select a file as the active configuration file.
2. Click **Apply**.

   The file you select is the active configuration file after you reboot the switch.

Downloading a Configuration File onto Your PC

To download a configuration file onto your PC, do the following:

1. Hover the cursor over the **System** tab.

   For an example of the System tab, see Figure 9 on page 41.

2. From the System tab drop-down menu, select **Configuration Files**.

   For an example of the **Configuration Files** page, See Figure 15 on page 50.

3. Click **Download** next to the file name that you want to download.

   For an example of the File Download popup window, see Figure 16.

.

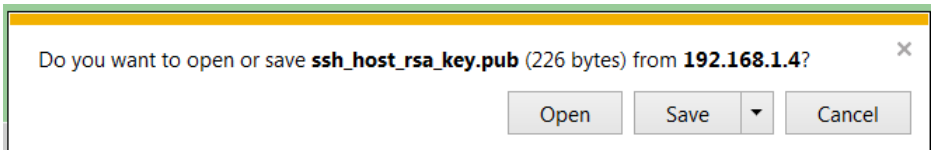


Figure 16. File Download Popup Window

4. Follow the instructions of your web browser to select a location and save the file.

Deleting a Configuration

To delete a configuration file, do the following:

1. Hover the cursor over the **System** tab.

   For an example of the System tab, see Figure 9 on page 41.

2. From the System tab drop-down menu, select **Configuration Files**.

   For an example of the **Configuration Files** page, See Figure 15 on page 50.

3. Click **Delete** next to the file name that you want to download.

   The file is deleted.

Managing Local User Accounts

The switch comes with one local manager account. The account, which has the username “manager” and default password “friend,” is referred to as a local account because it is the switch that authenticates the username and password when a manager logs on using the account.

This section explains how to create additional local user accounts, how to change passwords and privileges, and how to delete a manager account. See the following:

- ❒ “Adding a New User Account” on page 52
- ❒ “Changing a User Password” on page 53
- ❒ “Changing the User Privilege” on page 54
- ❒ “Deleting a User Account” on page 55

The switch also supports remote manager accounts that are not authenticated by the switch, but by a RADIUS or TACACS+ server on your network. For information, see Chapter 17, “RADIUS and TACACS+ Clients” on page 187.

Adding a New User Account

To add a local user account, do the following:

1. From the home page, hover the cursor over the **System** tab.
2. From the System tab drop-down menu, select **User Management**.

   For an example of the User Management page, see Figure 17.

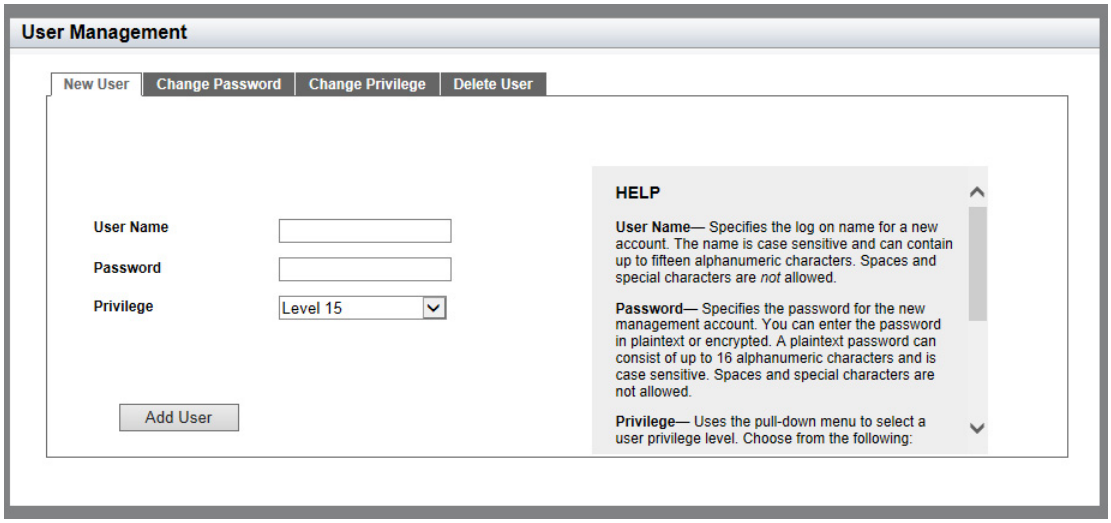


Figure 17. User Management Page

3. Add a new user by doing the following:

   - **User Name**— Enter a new logon name for the new account. The name is case-sensitive and can contain up to 15 alphanumeric characters. Spaces and special characters are *not* allowed.
   - **Password**— Enter the password for the new account in plain text. The password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are *not* allowed.
   - **Privilege**— Select a user privilege level from the pull-down menu. Choose from the following:

     Level 15: Management accounts with a user level of 15 have unrestricted access to the management software. This is the default setting.

     Level 1: Management accounts with a user level of 1 have restricted access to the management software. Accounts with this level are allowed to view the settings on the switch, but not allowed to change them.

4. Click **Add User**.

5. Click **SAVE** to save your changes to the startup configuration file.

Changing a User Password

To change a user password, do the following:

1. From the home page, hover the cursor over the **System** tab.

2. From the System tab drop-down menu, select **User Management**.

   The User Management page is displayed. See Figure 17 on page 52.

3. From the User Management page, select the **Change Password** tab.

   The User Management page with the Change Password tab is displayed. See Figure 18 on page 54.

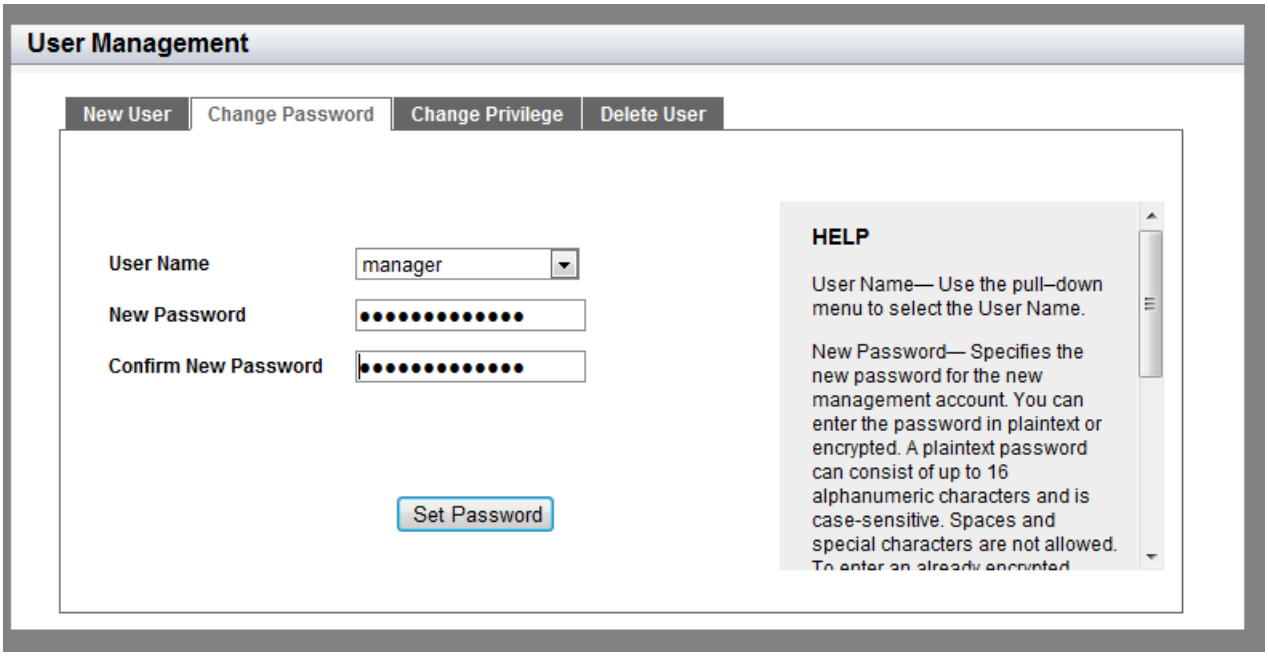


Figure 18. User Management Page with Change Password Tab

4. Use the pull-down menu next to the **User Name** field to select a username.

   The username must already exist.

5. Enter a new password in plaintext in the **New Password** field.

   A password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are *not* allowed.

6. Re-enter the new password in the **Confirm New Password** field.

7. Click **Set Password**.

8. Click **SAVE** to save your changes to the startup configuration file.

Changing the User Privilege

To change a privilege of a user, do the following:

1. From the home page, hover the cursor over the **System** tab.

2. From the System tab drop-down menu, select **User Management**.

   The User Management page is displayed. See Figure 17 on page 52.

3. From the User Management page, select the **Change Privilege** tab.

   The User Management page with the Change Privilege tab is displayed. See Figure 19 on page 55.

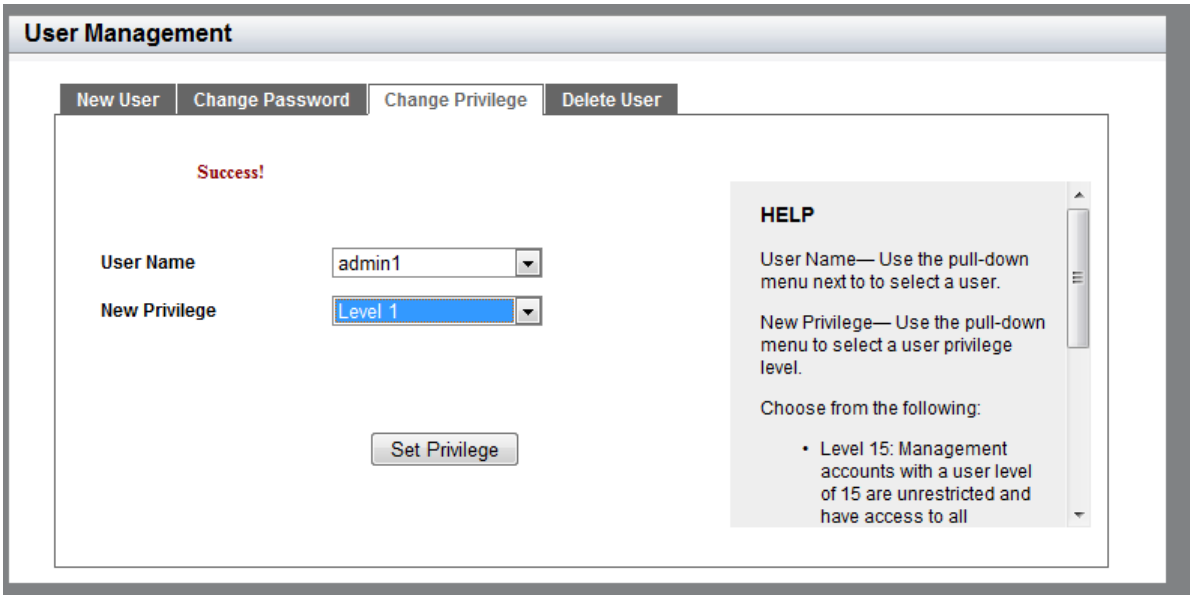


Figure 19. User Management Page with Change Privilege Tab

4. Use the pull-down menu next to the **User Name** field to select a user.
5. Use the pull-down menu next the New **Privilege** field to select a user privilege level. Choose from the following:
   - **Level 15**— Management accounts with a user level of 15 have unrestricted access to the management software.
   - **Level 1**— Management accounts with a user level of 1 have restricted access to the management software. Accounts with this level are allowed to view the settings on the switch, but not allowed to change them.
6. Click **Set Privilege**.
7. Click **SAVE** to save your changes to the startup configuration file.

Deleting a User Account

To delete a user account from the switch, do the following:

1. From the home page, hover the cursor over the **System** tab.
2. From the System tab drop-down menu, select **User Management**.

   The User Management page is displayed. See Figure 17 on page 52.
3. From the User Management page, select the **Delete User** tab.

   The User Management page with the Delete User tab is displayed. See Figure 20 on page 56.

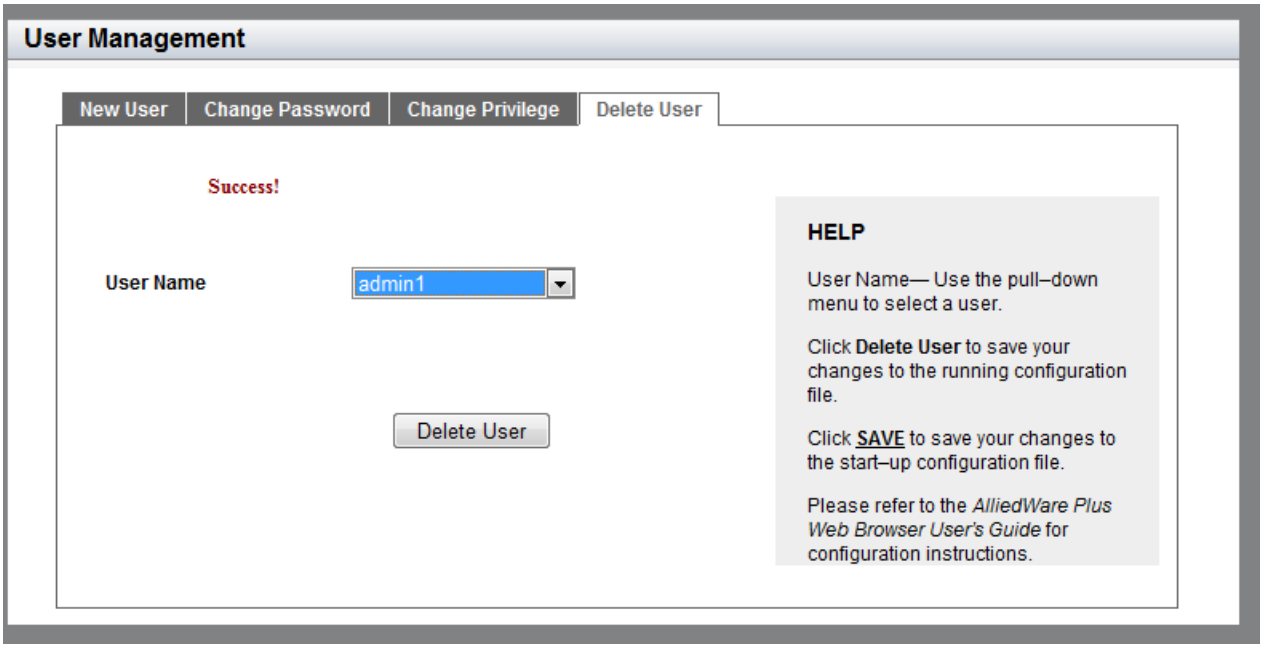


Figure 20. User Management Page with Delete User Tab

4. Use the pull-down menu to select a user.
5. Click **Delete User**.
6. Click **SAVE** to save your changes to the startup configuration file.

Rebooting a Switch

Resetting the switch ends your web browser management session. To continue managing the switch, you must log in again.

> **Note**
> All unsaved changes are discarded when you reset a switch. To save your changes to the startup configuration file, click **SAVE**.

To reboot a switch, perform the following procedure:

1. Hover the cursor over the **System Tab**.
2. From the System tab drop-down menu, select **Dashboard**.

   The Dashboard Page is displayed. See Figure 3 on page 28.
3. Select **Reboot** at the bottom of the page.

   A confirmation prompt is displayed indicating that the connection to the web is lost during a reboot.
4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

> **Note**
> The switch does not forward packets while it initializes the management software and loads its active configuration file. This process takes between 20 seconds to 2 minutes to complete, depending on the number and types of commands in the configuration file.

Upgrading the Software

The latest version of the AlliedWare Plus™ Management Software is available from the Allied Telesis website. You can download the software image file on your workstation and upload the file onto the switch.

To upgrade the AT-FS970M software, perform the following procedure:

1. Open a new browser and enter the following:

   http://www.alliedtelesis.com/support/software

   The Allied Telesis Software Download page is displayed.

2. Select your hardware product model from the pull-down menu next to the Product field. If the model is not listed, click the **Log in to access restricted software** link, then skip to Step 4.

3. Click the software file that you want to upload to the switch.

   The User Login page is displayed. See Figure 21.

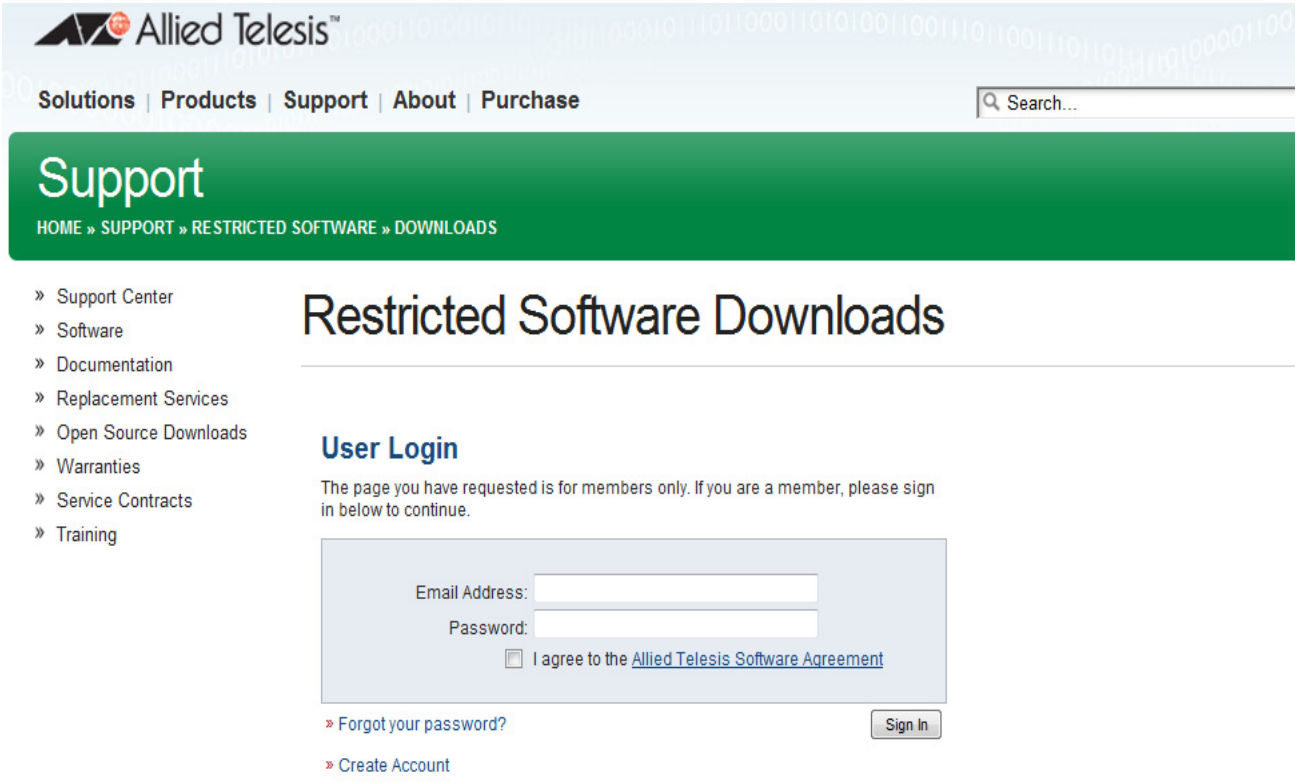


Figure 21. User Login Page on the Allied Telesis Website

4. Enter your email address and password, then click the **Sign In** button.

   Note
   If you do not know your password, click the Create Account link and follow the instructions on the page.

5. Download the software image file to your workstation.

6. Go back to the AT-FS970M web interface and select **Dashboard** from the System tab drop-down menu.

   The Dashboard Page is displayed. See Figure 3 on page 28.

   Note
   All unsaved changes are discarded when you upgrade the software on a switch. To save your changes to the startup configuration file, click **SAVE**.

7. Select **System Upgrade** at the bottom of the page.

   The System Upgrade page is displayed. See Figure 22.

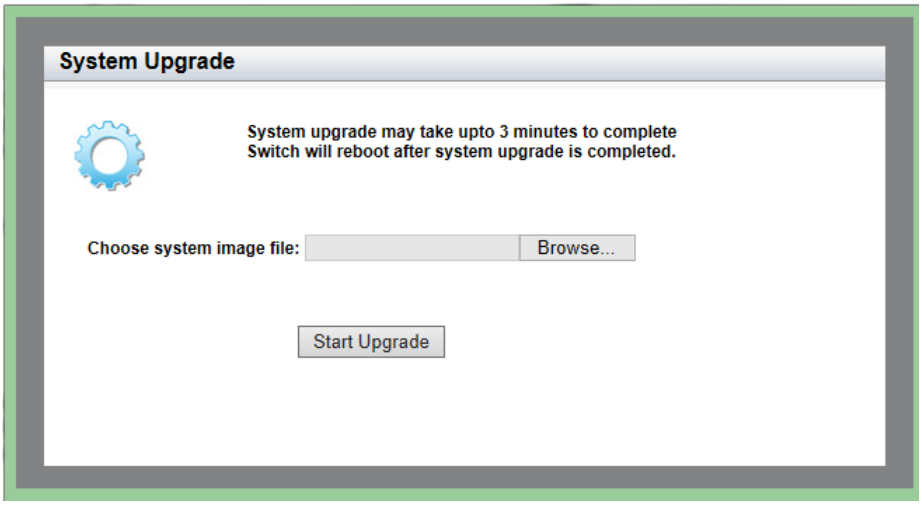


Figure 22. System Upgrade Page

8. Click **Browse** to select an image file.

9. Click **Open** to select the file that you downloaded in Step 5.

10. Click **Start Upgrade** to begin the software upgrade or close the System Upgrade page to cancel the procedure.

    The upgrade process takes approximately three minutes.

Note
Upgrading the system software on the switch ends your current web browser management session. To continue managing the switch, you must log in again.

Displaying System Information

To view basic information about the switch, select the **System** Tab.

The Dashboard Page is displayed as shown in Figure 3 on page 28.

The following fields are displayed:

- **Up Time**— Length of time since the switch was last reset or power-cycled in days, hours, minutes and seconds.

The System section displays the following information:

- **MAC Address—** MAC address of the switch.
- **Contact**— Contact person for the switch. To specify this field, see "Setting the Switch Information" on page 48.
- **Serial No.**— Unique serial number of the switch.
- **Location**— Location of the switch. To specify this field, see "Setting the Switch Information" on page 48.
- **System Name**— Name of the switch. To specify this field, see "Setting the Switch Information" on page 48.
- **Version**— Version number of the AT-FS970M software.

The Services section displays the following information:

- **IPv6 Management**— Indicates if IPv6 Management is enabled or disabled on the switch.
- **Spanning Tree**— Indicates if STP, RSTP, or MSTP is enabled on the switch. The default setting is "RSTP."
- **802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- **SNMP**— SNMP setting of the switch.
- **QoS**— Indicates if QoS is enabled or disabled on the switch.
- **RIP**— RIP setting of the switch
- **HTTP**— HTTP setting of the switch
- **LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- **Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- **SFLOW**— Indicates if sFlow is enabled or disabled on the switch.
- **SSH**— Indicates if SSH is enabled or disabled on the switch.
- **IGMP Snooping—** Indicates if IGMP Snooping is enabled or disabled on the switch.
- **Remote Logging**— Indicates if the remote log is enabled or disabled on the switch.

- **IGMP Snooping Querier**— Indicates if IGMP Snooping Querier is enabled or disabled on the switch.

The Administration Options section displays the following information:

- **System Upgrade**— Click this link to go to the System Upgrade page to upgrade your system software. See “Upgrading the Software” on page 58.
- **Reboot**— Click this link to reboot the switch. For instructions, see “Rebooting a Switch” on page 57.

Chapter 4

Setting Port Parameters

This chapter describes how to display and modify the port settings such as back pressure and flow control. In addition, it provides procedures to display and modify storm control settings.

This chapter contains the following sections:

For additional information about the port parameters and the storm control feature, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Port Parameters
- ❒ Port Parameter Commands

Port Numbers on the Switch

The ports on the switch are identified in the format shown in Figure 23.

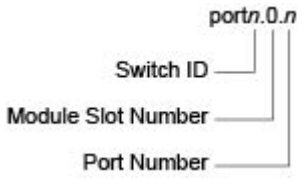


Figure 23. Port Number

- Switch ID: This number is used if the switch supports stacking. It is the switch's ID number in a stack. This number should always be 1 for AT-FS970M Series switches because they do not support stacking.
- Module Slot ID: This number is used to identify a slot in a modular switch. This number is always 0 for AT-FS970M Series switches because they are not modular switches.
- Port number: This is the port number.

Displaying the Port Parameters

To display the settings for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24.

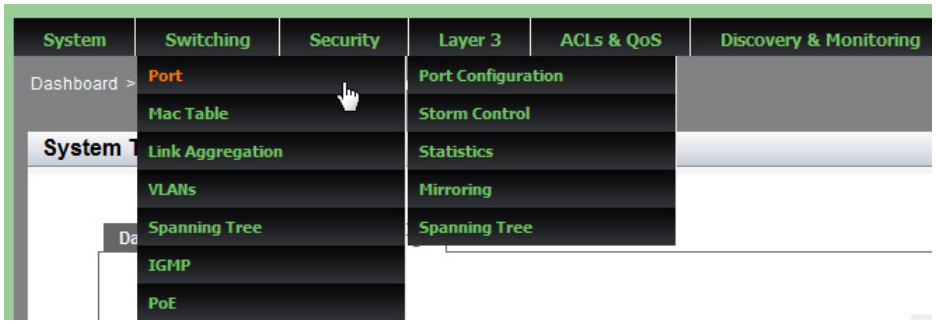


Figure 24. Switching Tab with Port Tab

2. From the Switching tab, hover over **Port**.

   The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Port Configuration** from the drop-down menu.

   The Port Configuration page is displayed. See Figure 25.

Port Configuration

	Interface	Type	Status	Link	Auto-Neg	Speed	Duplex	Polarity	Back Pressure	Back Pressure Limit	Flow Control	Flow Control Limit	Description
Edit	port1.0.1	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.2	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.3	10/100Base-T	Enabled	Up	Auto	100Mbps	Full	AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.4	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.5	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.6	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.7	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.8	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.9	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.10	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.11	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	

Figure 25. Port Configuration Page

4. The following fields are displayed:

   - **Interface**— Port ID.

- **Type**— Transmission speed and medium, copper or fiber optic, of the port. For example, 1000Base-SX indicates that the port is a fiber optic gigabit standard.
- **Status**— Indicates if the port is enabled or disabled. The default setting is “Enabled.” Disabling a port turns off its receiver and transmitter so that the port cannot forward traffic.
- **Link**— Indicates whether the port has successfully connected to a port on another switch or unit.
- **Auto-Neg**— Auto-Negotiation. The setting is “Auto” or “Manual.” The default is “Auto.”
- **Speed**— Speed of the port. The possible options are 10 Mbps, 100 Mbps, and 1000 Mbps.
- **Duplex**— Duplex mode of the twisted-pair port. The setting is “Half” or “Full.”
- **Polarity**— Indicates the port’s wiring configuration is MDI (medium dependent interface), MDI-X (medium dependent interface crossover), or the auto setting. This setting only applies to a twisted-pair port that is operating at 10 or 100 Mbps.
- **Back Pressure**— Indicates if back pressure is enabled or disabled on the port. Back pressure is used by a port during periods of packet congestion to temporarily stop its network counterpart from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates back pressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission. The default setting is “Disabled.”
- **Back Pressure Limit**— Threshold level for back pressure on the port. Specifies the number of cells for back pressure. The default value is 7935 cells.
- **Flow Control**— Indicates if flow control (send and receive) is enabled or disabled on a port. If flow control is enabled, a port sends pause packets when it reaches the point of packet congestion. Also, the port stops transmitting packets when it receives pause packets from its local or remote counterpart. When flow control is disabled, the port transmits regardless of packet congestion. In addition, the port continues transmitting packets when it receives pause packets from its local or remote counterpart. The default is “Disabled.”
- **Flow Control Limit**— Threshold level for flow control on a port. The default value is 7935.
- **Description**— Description of a port. To specify this field, see “Changing the Port Settings” on page 67.

Changing the Port Settings

You can change the settings of one port at a time. Use the following procedure to change the port settings or reset a port to its default value,

To change the port settings, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Port Configuration**.

   The Port Configuration page is displayed. See Figure 25 on page 65.

4. Click **Edit** next to the port that you want to modify.

   The Port Configuration Modify page is displayed. See Figure 26 on page 68.

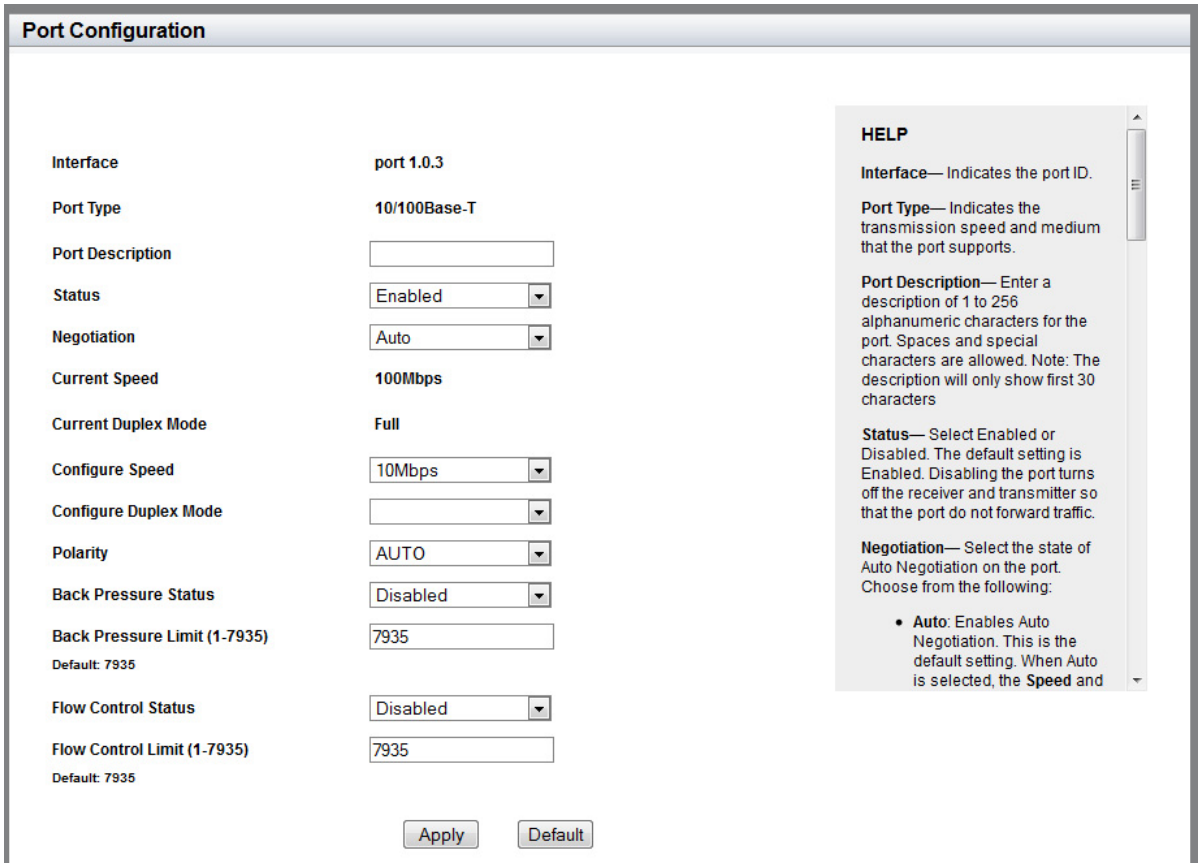


Figure 26. Port Configuration Modify Page

5. Specify the following fields as needed:

   - **Interface**— Indicates the port ID.
   - **Port Type**— Indicates the transmission speed and medium, copper or fiber, that the port supports.
   - **Port Description**— Enter a description of the port. You can enter up to 80 alphanumeric characters; however, only 30 characters are displayed in the Port Configuration List page. Spaces and special characters are allowed.
   - **Status**— Select either “Enabled” or “Disabled.” The default setting is enabled. Disabling a port turns off its receiver and transmitter so that the port does not forward traffic. You may want to disable a port if there is a problem with a cable or network device.
   - **Negotiation**— Select the state of Auto Negotiation from the pull-down menu. Setting “Auto” enables Auto Negotiation, and setting “Manual” disables Auto Negotiation. The default setting is “Auto.” When the setting for this field is “Auto,” the **Configure Speed** and **Configure Duplex** fields change from white to brown, and you

cannot select them. To change the **Configure Speed** and **Configure Duplex** fields, change the Negotiation setting to "Manual."

Note
When the port type is 1000Base fiber optic, the Negotiation must be "Auto", and you are not allowed to change the setting to "Manual."

- **Current Speed**— Displays the current speed of the port.
- **Current Duplex Mode**— Displays the current duplex mode setting of the port.
- **Configure Speed**— Select a port speed from the pull-down menu. For example, for a 10/100Base-T port, the options are 10 and 100. For a 1000Base-SX/LX port, 1000 is the only option. You can enter a value in this field when the Negotiation is set to "Manual."
- **Configure Duplex Mode**— Select the duplex mode of the twisted-pair port. Choose from Half, Full, or Auto. A port operating in half-duplex mode can either receive or transmit packets, but not both at the same time. Ports operating in full-duplex can both send and receive packets, simultaneously.
- **Polarity**— Select the wiring configuration of the twisted-pair port. When a port is operating at 1000 Mbps, the only option is "AUTO." When operating at 10 or 100 Mbps, in either half- or full-duplex mode, the options are "AUTO," "MDI," and "MDI-X."

  To forward traffic, a port on the switch and a port on a network device must have different settings. For instance, the wiring configuration of a switch port has to be MDI if the wiring configuration on a port on a network device is MDIX.

  To set the polarity to either "MDI" or "MDI-X" on a port, the Negotiation setting must be "Manual." A port with the Auto-Negotiation must set the polarity to "AUTO."

- **Back Pressure Status**— Enable or disable back pressure on a port that is operating at 10 or 100 Mbps in half-duplex mode. Back pressure is used by a port during periods of packet congestion to temporarily stop their network counterparts from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates back pressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission.

  To enable or disable back pressure on a port, the speed and duplex mode must be specified manually.

- **Back Pressure Limit (1 - 7935)**— Enter a threshold level for back pressure on the port. Enter the number of cells for back pressure.

A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

- **Flow Control Status**— Enable or disable the flow control feature. By default, flow control is disabled on the port.
- **Flow Control Limit (1 - 7935)**— Set the threshold level for flow control on the port. Enter the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

6. To set the port to the default port value, click **Default**. Otherwise skip this step.
7. Click **Apply**.
8. Click **SAVE** to save your changes to the startup configuration file.

Displaying the Storm Control Settings

To display the storm control settings, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Storm Control**.

   The Storm Control List page is displayed. See Figure 27.

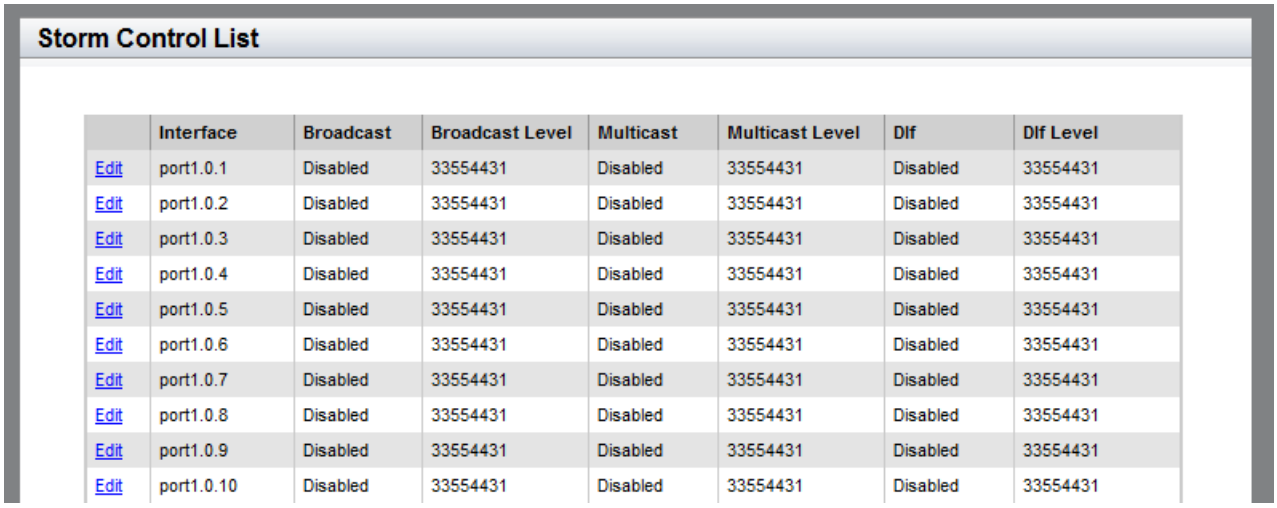


Figure 27. Storm Control List Page

The following fields are displayed:

- **Interface**— Port ID.
- **Broadcast**— Indicates whether the Broadcast threshold setting is enabled or disabled.
- **Broadcast Level**— Maximum number of ingress packets per second of broadcast packets the port receives. Broadcast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- **Multicast**— Indicates whether the Multicast threshold setting is enabled or disabled.
- **Multicast Level**— Indicates the maximum number of ingress packets per second of multicast packets the port receives.

Multicast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

- **Dlf**— Indicates whether the unknown unicast threshold setting is enabled or disabled.
- **Dlf Level**— Maximum number of ingress packets per second of unknown unicast packets the port receives. Unknown unicast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

Modifying the Storm Control Settings

To modify the storm control settings, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Storm Control**.

   The Storm Control List page is displayed. See Figure 25 on page 65.

4. Click **Edit** on the port that you want to modify.

   The Storm Control Settings page is displayed. See Figure 28.

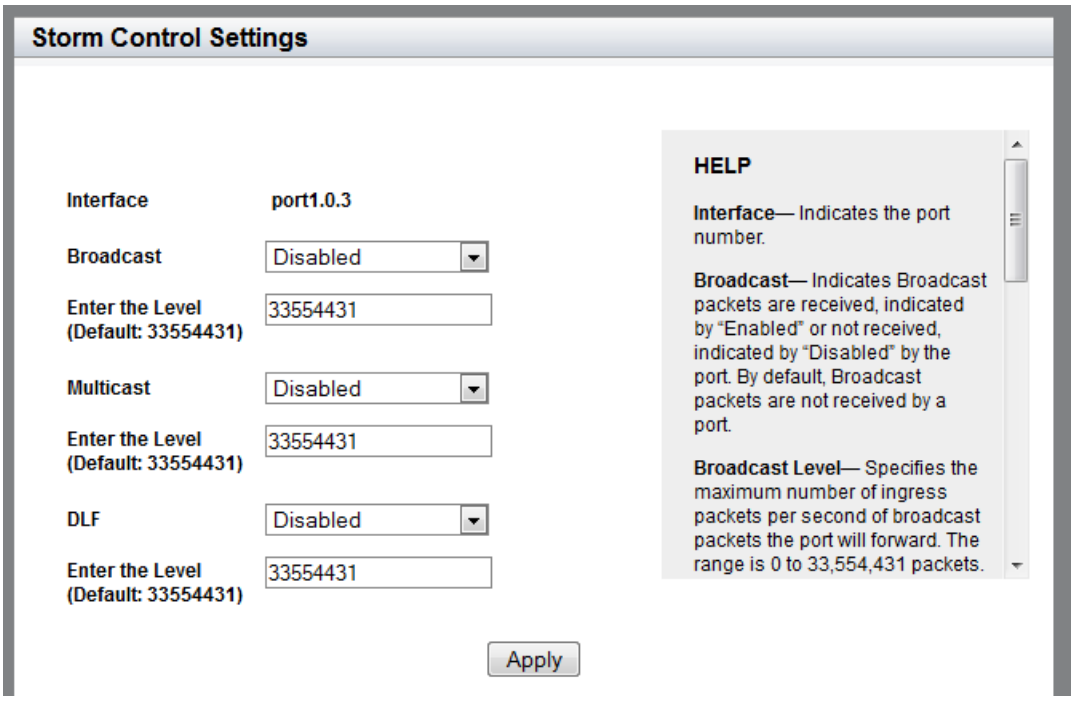


Figure 28. Storm Control Settings Page

5. Change the following fields as needed:

   - **Broadcast**— Enable or disable the broadcast storm control feature. When this feature is enabled, the port discards ingress broadcast packets that exceed the specified level. This feature is disabled by default.
   - **Enter the Level**— Enter the maximum number of ingress packets per second of broadcast packets the port receives. Broadcast packets that exceed this level are discarded when the feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
   - **Multicast**— Enable or disable the multicast storm control feature. When this feature is enabled, the port discards ingress multicast packets that exceed the specified level. This feature is disabled by default.
   - **Enter the Level**— Enter the maximum number of ingress packets per second of multicast packets the port receives. Multicast packets that exceed this level are discarded when this feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
   - **DLF**— Enable or disable the unknown unicast storm control feature. When this feature is enabled, the port discards ingress unknown packets that exceed the specified level.This feature is disabled by default.
   - **Enter the Level**— Enter the maximum number of ingress packets per second of unknown unicast packets the port receives. Unknown unicast packets that exceed this level are discarded when this feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

6. Click **Apply**.

7. Click **SAVE** to save your changes to the startup configuration file.

Chapter 5

Setting Port Statistics

This chapter describes how to display and clear port statistics. Within the AlliedWare Plus™ software, you can display and clear transmit, receive, and interface port statistics.

This chapter contains the following topics:

For additional information about port statistics, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Port Parameters
- ❒ Port Parameter Commands

Displaying Port Statistics

You can display several types of port statistics. See the following sections:

- “Displaying Transmit and Receive Port Statistics” on page 76
- “Displaying Receive Statistics” on page 77
- “Displaying Transmit Statistics” on page 79
- “Displaying Interface Statistics” on page 80

Displaying Transmit and Receive Port Statistics

To display the transmit and receive statistics for all of the switch ports, do the following:

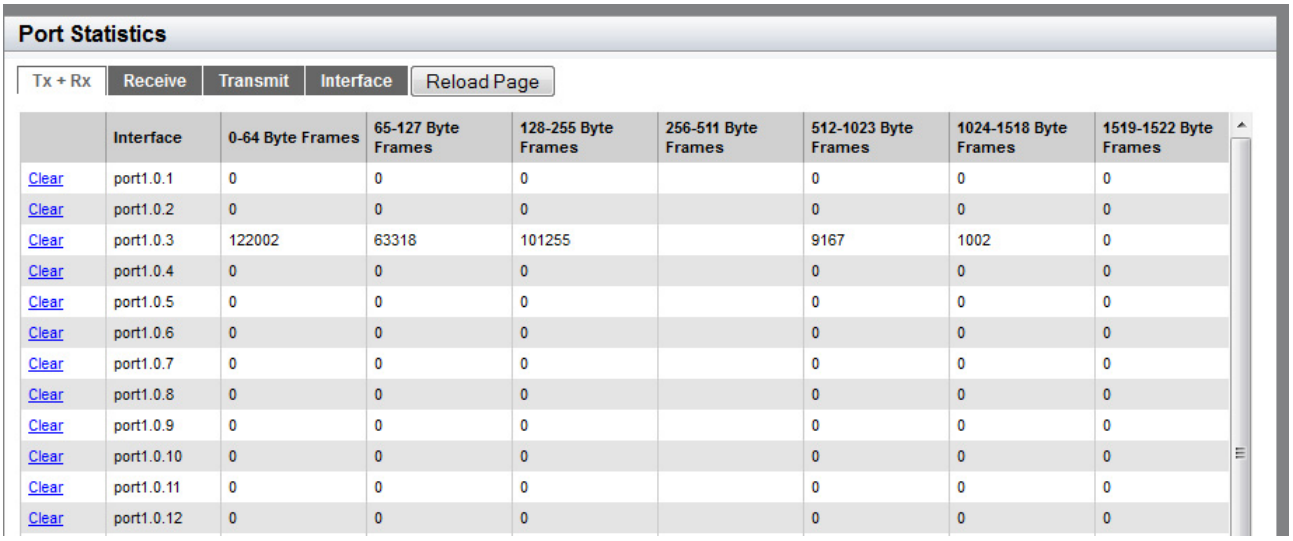
1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Statistics**.

   The Port Statistics page is displayed with the Tx + Rx tab automatically selected. See Figure 29.



	Interface	0-64 Byte Frames	65-127 Byte Frames	128-255 Byte Frames	256-511 Byte Frames	512-1023 Byte Frames	1024-1518 Byte Frames	1519-1522 Byte Frames
Clear	port1.0.1	0	0	0		0	0	0
Clear	port1.0.2	0	0	0		0	0	0
Clear	port1.0.3	122002	63318	101255		9167	1002	0
Clear	port1.0.4	0	0	0		0	0	0
Clear	port1.0.5	0	0	0		0	0	0
Clear	port1.0.6	0	0	0		0	0	0
Clear	port1.0.7	0	0	0		0	0	0
Clear	port1.0.8	0	0	0		0	0	0
Clear	port1.0.9	0	0	0		0	0	0
Clear	port1.0.10	0	0	0		0	0	0
Clear	port1.0.11	0	0	0		0	0	0
Clear	port1.0.12	0	0	0		0	0	0

Figure 29. Port Statistics Page with Tx + Rx Tab

The following fields are displayed:

- **Interface**— Port ID.
- **0-64 Byte Frames**— Number of frames transmitted by the port that contains 0 to 64 bytes.
- **65-127 Byte Frames**— Number of frames transmitted by the port that contains 65 to 127 bytes.
- **128-255 Byte Frames**— Number of frames transmitted by the port that contains 128 to 255 bytes.
- **256-511 Byte Frames**— Number of frames transmitted by the port that contains 256 to 511 bytes.
- **512-1023 Byte Frames**— Number of frames transmitted by the port that contains 512 to 1023 bytes.
- **1024-1518 Byte Frames**— Number of frames transmitted by the port that contains 1024 to 1518 bytes.
- **1519-1522 Byte Frames**— Number of frames transmitted by the port that contains 1519 to 1522 bytes.

Displaying Receive Statistics

To display the statistics on the Receive Statistics tab, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

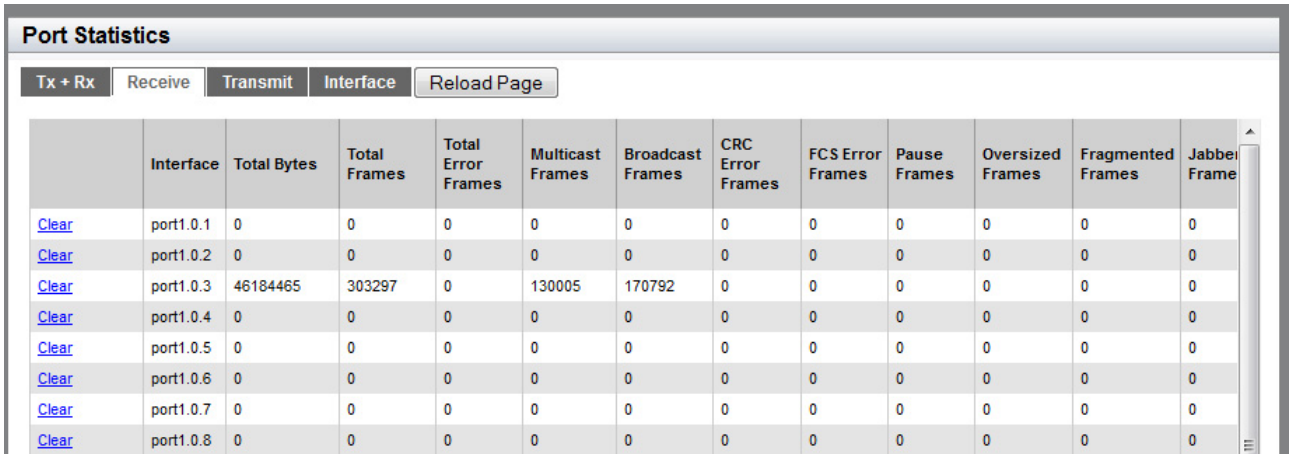
2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Statistics**.

   The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 76.

4. Click on the **Receive** Tab.

   The Port Statistics with the Receive tab selected is displayed. See Figure 30 on page 78.



	Interface	Total Bytes	Total Frames	Total Error Frames	Multicast Frames	Broadcast Frames	CRC Error Frames	FCS Error Frames	Pause Frames	Oversized Frames	Fragmented Frames	Jabber Frame
Clear	port1.0.1	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.2	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.3	46184465	303297	0	130005	170792	0	0	0	0	0	0
Clear	port1.0.4	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.5	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.6	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.7	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.8	0	0	0	0	0	0	0	0	0	0	0

Figure 30. Port Statistics with the Receive Tab

The following fields are displayed:

- **Interface**— Port ID.
- **Total Bytes**— Number of received bytes.
- **Total Frames**— Number of received frames.
- **Total Error Frames**— Total number of received frames with errors.
- **Multicast Frames**— Number of received multicast frames.
- **Broadcast Frames**— Number of received broadcast frames.
- **CRC Error Frames**— Number of frames with a cyclic redundancy check (CRC) error, but with the proper length (64 -1518 bytes) received by the port.
- **FCS Error Frames**— Number of ingress frames that had frame check sequence (FCS) errors.
- **Pause Frames**— Number of received flow-control pause frames.
- **Oversized Frames**— Number of received frames that exceeded the maximum size as specified by IEEE 802.3 (1518 bytes, including the CRC).
- **Fragmented Frames**— Number of received fragmented frames.
- **Jabber Frames**— Number of occurrences of corrupted data or useless signals the port has encountered.

Note
The following fields are not displayed in Figure 30.

- **Undersize Frames**— Number of received frames that were less than the minimum length as specified by IEEE 802.3 (64 bytes, including the CRC).
- **Dropped Frames**— Number of frames successfully received and buffered by the port, but discarded and not forwarded.
- **MTU Exceed Discarded Frames**— Number of received frames with an MTU that exceeds the MTU of the switch. These frames are discarded.
- **MAC Error Frames**— Number of Receive Error events seen by the receive side of the MAC.

Displaying Transmit Statistics

To display the statistics on the Transmit Statistics tab, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Statistics**.

   The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 76.

4. Click the **Transmit** tab.

   The Port Statistics with the Transmit tab selected is displayed. See Figure 31.

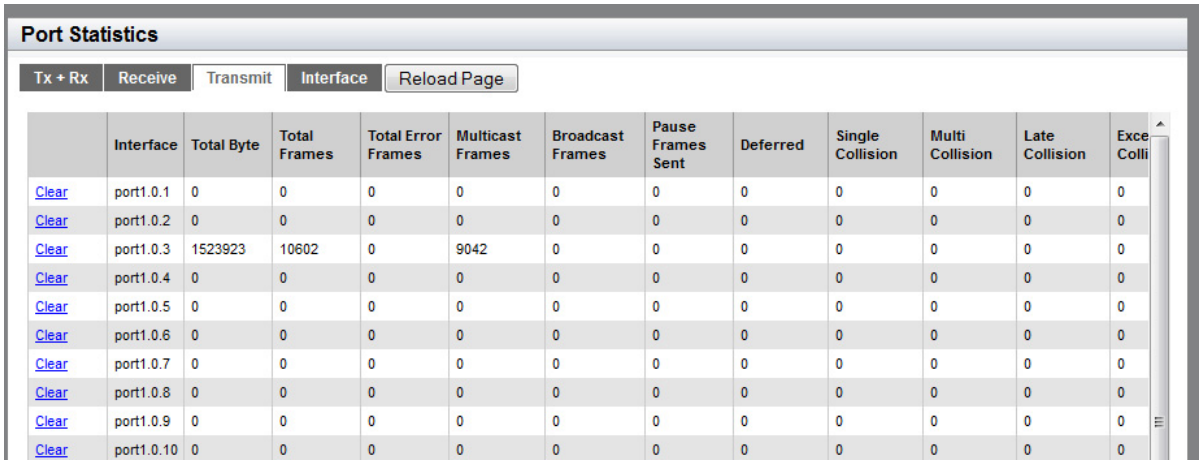


Figure 31. Port Statistics with the Transmit Tab

The following fields are displayed:

- **Interface**— Port ID.
- **Total Bytes**— Number of transmitted bytes.

- **Total Frames**— Number of transmitted frames.
- **Total Error Frames**— Number of transmitted frames with errors.
- **Multicast Frames**— Number of transmitted multicast frames.
- **Broadcast Frames**— Number of transmitted broadcast frames.
- **Pause Frames Sent**— Number of transmitted flow-control pause frames.
- **Deferred**— Number of egress frames that the port could not immediately transmit.
- **Single Collision**— Number of frames that were transmitted after at least one collision.
- **Multi Collision**— Number of frames that were transmitted after more than one collision.
- **Late Collision**— Number of late collisions.
- **Excessive Collision**— Number of excessive collisions.
- **Total Collision Frames**— Total number of collisions on the port.
- **MAC Error Frames**— Number of frames not transmitted correctly or dropped due to an internal MAC transmit error.

Displaying Interface Statistics

To display the interface statistics, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

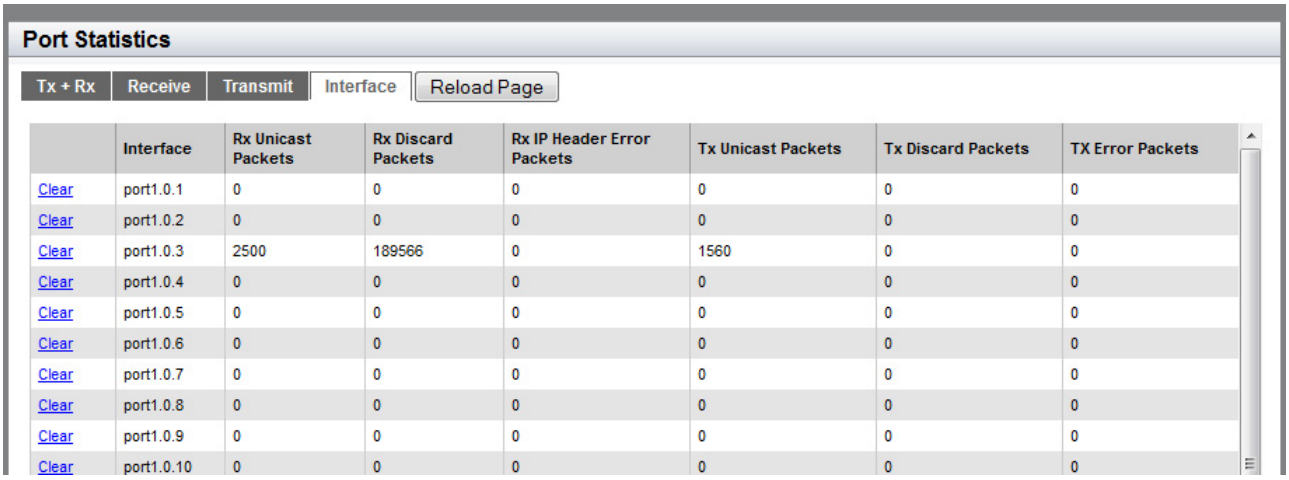
2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Statistics**.

   The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 76.

4. Click the **Interface** tab.

   The Port Statistics Page with the Interface tab selected is displayed. See Figure 32 on page 81.



	Interface	Rx Unicast Packets	Rx Discard Packets	Rx IP Header Error Packets	Tx Unicast Packets	Tx Discard Packets	TX Error Packets
Clear	port1.0.1	0	0	0	0	0	0
Clear	port1.0.2	0	0	0	0	0	0
Clear	port1.0.3	2500	189566	0	1560	0	0
Clear	port1.0.4	0	0	0	0	0	0
Clear	port1.0.5	0	0	0	0	0	0
Clear	port1.0.6	0	0	0	0	0	0
Clear	port1.0.7	0	0	0	0	0	0
Clear	port1.0.8	0	0	0	0	0	0
Clear	port1.0.9	0	0	0	0	0	0
Clear	port1.0.10	0	0	0	0	0	0

Figure 32. Port Statistics Page with Interface Tab

The following fields are displayed:

- **Interface**— Port ID.
- **Rx Unicast Packets**— Number of ingress unicast packets.
- **Rx Discard Packets**— Number of ingress packets that were discarded prior to transmission because of an error.
- **Rx IP Header Error Packets**— Number of ingress packets that were discarded because of an IP Header error.
- **Tx Unicast Packets**— Number of egress unicast packets.
- **Tx Discard Packets**— Number of egress packets that were discarded prior to transmission because of an error.
- **Tx Error Packets**— Number of egress error packets.

Clearing Port Statistics

To clear the statistics for a port, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Statistics**.

   The Port Statistics Page with Tx + Rx tab selected is displayed. See Figure 29 on page 76.

4. Select the desired Port Statistics tab. Choose from the following:

   - **Tx+Rx**— Transmit and receive statistics.
   - **Receive**— Receive statistics.
   - **Transmit**— Transmit statistics.
   - **Interface**— Interface statistics.

5. Click **Clear** on the port that you want to clear.

Reloading Statistics

Port statistics are constantly counting, and the values are changing so that the data displayed in the Port Statistics pages are not the most recent. To display the latest data possible, click on the **Reload Page** button on a Port Statistics page.

Figure 33 shows the Reload Page button on the Port Statistics page as an example.

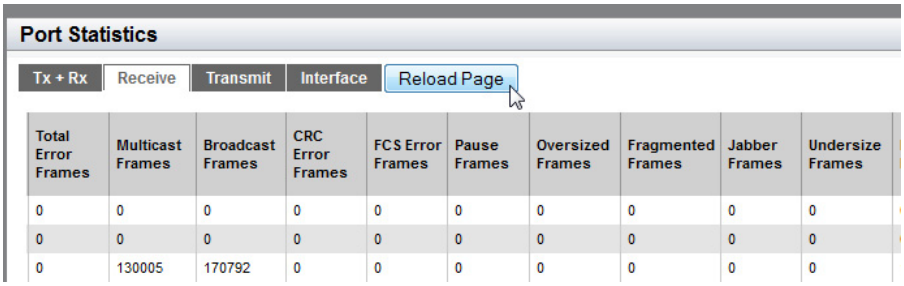


Figure 33. Port Statistics Page with the Reload Page Button

Chapter 6

Port Mirroring

The port mirror is a management tool that allows you to monitor the traffic on one or more ports on the switch. It works by copying the traffic from source ports to a destination port where the traffic can be monitored with a network analyzer. The port mirror can be used to troubleshoot network problems or to investigate possible unauthorized network access. The performance and speed of the switch is not affected by the port mirroring feature.

This chapter provides a brief description of the port mirroring feature and explains how to display and set port mirroring. See the following sections:

For more information about port mirroring, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Port Mirror
- ❒ Port Mirror Commands

Overview

To use the port mirroring feature, you must designate one or more source ports and one destination port. The source ports are the ports whose packets are mirrored and monitored. The destination port is the port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port on the switch.

Here are guidelines for setting the port mirroring feature:

- ❒ Port mirroring can have one destination port.
- ❒ Port mirroring can have more than one source port. This allows you to monitor the traffic on multiple ports at the same time. For example, you might monitor the traffic on all the ports of a particular VLAN.
- ❒ You can select whether to mirror the receive traffic, the transmit traffic, or both, on the source ports.
- ❒ The destination port must not be a member of a static port trunk or an LACP trunk.

Displaying Port Mirroring Settings

To display the port mirroring assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring**.

   The Port Mirroring List page is displayed. See Figure 34.

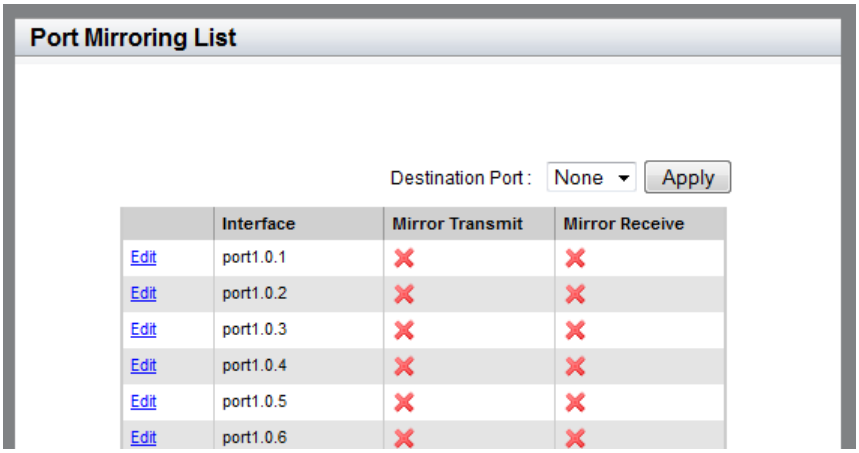


Figure 34. Port Mirroring List Page

The following fields are displayed:

- **Destination Port**— Use the pull-down menu to select the port where the packets from the source ports are copied and where the network analyzer is connected. You can assign only one destination port to the switch.
- **Interface**— Port ID.
- **Mirror Transmit**— Source port whose transmitted (egress) packets are mirrored and monitored. In this case, transmit is the specified direction in which the packets are mirrored. There can be multiple source ports on the switch.
- **Mirror Receive**— Source port whose received (ingress) packets are mirrored and monitored. In this case, receive is the specified direction in which the packets are mirrored. There can be multiple source ports on the switch.

Assigning a Destination Port

The destination port is the source port where the packets are copied. You can only assign one destination port to the switch.

To assign a destination port, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring** from the drop-down menu.

   The Port Mirroring List page is displayed. See Figure 34 on page 87.

4. Select the pull-down menu next to the **Destination Port** field at the top of the page.

5. Click on the port that you want to designate as the destination port.

   You can only assign one destination port to a switch.

6. Click **Apply**.

   The **Edit** option is removed from the port. This indicates the destination port for the switch.

7. Click **SAVE** to save your changes to the startup configuration file.

Specifying Direction Type

To specify source ports and type of packet direction, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

   The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring** from the drop-down menu.

   The Port Mirroring List page is displayed. See Figure 34 on page 87.

4. Click Edit next to the port that you want to specify as a source port for mirroring.

   The Modify Port Mirroring Page is displayed. See Figure 35.

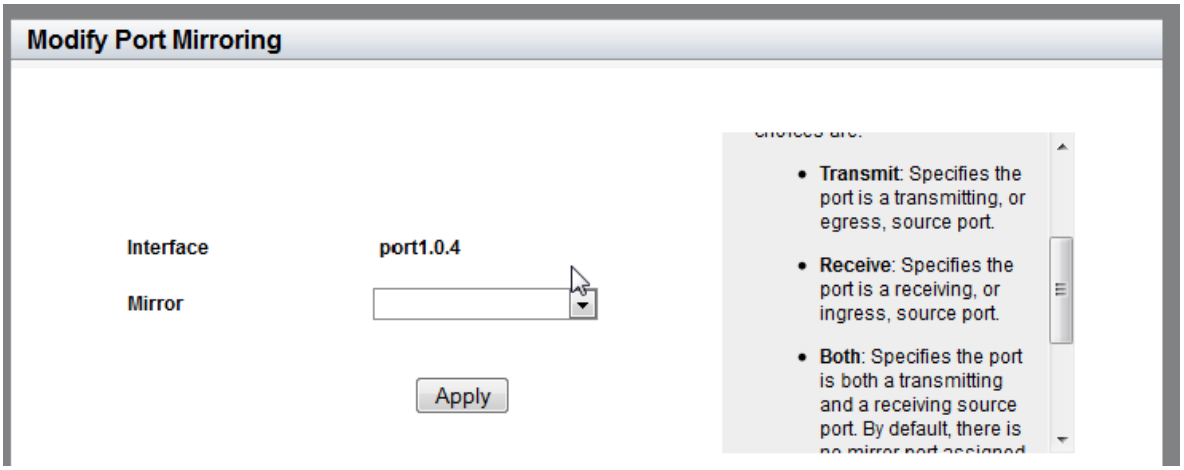


Figure 35. Modify Port Mirroring Page

5. Select the type of mirroring for the port. The options are:

   - **Transmit**— Egress traffic on this port to be copied to the destination port.
   - **Receive**— Ingress traffic on this port to be copied to the destination port.
   - **Both**— Both the egress and ingress traffic on this port to be copied to the destination port.

   By default, there is no port assigned to port mirroring.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Deleting Port Mirroring Settings

To delete the existing port mirroring settings, assign the port to "None" by doing the following:

1. Display the port mirroring assignments. See "Displaying Port Mirroring Settings" on page 87.

   The Port Mirroring List page is displayed. See Figure 34 on page 87.

2. Select the pull-down menu next to the **Destination Port** field at the top of the page.

3. Click on "None."

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Chapter 7

Spanning Tree Protocol on a Port

The Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

This chapter provides a brief description of the spanning tree protocols and explains how to set spanning tree on a port. See the following sections:

Note
For information about how to set a spanning tree protocol for the switch, see Chapter 12, “Spanning Tree Protocols on the Switch” on page 143.

For more information about the spanning tree protocols, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Spanning Tree and Rapid Spanning Tree Protocols
- ❒ Spanning Tree Protocol (STP)
- ❒ STP Commands
- ❒ Rapid Spanning Tree Protocol (RSTP)
- ❒ RSTP Commands

Overview

STP and RSTP prevent loops from forming by ensuring that only one path is available at a time between the switches in your network. Where multiple paths exist, these spanning tree protocols place the extra paths in a standby or blocking mode. In addition, these protocols can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms as well as maintain network connectivity by activating backup redundant paths.

One of the primary differences between the STP and RTP protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines 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.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent lost of data packets. RSTP is much faster than STP. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network.

Only one spanning tree can be active on the switch at a time. The default setting is RSTP.

Displaying Port Spanning Tree Protocol Settings

To display the Spanning Tree Protocol settings for all of the switch ports, do the following:

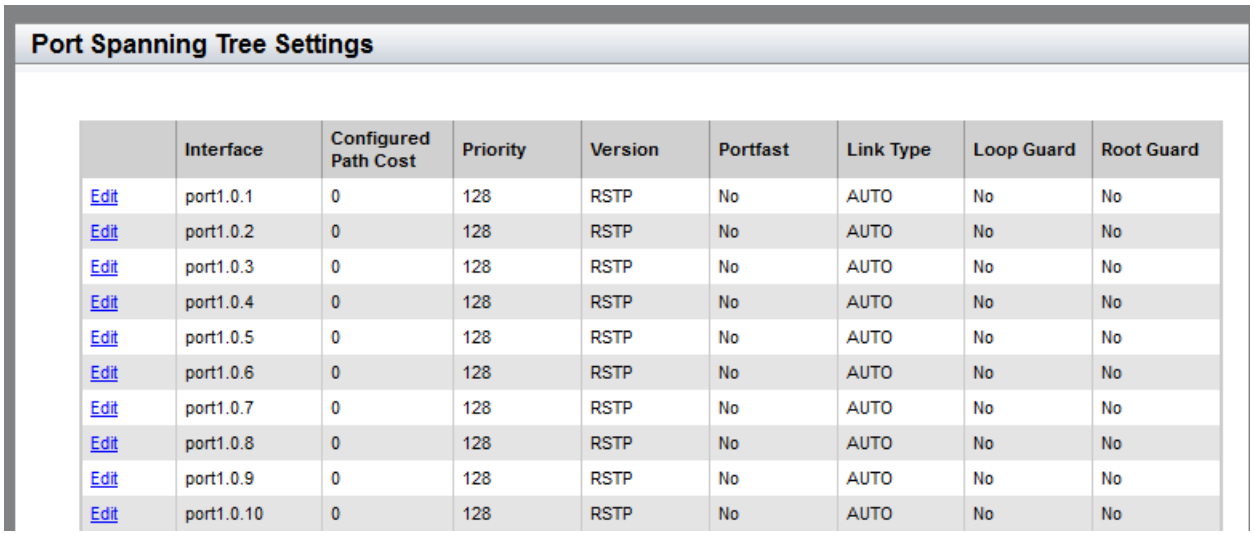
1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Spanning Tree**.

   The Port Spanning Tree Settings page is displayed. See Figure 36.



	Interface	Configured Path Cost	Priority	Version	Portfast	Link Type	Loop Guard	Root Guard
Edit	port1.0.1	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.2	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.3	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.4	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.5	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.6	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.7	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.8	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.9	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.10	0	128	RSTP	No	AUTO	No	No

Figure 36. Port Spanning Tree Settings Page

The following fields are displayed:

- **Interface**— Port ID.
- **Configured Path Cost**— Cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200,000,000.
- **Priority**— Port priority number for the switch. The device with the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

- **Version**— Spanning Tree Protocol version: STP, RSTP, or MSTP. The default setting is RSTP.
- **Portfast**— Indicates if the port is designated as an edge port. If a port on the switch is not connected to a switch or a network that is running the spanning tree protocol, you can designate it as an edge port. A port that is designated as an edge port transitions from the blocking to forwarding state immediately to minimize the time that the port must wait for spanning tree to converge.

  If an edge port starts to receive BPDUs, the spanning tree protocol no longer considers the port as an edge port.

- **Link Type**— Indicates one of the following:

  Shared: The shared link type disables rapid transition of the port to the forwarding state during the convergence process. You may want to set Link Type to Shared when the port is connected to a hub with multiple switches connected to it.

  PTP: The point-to-point link type allows for rapid transition of the port to the forwarding state during the convergence process.

  AUTO: The switch automatically determines the link type of the port.

- **Loop Guard**— Indicates the BPDU loop-guard feature on the port is enabled (Yes) or disabled (No). If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset.

  This feature is supported in RSTP and not supported on edge ports. The default setting for BPDU loop-guard on a port is disabled.

- **Root Guard**— Indicates if the Root Guard feature is enabled or disabled.

Modifying Port Spanning Tree Protocol Settings

To modify port settings for Spanning Tree Protocol, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Spanning Tree**.

   The Port Spanning Tree page is displayed. See Figure 36 on page 95.

4. Click Edit on the port that you want to change.

   The Modify Port Spanning Tree Settings page is displayed. See Figure 37.

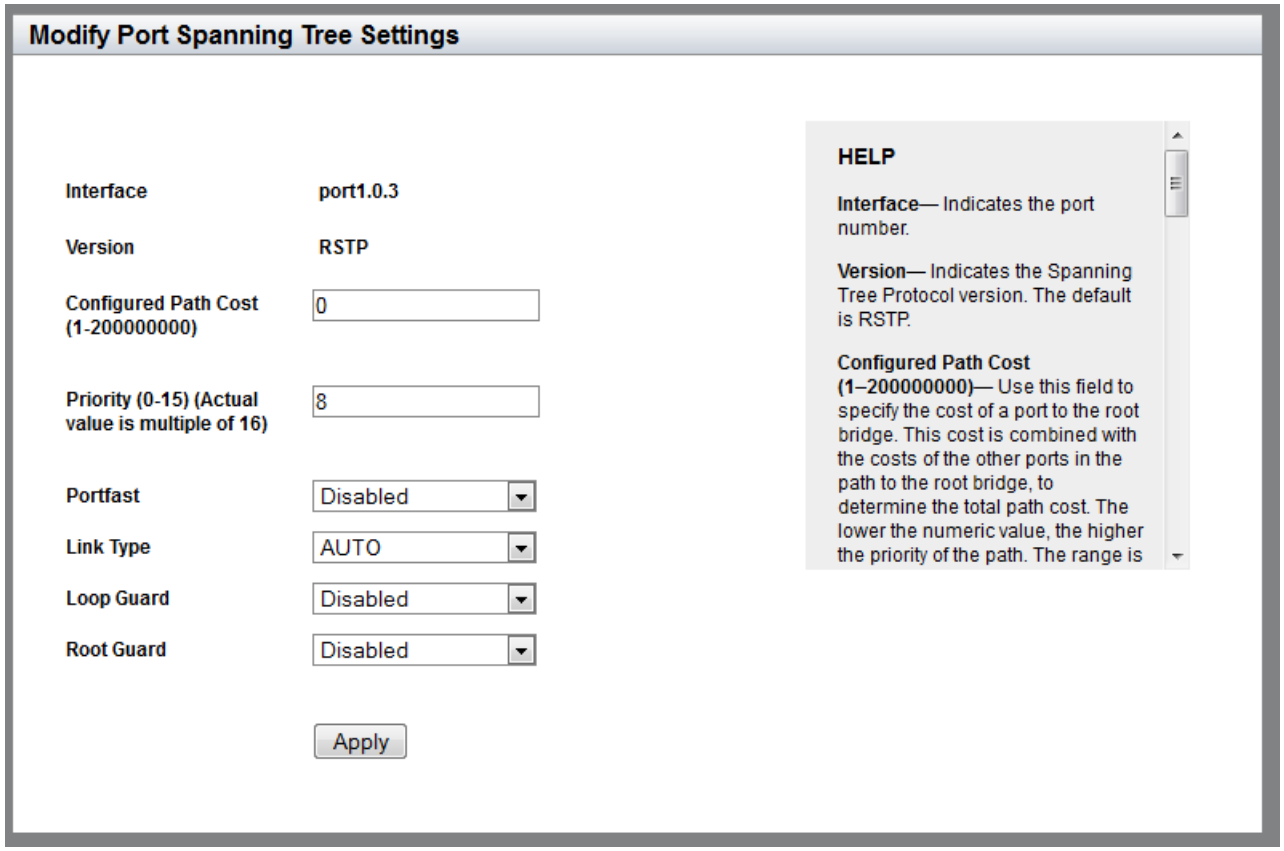


Figure 37. Modify Port Spanning Tree Settings Page

5. Change the following settings as needed:

   - **Interface**— Indicates the port ID.

- **Version**— Indicates the Spanning Tree Protocol version. The default setting is RSTP.
- **Configured Path Cost**— Enter the cost of the port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200,000,000. The default value is 0.
- **Priority (0-15)**— Enter the priority value of the port. You can influence which port is elected for a specific port role.

  For example, when the switch has the two ports with the same path cost, and the path cost is the lowest on the switch, it uses the port priority value to determine which port is the root port.

  If both priority values of these two ports are the same, the switch elects a port with the lower port ID.

  The range of the priority value is 0 to 240, in increments of 16, for a total of 16 increments. See Table 1. Specify the increment of the desired value. The default port priority is 128 (increment 8).

Table 1. STP Port Priority Value Increments

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

- **PortFast**— Select “Enabled” to assign the port as an edge port, or “Disabled” to assign the port as an non-edge port. Assign the port as an edge port if the port is not connected to spanning tree devices or to LANs that have spanning tree devices. An edge port transitions from the blocking to forwarding state immediately so that the host connected to the edge port can connect to the network immediately, rather than waiting for spanning tree to converge.

  When an edge port starts to receive BPDUs, the switch no longer considers the port as an edge port.

- **Link Type**— Choose from the following settings:

  AUTO: The switch determines the link type of the port is either PTP or Shared. If a port is set to full-duplex mode, the link type is point-to-point. If a port is set to half-duplex mode, the link type is shared.

  PTP: Allows the port rapid transition to the forwarding state during the convergence process of the spanning tree domain.

  Shared: Disables rapid transition. You may want to set the link type to shared if the port is connected to a hub with multiple switches connected to it.

- **Loop Guard**— Enable or disable the BPDU loop-guard feature on the port. If a port with the loop guard activated stops receiving BPDU packets, the switch automatically shut down the port. A port that is disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.
- **Root Guard**— Enable or disable the Root Guard feature.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Chapter 8

Setting the MAC Address

The procedures in this chapter describe how to display the MAC address table that resides on the switch, as well as how to add a unicast or multicast MAC addresses to the table. Procedures to modify and delete MAC addresses within the table are also included in this chapter.

See the following sections:

For more information about MAC addresses, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- MAC Address Table
- MAC Address Table Commands

Displaying the Unicast MAC Addresses

To display the unicast MAC addresses, do the following:

1. Hover the cursor over the Switching Tab.

   The Switching Tab is displayed. See Figure 38.

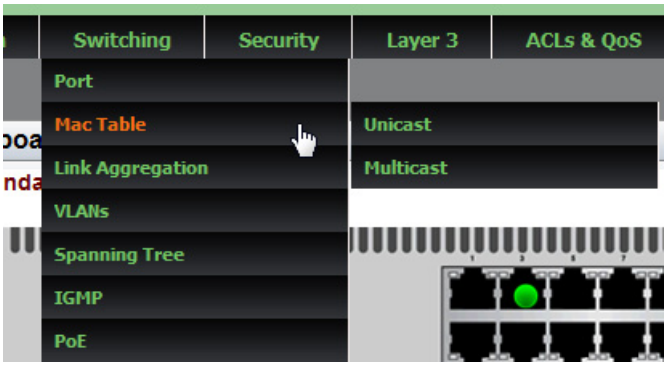


Figure 38. Switching Tab

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

   The Unicast MACs page is displayed. See Figure 39.

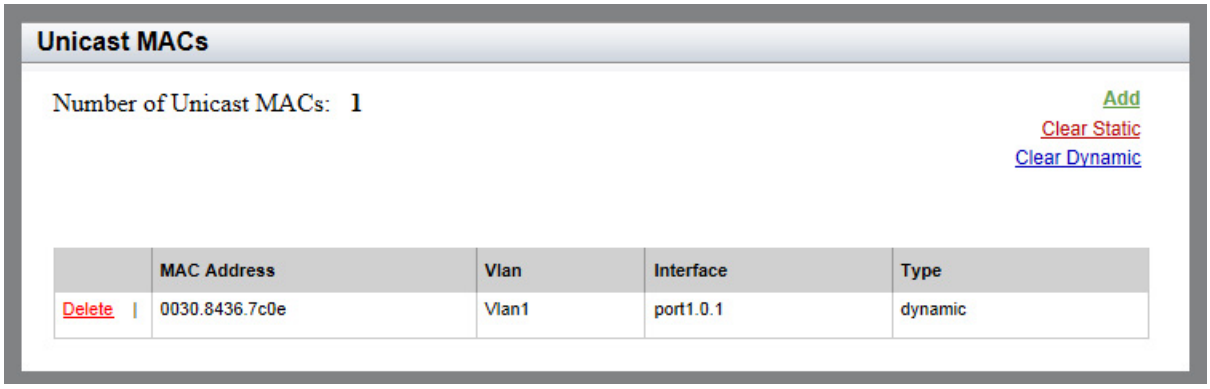


Figure 39. Unicast MACs Page

The following fields are displayed:

- **MAC Address**— Dynamic and static unicast MAC addresses learned on or assigned to the port.
- **Vlan**— ID number of the VLAN that the node designated by the MAC address belongs to. The default VLAN is Vlan1.
- **Interface**— Port number where the address was learned on or assigned to.
- **Type**— Type of MAC address entry, static or dynamic.

Displaying the Multicast MAC Addresses

To display the multicast MAC addresses, do the following:

1. Hover the cursor over the Switching tab.

   The Switching Tab is displayed. See Figure 38 on page 102.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

   The Multicast MACs Page is displayed. See Figure 40.

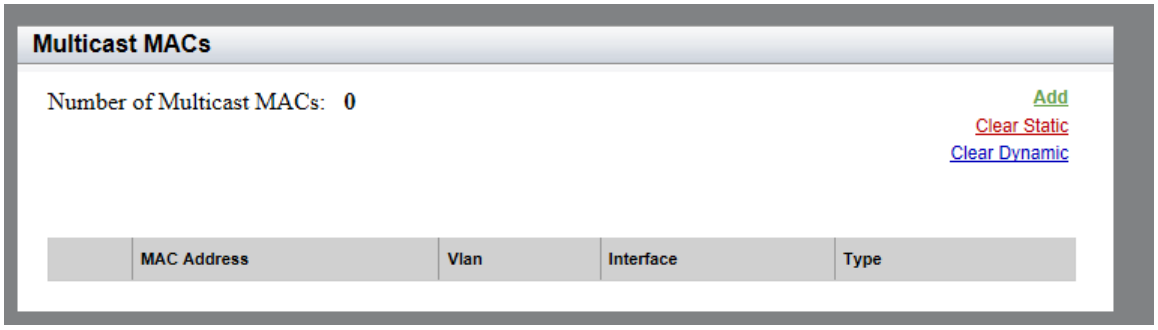


Figure 40. Multicast MACs Page

The following fields are displayed:

- **MAC Address**— Dynamic or static unicast MAC address learned on or assigned to the port.
- **Vlan**— ID number of the VLAN where the multicast application and the host nodes are members. The default VLAN is Vlan1.
- **Interface**— Port where the address was learned or assigned.
- **Type**— Type of MAC address entry: static or dynamic.

Assigning a Unicast MAC Address

To assign a unicast MAC address to the MAC address table, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

   The Unicast MACs page is displayed. See Figure 39 on page 102.

3. Click Add.

   The Unicast MAC Page is displayed. See Figure 41.

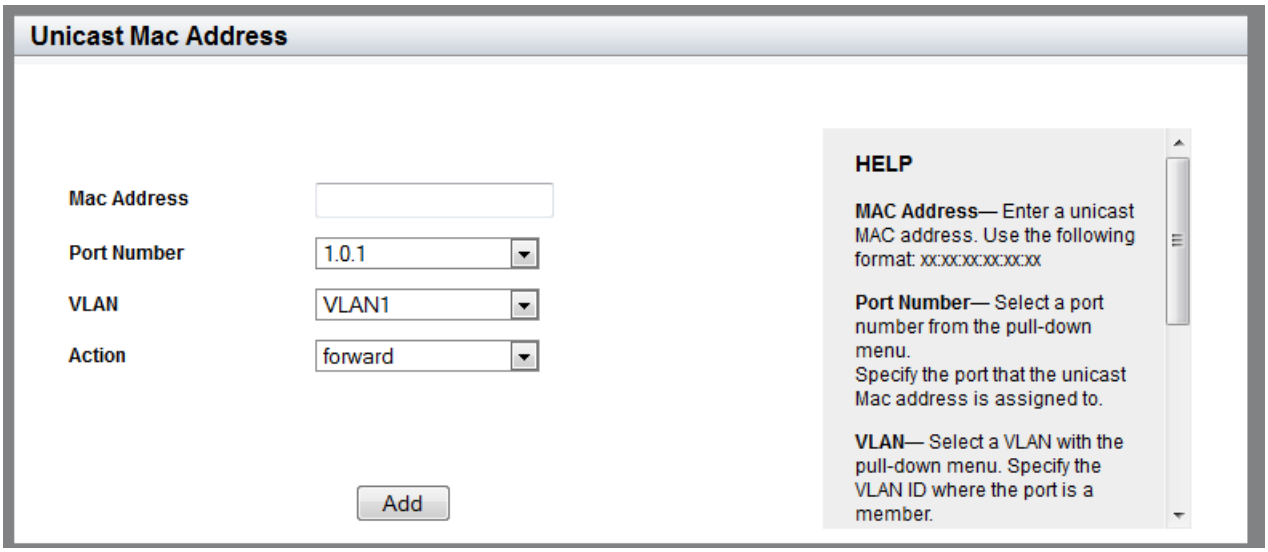


Figure 41. Unicast MAC Address Page

4. To add a new unicast MAC address, do the following:

   - **MAC Address**— Enter a unicast MAC address. Use the following format:

     xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

   - **Port Number**— Select the port number to which the end node of the MAC address is connected.
   - **VLAN**— Select a VLAN where the port is a member.
   - **Action**— Select one of the following options:

Forward: Specifies the port to forward packets that have the designated source MAC address.

Discard: Specifies the port to discard packets that have the designated source MAC address.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a Multicast MAC Address

To assign a multicast MAC address to the MAC address table, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

   The Multicast MACs page is displayed. See Figure 40 on page 104.

3. Click Add.

   The Multicast MAC Address page is displayed. See Figure 42.

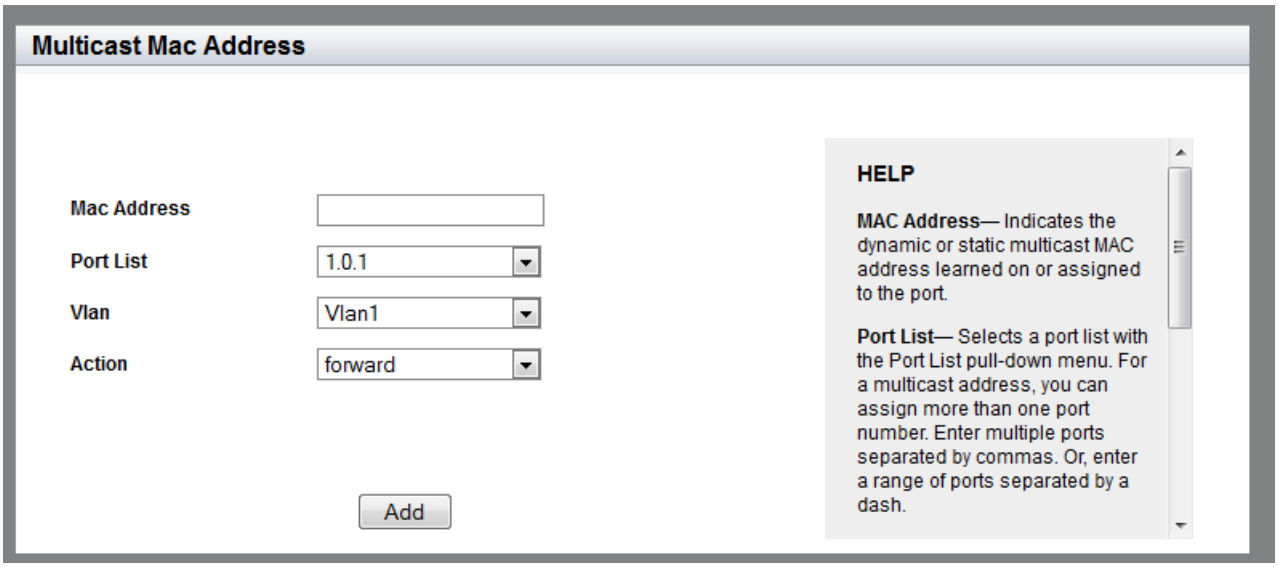


Figure 42. Multicast MAC Address Page

4. To add a new multicast MAC address, do the following:

   - **MAC Address**— Enter a multicast MAC address. Use the following format:

     xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

   - **Port Number**— Select the port number to which the end node of the MAC address is connected.
   - **Vlan**— Select a VLAN where the port is a member.
   - **Action**— Select one of the following options:

Forward: Specifies the port to forward packets that have the designated source MAC address.

Discard: Specifies the port to discard packets that have the designated source MAC address.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting a Unicast MAC Address

To delete a unicast address or clear all static or dynamic unicast addresses, do the following:

1. Hover the cursor over the Switching tab.

   The Switching tab is displayed. See Figure 38 on page 102.

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

   The Unicast MACs page is displayed. See Figure 39 on page 102.

3. Do one of the following:

   - To clear all of the static unicast addresses in the MAC address table, click Clear Static.
   - To clear the dynamic unicast addresses in the MAC address table, click Clear Dynamic.
   - To delete a specific MAC address, click Delete next to the MAC address that you want to delete.

Deleting a Multicast MAC Address

To delete a multicast address or clear all static or dynamic multicast addresses, do the following:

1. Hover the cursor over the Switching Tab.

   The Switching Tab is displayed. See Figure 38 on page 102.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

   The Multicast MACs page is displayed. See Figure 40 on page 104.

3. Do one of the following:

   - To clear all of the static multicast addresses in the MAC address table, click Clear Static.
   - To clear all of the dynamic multicast addresses in the MAC address table, click Clear Dynamic.
   - To delete a specific MAC address, click Delete next to the MAC address that you want to delete.

Chapter 9

Link Aggregation Control Protocol (LACP)

LACP is used to increase the bandwidth between the switch and other LACP compatible devices by grouping ports together to form single virtual links.

This chapter provides a brief description of LACP and explains how to display and set LACP. See the following sections:

For more information about LACP trunks, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- Link Aggregation Control Protocol (LACP)
- LACP Commands

Overview

LACP trunks are similar in function to static port trunks, but they are more flexible. The implementations of static trunks tend to be vendor-specific and may not always be compatible. In contrast, the implementation of LACP in the switch is compliant with the IEEE 802.3ad standard. It is interoperable with equipment from other vendors that also comply with the standard. This makes it possible to create LACP trunks between the switch and network devices from other manufacturers.

The main component of an LACP trunk is an aggregator. An aggregator is a group of ports on the switch. The ports of an aggregator are further grouped into a trunk, referred to as an aggregate trunk. An aggregator can have only one trunk. You have to create a separate aggregator for each trunk on the switch.

An aggregate trunk can consist of any number of ports on the switch, but only a maximum of eight ports can be active at a time. If an aggregate trunk contains more ports than can be active at one time, the extra ports are placed in standby mode. Ports in standby mode do not pass network traffic, but they do transmit and accept LACP data unit (LACPDU) packets, which the switch uses to search for LACP compliant devices.

Displaying LACP Trunks

To display the LACP trunk assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation menu, see Figure 43.

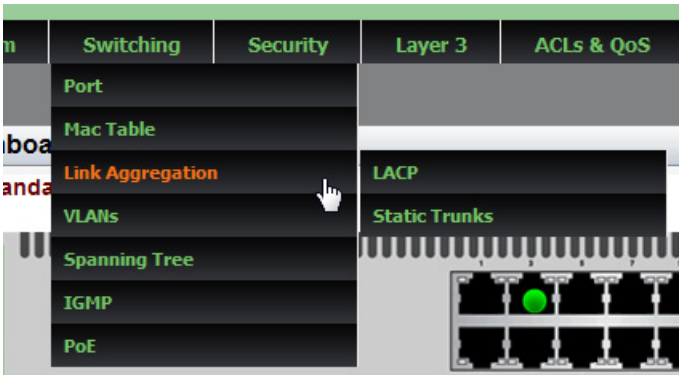


Figure 43. Switching Tab with Link Aggregation Selected

3. Move the cursor to the right and select **LACP**.

   The LACP Trunks page is displayed. See Figure 44.

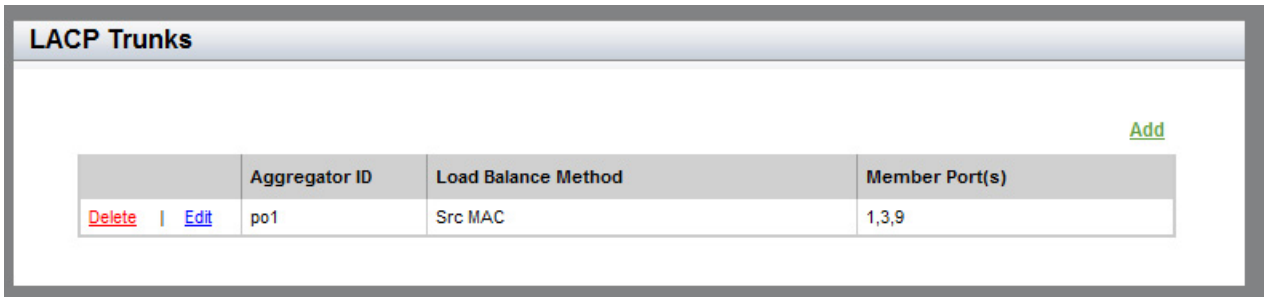


Figure 44. LACP Trunks Page

4. The following fields are displayed:

   - **Aggregator ID**— ID assigned by the user to the aggregator. It can be any number between 1-32.

- **Load Balance Method**— Load distribution methods of the aggregators. An aggregator can have only one load distribution method. The load distribution method determines the manner in which the switch distributes the egress packets among the active ports of an aggregator. The packets can be distributed by source MAC or IP address, destination MAC or IP address, or by both source and destination addresses.
- **Member Port(s)**— Member ports of the aggregator.

Adding an LACP Trunk

To create an LACP trunk, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 43 on page 113.

3. Move the cursor to the right and select **LACP**.

   The LACP Trunks page is displayed. See Figure 44 on page 113.

4. From the LACP Trunks page, click Add.

   The Add LACP Trunk page is displayed. See Figure 45.

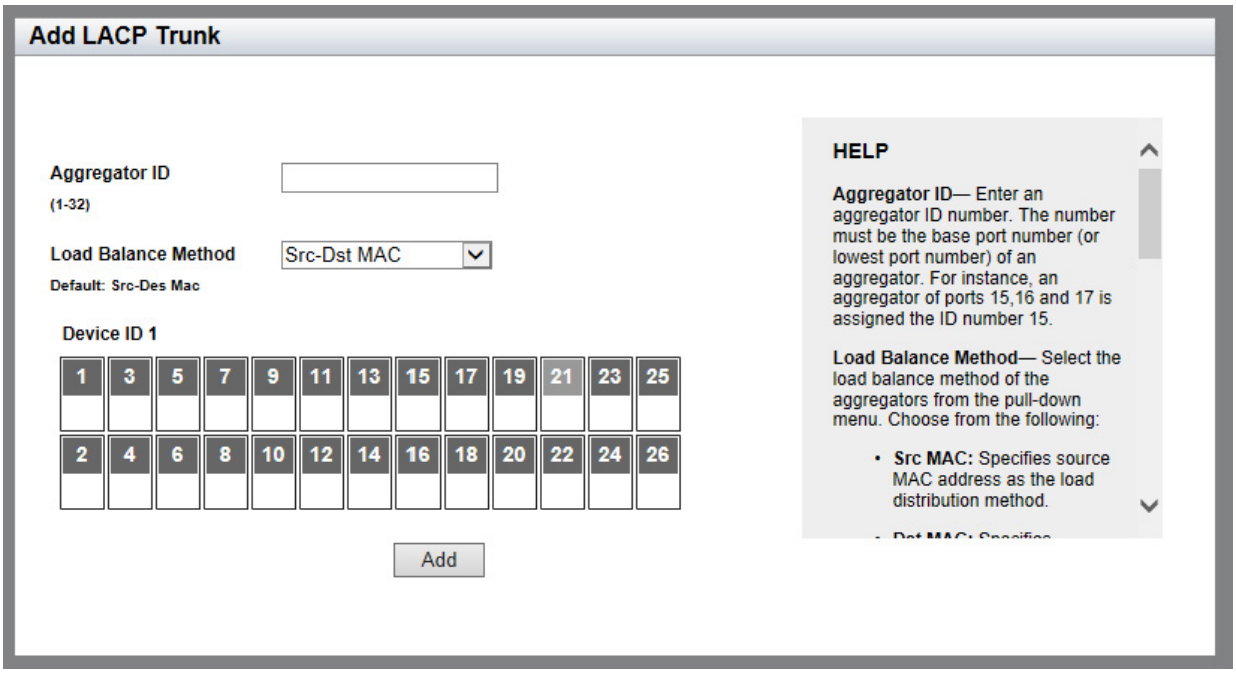


Figure 45. Add LACP Trunk Page

5. Enter an aggregator ID number in the **Aggregator ID** field. The number can be from 1-32.
6. Select the Load Balance Method. Choose from the following:
   - **Src MAC**— Source MAC address as the load distribution method.
   - **Dst MAC**— Destination MAC address as the load distribution method.
   - **Src-Dst MAC**— Source address and destination MAC address as the load distribution method.
   - **Src IP**— Source IP address as the load distribution method.
   - **Dst IP**— Destination IP address as the load distribution method.
   - **Src-Dst IP**— Source IP address and destination IP address as the load distribution method.
7. Click a port number to add to the aggregator. A green check mark indicates a port has been selected. You can select multiple ports.

   To deselect a port, click the box that indicates the port number.
8. Click **Add**.

   A confirmation message is displayed.
9. Click **SAVE** to save your changes to the startup configuration file.

Modifying an LACP Trunk

To modify the LACP Trunk settings, see the following procedure:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 43 on page 113.

3. Move the cursor to the right and select **LACP**.

   The LACP Trunks page is displayed. See Figure 44 on page 113.

4. From the LACP Trunks page, click Edit next to the Aggregator ID that you want to change.

   The Modify LACP Trunk page is displayed. See Figure 46.

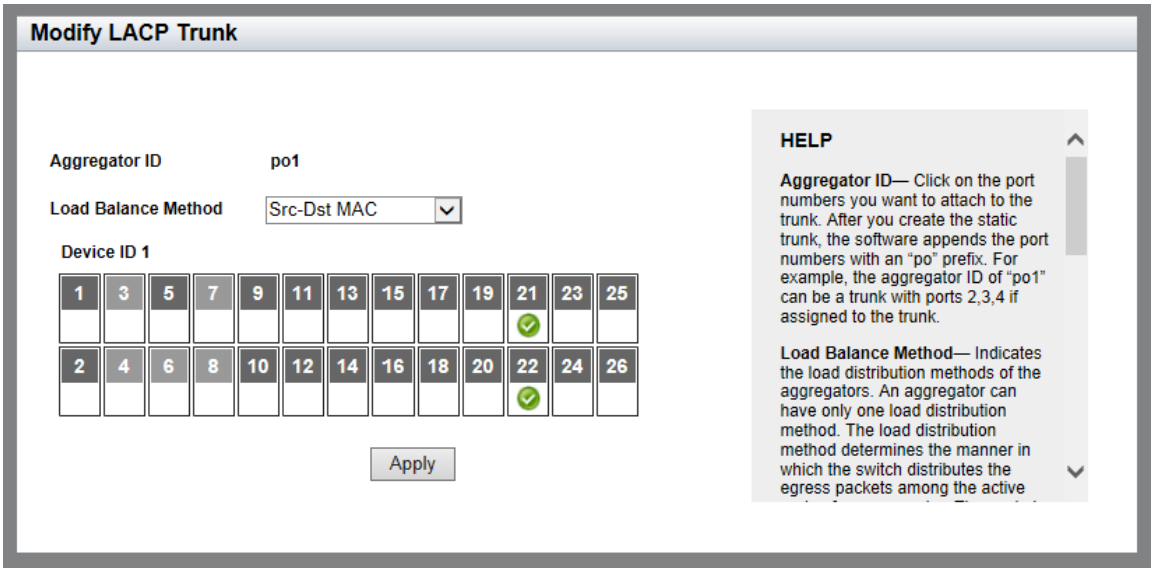


Figure 46. Modify LACP Trunk Page

5. Select the Load Balance Method. Choose from the following:
   - **Src MAC**— Source MAC address as the load distribution method.
   - **Dst MAC**— Destination MAC address.
   - **Src-Dst MAC**— Source address/destination MAC address.
   - **Src IP**— Source IP address.
   - **Dst IP**— Destination IP address.
   - **Src-Dst IP**— Source address/destination IP address.
6. Add or remove the member ports of the aggregator by clicking on the ports.

   A check mark indicates the port has been selected.
7. Click **Apply**.

   A confirmation message is displayed.
8. Click **SAVE** to save your changes to the startup configuration file.

Deleting an LACP Trunk

To delete an LACP trunk, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 43 on page 113.

3. Move the cursor to the right and select **LACP**.

   The LACP Trunks page is displayed. See Figure 44 on page 113.

4. From the LACP Trunks page, click Delete next to the Aggregator ID that you want to delete.

5. Click **SAVE** to save your changes to the startup configuration file.

Chapter 10

Setting Static Port Trunks

Static port trunks are groups of two to eight ports that act as single virtual links between the switch and other network devices. This chapter describes how to display, create, and modify static trunks. See the following sections:

For additional guidelines and information regarding static port trunks, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- Static Port Trunks
- Static Port Trunk Commands

Overview

Static port trunks are commonly used to improve network performance by increasing the available bandwidth between the switch and other network devices, as well as to enhance the reliability of the connections between network devices.

When you create a static port trunk, you can designate how the traffic is distributed across the physical links of the switch by defining the load distribution method.

Static port trunks do not permit standby ports, unlike LACP trunks (which are described in Chapter 9, “Link Aggregation Control Protocol (LACP)” on page 111). If a link is lost on a port in a static port trunk, the trunk’s total bandwidth is reduced. Although the traffic carried by a lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until a lost link is reestablished or another port is manually added to the trunk.

Here are some guidelines regarding static port trunks:

- A static trunk can have up to eight ports.
- The switch supports up to a total of 32 static port trunks and LACP trunks at a time. An LACP trunk is counted against the maximum number of trunks when it is active.
- The ports of a static port trunk can be all Ethernet ports or all SFP ports. Static port trunks *cannot* have both types of ports.
- The ports of a trunk can be consecutive (for example ports 5-9) or nonconsecutive (for example, ports 4, 8, 11, 20).

Displaying Static Trunk Settings

To display the static port trunks for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation tab, see Figure 47.

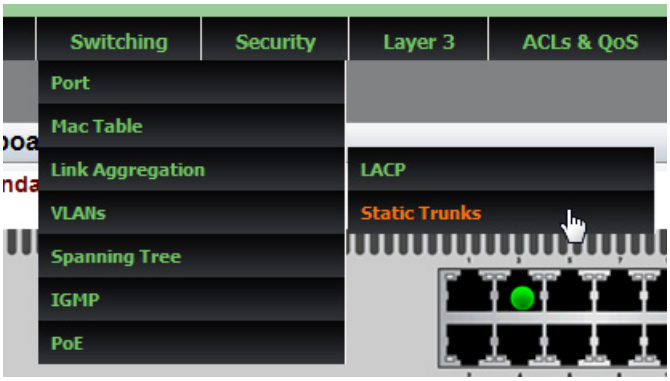


Figure 47. Switching Tab with Static Trunks

3. Move the cursor to the right and select **Static Trunks**.

   The Static Trunks page is displayed as shown in Figure 48. By default, no static trunks are specified on the switch.

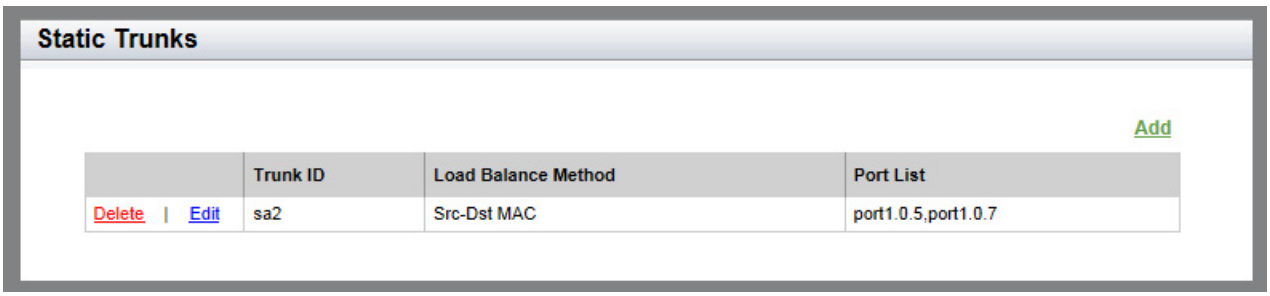


Figure 48. Static Trunks Page

The following fields are displayed:

- **Trunk ID**— ID number of the static trunk.
- **Load Balance Method**— Indicates one of the following:

  Src MAC: Source MAC address is the load distribution method.

Dst MAC: Destination MAC address is the load distribution method.

Src-Dst MAC: Source address and destination MAC address is the load distribution method.

Src IP: Source IP address is the load distribution method.

Dst IP: Destination IP address is the load distribution method.

Src-Dst IP: Source address and destination IP address is the load distribution method.

- **Port List**— List of ports that are members of the static trunk.

Adding Static Trunks

Review the following information before creating a new static port trunk:

- When you create a new trunk, the settings of the lowest-numbered port are copied to the other ports so that all the ports have the same settings. Therefore, you must examine and verify that the speed, duplex mode, and flow control settings of the lowest-numbered port are correct for the network device to which the trunk is connected.
- All ports of a trunk must be members of the same VLAN.
- Ports can be members of one static port trunk at a time. A port that is already a member of a trunk cannot be added to another trunk. To accomplish this, you must first remove the member port from its current trunk assignment. For instructions, see "Adding Static Trunks" on page 125.

To create a static port trunk, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 47 on page 123.

3. Move the cursor to the right and select **Static Trunks**.

   The Static Trunks page is displayed. See Figure 48 on page 123.

4. From the Static Trunks page, click Add.

   The Add Static Trunk page is displayed. See Figure 49 on page 126.

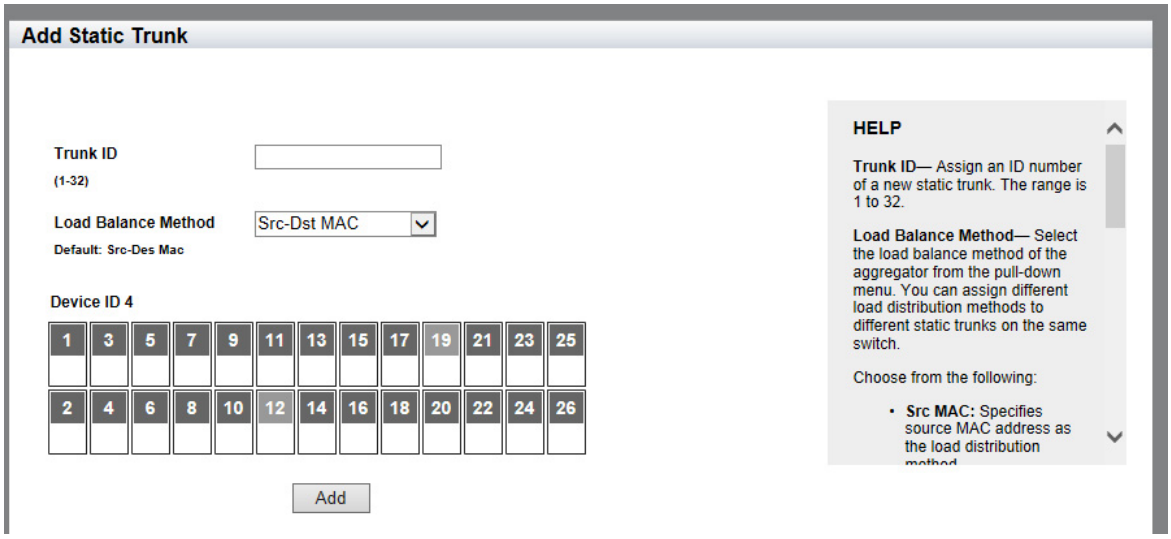


Figure 49. Add Static Trunk Page

5. Assign an ID number of a new static trunk in the **Trunk ID** field. The range is 1 to 32.
6. Select the **Load Balance Method**. You can assign different load distribution methods to different static trunks on the same switch.

   Choose from the following:

   - **Src MAC**— Source MAC address.
   - **Dst MAC**— Destination MAC address.
   - **Src-Dst MAC**— Source address and destination MAC address.
   - **Src IP**— Source IP address.
   - **Dst IP**— Destination IP address.
   - **Src-Dst IP**— Source address and destination IP address.
7. Select a member port in the **Device ID** table by clicking a box that indicates a port number. You can select multiple ports. A green check mark indicates a port has been selected.

   To deselect a port, click the box that indicates the port number.
8. Click **Add**.

   A confirmation message is displayed.
9. Click **SAVE** to save your changes to the startup configuration file.

Modifying the Static Trunk Settings

Review the following information if you are adding ports to an existing trunk:

- The ports of a static trunk must be members of the same VLAN.
- If the new port added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment.

To add or remove member ports from a static port trunk, or modify the load balance method, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 47 on page 123.

3. Move the cursor to the right and select **Static Trunks**.

   The Static Trunks page is displayed. See Figure 48 on page 123.

4. From the Static Trunks page, click Edit.

   The Modify Static Trunk page is displayed. See Figure 50.

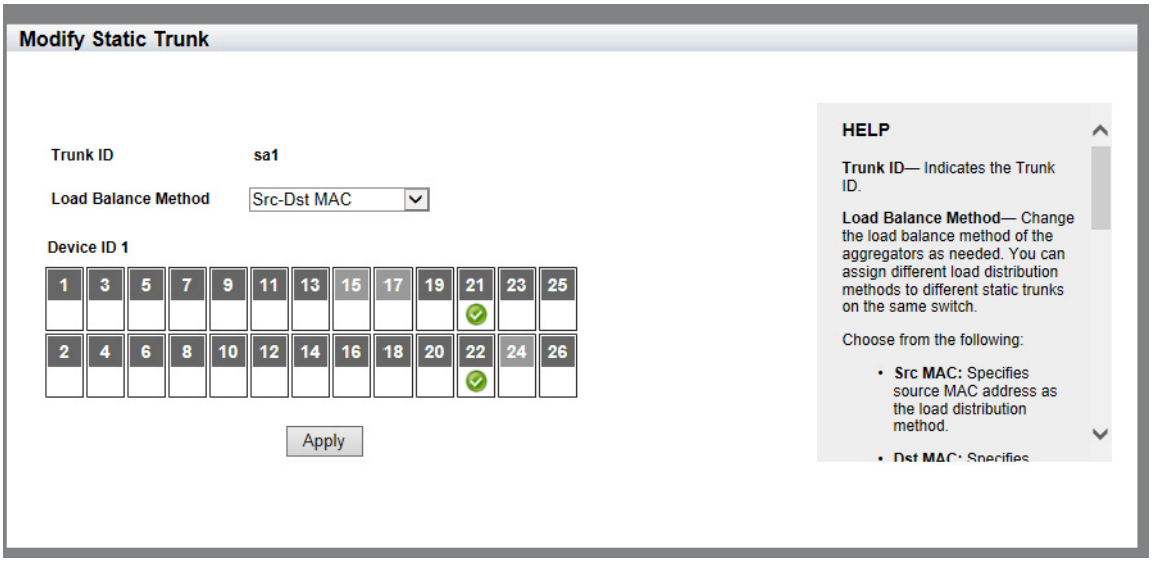


Figure 50. Modify Static Trunk Page

5. Change the **Load Balance Method** as needed. You can assign different load distribution methods to different static trunks on the same switch.

   Choose from the following:

   - **Src MAC**— Source MAC address.
   - **Dst MAC**— Destination MAC address.
   - **Src-Dst MAC**— Source address/destination MAC address.
   - **Src IP**— Source IP address.
   - **Dst IP**— Destination IP address.
   - **Src-Dst IP**— Source address/destination IP address.

6. Select the member ports that you want to add to or remove from the static trunk by clicking on the ports.

   Caution
   To prevent the formation of network loops in your network topology, do not remove ports from a static port trunk without first disconnecting their network cable. Network loops can result in broadcast storms that can adversely affect network performance.

7. Click **Apply**.

   A confirmation message is displayed.

8. Click **SAVE** to save your changes to the startup configuration file.

Deleting Static Trunks

To delete a static port trunk, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab, hover over **Link Aggregation**.

   For an example of the Link Aggregation selection, see Figure 47 on page 123.

3. Move the cursor to the right and select **Static Trunks**.

   The Static Trunks page is displayed. See Figure 48 on page 123.

4. From the Static Trunks page, click Delete next to the Trunk ID that you want to delete.

Chapter 11

Setting Port-based and Tagged VLANs

This chapter provides a brief description of VLANs and explains how to display, create, and modify port-based and tagged VLANs. See the following sections:

For additional information about VLANs, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Port-based and Tagged VLANs
- ❒ Port-based and Tagged VLAN Commands

Overview

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

VLANs let you segment your network through the switch's management software so that you can group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you can create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting. Setting port-based and tagged VLANs is supported via the web interface.

Port-based VLANs

A port-based VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time. A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. In addition, a port-based VLAN can span switches and consist of ports from multiple Ethernet switches.

Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's port VLAN identifier (PVID).

Port VLAN Identifier

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

For example, if you create a port-based VLAN on the switch and assign it the VID 5, the PVID for each port in the VLAN must be assigned the value of 5.

Tagged VLANs

The second type of VLAN is the tagged VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number uniquely identifies each VLAN in a network.

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

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

Tagged and Untagged Ports

You need to specify which ports are members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which are untagged when you create the VLAN.

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

Native VLAN

A tagged port supports traffic coming from multiple VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). If a native VLAN is assigned to the tagged port, when the tagged port receives untagged frames, it forwards those frames to the native VLAN.

Displaying VLANs

To display the VLAN assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. For an example of the VLANs page, see Figure 51.

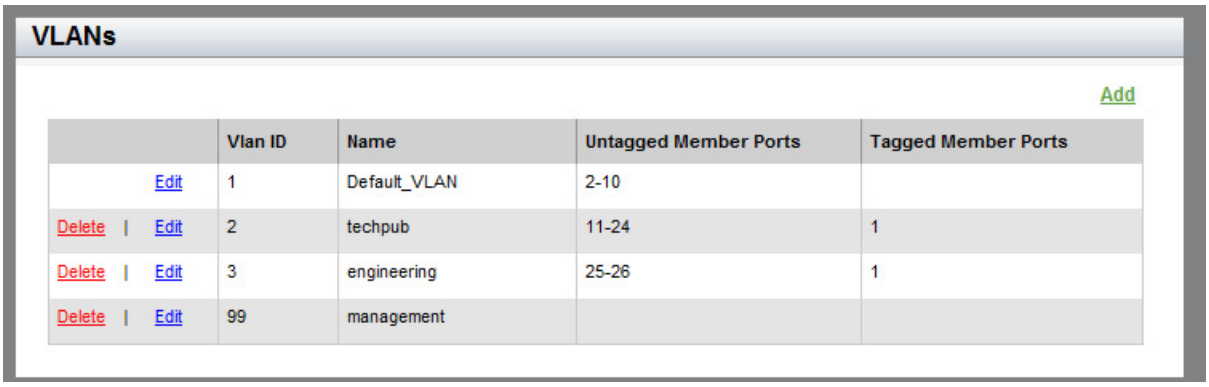


Figure 51. VLANs Page

The following fields are displayed:

- **Vlan ID**— VLAN identifier. The range is 1 to 4094. The VID of 1 is the default VLAN.
- **Name**— VLAN name.
- **Untagged Member Ports**— Untagged ports that belong to the VLAN.
- **Tagged Member Ports**— Tagged ports that belong to the VLAN.

Note
By default, there is one VLAN configured. This is the default VLAN, with a VLAN ID of 1. All ports on the switch are assigned to the default VLAN. All ports in VLAN ID 1 are untagged by default.

Adding a VLAN

To create a VLAN, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. See Figure 51 on page 134.

3. From the VLANs page, click Add.

   The Add VLAN page is displayed. See Figure 52.

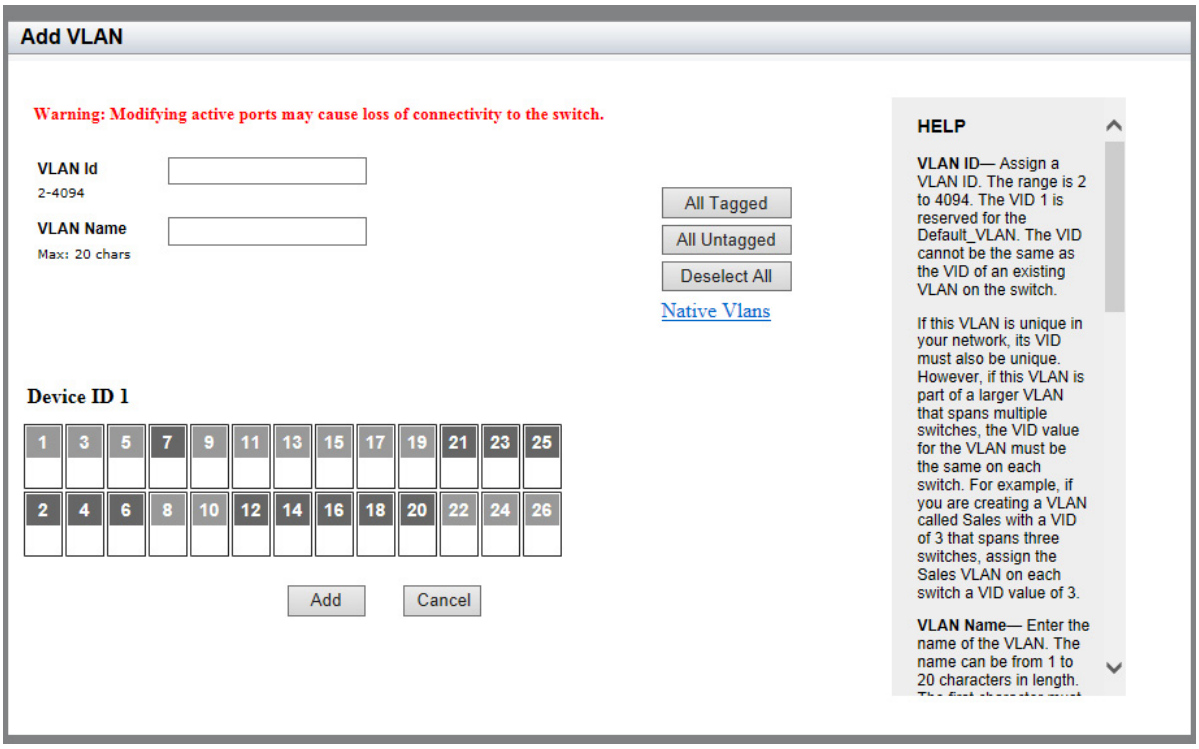


Figure 52. Add VLAN Page

4. Enter the following settings as needed:

   - **VLAN ID**— Assign a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch.

     If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN that spans multiple switches, the VID value for the VLAN must be the same on each

switch. For example, if you are creating a VLAN called Sales with a VID of 3 that spans three switches, assign the Sales VLAN on each switch the VID value of 3.

- **VLAN Name**— Specify the name of a VLAN. The name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). You cannot assign the name of name of an existing VLAN on the switch.

  VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.

- **Device ID**— Assign a “T”, “U”, or “H” by clicking a port number until the desired choice appears in the box below the port number. A “T” indicates the port is a tagged port. A “U” indicates the port is an untagged port. An "H" indicates the port does not belong to any VLANs on the switch as an untagged port. To remove the port from the VLAN, click the port number until the box is unchecked.

Note
For information about tagged and untagged ports, see “Overview” on page 132.

- **All Tagged**— Click this button to make all ports on the switch tagged ports.
- **All Untagged**— Click this button to make all ports on the switch untagged ports.
- **Deselect All**— Click this button to deselect, or uncheck, all of the selected ports.

5. Click **Add**.

   A confirmation message is displayed.

6. Click **SAVE** to save your changes to the startup configuration file.

Modifying VLANs

To modify the VLAN settings, see the following procedure:

Caution
Modifying the VLAN membership of active ports may cause loss of connectivity to the switch.

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. See Figure 51 on page 134.

3. From the VLANs page, click Edit next to the VLAN ID that you want to modify.

   The Edit VLAN page is displayed. See Figure 53.

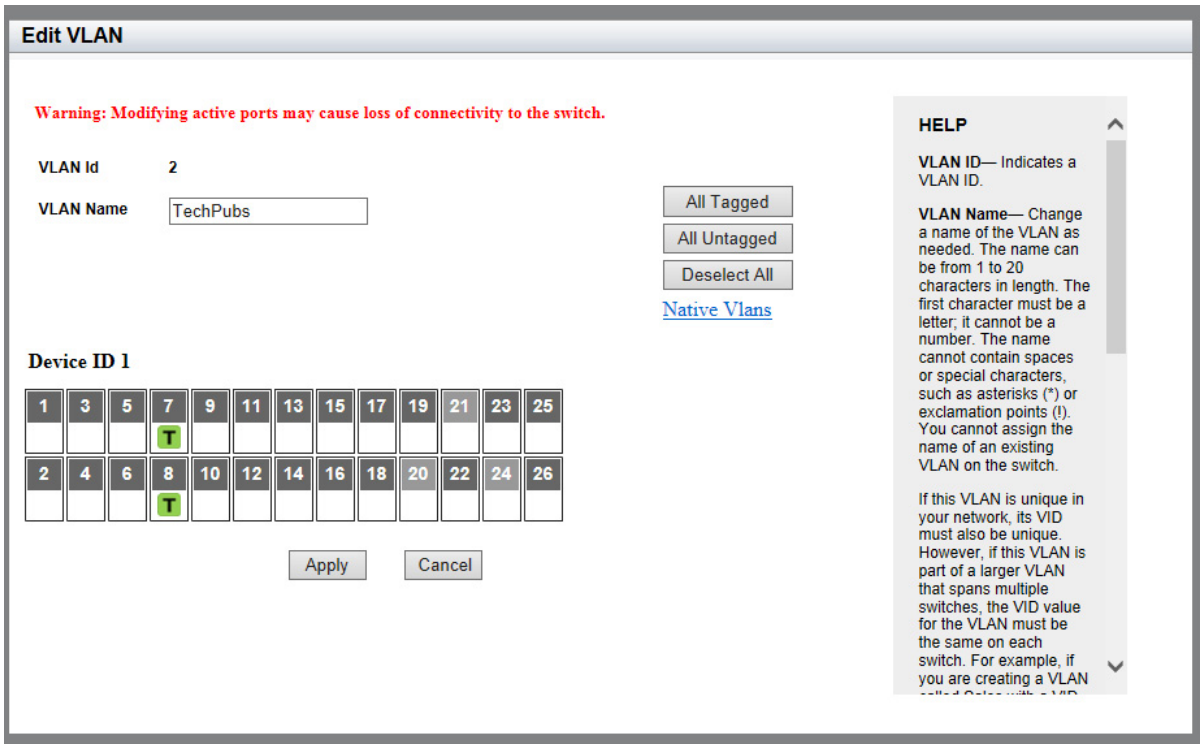


Figure 53. Edit VLAN Page

4. Change the following fields as needed:

   - **VLAN Name**— Change the name of a VLAN. The name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). You cannot assign the name of an existing VLAN on the switch.

     VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.

   - **Device ID**— Assign a “T”, “U”, or “H” by clicking a port number until the desired choice appears in the box below the port number. A “T” indicates the port is a tagged port. A “U” indicates the port is an untagged port. An "H" indicates the port does not belong to any VLANs on the switch as an untagged port. To remove the port from the VLAN, click the port number until the box is unchecked.

     Note
     When a port does not have any mark, the port belongs to the default VLAN. When you assign an “H” to a port, the switch removes the untagged port from the VLAN and also removes the untagged port from the default VLAN. For more information, see “Removing an Untagged Port from a VLAN” on page 141.

   - **All Tagged**— Click this button to make all ports on the switch tagged ports.
   - **All Untagged**— Click this button to make all ports on the switch untagged ports.
   - **Deselect All**— Click this button to deselect, or uncheck, all of the selected ports.

5. Click **Apply**.

   A confirmation message is displayed.

6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a Native VLAN

A VLAN can be assigned to a tagged port so that untagged ingress traffic is placed on the VLAN. This VLAN is referred to as the native VLAN.

To assign a native VLAN to a tagged port, perform the following procedure:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. See Figure 51 on page 134.

3. From the VLANs page, click Add.

   The Add VLAN page is displayed. See Figure 52 on page 135.

4. From Add VLANs page, click Native VLAN.

   The Native VLAN page is displayed. See Figure 54.

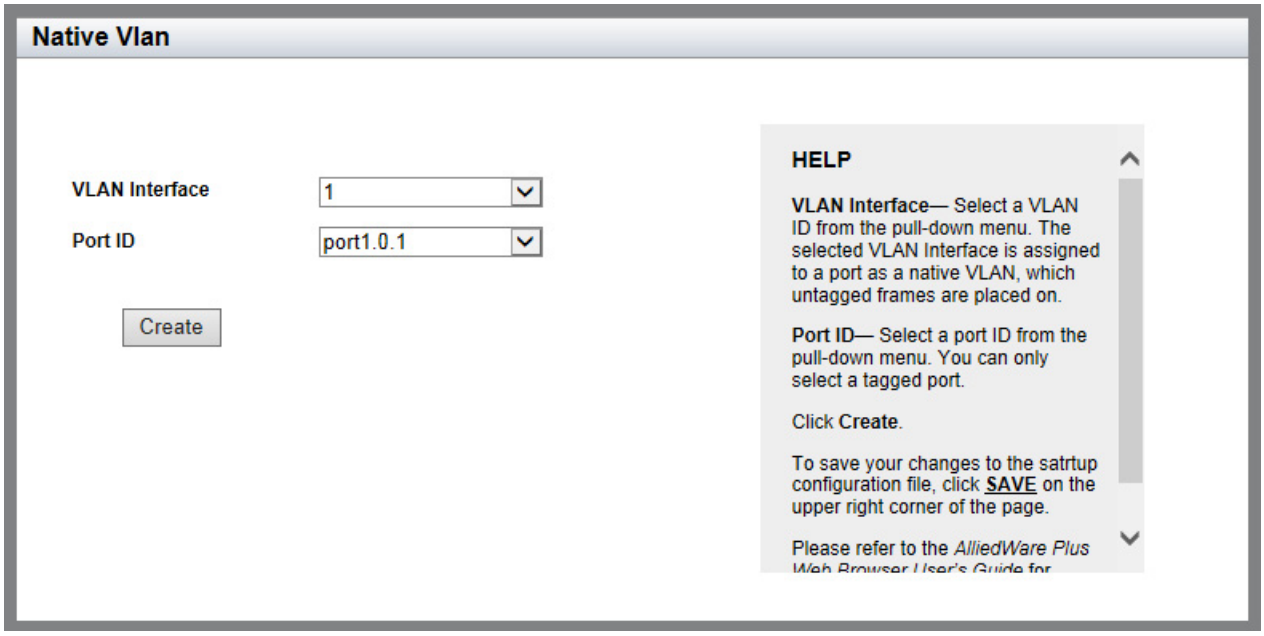


Figure 54. Native VLAN Page

5. Change the following fields as needed:

   - **VLAN Interface**— Select a VLAN ID from the pull-down menu.The selected VLAN Interface is assigned to a port as a native VLAN, on which untagged frames are placed.
   - **Port ID**— Select a port ID from the pull-down menu. You can only select a tagged port.

6. Click **Create**.

   A confirmation message is displayed.

7. Click **SAVE** to save your changes to the startup configuration file.

Removing an Untagged Port from a VLAN

By default, all the ports on the switch belong to the default VLAN, VLAN1, as untagged ports. When you assign a port to another VLAN as an untagged port, the switch removes the untagged port from the original VLAN and then assigns it to the new VLAN.

Caution
Modifying the VLAN membership of active ports may cause loss of connectivity to the switch.

To remove an untagged port from the VLAN and leave the port not belonging to any VLAN, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. See Figure 51 on page 134.

3. From the VLANs page, click Edit next to the VLAN that the untagged port you want to remove belongs to.

   The Edit VLAN page is displayed. See Figure 53 on page 137.

4. Click a port number until the port is marked as "H" to check the port with an "H" mark. An "H" indicates the port is removed from all VLANs on the switch as an untagged port.

   Note
   When you remove a "U" mark from a port and leave no mark on the port, and then click **Apply**, the switch removes the port from the VLAN and assigns it to the default VLAN as an untagged port. When you check a port with an "H" mark, the switch removes the port from the VLAN, but does not assign it to any VLAN. Even when a port does not belong to any VLAN as an untagged port, the port can be a member of a VLAN as a tagged port.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Deleting VLANs

Caution
Deleting VLANs that active ports belong to may cause loss of connectivity to the switch.

To delete a VLAN, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **VLANs**.

   The VLANs page is displayed. See Figure 51 on page 134.

3. From the VLANs page, click Delete next to the VLAN that you want to remove.

   The selected VLAN is removed.

   Note
   You cannot remove the default VLAN, which has a VLAN ID of 1.

4. Click **SAVE** to save your changes to the startup configuration file.

Chapter 12

Spanning Tree Protocols on the Switch

This chapter provides a brief description of both the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP), and explains how to set the spanning tree protocols on the switch. See the following sections:

Note
For information about how to set a spanning tree protocol on the ports, see Chapter 7, “Spanning Tree Protocol on a Port” on page 93.

For more information about spanning tree, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Spanning Tree and Rapid Spanning Tree Protocols
- ❒ Spanning Tree Protocol (STP)
- ❒ STP Commands
- ❒ Rapid Spanning Tree Protocol (RSTP)
- ❒ RSTP Commands

Overview

Both STP and RSTP guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode. In addition, STP and RSTP can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms and maintain network connectivity by activating backup redundant paths.

One of the primary differences between the two protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines 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.

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

RSTP is much faster than STP. It can complete a convergence in seconds, and in turn, greatly diminish the possible impact the process can have on your network. With STP or RSTP, only one spanning tree can be active on the switch at a time. The default setting is RSTP.

The AT-FS970M Series switch supports MSTP; however, the web browser interface does not support MSTP configuration. You must use the CLI to configure MSTP on the switch. See “Multiple Spanning Tree Protocol” in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*.

Displaying and Modifying Spanning Tree Protocol Settings on the Switch

To display and modify Spanning Tree Protocol settings on the switch, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 24 on page 65.

2. From the Switching tab drop-down menu, select **Spanning Tree**.

   The Spanning Tree Settings page is displayed. See Figure 55.

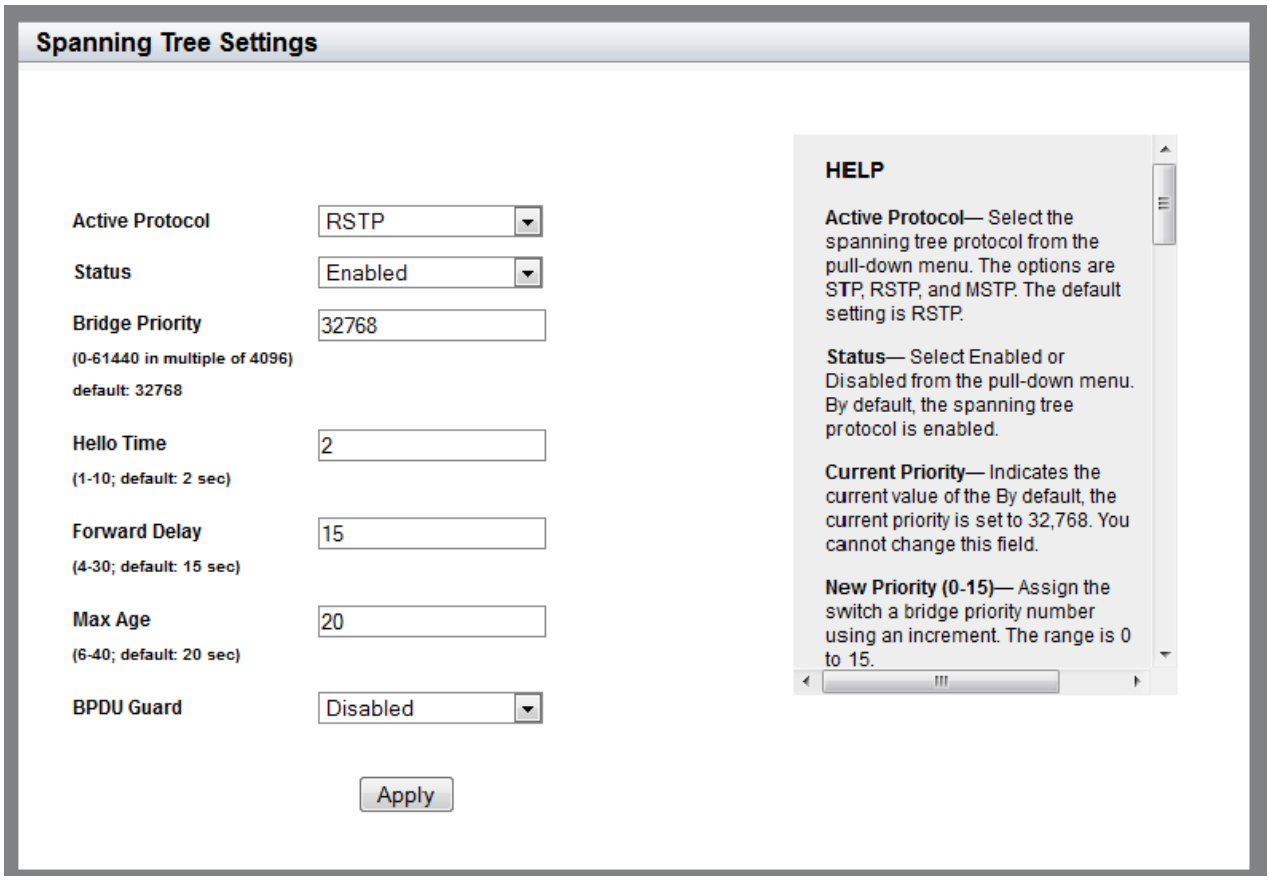


Figure 55. Spanning Tree Settings Page

The following fields are displayed. Change the settings as needed:

- **Active Protocol**— Select the spanning tree protocol from the pull-down menu. The options are STP and RSTP. The default setting is RSTP.

Note
If you try to select MSTP from the menu, a message will appear indicating that MSTP can only be set via the Command Line Interface and will not allow the selection. To set the protocol to MSTP, and for more information on MSTP, see *Section VII: Spanning Tree Protocols* in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide* and refer to the *STP, RSTP and MSTP Protocols*, and *MSTP Commands* chapters.

- **Status**— Enable or disable the spanning tree protocol on the switch. By default, the spanning tree protocol is enabled.
- **Bridge Priority**— Assign the switch a bridge priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. You can use the priority number to influence which switch becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

  The actual range is 0 to 61440, in increments of 4096, for a total of 16 increments, shown in Table 2. You specify the increment of the value, from 0 to 15. The default is 32768, which is increment 8.

Table 2. STP Bridge Priority Value Increments

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

Note
Set the hello time, forward delay, and max-age fields according to the following formulas, as specified in IEEE Standard 802.1d:
max-age <= 2 x (forward time - 1.0 second)
max-age => 2 x (hello time + 1.0 second)

- **Hello Time**— Enter the hello time in seconds. The hello time is the frequency that the switch sends bridge protocol data units (BPDUs), which contain spanning tree configuration information. The range is 1 to 10 seconds.

  This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- **Forward Delay**— Enter the forward delay time in seconds. The forward delay specifies how long the ports remain in the listening and learning or discarding states before they transition to the forwarding state. The range is 4 to 30 seconds.

  This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- **Max Age**— Enter the max age in seconds. The max age determines how long BPDUs are stored by the switch before they are deleted. The default setting is 20 seconds. The range is 6 to 40 seconds.

  This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- **BPDU Guard**— Enable or disable the BPDU guard feature on the switch. When the BPDU guard feature is enabled on the switch, the switch monitors edge ports and disables them if they receive BPDU packets.

3. Click **Apply**.

4. Click **SAVE** to save your changes to the startup configuration file.

Chapter 13

Internet Group Management Protocol (IGMP) Snooping

This chapter provides a brief description of IGMP Snooping and explains how to set this feature on the switch. See the following sections:

For more information about IGMP, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Internet Group Management Protocol (IGMP) Snooping
- ❒ IGMP Commands

Overview

IGMP snooping allows the switch to control the flow of multicast packets from its ports. It enables the switch to forward packets of a multicast group to only ports connected to members of the multicast group. When the switch is not using IGMP snooping and receives multicast packets, it floods the packets out all its ports, except the port on which it received the packets. Such flooding of packets can negatively impact network performance.

IGMP is used by IPv4 routers to create lists of nodes that are members of multicast groups. A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a report. A report indicates that an end node wants to become a member of a multicast group. Nodes that join a multicast group are referred to as host nodes. After joining 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 from 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 from the port. This improves network performance by restricting the multicast packets only to router ports where host nodes are located.

The switch monitors the flow of queries from routers and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets to only 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 to only those switch ports that are connected to host nodes.

The 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.

Note
When IGMP snooping is disabled on the switch, all reports are suppressed on a port. The default setting for IGMP snooping on the switch is disabled.

Displaying and Modifying IGMP Snooping Configuration

To display and modify the IGMP Configuration settings, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching Tab is displayed. See Figure 56.

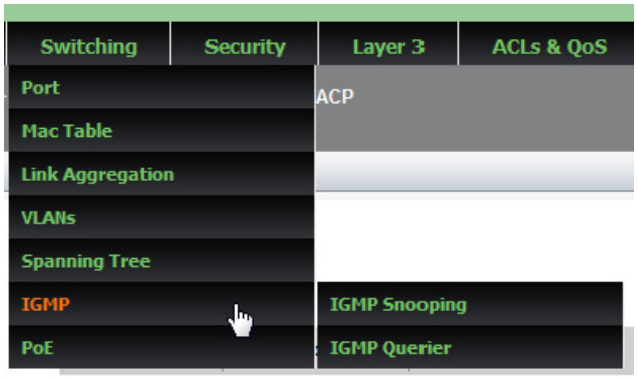


Figure 56. Switching IGMP Tab

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

   The IGMP Snooping Configuration page is displayed. See Figure 57 on page 152.

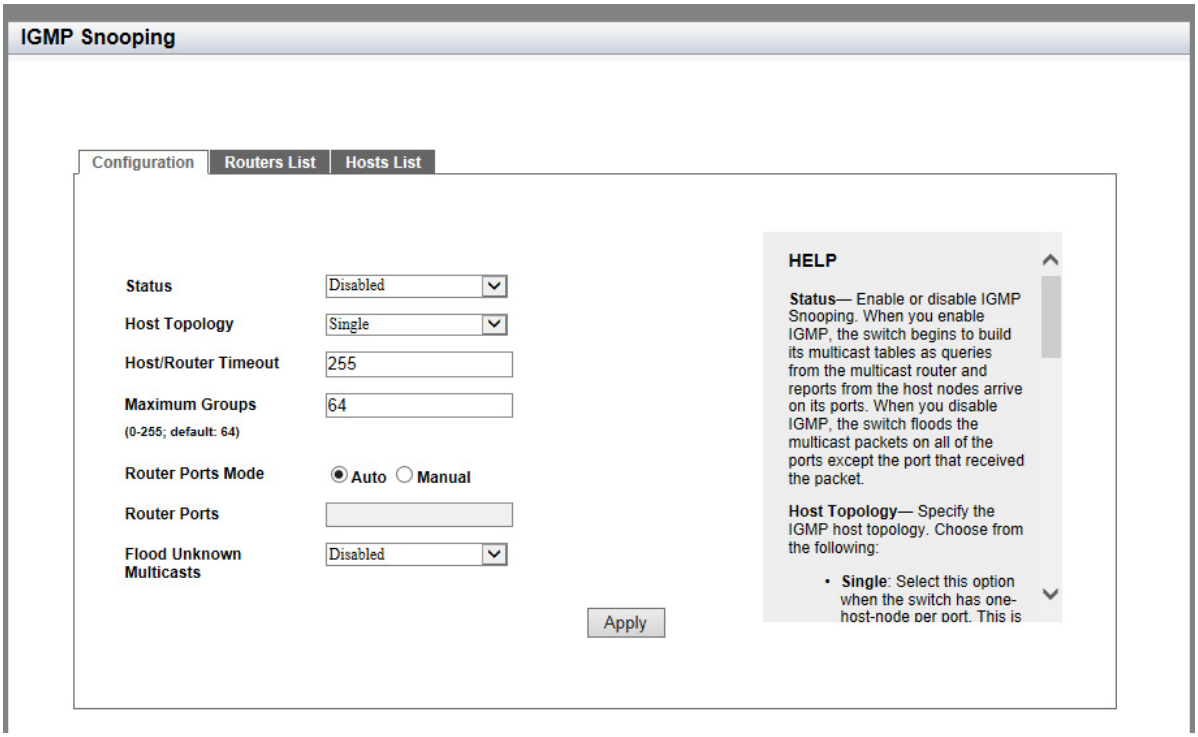


Figure 57. IGMP Snooping Page with Configuration Tab

3. Change the following settings as needed:

   - **Status**— Enable or disable IGMP Snooping. When you enable IGMP, the switch begins to build its multicast tables as queries from the multicast router and reports from the host nodes arrive on its ports. When you disable IGMP, the switch floods the multicast packets on all of the ports except the port that received the packet. By default, the switch is set to “Disabled.”
   - **Host Topology**— Specify the IGMP host topology. Choose between “Single” and “Multiple.” Select “Single” when the switch has one host-node per port. Select “Multiple” when the switch has more than one host-node per port. By default, the switch is set to “Single.”
   - **Host/Router Timeout**— Specify the host/router time in seconds that the switch times out when it finds inactive host nodes and multicast routers. The range is from 0 to 86,400 seconds (24 hours). The default is 255 seconds. Setting the timeout to zero (0) disables the timer.
   - **Maximum Groups**— Specify the maximum number of multicast addresses the switch is allowed to learn. The range is 0 to 255 multicast addresses. The default is 64.
   - **Router Ports Mode**— Check a radio button to select the router ports mode. Choose from the following:

Auto: The switch automatically detect ports that are connected to multicast routers.

Manual: You manually specify ports that are connected to multicast routers.

- **Router Ports**— Specify the port ID of a port that is connected to a multicast router. You can enter a port ID in this field only when the Router Ports Mode is "Manual."
- **Flood Unknown Multicasts**— Select Enabled to disable the automatic suppression of unknown multicast traffic on the switch. Select Disabled to enable the automatic suppression of unknown multicast traffic on the switch.

4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Disabling IGMP Snooping

To disable the IGMP Configuration on the switch, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 56 on page 151.

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

   The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 57 on page 152.

3. Use the pull-down menu next to the **Status** field to select “Disabled.”

   When you disable IGMP snooping, the switch floods the multicast packets on all of the ports except those that receive the packets.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Displaying the Routers List

To display the IGMP Routers List, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 56 on page 151.

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

   The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 57 on page 152.

3. Click the **Routers List** tab.

   The Routers List page is displayed. See Figure 58.

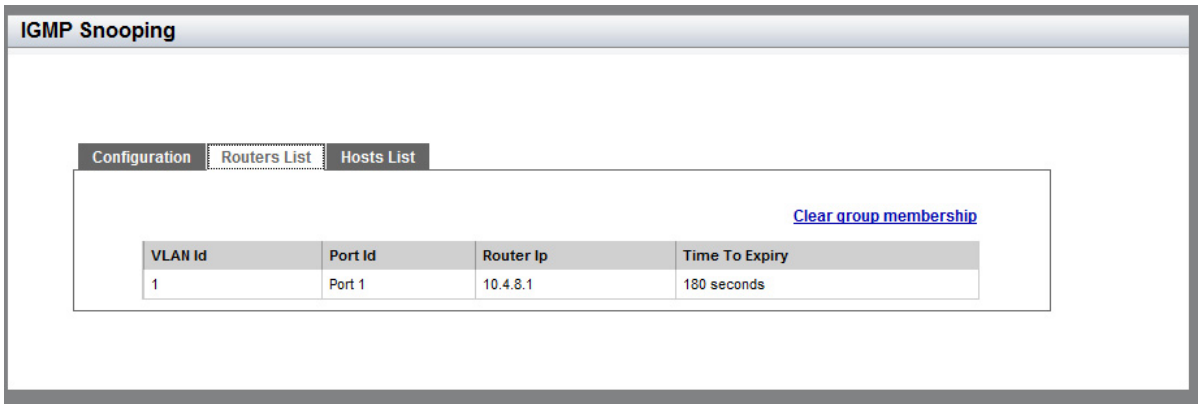


Figure 58. IGMP Snooping Page with Routers List Tab

The following settings are displayed:

- **VLAN ID**— ID number of the VLAN of the router port.
- **Port ID**— The port that a multicast router is connected to. If the switch learned a router on a port trunk, the trunk ID number, instead of a port number, is displayed.
- **Router IP**— IP address of the multicast router.
- **Time to Expiry**— Number of seconds remaining before the switch times out a multicast router if there is no further IGMP query from it.

Clearing the Routers List

To clear the group membership on the IGMP Routers List, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 56 on page 151.

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

   The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 57 on page 152.

3. Click the **Routers List** tab.

   The IGMP Snooping page with the Routers List tab selected is displayed. See Figure 58 on page 155.

4. Click **Clear group membership** to remove all multicast router ports in the list.

Displaying the Hosts List

To display the IGMP Hosts List, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 56 on page 151.

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

   The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 57 on page 152.

3. Click the **Hosts List** tab.

   The Hosts List page is displayed. See Figure 59.

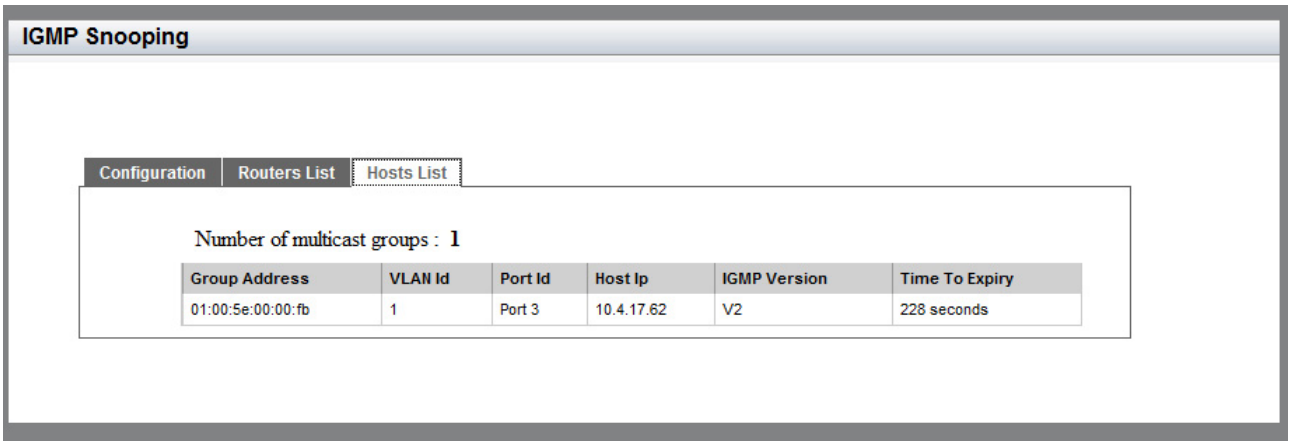


Figure 59. IGMP Snooping Page with Hosts List Tab

The following settings are displayed:

- **Group Address**— Multicast address of the group.
- **VLAN ID**— VLAN ID of the host node.
- **Port ID**— Port of the host node. If the host node is on a port trunk, this field displays the trunk ID number instead of the port number.
- **Host IP**— IP address of the host node.
- **IGMP Version**— IGMP versions used by the host node.
- **Time to Expiry**— Number of seconds remaining before the host node is timed out if it does not send an IGMP report.

Chapter 14

IGMP Snooping Querier

This chapter provides a brief description of IGMP Snooping Querier and explains how to set this feature on the switch. See the following sections:

For more information about IGMP, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ IGMP Snooping Querier
- ❒ IGMP Snooping Querier Commands

Overview

Multicast routers are an essential part of IP multicasting. They send out queries to the network nodes to determine group memberships, route the multicast packets across networks, and maintain lists of the multicast groups and the ports where group members are located.

IGMP snooping querier can be used in place of multicast routers in situations where IP multicasting is restricted to a single LAN, without the need for routing. This feature enables the switch to mimic a multicast router by sending out general IGMP queries to the host nodes.

IGMP snooping querier supports IGMP version 1, version 2, and version 3. By default, the switch sends version 2 messages. If it receives version 1 messages from any of the nodes, the switch sends version 1 queries. If the switch receives version 3 messages, all nodes respond with version 3 messages. By default, the interval at which the querier sends out IGMP querier reports is 125 seconds. The switch reverts to version 2 queries if, after 255 seconds, no additional version 1 or version 3 messages are received.

The switch must have an IP address to add to the queries as its source address. In addition, the address must be a member of the same network as the host nodes and the multicasting source. You assign an IP address to the switch by creating a routing interface in the VLAN. Then, apply the IP address to the VLAN where it sends its queries to enable IGMP snooping querier on the VLAN. Allied Telesis recommends using the Default VLAN, which has a VID of 1.

IGMP snooping querier must be used in conjunction with IGMP snooping. Activate IGMP snooping on all of the switches in the LAN, including the switches running the IGMP snooping querier. The switches use IGMP snooping to monitor the responses of the host nodes to the general IGMP queries sent by the IGMP snooping querier. From the responses, they create lists of ports that have host nodes that want to join the various multicast groups and forward the multicast packets to only those ports.

Figure 60 on page 161 provides an example of IGMP snooping querier on a LAN. It consists of a single switch with one VLAN, the Default VLAN. Both IGMP snooping and IGMP snooping querier are enabled on the switch. You assign a routing interface to the VLAN, with an IP address that belongs to the same subnet as the multicast source and the host nodes.

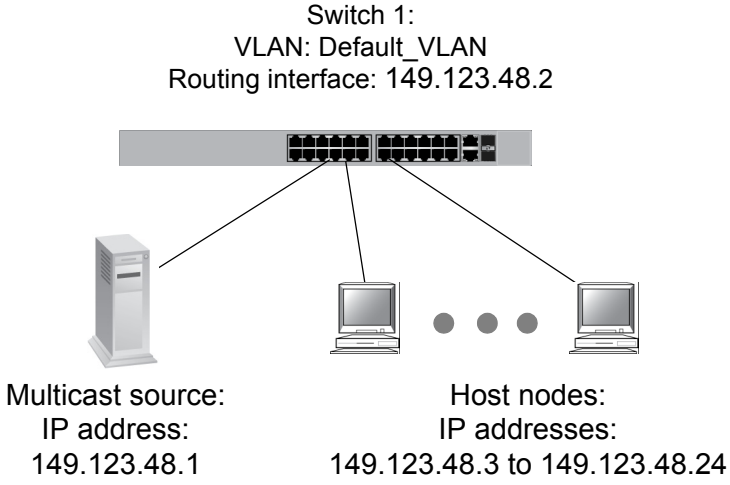


Figure 60. IGMP Snooping Querier with One Querier

Table 3 lists the switch settings that are illustrated in Figure 60.

Table 3. IGMP Snooping Querier with One Querier

Switch	Routing Address	IGMP Snooping	IGMP Snooping Querier	Querier Status
1	149.123.48.2	Enabled	Enabled	Active

Assigning Multiple Queriers

IGMP snooping querier supports multiple queriers. A total of three queriers are supported, one active querier and up to two standby queriers. The active querier is the querier with the lowest IP address. The standby querier has the second lowest IP address, and the switch with the highest IP address is the second standby querier.

The difference between the active and standby queriers is that only the active querier registers IGMP reports. A standby querier does not update its MAC tables, so IGMP reports are not registered on the switch.

When you assign multiple queriers to a LAN, the software must decide which is the active querier and which is the standby querier. This task falls to a switch in the network that has IGMP snooping enabled, but IGMP snooping querier disabled. Consequently, a LAN with multiple queriers requires this extra switch.

For example, to assign two queriers to a network, you need three switches. First, enable IGMP snooping on all three switches. Then enable IGMP snooping querier on two switches, for this example, switches 1 and 3. Switch 2 determines which of the querier-enabled switches has the lowest IP address and deems that switch the active querier. The switch

with the second lowest IP address is made the standby querier, again by switch 2. In the case where there are three queriers, the switch in the network with IGMP snooping enabled and IGMP querier disabled determines the standby querier and then the second standby querier by comparing their IP addresses.

The following example consists of a LAN with three switches. See Figure 61. IGMP snooping is enabled on all three switches. However, IGMP snooping querier is enabled on switches 1 and 3. Switch 2 determines that switch 1 has the lowest IP routing address and forwards all multicast packets to switch 1, making switch 1 the active querier. Switch 3 becomes the standby querier in case switch 1 stops transmitting query packets.

Note
Switches 1 and 3 are only sending queriers. Neither switch detects nor displays an opposing querier.

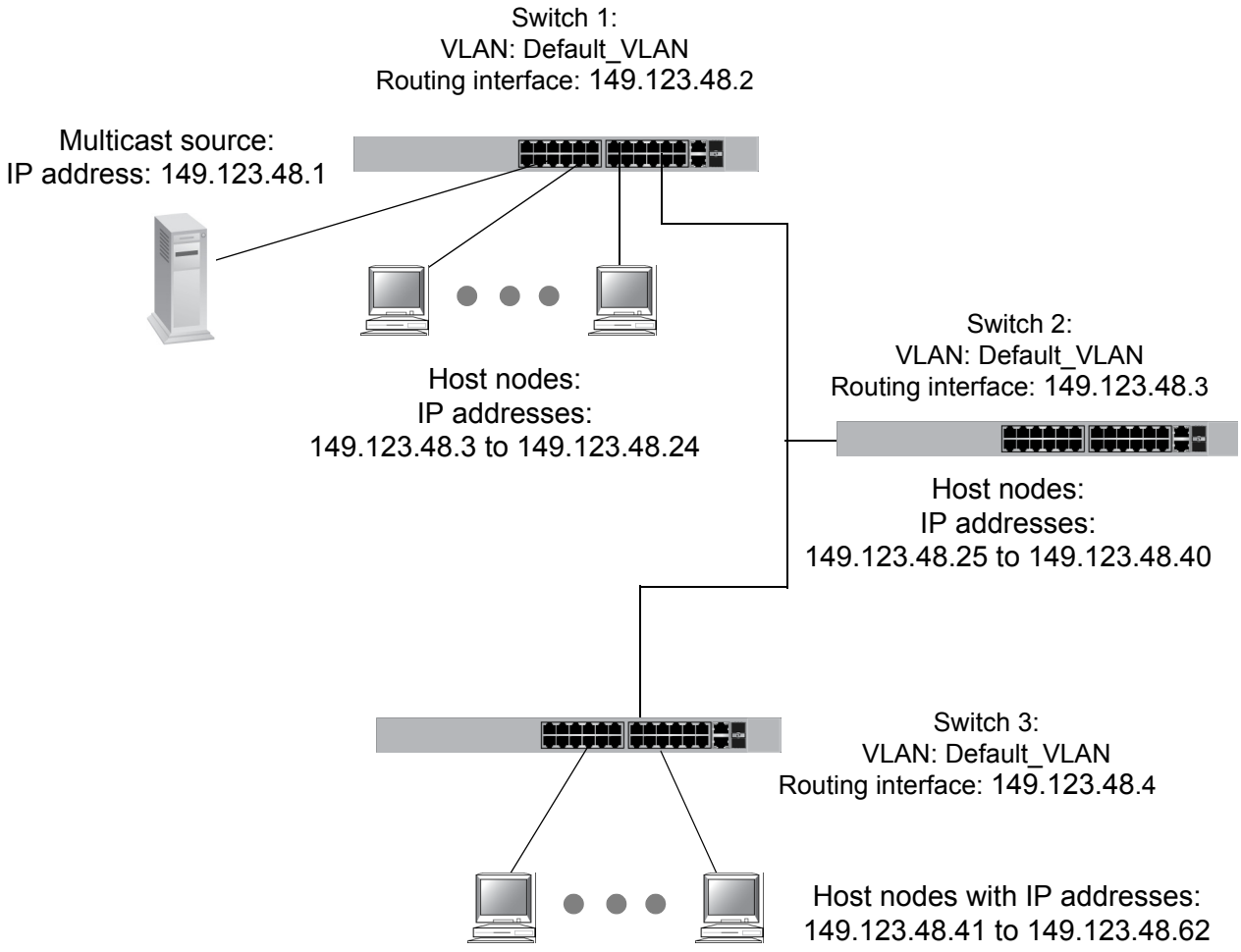


Figure 61. IGMP Snooping Querier with Two Queriers

Table 4 lists the switch settings that are illustrated in Figure 61 on page 162.

Table 4. IGMP Snooping Querier with Two Queriers

Switch	Routing Address	IGMP Snooping	IGMP Snooping Querier	Querier Status
1	149.123.48.2	Enabled	Enabled	Active
2	149.123.48.3	Enabled	Disabled	None
3	149.123.48.4	Enabled	Enabled	Standby

Guidelines

The guidelines for IGMP snooping querier are listed here:

- The network can have only one LAN.
- The network cannot have any multicast routers.
- IGMP snooping must be enabled on the switch.
- IGMP snooping querier should be enabled on only one switch. Other switches in the LAN should use IGMP snooping.
- IGMP snooping querier must be applied to the VLAN on which the queries are to be sent.
- The VLAN must be assigned a routing interface with an IP address that is a member of the same network as the host nodes and the source node of the multicast packets. The switch adds the IP address to the queries as its source address.
- If you want to add or remove ports from the VLAN after activating IGMP snooping querier, you must disable IGMP snooping querier, modify the VLAN, and then enable it again.
- The switch supports IGMP versions 1, 2, and 3. The switch normally sends just version 2 messages. If it receives a version 1 message, it sends version 1 messages on all of the ports. If the switch does not receive any further version 1 messages for 400 seconds, the switch reverts to sending version 2 messages.
- If the switch receives a query either from a multicast router or from another switch with IGMP snooping querier, it suspends IGMP snooping querier and sends no further queries for 225 seconds. If the switch does not receive any further queries, it reactivates the feature and resumes sending queries.
- IGMP snooping querier is supported on the base ports and SFP modules.

Displaying IGMP Snooping Querier

To display an IGMP Snooping Querier list, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching Tab is displayed. See Figure 62.

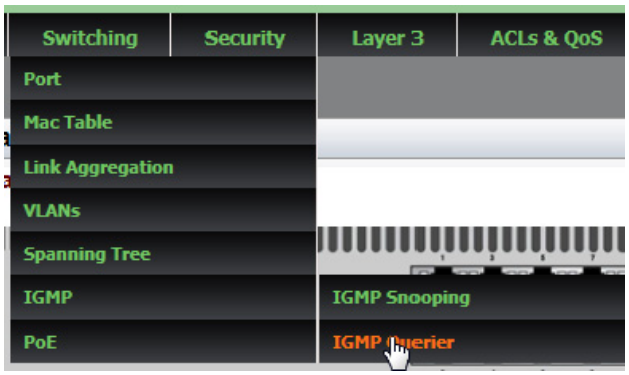


Figure 62. Switching IGMP Tab

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Querier**.

   The IGMP Snooping Querier page is displayed. See Figure 63.

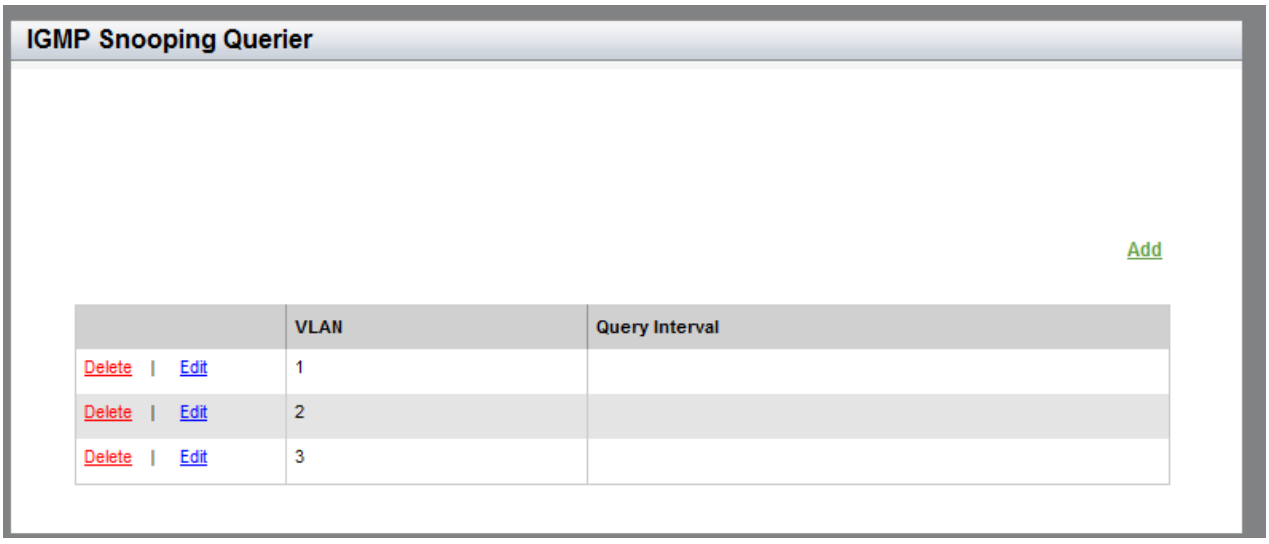


Figure 63. IGMP Snooping Querier Page

3. The following settings are displayed:

   - **VLAN**— VLAN ID.

- **Query Interval**— Time interval in seconds at which IGMP General Query messages are transmitted.

Modifying IGMP Snooping Query Interval

To modify the value of Query interval, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching Tab is displayed. See Figure 62 on page 165.

2. Hover over **IGMP** and then move the cursor to the right to select **IGMP Querier**.

   The IGMP Snooping Querier page is displayed. See Figure 63 on page 165.

3. From the IGMP Snooping Querier page, click Add or Edit.

   The Edit IGMP Snooping Querier page is displayed. See Figure 64.

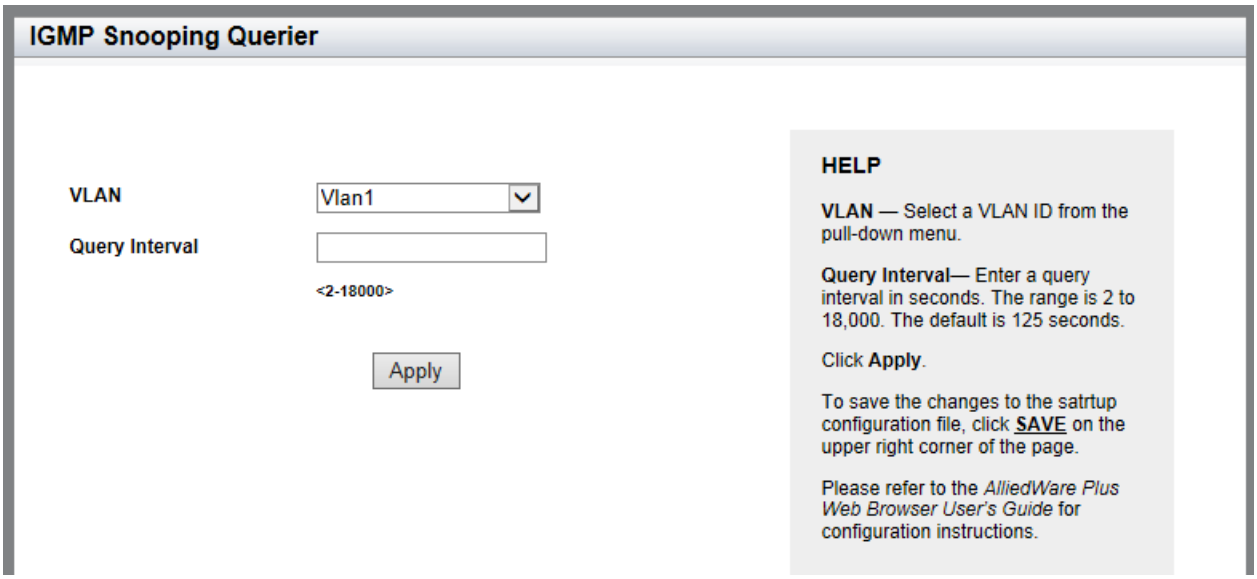


Figure 64. Edit IGMP Snooping Querier Page

4. Enter the following settings as needed:

   - **VLAN**— Select the VLAN ID from the pull-down menu.
   - **Query Interval**— Enter a query interval in seconds. The range is 2 to 18,000. The default is 125 seconds.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 15

Power Over Ethernet (PoE)

This chapter provides brief descriptions of PoE and explains how to change the configuration of a port on the PoE featured switch.

See the following sections:

For more information about PoE, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- Power Over Ethernet
- Power Over Ethernet Commands

Overview

The AT-FS970M/8PS, AT-FS970M/8PS-E, AT-FS970M/24PS, and AT-FS970M/48PS switches feature Power over Ethernet (PoE) on the 10/100Base-Tx ports. PoE is used to supply power to network devices over the same twisted pair cables that carry the network traffic.

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE-compatible devices wherever they are needed without having to worry about a nearby power source.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The AT-FS970M/8PS, AT-FS970M/8PS-E, AT-FS970M/24PS, and AT-FS970M/48PS switches are PSE devices providing DC power to the network cable and functioning as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes

PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The AT-FS970M PoE switches support all five classes listed in Table 5.

Table 5. IEEE Powered Device Classes

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	25.5W to 38.9W

Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs.

The AT-FS970M/8PS and AT-FS970M/8PS-E switches have one power supply. The AT-FS970M/24PS and AT-FS970M/48PS switches have two

power supplies and can be operated using either one power supply or both power supplies. One power supply is responsible for providing 185 watts of the power budget. Table 6 shows power budget per model.

Table 6. PoE Switch's Power Budget

Switch Model	When Using One Power Supply	When Using Two Power Supplies
AT-FS970M/8PS	185W	N/A
AT-FS970M/8PS-E	185W	N/A
AT-FS970M/24PS	185W	370W
AT-FS970M/48PS	185W	370W

Port Prioritization

As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs. However, when the PD power requirements exceed the total available power, the switch denies power to some ports based on a process called port prioritization.

The ports on the PoE switch are assigned to one of three priority levels. These levels and descriptions are listed in Table 7.

Table 7. PoE Port Priorities

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
High	Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
Low	This is the lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

Without enough power to support all the ports set to the same priority level at one time, the switch provides power to the ports based on the port number, in ascending order. For example, when all of the ports in the switch are set to the low priority level, and the power requirements are exceeded on the switch, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

Displaying PoE Port Settings

To display a list of the PoE port settings, do the following:

Note
The PoE pull-down menu item appears only when you are accessing a PoE featured switch.

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 65.

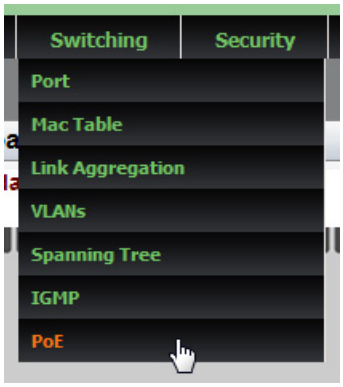


Figure 65. Switching Tab

2. From the Switching tab drop-down menu, select **PoE**.

   A list of PoE settings on the ports is displayed. See Figure 66 on page 173.

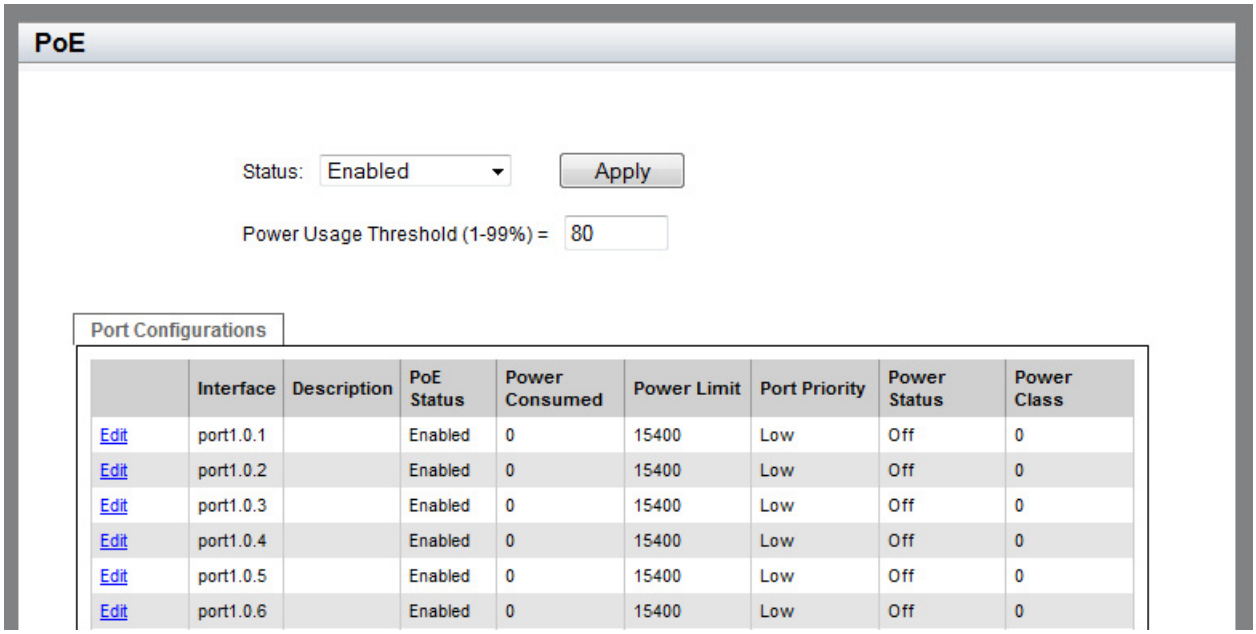


Figure 66. PoE Port List Page

The following fields are displayed:

- **Status**— Enable or disable PoE on the ports globally. By default, power is enabled on all ports.

> **Note**
> This status does not indicate that the PoE status of all the ports is the same. To find out the PoE status, you must examine the PoE status for a port individually.

- **Power Usage Threshold**— Power usage threshold in a percentage of the switch's total available power. The range is 1 to 99%.
- **Interface**— Port ID.
- **Description**— Description of the port.
- **PoE Status**— Indicates if power for the port is enabled or disabled. By default, power is enabled for all the ports on the switch.
- **Power Consumed**— Power consumption in milliwatts (mW) for the port.
- **Power Limit**— Power limit in milliwatts (mW) on the port.
- **Port Priority**— Port priority: Low, High, or Critical. For more details, see "Port Prioritization" on page 171.

- **Power Status**— Indicates if a powered device that is connected to the port is powered on or off. When powered on, it indicates Powered. When no powered device is connected to the port, indicates Off.
- **Power Class**— Class of the connected PD. The switch automatically detects to which class the connected PD belongs. For more details, see “PD Classes” on page 170.

Modifying PoE Settings Globally

To modify PoE settings on the switch, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 65 on page 172.

2. From the Switching tab drop-down menu, select **PoE**.

   Note
   The PoE pull-down menu item appears only when you are accessing an AT-FS970M PoE switch.

   The PoE setting page is displayed. See Figure 66 on page 173.

3. Change the following settings as needed:

   - **Status**— Enable or disable PoE globally for all the ports on the switch. Change this field when you want to change the PoE status for all the ports all at once.
   - **Power Threshold**— Set the power usage threshold in a percentage of the switch's total available power. The range is 1 to 99%. By default, the power threshold is 80% of the total available power of the switch.

   Note
   The power threshold value is used to monitor power consumption on the switch. You can configure the switch with an SNMP server to notify you when the switch reaches power consumption at the specified level. To configure an SNMP server, you must use the AlliedWare Plus™ Command Line Interface (CLI). See the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide.*

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Modifying PoE Settings on a Port

To display a list of the IPv4 interfaces, do the following:

1. Hover the cursor over the **Switching** tab.

   The Switching tab is displayed. See Figure 67.

2. From the Switching tab drop-down menu, select **PoE**.

   A list of PoE settings on the ports is displayed. See Figure 66 on page 173.

3. From the PoE page, click Edit next to the port number that you want to modify.

   The following page is displayed. See Figure 67.

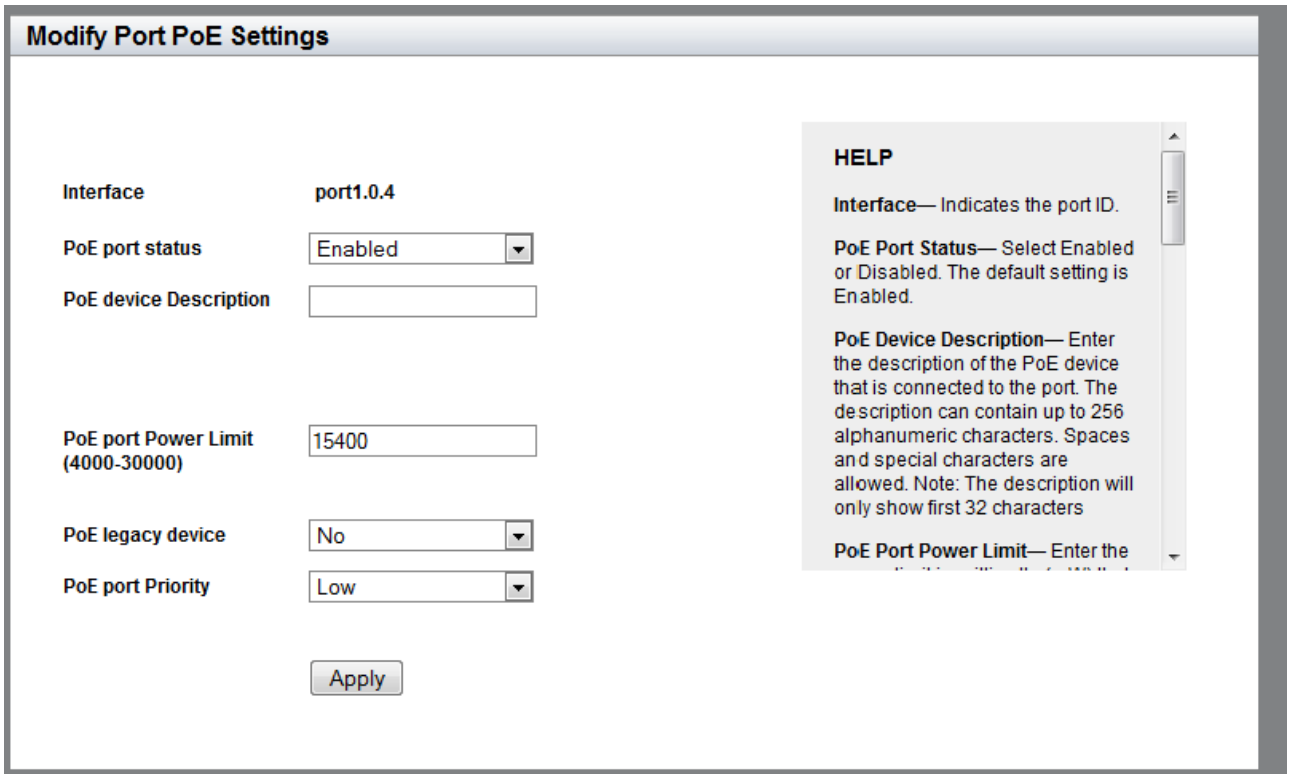


Figure 67. Modify Port PoE Settings Page

4. Change the following fields as needed:

   - **Interface**— Indicates the port ID.
   - **PoE Port Status**— Enable or disable the PoE port status.

- **PoE Device Description**— Enter the description of the PoE device that is connected to the port. The description can contain up to 256 alphanumeric characters. Spaces and special characters are allowed.
- **PoE Port Power Limit (4000 ~ 30000)**— Enter the power limit in milliwatts (mW) that the switch provides to a device connected to the port. The default is 15400 mW.
- **PoE Legacy Device**— Select "Yes" to allow the switch to supply power to a device that is connected to the port, even if the device is a legacy PD. Select "No" to not allow the switch to supply power if a device that is connected to the port is a legacy PD. By default, the PoE switch does not supply power to legacy PDs.

  Legacy PDs are PoE devices that were designed before the IEEE 802.3af and IEEE 802.3at PoE standards were finalized.
- **PoE Port Priority**— Select the PoE port priority from Low, High or Critical. For more details, see "Port Prioritization" on page 171.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 16

MAC Address-based Port Security

This chapter provides a brief description of MAC address-based port security and explains how to set this feature on the switch. See the following sections:

For more information about MAC address-based security, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ MAC Address-based Port Security
- ❒ MAC Address-based Port Security Commands

Overview

This feature lets you control access to the ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any additional devices.

For example, if you configure port 3 on the switch to learn five source MAC addresses, the port learns up to five address and forwards the ingress packets of the devices that belong to those addresses. If the port receives ingress packets that have source MAC addresses other than the five it has already learned, it discards those packets to prevent the devices from passing traffic through the switch.

Static Versus Dynamic Addresses

The MAC addresses that the ports learn can be stored as either static or dynamic addresses in the MAC address table in the switch. Ports that store the addresses as static addresses do not learn new addresses after they have learned their maximum number. In contrast, ports that store the addresses as dynamic addresses can learn new addresses when addresses are timed out from the table by the switch. The addresses are aged out according to the aging time of the MAC address table.

Intrusion Actions

The intrusion actions define what the switch does when ports that have learned their maximum number of MAC addresses receive packets that have unknown source MAC addresses. Intrusion actions are also called violation actions. The possible settings are:

- **Protect**— Ports discard those frames that have unknown MAC addresses. No other action is taken. For example, if port 14 is configured to learn 18 addresses, it starts to discard packets with unknown source MAC addresses after learning 18 MAC addresses.
- **Restrict**— This is the same as the protect action, except that the switch sends SNMP traps when the ports discard frames. For example, if port 12 is configured to learn two addresses, the switch sends a trap every time the port, after learning two addresses, discards a packet that has an unknown MAC address.
- **Shutdown**— The switch disables the ports and sends SNMP traps. For example, if port 5 is configured to learn three MAC addresses, it is disabled by the switch to prevent it from forwarding any further traffic if it receives a packet with an unknown source MAC address, after learning three addresses. The switch also sends an SNMP trap.

Guidelines

Here are the guidelines to MAC address-based port security:

- The filtering of a packet occurs on the ingress port, not on the egress port.
- You cannot use MAC address-based port security and 802.1x port-based access control on the same port. To specify a port as an Authenticator or Supplicant in 802.1x port-based access control, you must remove MAC address-based port security.
- MAC address-based port security is not supported on the optional GBIC, SFP, or XFP modules.

Displaying MAC Address-based Port Security Settings

To display the MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68.

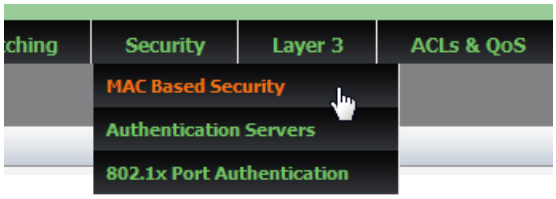


Figure 68. Security Tab

2. From the Security tab drop-down menu, select **MAC Based Security**.

   The MAC Based Port Security page is displayed. See Figure 69.

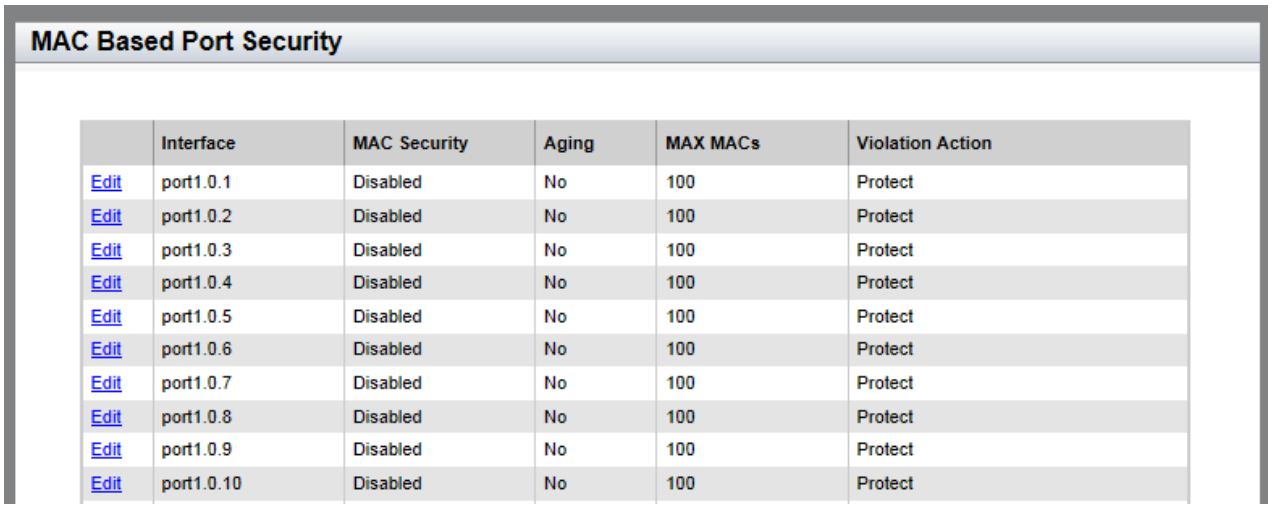


Figure 69. MAC Based Port Security Page

The following fields are displayed:

- **Interface**— Port ID.
- **MAC Security**— Indicates MAC address-based security is either “Enabled” or “Disabled” on a port. By default, this setting is disabled.
- **Aging**— Indicates one of the following:

Yes: Saves the source MAC addresses as dynamic addresses in the MAC address table.

No: Saves the source MAC addresses as static addresses in the MAC address table. This is the default setting.

- **MAX MACs**— Maximum number of dynamic MAC addresses the port is permitted to learn. The range is 0 to 255. By default, this field is set to 100.
- **Violation Action**— Indicates one of the following actions:

  Protect: Discards invalid frames. This is the default setting.

  Restrict: Discards invalid frames and sends SNMP traps.

  Shutdown: Sends SNMP traps and disables the port.

Modifying MAC Address-based Port Security Settings

To the modify the MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **MAC Based Security**.

   The MAC Based Port Security page is displayed. See Figure 69 on page 182.

3. Click Edit next to the port that you want to modify.

   The Modify MAC Based Port Security page is displayed. See Figure 70.

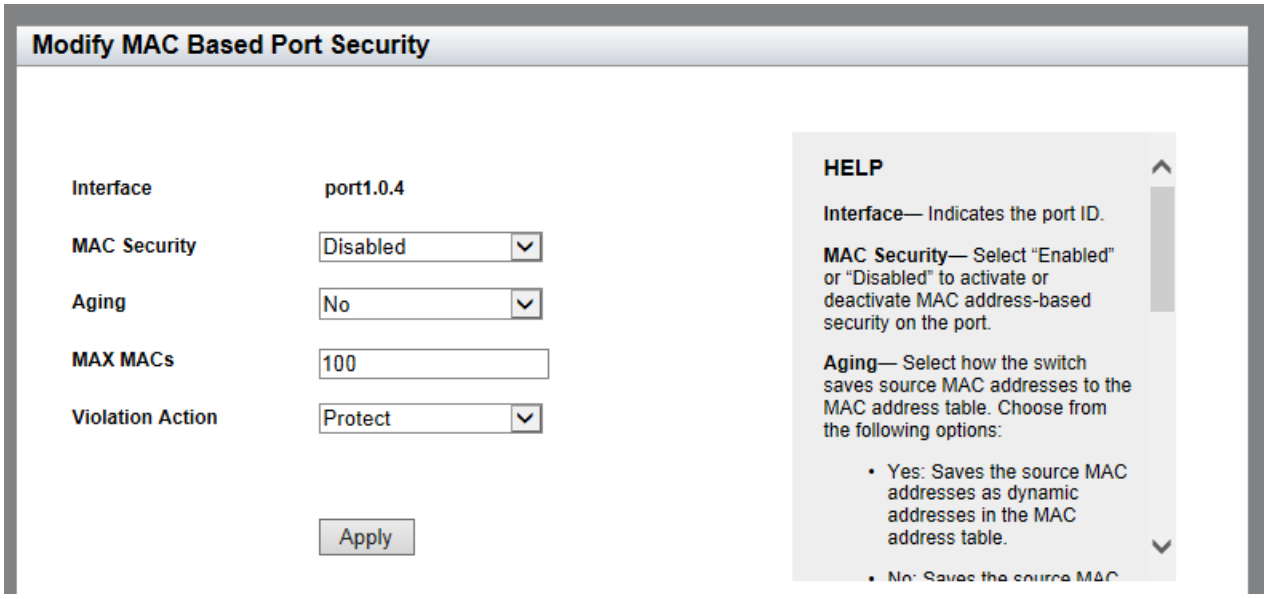


Figure 70. Modify MAC Based Port Security Page

4. Change the following settings as needed:

   - **Interface**— Indicates the port number. You cannot change this parameter from this page.
   - **MAC Security**— Select between "Enabled" and "Disabled" to activate or deactivate MAC address-based security on the port.
   - **Aging**— Select how the switch saves source MAC addresses to the MAC address table. Choose from the following options:

     Yes: Saves the source MAC addresses as dynamic addresses in the MAC address table.

     No: Saves the source MAC addresses as static addresses in the MAC address table.

   - **MAX MACs**— Enter the maximum number of source MAC addresses that the switch can learn and store for the port. The range is 0 to 255. The default is 100 addresses.
   - **Violation Action**— Select the intrusion action of the port. Choose from the following:

     Protect: Discards invalid frames.

     Restrict: Discards invalid frames and sends SNMP traps.

     Shut Down: Sends SNMP traps and disables the port.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Disabling MAC Address-based Port Security Settings

To deactivate MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **MAC Based Security**.

   The MAC Based Port Security page is displayed. See Figure 69 on page 182.

3. Click Edit next to the port that you want to remove.

   The Modify MAC Based Port Security page is displayed. See Figure 70 on page 184.

4. Use the pull-down menu next to the **MAC Security** field and select “Disabled.”

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 17

RADIUS and TACACS+ Clients

This chapter provides a brief description of both the RADIUS and TACACS+ clients and explains how to configure these clients on the switch.

See the following sections:

For more information about the authentication server features, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ RADIUS and TACACS+ Clients
- ❒ RADIUS and TACACS+ Client Commands

Overview

The switch has RADIUS and TACACS+ clients for remote authentication. Here are the features that use remote authentication:

- 802.1x port-based network access control. This feature lets you increase network security by requiring that network users log on with a username and password before the switch forwards their packets. This feature is described in Chapter 18, “802.1x Port-based Network Access” on page 201.
- Remote manager accounts. This feature lets you add manager accounts to the switch by transferring the authenticating task from the switch to an authentication server on your network. Accounts that the switch authenticates are called local accounts. This feature is described in “Managing Local User Accounts” on page 52.

The RADIUS client supports both features, but the TACACS+ client supports only the remote manager accounts feature. Here are the guidelines:

- Only one client can be active on the switch at a time.
- If you want to use only the remote manager account feature, you can use either RADIUS or TACACS+ because both clients support that feature.
- If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.

Remote Manager Accounts

The switch comes with one local manager account. The account is referred to as a local account because the switch authenticates the username and password when a manager uses the account to log on. If the username and password are valid, the switch allows the individual to access its management software. Otherwise, it cancels the login to prevent unauthorized access.

There are two ways to add more manager accounts. The first way is to create additional local accounts. For more information about local accounts, see “Managing Local User Accounts” on page 52.

The second way to add more accounts is with a RADIUS or TACACS+ authentication server on your network. With either authentication method, the authentication of the usernames and passwords of the manager accounts is performed by one or more authentication servers. The switch forwards the information to the servers when managers log on.

The following steps illustrate the authentication process that occurs between the switch and an authentication server when a manager logs on:

1. The switch uses its RADIUS or TACACS+ client to transmit the username and password to an authentication server on the network.
2. The server checks to see if the username and password are valid.
3. If the combination is valid, the authentication server notifies the switch, which completes the login process, allowing the manager access to its management software.
4. If the username and password are invalid, the authentication protocol server notifies the switch, which cancels the login.

Accounting Information

RADIUS and TACACS+ also provides a way to monitor usage by login users. You can configure the switch to send a start accounting message at the beginning of a session and a stop accounting message at the end of the session to an authentication sever.

Configuring RADIUS and TACACS+

To authenticate using a RADIUS or TACACS+ server, you must configure remote manager authentication and add authentication servers that the switch can access.

You can configure up to three servers each for the RADIUS and TACACS+ features. However, only one authentication method can be used at a time, either RADIUS or TACACS+.

To configure remote manager authentication and add authentication servers, choose from the following procedures:

- "Configuring RADIUS for Remote Manager Authentication" on page 191
- "Configuring TACACS+ for Remote Manager Authentication" on page 195

Placing RADIUS and TACACS+ Servers in the Client's List

When a user logs on to the switch, the authentication client polls the servers for authentication information in the order in which they are listed in the client. The order that you add a server determines its order on the client. For instance, the first server that you add becomes Server 1, the second server that you add becomes Server 2, and the third server that you add becomes Server 3.

When you remove a server from the switch, the place holder is retained. For example, you make the following assignments:

- Server 1 has an IP address of 192.168.10.11
- Server 2 has an IP address of 192.168.10.12
- Server 3 has an IP address of 192.168.10.13

When you delete Server 1, the server with an IP address of 192.168.10.12 remains Server 2; the server with an IP address of 192.168.10.13 remains Server 3. As a result, the next server that you add to the switch becomes Server 1.

Configuring RADIUS for Remote Manager Authentication

To configure remote manager authentication using RADIUS and add RADIUS servers to the switch, perform the following:

- "Configuring Remote Manager Authentication Using RADIUS" on page 191
- "Adding a RADIUS Server" on page 193

Configuring Remote Manager Authentication Using RADIUS

To configure the RADIUS server, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **Authentication Servers**.

   The Authentication Server Configuration page with the RADIUS tab selected is displayed. See Figure 71.

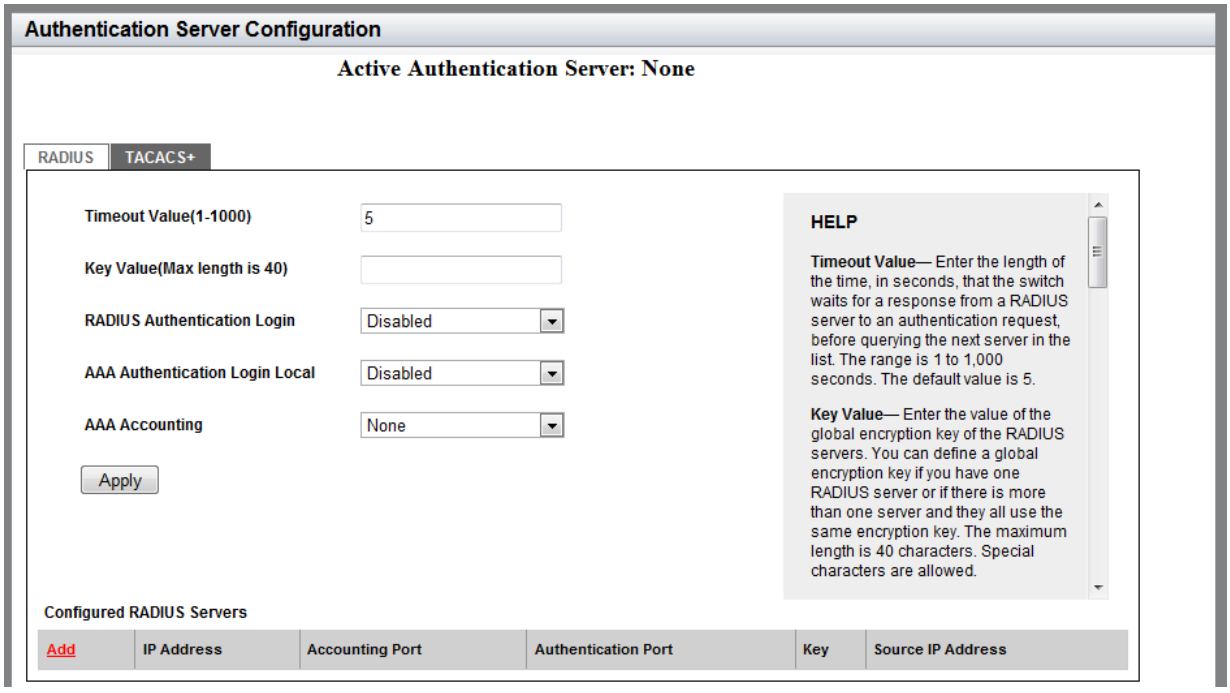


Figure 71. Authentication Server Configuration Page with RADIUS Tab

3. Change the following fields as needed:

   - **Timeout Value**— Enter the length of the time, in seconds, that the switch waits for a response from a RADIUS server to an

authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5 seconds.

- **Key Value**— Enter the value of the global encryption key of the RADIUS servers. You can define a global encryption key if you have one RADIUS server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

Caution
To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the client on the RADIUS Server Configuration Page. See “Adding a RADIUS Server” on page 193.

- **RADIUS Authentication Login**— Enable or disable RADIUS to authenticate user login. Choose from the following:

  Enabled: The RADIUS servers authenticate user login.

  Disabled: The RADIUS servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

- **AAA Authentication Login Local**— Enable or disable RADIUS to authenticate user login in combination with local manager accounts. Choose from the following:

  Enabled: The RADIUS servers authenticate the user login. When any RADIUS server is not available, authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

  Disabled: The RADIUS servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note
For additional information about the User Management page, see “Managing Local User Accounts” on page 52. For more information about the USERNAME command, see “Local Manager Accounts” in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*.

- **AAA Accounting**— Select a RADIUS accounting setting. Choose from the following:

  Start-Stop: Indicates that a start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.

  Stop-Only: Indicates a stop accounting message is sent at the end of the session.

  None: Indicates that sending accounting messages is disabled.

4. Click **Apply**.

   The Active Authentication Server field shown on the upper middle of the page indicates "RADIUS."

5. Click **SAVE** to save your changes to the startup configuration file.

Adding a RADIUS Server

To add a RADIUS server, do the following:

1. Click **Add** near the RADIUS server list.

   The RADIUS Server Add page is displayed. See Figure 72.

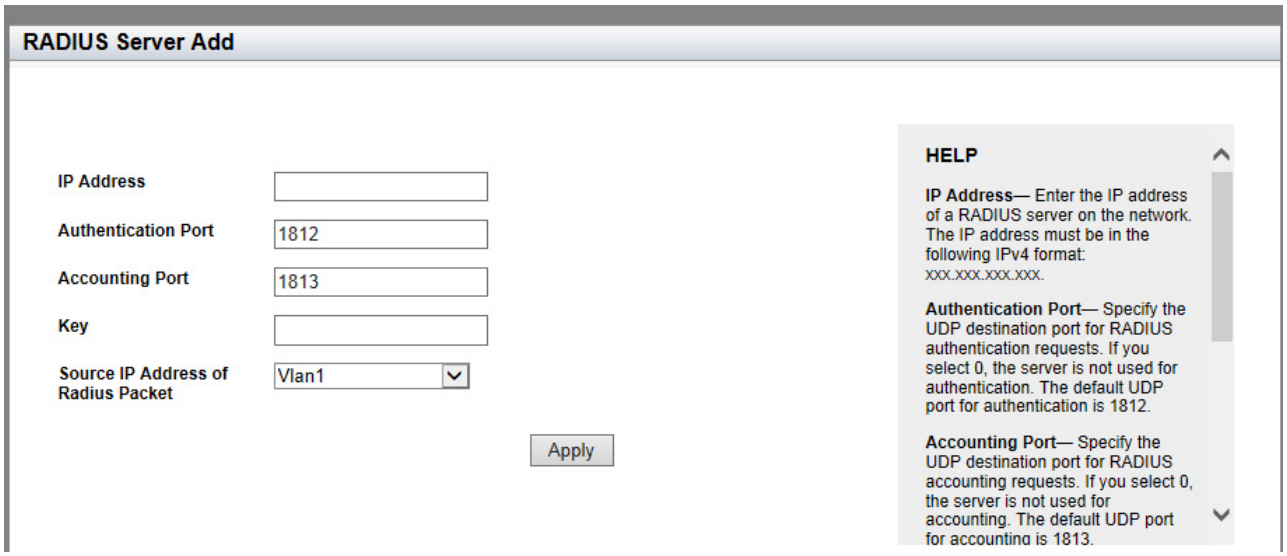


Figure 72. RADIUS Server Add Page

2. Configure the following as needed:

   - **IP Address**— Enter the IP address of a RADIUS server on the network. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.

- **Authentication Port**— Specify the UDP destination port for RADIUS authentication requests. If you select 0, the server is not used for authentication. The default UDP port for authentication is 1812.
- **Accounting Port**— Specify the UDP destination port for RADIUS accounting requests. If you select 0, the server is not used for accounting. The default UDP port for accounting is 1813.
- **Key**— Enter the encryption key for RADIUS communications between the switch and RADIUS server. The key must match the encryption key used by the RADIUS server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.
- **Source IP Address of Radius Packet**— Assign the RADIUS source interface to a VLAN ID. The RADIUS client uses the selected VLAN ID on every outgoing RADIUS packet. The default is Vlan1.

3. Click **Apply**.
4. Click **SAVE** to save your changes to the startup configuration file.

Configuring TACACS+ for Remote Manager Authentication

To configure remote manager authentication using TACACS+ and add TACACS+ servers to the switch, perform the following:

- "Configuring Remote Manager Authentication Using TACACS+" on page 195
- "Adding a TACACS+ Server" on page 198

Configuring Remote Manager Authentication Using TACACS+

To configure a TACACS+ server, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **Authentication Servers**.

   The Authentication Server Configuration page is displayed. See Figure 71 on page 191.

3. Click the **TACACS+** tab.

   The Authentication Server Configuration Page with the TACACS+ tab is displayed. See Figure 73 on page 196.

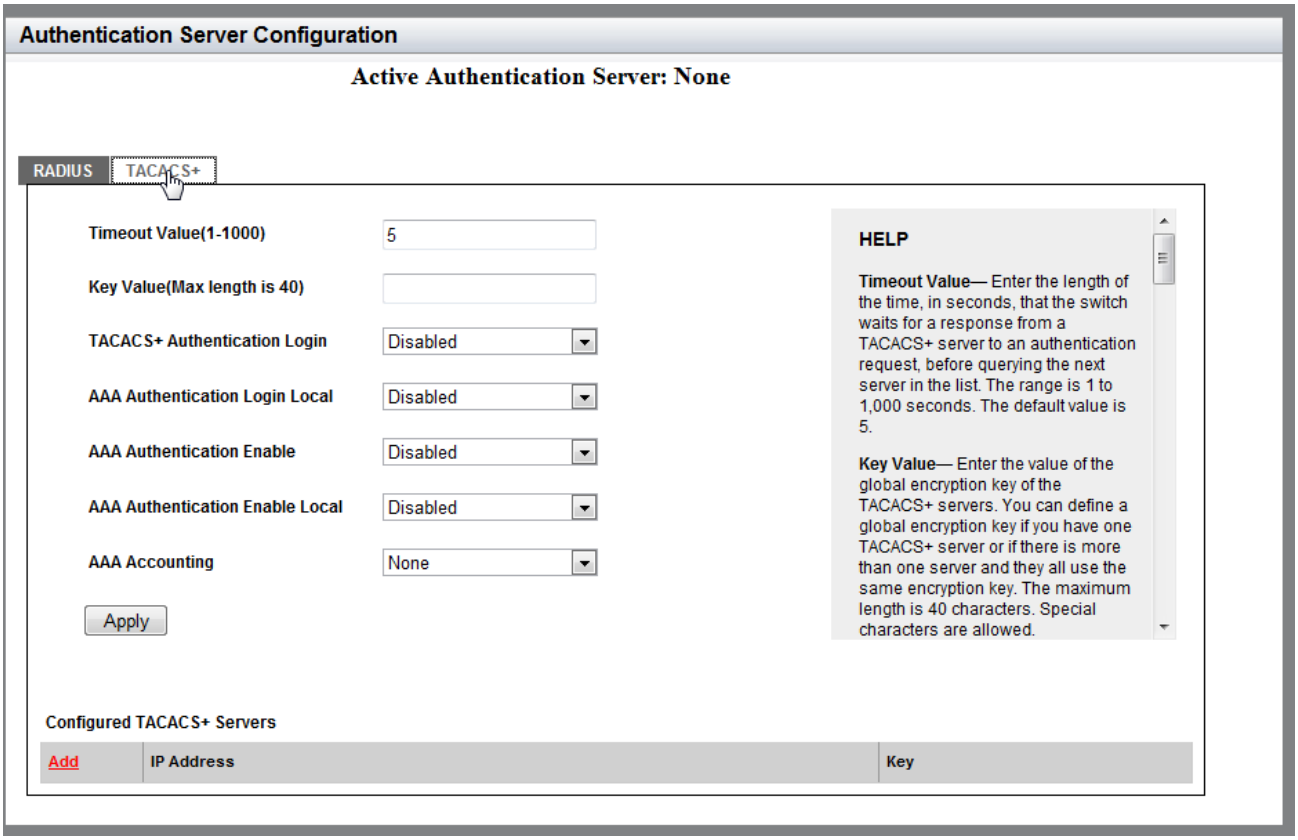


Figure 73. Authentication Server Configuration Page with TACACS+ Tab

4. Change the following as needed:

   - **Timeout Value**— Enter the length of the time, in seconds, that the switch waits for a response from a TACACS+ server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5.
   - **Key Value**— Enter the value of the global encryption key of the TACACS+ servers. You can define a global encryption key if you have one TACACS+ server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

Caution

To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the switch on the TACACS+ Server Add page. See “Adding a RADIUS Server” on page 193.

- **TACACS+ Authentication Login**— Enable or disable TACACS+ to authenticate user login. Choose from the following:

  Enabled: The TACACS+ servers authenticate user login.

  Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

- **AAA Authentication Login Local**— Enable or disable TACACS+ to authenticate user login in combination with local manager accounts. Choose from the following:

  Enabled: The TACACS+ servers authenticate user login. When any TACACS+ server is not available, authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

  Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note
For additional information about the User Management page, see "Managing Local User Accounts" on page 52. For more information about the USERNAME command, see Chapter 88: Local Manager Accounts in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide*.

- **AAA Authentication Enable**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:

  Enabled: The TACACS+ servers determine whether users can access the Privileged EXEC level using the TACACS+ enable password.

  Disabled: The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

- **AAA Authentication Enable Local**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:

  Enabled: The TACACS+ servers determine whether users can access the Privileged EXEC level using the TACACS+ enable password. When any TACACS+ server is not available,

authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

Disabled: The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

- **AAA Accounting**— Select a TACACS+ accounting setting. Choose from the following:

  Start-Stop: A start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.

  Stop-Only: A stop accounting message is sent at the end of the session.

  None: Sending accounting messages is disabled.

5. Click **Apply**.

   The Active Authentication Server field shown on the upper middle of the page indicates “TACACS+.”

6. Click **SAVE** to save your changes to the startup configuration file.

Adding a TACACS+ Server

To add a TACACS+ server, do the following:

1. Click **Add** at the bottom of the page.

   The TACACS+ Server Add page is displayed. See Figure 74.

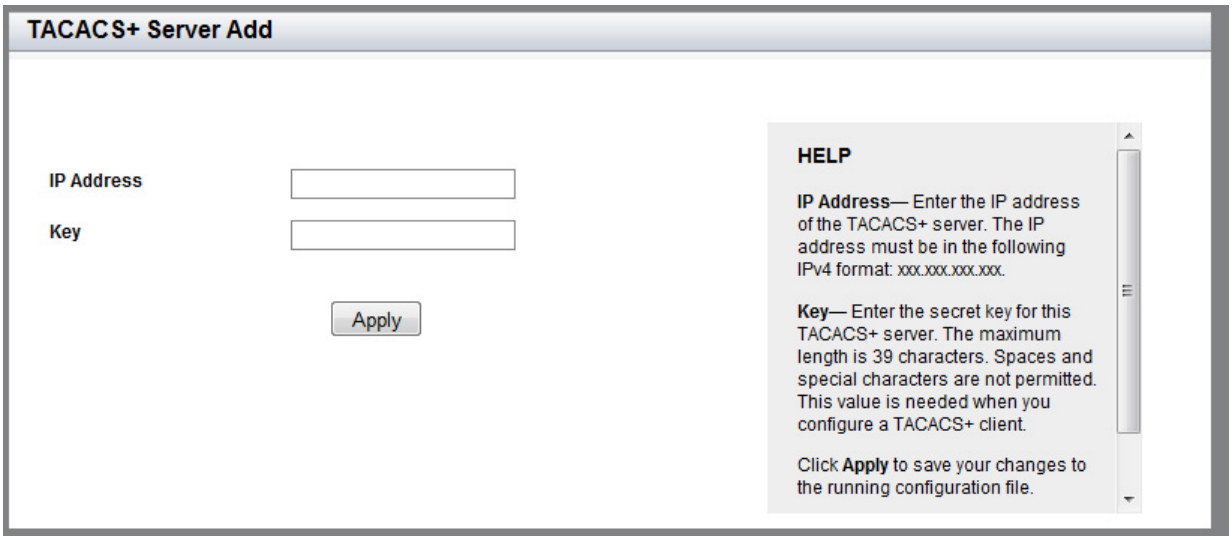


Figure 74. TACACS+ Server Add Page

2. Enter the following settings:

   - **IP Address**— Enter the IP address of the TACACS+ server. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.
   - **Key**— Enter the encryption key for TACACS+ communications between the switch and TACACS+ server. The key must match the encryption key used by the TACACS+ server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

3. Click **Apply**.

4. Click **SAVE** to save your changes to the startup configuration file.

Deleting an Authentication Server

To delete either an TACACS+ or RADIUS authentication server, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **Authentication Servers**.

   The Authentication Server Configuration page is displayed. See Figure 71 on page 191.

3. Click either the TACACS+ or the RADIUS tab, depending on the type of server you want to delete.

4. Click **Delete** next to the server that you want to delete.

5. Click **SAVE** to save your changes to the startup configuration file.

Chapter 18

802.1x Port-based Network Access

This chapter provides a brief description of the 802.1x Port-based Authentication feature and explains how to enable this feature on the switch, and specify authentication on a port.

See the following sections:

For more information about the 802.1x features, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- 802.1x Port-based Network Access Control
- 802.1x Port-based Network Access Control Commands

Overview

The 802.1x port-based network access control feature lets you control who can send traffic through, and receive traffic from, the individual switch ports. The switch does not allow an end node to send or receive traffic through a port until the user of the node has been authenticated by a RADIUS server.

This port-security feature is used to prevent unauthorized individuals from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users designated as valid network users on a RADIUS server are permitted to use the switch to access the network.

This port security method uses the RADIUS authentication protocol. To use the 802.1x port-based network access control feature, you must configure RADIUS and add RADIUS servers to the switch. For more information about RADIUS and its configuration, see Chapter 17, “RADIUS and TACACS+ Clients” on page 187.

Note
RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication protocol for 802.1x port-based network access control. This feature is not supported with the TACACS+ authentication protocol.

The switch does not authenticate any end nodes connected to its ports. Its function is to act as an intermediary between the end nodes or users and the RADIUS authentication server during the authentication process.

Port Roles

Part of the task to implementing this feature is specifying the roles of the ports on the switch. The roles are listed here:

- None Role:

  Switch ports in the none role do not participate in port-based access control. They forward traffic without authenticating the supplicants of the network devices. This is the default setting for the switch ports.

  Note
  A RADIUS authentication server cannot authenticate itself and must communicate with the switch through a port that is not configured as an authenticator port.

- Authenticator Role:

  The authenticator role activates port access control on a port. Ports in this role do not forward network traffic to or from network devices until the supplicants are authenticated by a RADIUS server. The authenticator role is appropriate when you want the switch to authenticate the supplicants of network devices before they can use the network.

  Figure 75 illustrates the none role and authenticator role.

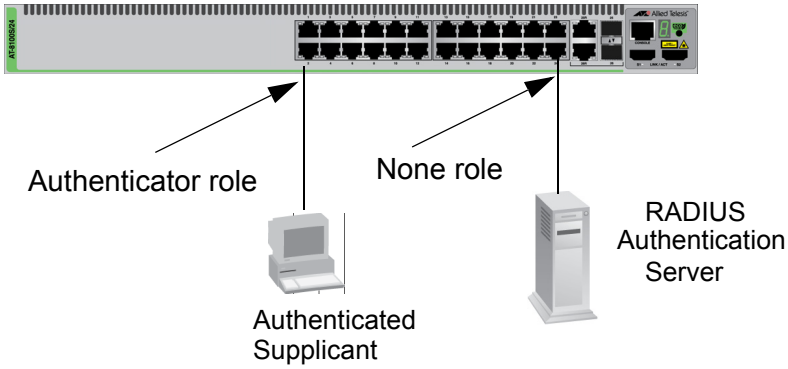


Figure 75. Example of Port Roles

Operating Modes

Authenticator ports have three modes:

- Single host mode

  An authenticator port set to the single host mode permits only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant.

  In Figure 76, port 6 is an authenticator port set to the single host mode. It permits only one supplicant to log on and forwards the traffic of only that supplicant.

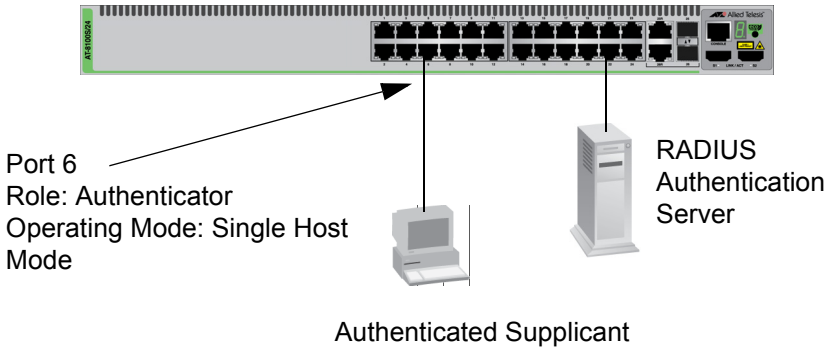


Figure 76. Single Host Mode

- Multiple host mode

  This mode permits multiple supplicants on an authenticator port. An authenticator host forwards packets from all supplicants once one supplicant has successfully logged on. This mode is typically used in situations where you want to add 802.1x port-based network access control to a switch port that is supporting multiple supplicants, but do not want to create individual accounts for all the supplicants on the RADIUS server.

  This is referred to as “piggy-backing.” After one supplicant has successfully logged on, the port permits the other supplicants to piggy-back onto the initial supplicant’s logon, so that they can forward packets through the port without being authenticated.

  Figure 77 is an example of this mode. Port 6 is connected to an Ethernet hub or non-802.1x-compliant switch, which in turn is connected to several supplicants. The switch does not forward the supplicant traffic until one of the supplicants logs on. Afterwards, it forwards the traffic of all the supplicants.

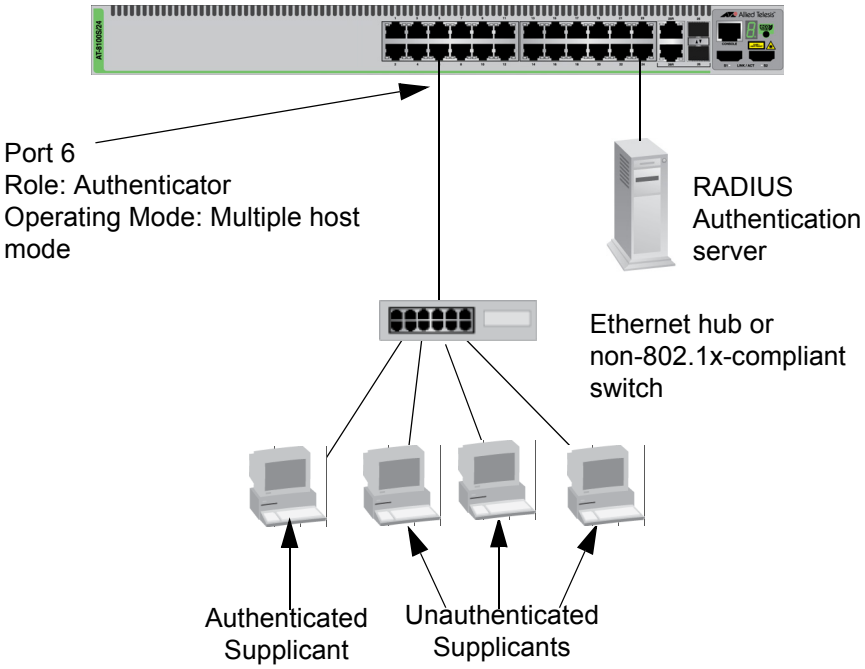


Figure 77. Multiple Host Operating Mode

- Multiple supplicant mode

  This mode authenticates all the supplicants on an authenticator port. This mode is appropriate in situations where an authenticator port is supporting more than one supplicant, and you want all supplicants to be authenticated. A switch in this mode can support up to a maximum of 208 supplicants.

An example of this authenticator operating mode is illustrated in Figure 78. The supplicants are connected to a hub or non-802.1x-compliant switch which is connected to an authenticator port on the switch. If the port is configured as 802.1x authenticator, the supplicants must successfully authenticate before they can forward traffic through the switch.

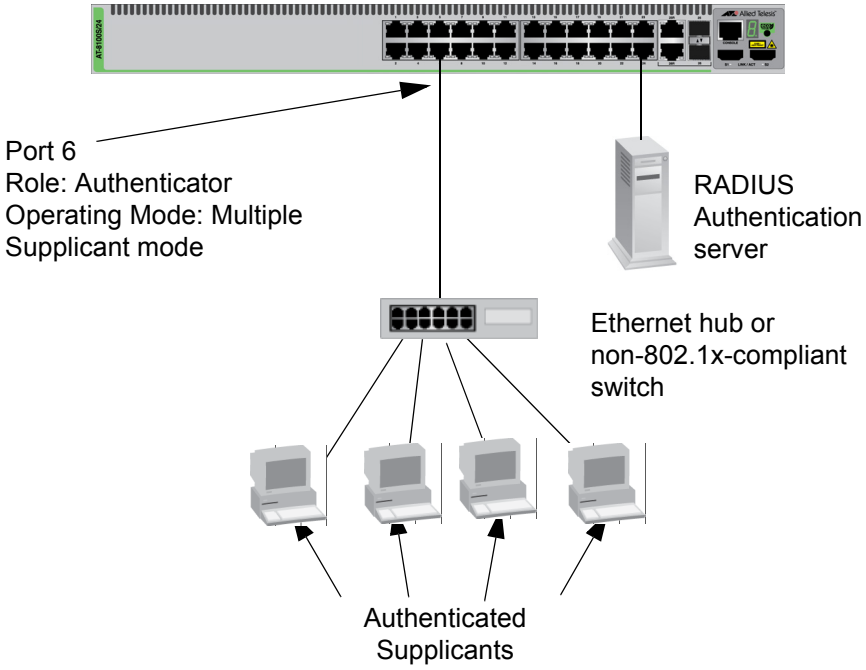


Figure 78. Multiple Supplicant Mode

Dynamic VLAN Assignments

With 802.1x port-based network access control, you can link a username and password combination or MAC address to a specific VLAN so that the switch automatically moves the port to the appropriate VLAN when a supplicant logs on. This frees the network manager from having to reconfigure VLANs as end users access the network from different points or where the same workstation is used by different individuals at different times.

To use this feature, you have to enter a VLAN identifier, along with other information, when you create a supplicant account on the RADIUS server. The server passes the identifier to the switch when a user logs on with a valid username and password combination or MAC address, depending on the authentication method.

How the switch responds when it receives VLAN information during the authentication process can differ depending on the operating mode of the authenticator port.

Guest VLAN

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a supplicant. However, you can specify an authenticator port to be a member of a Guest VLAN when no authenticated supplicant is logged on. Any guest user using the port is not required to log on and has full access to the resources of the Guest VLAN.

If the switch receives 802.1x packets on the port, signalling that an authenticated supplicant is logging on, it moves the port to its predefined VLAN and places it in the unauthorized state. The port remains in the unauthorized state until the logon process between the authenticated supplicant and the RADIUS server is completed. When the authenticated supplicant logs off, the port automatically returns to the Guest VLAN.

Note
The Guest VLAN feature is only supported on an authenticator port in the Single host operating mode.

Enabling 802.1x Port-based Authentication on the Switch

To enable the 802.1x port-based Authentication feature on a switch, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

   The 802.1x Authentication page is displayed. See Figure 79.

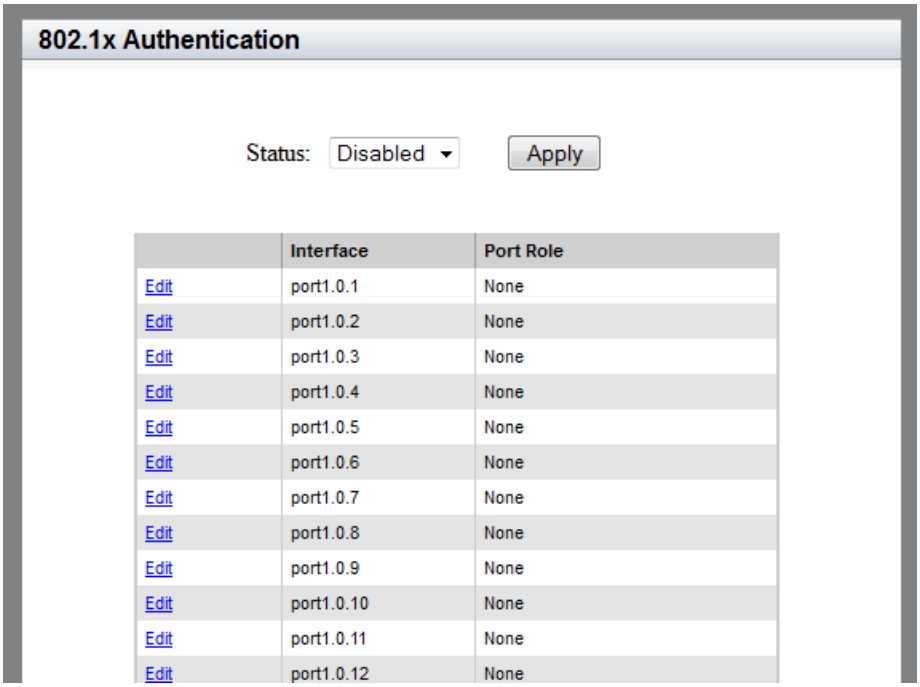


Figure 79. 802.1x Authentication Page

3. Use the pull-down menu next to the Status field to select "Enabled."

   The default setting is "Disabled."

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Configuring 802.1x Port-based Authentication

To set 802.1x port authentication on a port, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

   The 802.1x Authentication page is displayed. See Figure 79 on page 207.

3. Click Edit next to the port that you want to modify.

   The Modify 802.1x Authentication page is displayed. See Figure 80.

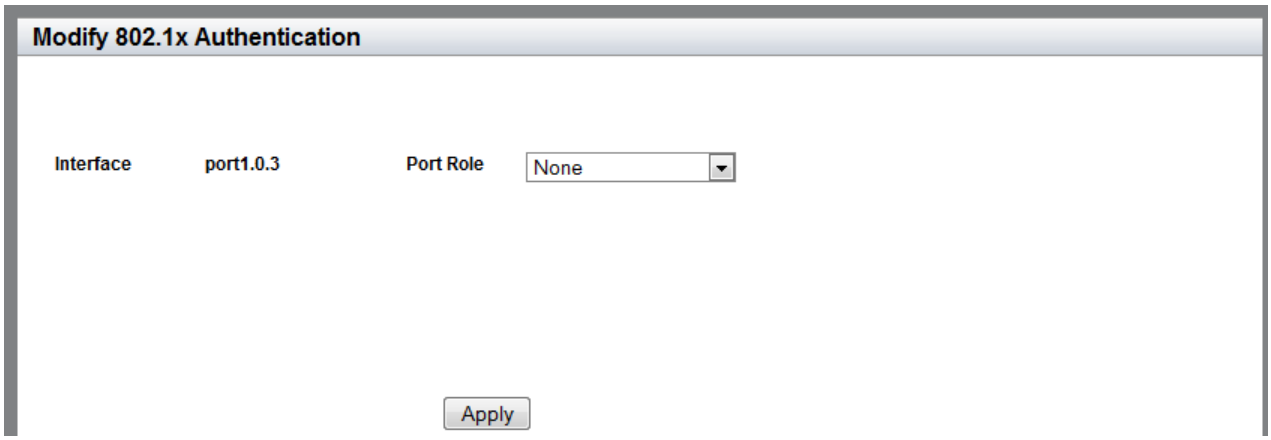


Figure 80. Modify 802.1x Authentication Page

4. Use the pull-down menu next to the **Port Role** field to select "Authenticator."

   The Modify 802.1x Authentication page "Authenticator" expands. See Figure 81 on page 209.

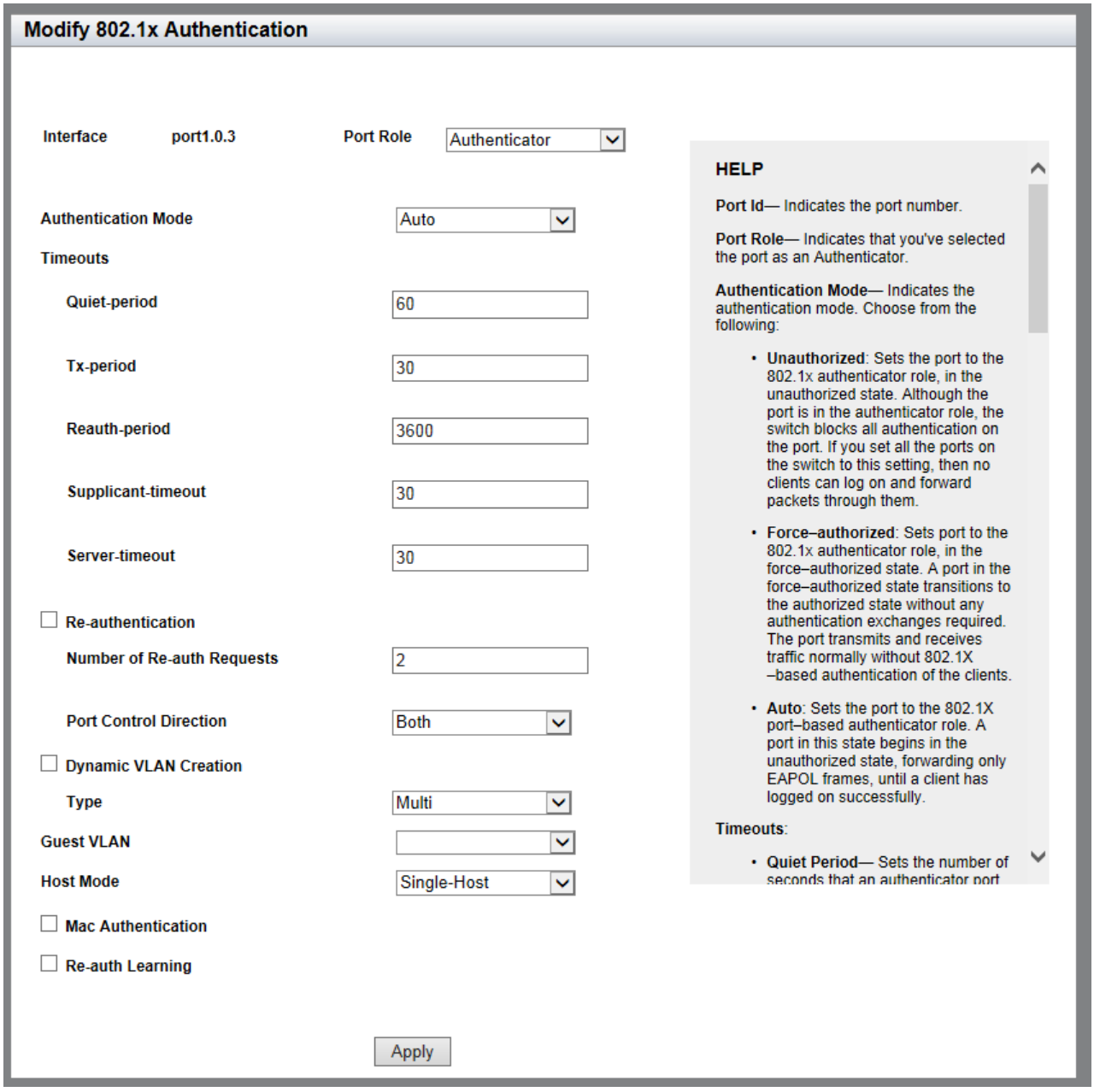


Figure 81. Modify 802.1x Authentication Page Expanded

5. Modify the following fields as needed:

   - **Interface**— Indicates the port ID. You cannot modify this parameter from this page.
   - **Port Role**— Specifies that you have selected the port as an Authenticator.

- **Authentication Mode**— Select the authentication mode. Choose from the following:

  Unauthorized: Sets the port in the unauthorized state. Although the port is in the authenticator role, the switch blocks all authentication on the port. If you set all the ports on the switch to this setting, then no supplicants can log on and forward packets through them.

  Force-authorized: Sets port in the force-authorized state. A port in the force-authorized state transitions to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1X-based authentication of the supplicants.

  Auto: Sets the port active in the authenticator role. A port in this state begins in the unauthorized state, forwarding only authentication frames, until a supplicant has logged on successfully.

- **Timeouts**

The following fields set the timers for this feature:

Quiet Period— Enter the number of seconds that an authenticator port remains in the quiet state following a failed authentication exchange with a supplicant. The range is 0 to 65,535 seconds. The default value is 60 seconds.

Tx-period— Enter the number of seconds that an authenticator port waits for a response to an EAP-request/ identity frame from a supplicant before retransmitting the request. The range is 1 to 65,535 seconds. The default value is 30 seconds.

Reauth-period— Enter the time interval that an authenticator port requires a supplicant to reauthenticate. The range is 1 to 65,535 seconds. The default value is 3,600 seconds.

Supplicant-timeout— Enter the retransmission time for the EAP-request frame from the authenticator port. The range is 1 to 600 seconds. The default value is 30 seconds.

Server-timeout— Enter the number of seconds the switch waits for a response from the authentication server. The range is 1 to 600 seconds. The default value is 30 seconds.

- **Re-authentication**— Check the checkbox to activate reauthentication on the authenticator port. The supplicant periodically reauthenticates according to the time interval set with the Reauth-period timer.
- **Number of Re-auth Requests**— Enter the maximum number of

times the switch retransmits EAP Request packets to a supplicant before it times out an authentication session. The range is 1 to 10 retransmissions. The default value is 2.

- **Port Control Direction**— Select whether the authenticator port that is in the unauthorized state should forward egress broadcast and multicast traffic. Choose from the following:

  In: Specifies that the authenticator port in the unauthorized state should forward egress broadcast and multicast traffic, and discard the ingress broadcast and multicast traffic. This is the default setting.

  Both: Specifies that the authenticator port in the unauthorized state should discard both ingress and egress broadcast and multicast traffic.

- **Dynamic VLAN Creation**— Check the checkbox to activate dynamic VLAN assignments of the authenticator port.
- **Type**— Select the type of dynamic VLAN assignments. Choose from the following:

  Single: Specifies that an authenticator port forwards packets of only those supplicants that have the same VID as the supplicant who initially logged on.

  Multi: Specifies that an authenticator port forwards packets of all supplicants, regardless of the VIDs in their supplicant accounts on the RADIUS server.

- **Guest VLAN**— Select the ID number of a VLAN that is the guest VLAN of an authenticator port. You can select only one VID.
- **Host Mode**— Select the operating mode on an authenticator port. Choose from the following:

  Single-host: Specifies the single host operating mode. An authenticator port set to this mode forwards only those packets from the one supplicant who initially logs on. This is the default setting.

  Multi-host: Specifies the multiple host operating mode. An authenticator port set to this mode forwards all packets after one supplicant logs on. This is referred to as piggy-backing.

  Multi-supplicant: Specifies the multiple supplicant operating mode. An authenticator port set to this mode requires that all supplicants log on.

- **Mac Authentication**— Check the checkbox to activate MAC address-based authentication on the authenticator port. An authenticator port that uses this type of authentication extracts the source MAC address from the initial frame from a supplicant and

automatically sends it as the supplicant's username and password to the authentication server.

This authentication method does not require 802.1x client software on supplicant nodes.

- **Re-Auth Learning**— Check the checkbox to force the port that is using MAC address authentication into the unauthorized state. You may use this setting to reauthenticate the nodes on the authenticator port.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Disabling 802.1x Port-based Authentication on the Switch

To disable the 802.1x port-based Authentication feature on a switch, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

   The 802.1x Authentication page with the Status field set to "Enabled" is displayed. See Figure 82.

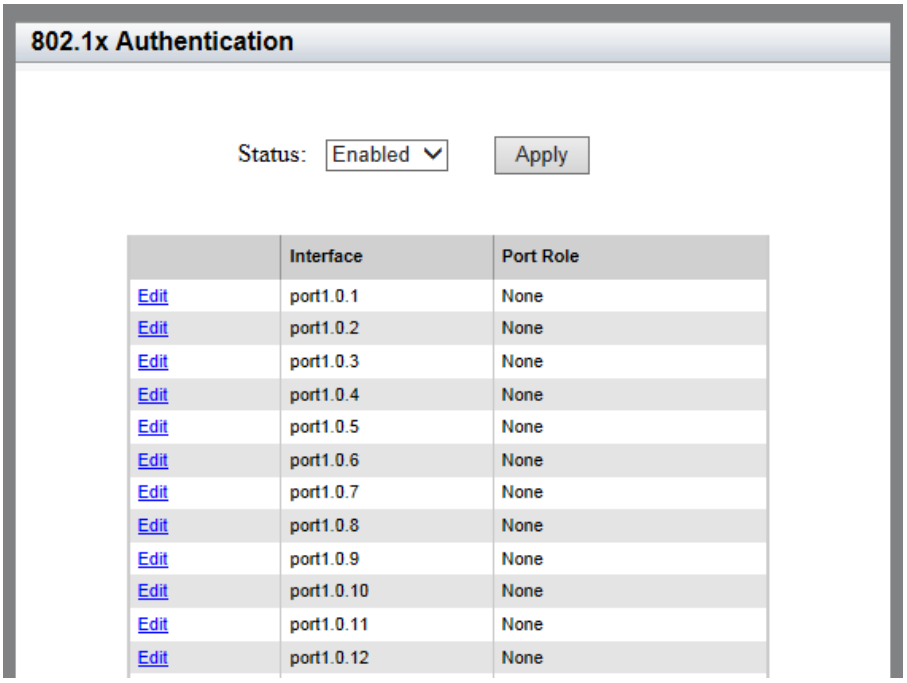


Figure 82. 802.1x Authentication Page with Status Enabled

3. Use the pull-down menu next to the **Status** field to select "Disabled."
4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Disabling 802.1x Port-based Authentication on a Port

To disable 802.1x port authentication on a port, do the following:

1. Hover the cursor over the **Security** tab.

   The Security tab is displayed. See Figure 68 on page 182.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

   The 802.1x Authentication page is displayed. See Figure 79 on page 207.

3. Click Edit next to the port that you want to modify.

   The Modify 802.1x Authentication page is displayed. See Figure 80 on page 208.

4. Use the pull-down menu next to the **Port Role** field to select “None.”

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 19

Setting IPv4 and IPv6 Addresses

This chapter provides brief descriptions of management IPv4 and IPv6 addresses and explains how to specify both types of IP addresses on the switch.

See the following sections:

For more information about the IP management address, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ IPv4 and IPv6 Management Addresses
- ❒ IPv4 and IPv6 Management Address Commands

Overview

The management IP address is an IP address that the switch uses to identify itself to other network devices, such as TFTP servers and Telnet clients. The management address can be any IPv4 address, or an IPv6 address for some features, that is assigned to a VLAN on the switch. The features listed in Table 8 require that the switch is assigned a management IP address.

You can assign an IP address only to a VLAN interface. You can assign one IPv4 address per VLAN. The switch can have as many IPv4 addresses as there are VLANs on the switch. You can assign an IPv6 address to any VLAN; however, you can assign only one IPv6 address to the switch.

You can use an IPv6 address as the management IP address. However, as shown in Table 8, the IPv6 address supports only the TACACS+ client and HTTP clients. To use features that are not supported by the IPv6 address, you must use an IPv4 address as the management IP address.

Note
In the Command Line Interface, there are additional features that require either an IPv4 or IPv6 address.

Table 8. Web Interface Features that Require an IP Management Address

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address
802.1x port-based network access control	Used for port security.	yes	no
RADIUS client	Used for remote management authentication and for 802.1x port-based network access control.	yes	no
sFlow agent	Used to transmit packet statistics and port counters to an sFlow collector on your network.	yes	no
TACACS+ client	Used for remote management authentication using a TACACS+ server on your network.	yes	yes

Table 8. Web Interface Features that Require an IP Management Address (Continued)

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address
HTTP client	Used for a web browser to bring the AT-FS970M web interface on your network.	yes	yes

IP Management Guidelines

See the following list for guidelines about assigning a management IPv4 or IPv6 address to the switch:

- You can assign one IPv4 address per VLAN.
- Any IPv4 address can be used as the management IP address.
- The switch can have only one IPv6 address.
- The management IPv4 address can be any IPv4 address assigned to a VLAN on the switch. For background information on VLANs, see Chapter 11, "Setting Port-based and Tagged VLANs" on page 131.
- In the AT-FS970M Series Version 2.3.1.0 web interface, the IPv4 address is assigned as the static address. The web interface does not support the assignment of an IPv4 address from a DHCP server. When you want to assign an IPv4 address from a DHCP server, see the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User's Guide*.
- An IPv6 address is assigned as the static address. The switch does not support the assignment of an IPv6 address from a DHCP server.
- To assign the default gateway IPv4 address, you must assign it as the static route. For assigning a static route, see Chapter 21, "Setting Static Routes" on page 243.
- To assign the default gateway IPv6 address, you must add it when you assign the management IPv6 address. See Chapter 19, "Adding an IPv6 Address" on page 225.
- The IPv4 management address and the default gateway IPv4 address must be members of the same network.
- The IPv6 management address and the default gateway IPv6 address must be members of the same network.

Displaying IPv4 Interfaces

To display a list of the IPv4 interfaces, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 83.

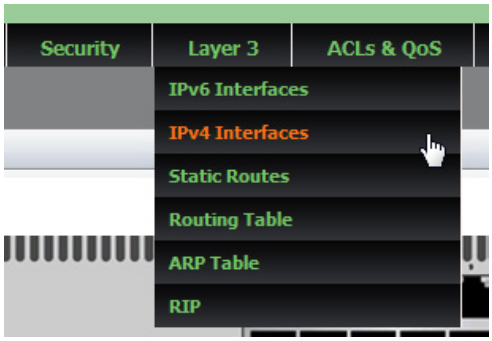


Figure 83. Layer 3 Tab

2. From the **Layer 3** tab drop-down menu, select **IPv4 Interfaces**.

   A list of IPv4 interfaces is displayed. See Figure 84.

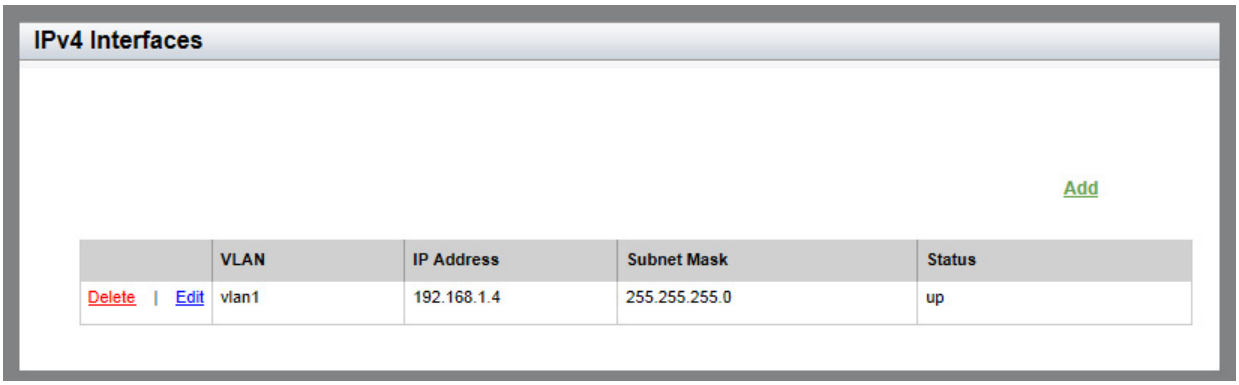


Figure 84. IPv4 Interfaces Page

The following fields are displayed:

- **VLAN**— VLAN number that has an IP interface.
- **IP Address**— IP address that the VLAN is assigned to.
- **Subnet Mask**— Subnet mask of the IP address.
- **Status**— Status of the link.

Adding an IPv4 Address

To assign an IPv4 address, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 83 on page 218.

2. From the **Layer 3** tab drop-down menu, select **IPv4 Interfaces**.

   A list of IPv4 interfaces is displayed. See Figure 84 on page 218.

3. Click **Add**.

   The IP Address Configuration Page is displayed. See Figure 85.

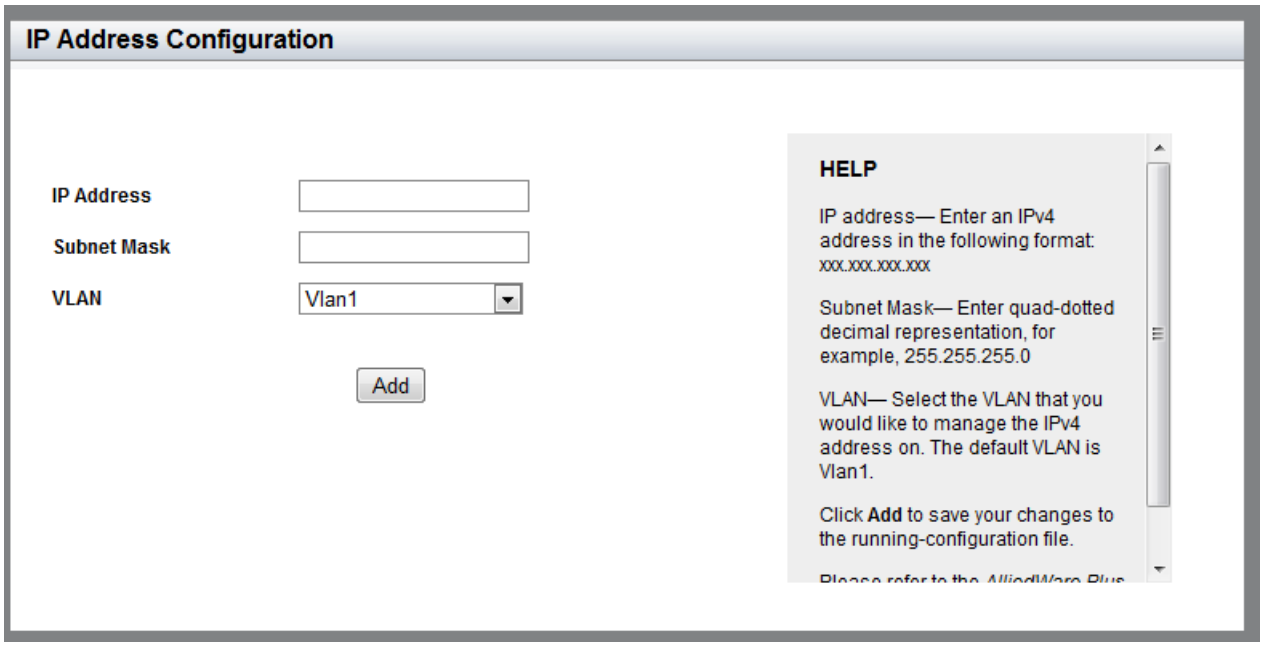


Figure 85. IP Address Configuration Page

4. Enter the following fields:

   - **IP Address**— Enter the IP address that you want to add.
   - **Subnet Mask**— Enter the subnet mask of the IPv4 address in quad-dotted decimal representation, for example, 255.255.255.0.
   - **VLAN**— Select the VLAN ID that you want to assign the IPv4 address to.

5. Click **Add**.

6. Click **SAVE** to save your changes to the startup configuration file.

Changing an IPv4 Address

To display a list of the IPv4 interfaces, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 83 on page 218.

2. From the **Layer 3** tab drop-down menu, select **IPv4 Interfaces**.

   A list of IPv4 interfaces is displayed. See Figure 84 on page 218.

3. From the IPv4 Interfaces page, click Edit next to the VLAN ID that you want to modify.

   The following page is displayed. See Figure 86.

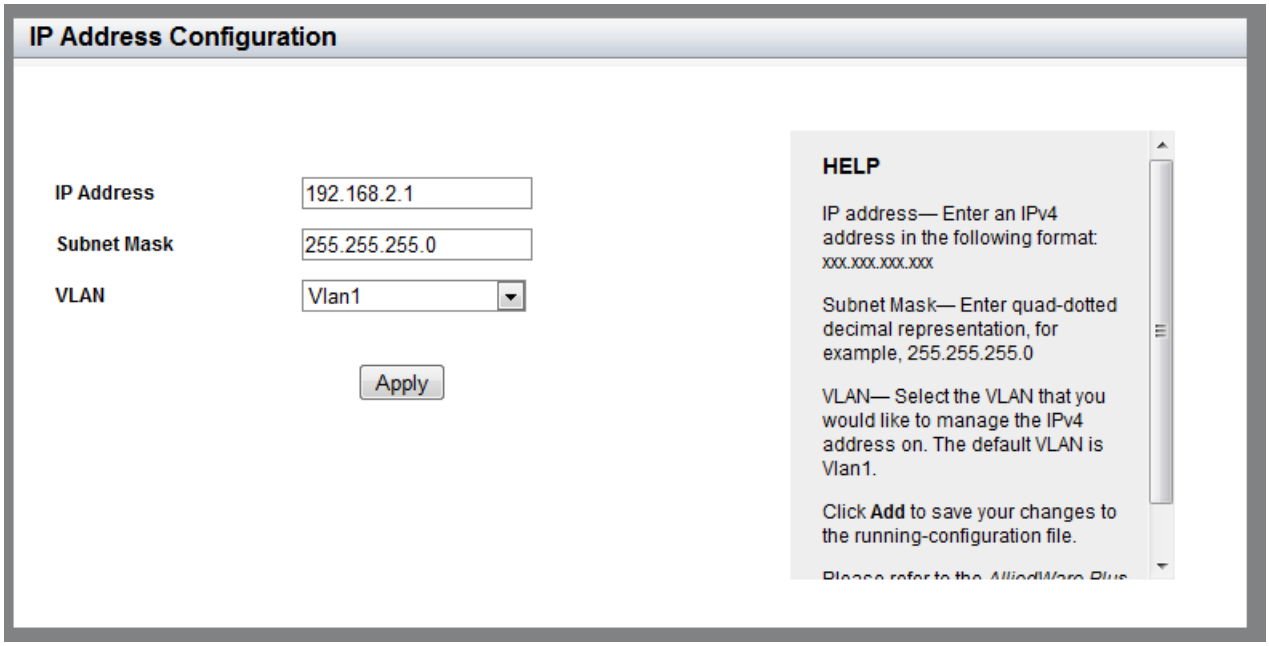


Figure 86. Edit IP Address Configuration Page

4. Change the following fields as needed:

   - **IP Address**— Enter the IP address that the VLAN is assigned to.
   - **Subnet Mask**— Enter the subnet mask of the IPv4 address.
   - **VLAN**— Select the VLAN to manage the IP address.

Note
If you change the IP address that you use to access the web interface, you lose the connection to the switch. Start a management session again by opening a web browser on your PC and entering the new IP address of the switch.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting an IPv4 Address

To delete an IPv4 address, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 83 on page 218.

2. From the **Layer 3** tab drop-down menu, select **IPv4 Interfaces**.

   A list of IPv4 interfaces is displayed. See Figure 84 on page 218.

3. From the IPv4 Interfaces page, click Delete on the same line as the IPv4 address that you want to delete.

   The selected IPv4 address is removed from the VLAN.

Displaying the IPv6 Interface

To display a list of the IPv6 interface, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 87.

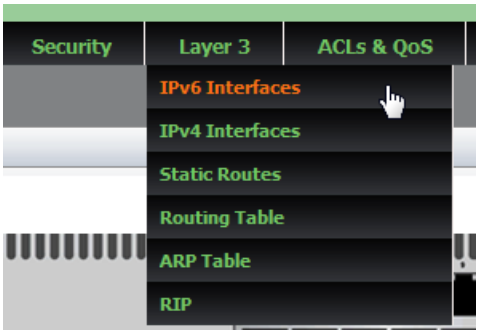


Figure 87. Layer 3 Tab

2. From the **Layer 3** tab drop-down menu, select **IPv6 Interface**.

   The IPv6 interface is displayed if one has already been assigned. See Figure 88.

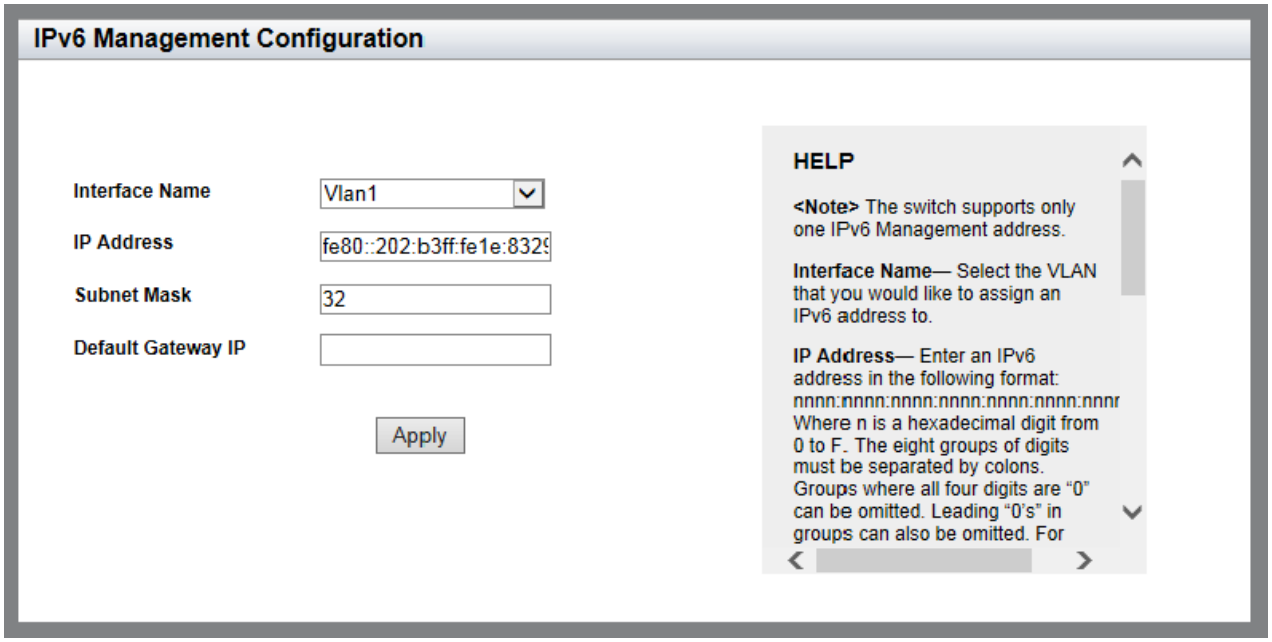


Figure 88. IPv6 Interface Page

The following fields are displayed:

- **Interface Name**— VLAN number that the management IPv6 address is assigned to.
- **IP Address**— Management IPv6 address.
- **Subnet Mask**— Subnet mask of the management IPv6 address.
- **Default Gateway IP**— Default gateway IP address (if assigned).

Adding an IPv6 Address

The switch supports only one IPv6 address. As a result, you can add an IPv6 address only when no IPv6 address is assigned to the switch.

To assign an IPv6 address, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 87 on page 223.

2. From the **Layer 3** tab drop-down menu, select **IPv6 Interface**.

   The IPv6 Interface page is displayed. Ensure that no IPv6 address is displayed.

3. Click **Add**.

   The IPv6 Management Configuration Page is displayed. See Figure 89.

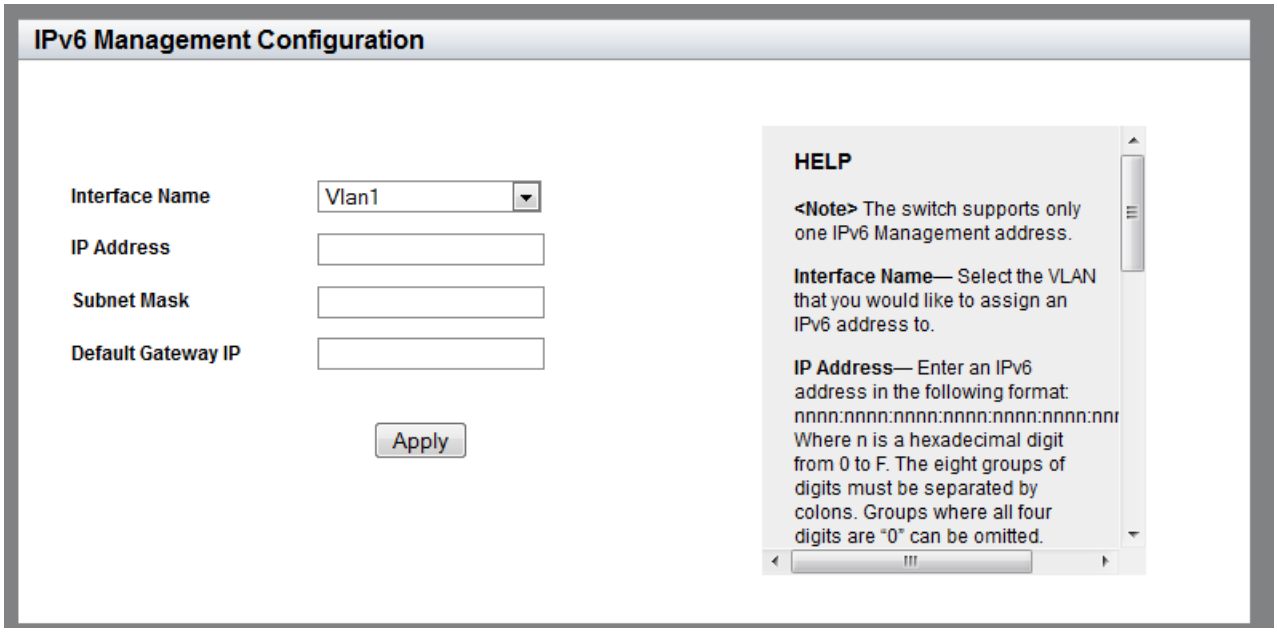


Figure 89. IPv6 Management Configuration Page

4. Select a VLAN to assign to the IPv6 address by using the pull-down menu next to the **Interface Name** field.

   You can only select a VLAN that you have configured previously. For information about how to assign a VLAN, see Chapter 11, "Setting Port-based and Tagged VLANs" on page 131.

5. Enter an IPv6 address in the **IP Address** field in the following format:

   nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

   Where n is a hexadecimal digit from 0 to F. The eight groups of digits must be separated by colons. Groups where all four digits are “0” can be omitted. Leading “0’s” in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

   12c4:421e:09a8:0000:0000:0000:00a4:1c50

   12c4:421e:9a8::a4:1c50

6. Enter the number of subnet mask bits in the **Subnet Mask** field.

7. Enter an IPv6 default gateway address in the **Default Gateway IP** field.

   Use this field to assign the switch an IPv6 default gateway address. A default gateway is an address of an interface on a router or other Layer 3 device. It defines the first hop to reaching the remote subnets or networks where the network devices are located.

8. Click **Apply**.

9. Click **SAVE** to save your changes to the startup configuration file.

Changing IPv6 Addresses

To edit the management IPv6 interface, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 87 on page 223.

2. From the **Layer 3** tab drop-down menu, select **IPv6 Interface**.

   The IPv6 interface is displayed if one has already been assigned. See Figure 88 on page 223.

3. From the IPv6 Interface page, click Edit.

   The following page is displayed. See Figure 90.

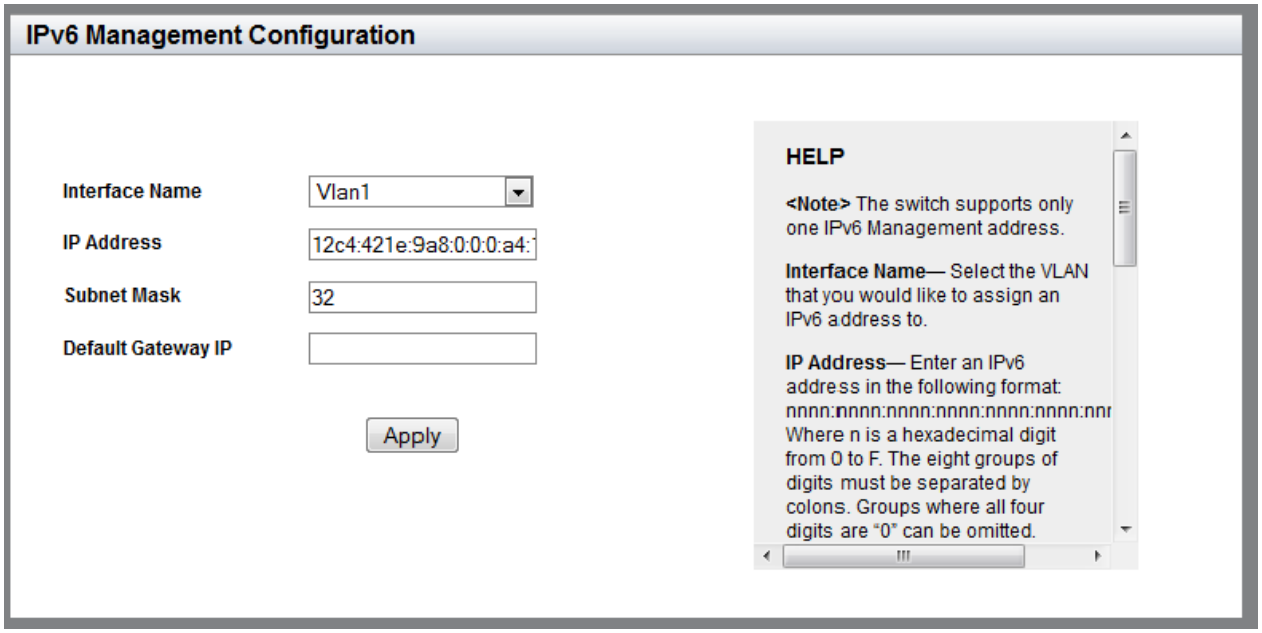


Figure 90. Edit IPv6 Management Configuration Page

4. Change the following fields as needed:

   - **VLAN**— Select the VLAN number that the management IPv6 address is assigned to.
   - **IP Address**— Enter the management IPv6 address.
   - **Subnet Mask**— Enter the number of subnet mask bits of the management IPv6 address.
   - **Default Gateway IP**— Enter the default gateway IPv6 address.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting IPv6 Addresses

To delete an IPv6 address, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 87 on page 223.

2. From the **Layer 3** tab drop-down menu, select **IPv6 Interface**.

   The IPv6 interface is displayed, if any. See Figure 88 on page 223.

3. From the IPv6 Interface page, click **Clear**.

   The management IPv6 address is removed from the switch.

Chapter 20

Access Control Lists (ACL)

This chapter provides a brief description of the Access Control Lists (ACL) feature and explains how to use these features on the switch.

See the following sections:

For information about the QoS feature, see Chapter 22, “Quality of Service (QoS)” on page 251.

For more information about the ACL feature, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Advanced Access Control Lists (ACL)
- ❒ ACL Commands

Overview

Access Control Lists (ACLs) act as filters to control the ingress packets on ports. They are commonly used to restrict the types of packets that ports accept to increase port security and create physical links dedicated to carrying specific types of traffic. For instance, you can configure ACLs to permit ports to accept only ingress packets that have a specific source IP address or destination IP address.

You create an ACL first and then assign it to a port. ACLs take effect immediately when they are assigned to ports. To create an ACL, you assign filtering criteria to select a type of traffic, assign an action of dropping the traffic, forwarding the traffic to another port, or copying and mirroring the traffic to another port. The port filters the ingress traffic and takes an action based on the ACL that is assigned to the port.

Using the AT-FS970M web interface, you can configure two types of ACLs:

- IPv4 ACLs
- MAC ACLs

IPv4 ACLs use IPv4 addresses as filtering criteria while MAC ACLs use only MAC addresses as filtering criteria. For IPv4 ACLs, you can specify TCP or UDP port numbers to filter the traffic. In addition, IPv4 ACLs are only compatible with IPv4 addresses. They are not compatible with IPv6 addresses.

Classifier Number Ranges

IPv4 and MAC ACLs are identified by classifier numbers. When you create an ACL, you must choose the correct classifier number based on which ACL you want to create. See the IPv4 and MAC ACL classifier number ranges displayed in Table 9.

Table 9. ACL Classifier Number Ranges

Type of ACL	Classifier Number Range
IPv4 ACLs	3000 - 3699
MAC ACLs	4000 - 4699

Filtering Criteria

ACLs identify packets using filtering criteria. The AT-FS970M web interface offers five criteria:

- Source and destination IPv4 addresses
- Source and destination MAC addresses
- Source and destination TCP ports

- Source and destination UDP ports
- VLAN IDs

IPv4 Address and Mask

The mask of an IPv4 address is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for first the twenty-four bits of the network portion of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

Actions

The action defines the response to packets that match the filtering criterion of the ACL. There are three actions for ACLs:

- **Deny**— A deny action instructs ports to discard the specified ingress packets.
- **Permit**— A permit action instructs ports to forward ingress packets that match the specified traffic flow of the ACL. By default, all ingress packets are forwarded by the ports.
- **Copy to mirror**— This action causes a port to copy all ingress packets that match the ACL to the destination port of the mirror port.

How Ingress Packets are Compared Against ACLs

Ports that do not have an ACL forward *all* ingress packets. Ports with one or more deny ACLs discard ingress packets that match the ACLs and forward all other traffic. A port that has one deny ACL that specifies a particular source IP address, for example, discards all ingress packets with the specified source address and forwards all other traffic. In situations where a port has more than one deny ACL, packets are discarded at the first match.

Since ports forward all ingress packets unless they have deny ACLs, permit ACLs are only necessary in situations where you want a port to forward packets that are a subset of a larger traffic flow that is blocked: for example, a port that forwards only packets having a specified destination IP address. A permit ACL specifies the packets with the intended destination IP address, and a deny ACL specifies all traffic.

When ports have both permit and deny ACLs, you must add the permit ACLs first, because packets are compared against the ACLs in the order they are added to the ports. If a permit ACL is added after a deny ACL, ports are likely to discard packets specified by the permit ACL, thus causing them to block packets you want them to forward.

Guidelines

Here are the ACL guidelines:

- An ACL can have a permit, deny, or copy-to-mirror action. The permit action allows ports to forward ingress packets of the designated traffic flow, while the deny action causes ports to discard packets. The copy-to-mirror action causes a port to copy all ingress packets that match the ACL to the destination port for mirroring.
- A port can have more than one ACL.
- An ACL can be assigned to more than one port.
- ACLs filter ingress packets on ports, but they do not filter egress packets. As a result, you must apply ACLs to the ingress ports of the designated traffic flows.
- ACLs for static port trunks or LACP trunks must be assigned to the individual ports of the trunks.
- A port that has more than one ACL checks the ingress packets in the order in which the ACLs are added and forwards or discards packets at the first match. The order matters when applying ACLs to a port.
- An ACL can have multiple filtering criteria. For example, an ACL filters with a specific source IP address and UDP port number.
- Because ports, by default, forward all ingress packets, permit ACLs are only required in circumstances where you want ports to forward packets that are subsets of larger packet flows that are blocked by deny ACLs.

Creating an ACL

To create an ACL, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 91.

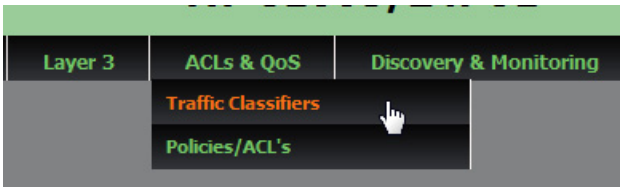


Figure 91. ACLs and QoS Tab

2. From the **ACLs & QoS** tab drop-down menu, select **Traffic Classifiers**.

   The Traffic Classifiers page is displayed. See Figure 92.

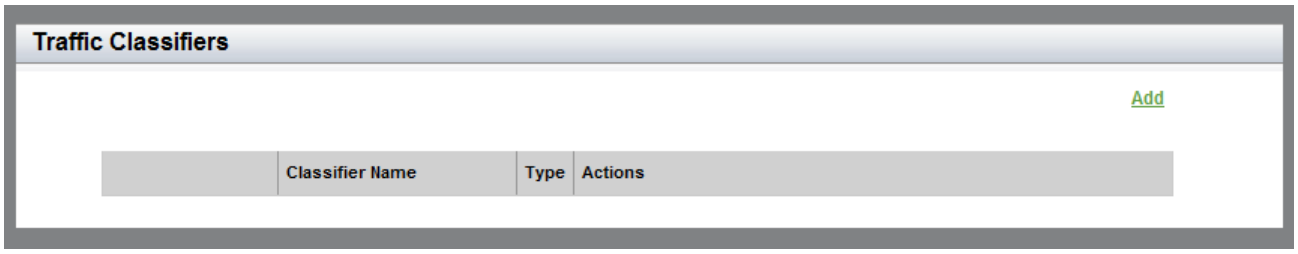


Figure 92. Traffic Classifiers Page

3. Click Add on the right, above the table.

   The Traffic Classification page is displayed. See Figure 93 on page 236.

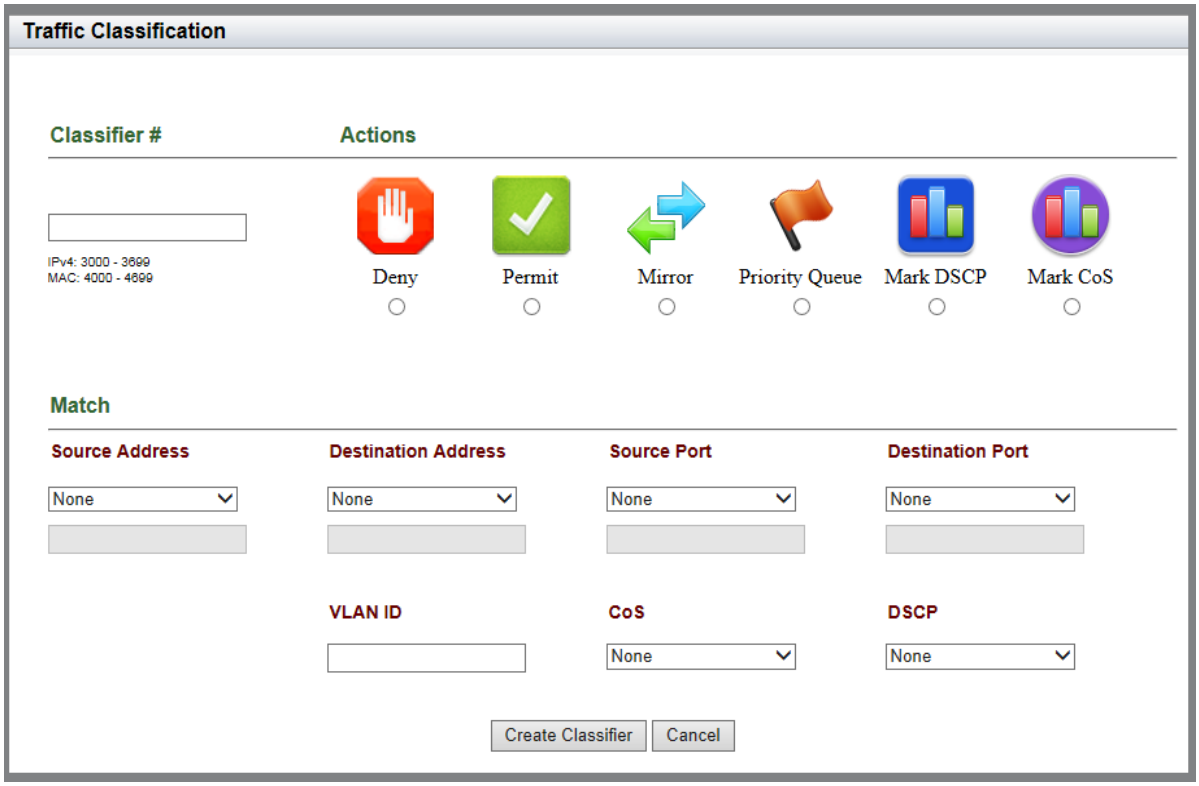


Figure 93. Traffic Classification Page

4. Enter and select the following fields as needed:

   - **Classifier #**— Enter a classifier number to identify an ACL. Choose a number from the following ranges:

     IPv4 ACL: 3000 to 3699

     MAC ACL: 4000 to 4699

   - **Actions**— Click a radio button to select an action from the following options:

     Deny: Instructs ports to discard the ingress packets that match the specified filtering criteria.

     Permit: Instructs ports to forward ingress packets that match the specified filtering criteria. By default, all ingress packets are forwarded by the ports.

     Mirror: Instructs ports to copy all ingress packets that match the filtering criteria to the mirror port.

     When you select Mirror, a pull-down menu appears below the action icons. Select a port number (for example, port1.0.1)

from the menu. The menu for Mirror to Port is displayed, as shown in Figure 94.

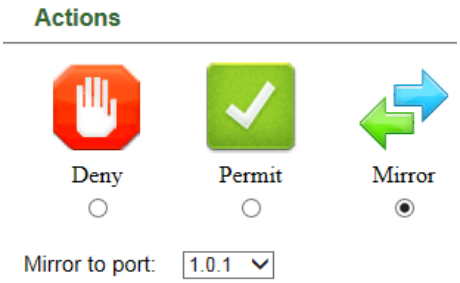


Figure 94. Menu for Mirror to Port

- **Mirror to Port**— Use the menu to select a destination port number for mirroring to which you want the switch to send copies of the packets that match the specified filtering criteria.

Note
The action options of Priority Queue, Mark DSCP, and Mark CoS are for the Quality of Service (QoS) feature. For information about creating a QoS policy, see "Creating a QoS Policy" on page 255.

Match:

- **Source Address**— Enter a source address to match ingress packets. Enter one of the following:

  IPv4 Address and mask: Select **IPv4**, then enter an IPv4 source address followed by a slash (/) and a mask if you are creating an IPv4 ACL. The keyword "any" matches all packets on the source address.

  MAC Address and mask: Select **MAC**, then enter a MAC source address followed by a slash (/) and a mask if you are creating a MAC ACL. The keyword "any" matches all packets on the source address. The wildcard mask for MAC addresses must be either "0" (zero) or "F" to indicate the parts of MAC address to filter. "F" means anything; "0" (zero) means it has to match.

- **Destination Address**— Enter a destination address to match ingress packets. Enter one of the following:

  IPv4 Address and mask: Select **IPv4**, then enter an IPv4 source address followed by a slash (/) and a mask if you are creating an IPv4 ACL. The keyword "any" matches all packets on the destination address.

MAC Address and mask: Select **MAC**, then enter a MAC source address followed by a slash (/) and a mask if you are creating a MAC ACL. The keyword “any” matches all packets on the destination address. The wildcard mask for MAC addresses must be either “0” (zero) or “F” to indicate the parts of MAC address to filter. “F” means anything; “0” (zero) means it has to match.

Note
The Source Port and Destination Port fields are applicable only to IPv4 ACLs.

- **Source Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed. This field is optional.
- **Destination Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed. This field is optional.
- **VLAN ID**— Enter a VLAN ID. Use this field if you want the ACL to filter tagged packets.

Note
The matching criteria of **CoS** and **DSCP** are for the Quality of Service (QoS) feature. For information about creating a QoS, see “Creating a QoS Policy” on page 255.

5. Click **Create Classifier**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning an ACL to Ports

Before assigning ACLs to ports, ACLs must be available on the switch. To create an ACL, see "Creating an ACL" on page 235.

To assign an ACL to ports, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 91 on page 235.

2. From the **ACLs & QoS** tab drop-down menu, select **Policies/ACLs**.

   The Policies/ACLs page is displayed. See Figure 95.

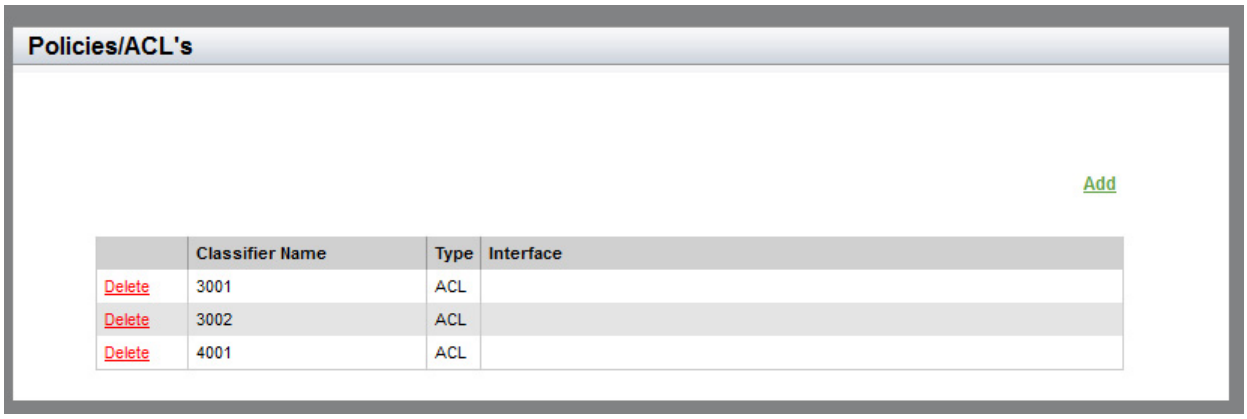


Figure 95. Policies/ACLs Page

3. Click Add on the right above the table.

   The Traffic Classifiers page is displayed. See Figure 96 on page 240.

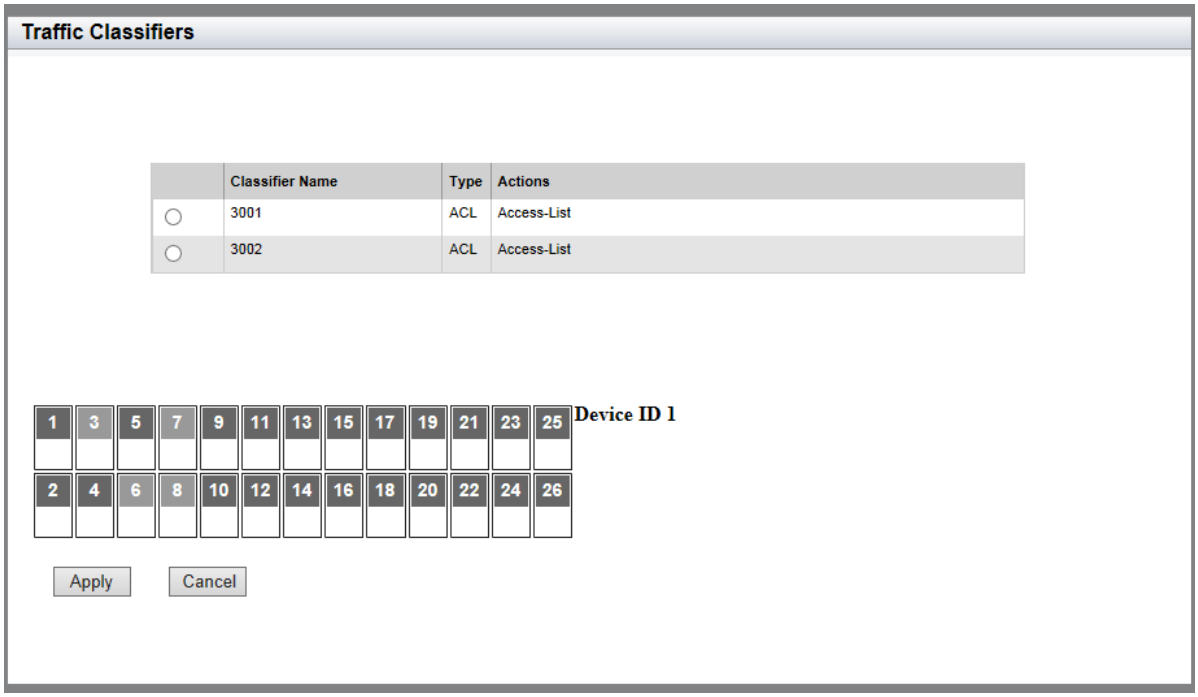


Figure 96. Traffic Classifiers Page from Policies/ACLs Page

4. Click a radio button to select an ACL.
5. Check one or multiple port numbers to select ports to apply the ACL.
6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Displaying a List of ACLs

To display a list of ACLs, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 91 on page 235.

2. From the **ACLs & QoS** tab drop-down menu, select **Traffic Classifiers**.

   The Traffic Classifiers page is displayed. See Figure 97.

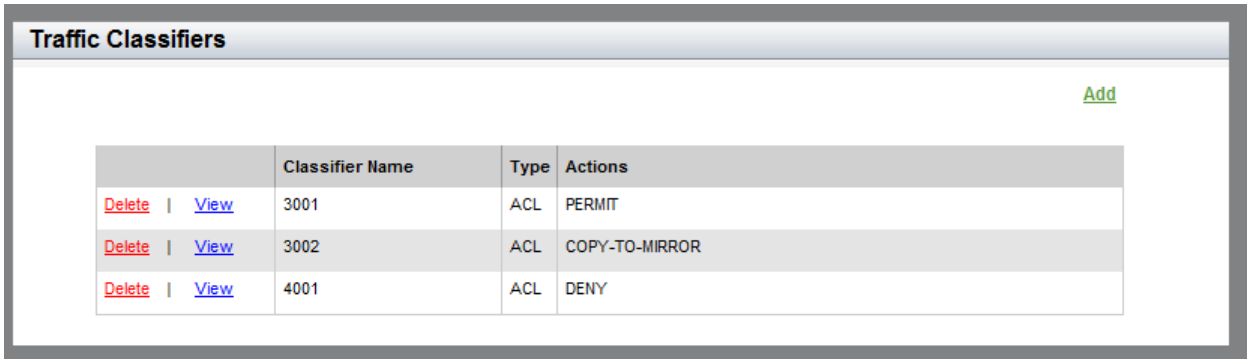


Figure 97. Traffic Classifiers Page

3. The following fields are displayed:

   - **Classifier Number**— ACL or QoS classifier number.
   - **Type**— ACL or QoS.
   - **Actions**— Actions assigned to the classifier.

Note
This list includes QoS policies as well as ACLs.

Chapter 21

Setting Static Routes

To make remote networks communicate, you must add static routes or dynamic routes, or both, to the routing table. Static routes are configured manually to add routing information to the routing table. This chapter provides information about static routes.

The procedures in this chapter describe how to display a list of static routes on the switch, and how to add and delete a static route. See the following sections:

For more information about static routes, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Internet Protocol Version 4 Packet Routing
- ❒ IPv4 Routing Commands

Displaying Static Routes

To display the static routes, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 98.

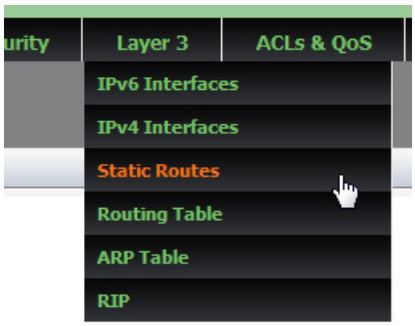


Figure 98. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, select **Static Routes**.

   A list of static routes is displayed. See Figure 99.

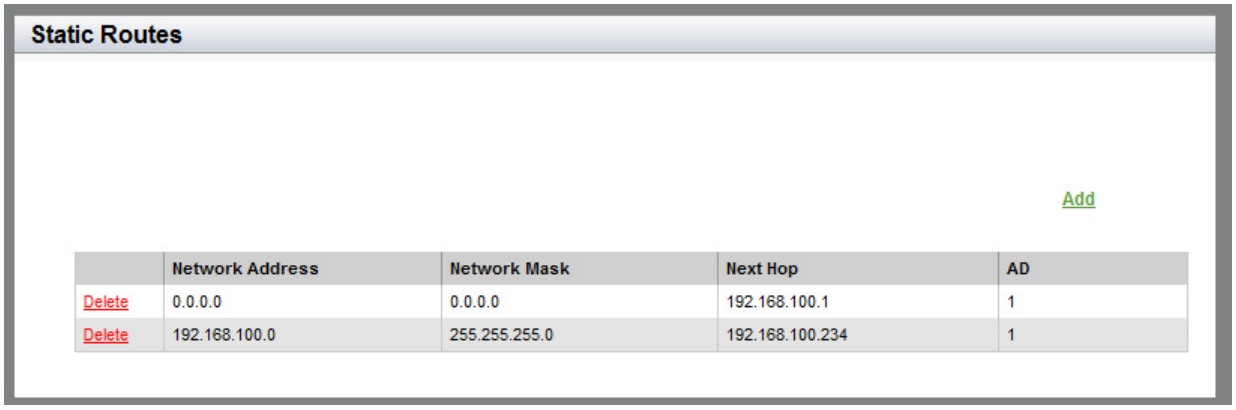


Figure 99. Static Routes Page

The following fields are displayed:

- **Network Address**— IP address of the destination network. The IP address for a default route is 0.0.0.0.
- **Network Mask**— Subnet mask of the destination network.
- **Next Hop**— IP address of the next hop to the route.
- **AD**— Value of the administrative distance specified to the route.

Adding a Static Route

To add a static route, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 98 on page 244.

2. From the Layer 3 tab drop-down menu, select **Static Routes**.

   A list of static routes is displayed. See Figure 99 on page 244.

3. Click **Add**.

   The Add Static Route Page is displayed. See Figure 100.

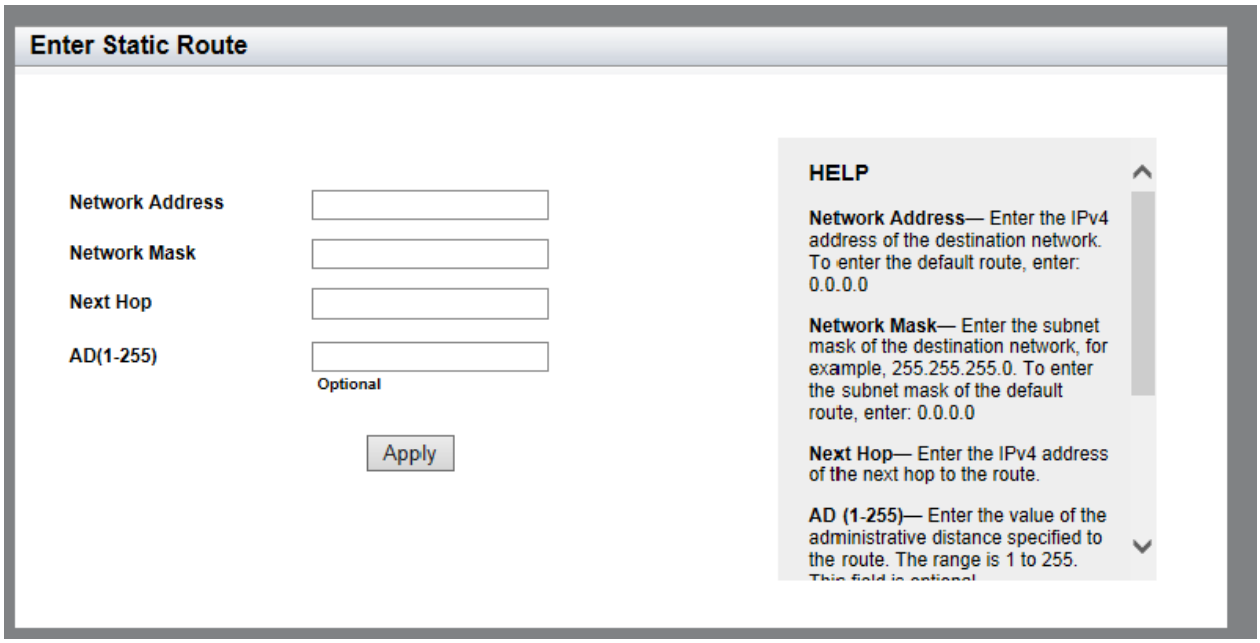


Figure 100. Add Static Route Page

4. Enter the destination network address in the **Network Address** field.
5. Enter the subnet mask of the destination network in the **Network Mask** field.
6. Enter the IP address of the next hop in the **Next Hop** field.
7. Enter the value of the metric for the route in the **AD** field. The range is 1 to 255.

   The field is optional. The default is 1.

8. Click **Apply**.
9. Click **SAVE**.

Deleting a Static Route

To delete a static route entry, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 98 on page 244.

2. From the Layer 3 tab drop-down menu, select **Static Routes**.

   A list of static routes is displayed. See Figure 99 on page 244.

3. Click Delete next to the network address that you want to delete.

Displaying the Routing Table

The routing table includes static routes and dynamic routes. The switch decides which route is the best based on the routing table.

To display the routing table, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 101.

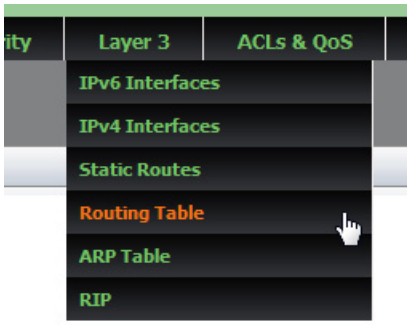


Figure 101. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, select **Routing Table**.

   A list of routes is displayed. See Figure 102.

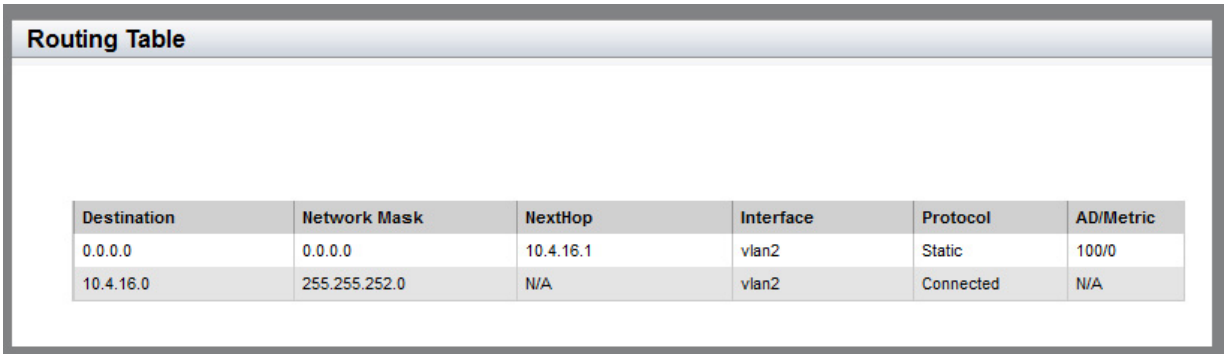


Figure 102. Routing Table Page

The following fields are displayed:

- **Destination**— Destination network address.
- **Network Mask**— Subnet mask of the destination network address.
- **Nexthop**— IP address of the next hop to the route.
- **Interface**— VLAN ID of the interface.

- **Protocol**— How this route is established.

  "Static" indicates that the route was added statically; "RIP" indicates that the route was added dynamically using the RIP protocol; "Connected" indicates that the route is connected directly.

- **AD/Metric**— Value of the administrative distance specified to the route, and the number of routing devices a packet must travel through to reach the destination.

Chapter 22

Quality of Service (QoS)

This chapter provides a brief description of the QoS feature and explains how to use the feature on the switch.

See the following sections:

For information about the ACL feature, see Chapter 20, “Access Control Lists (ACL)” on page 231.

For more information about the QoS feature, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Quality of Service (QoS)
- ❒ Quality of Service (QoS) Commands

Overview

Quality of Service (QoS) is a feature that classifies and prioritizes traffic to guarantee a certain level of performance in converged networks, which run voice and video services on data networks. QoS can give certain traffic types preferential treatment. For example, QoS is used to provide the users of IP phones the same quality of voice transmission as conventional telephone service provides. With QoS, you can ensure that voice packets have a higher priority throughout the network.

To give the different forwarding treatment to traffic, QoS assigns a priority class to packets upon entry into the network. Then, switches and routers along the path use the class information to select a certain behavior for the packet and provide appropriate QoS treatment.

Class Information

In the Layer 3 IP packet, the class information is carried in the Differentiated Services Code Point (DSCP) field. The class information can also be carried as a Class of Service (CoS) value in the Layer 2 frame. Layer 2 Inter-Switch Link (ISL) frame headers have a User field that carries a class of service (CoS) value; Layer 2 802.1Q frame headers have a Tag Control Information field that carries the CoS value.

You can use DSCP and CoS values as filtering criteria to classify incoming packets. You also can configure QoS to assign a new value to the DSCP and CoS to the packets that match the specified filtering criteria.

Priority Queue

Each egress port has eight egress queues allocated. By default, all queues on all ports are serviced in strict priority order. This means that the highest numbered priority queue, queue 7, is emptied first. When queue 7 is completely empty, the next highest priority queue, queue 6, is processed. This process is continued until you reach queue 0. For a strict priority queue to be processed, all higher priority queues must be empty.

You can configure QoS to set the packets that match the specified filtering criteria to an egress queue on a port.

Classifier Number Ranges

QoS policies are identified by classifier numbers. When you create a QoS policy, you must choose the correct classifier number based on whether you specify an IP address or MAC address as a filtering criterion. See the classifier number ranges for QoS policies in Table 10.

Table 10. Classifier Number Ranges for QoS

Filtering Criterion	Classifier Number Range
Specifying an IPv4 address	3000 - 3699

Table 10. Classifier Number Ranges for QoS

Filtering Criterion	Classifier Number Range
Specifying a MAC address	4000 - 4699
Specifying no address	3000 - 3699 and 4000 - 4699

Filtering Criteria

QoS policies identify packets using filtering criteria. The AT-FS970M web interface offers seven criteria:

- Source and destination IP addresses
- Source and destination MAC addresses
- Source and destination TCP ports
- Source and destination UDP ports
- VLAN IDs
- CoS value
- DSCP value

Actions

The action defines the response to packets that match the filtering criteria of a QoS policy. There are three actions that you can choose from using the AT-FS970M web interface:

- **Priority Queue**— This action causes a port to place all ingress packets that match the filtering criteria to the specified priority queue.
- **Mark DSCP**— This action causes a port to change the DSCP value of all ingress packets that match the filtering criteria with the specified DSCP value.
- **Mark CoS**— This action causes a port to change the CoS value of all ingress packets that match the filtering criteria with the specified CoS value.

How Ingress Packets are Selected with Filtering Criteria

A QoS policy can have more than one filtering criterion. A QoS policy that has one filtering criterion that specifies a particular source IP address, for example, selects only packets with the specified source address and applies the specified action. A QoS policy that has two filtering criteria that specify a particular VLAN ID and DSCP value, for example, selects only packets that match the specified VLAN ID *and* DSCP value.

Guidelines

Here are the QoS guidelines:

- A QoS policy can have a "Priority Queue," "Mark DSCP," or "Mark CoS" action. The priority queue action allows a port to place ingress packets that match the filtering criteria to the specified priority queue. The Mark DSCP action causes a port to change the DSCP value of all ingress packets that match the filtering criteria with the specified DSCP

value. The mark CoS action causes a port to change the CoS value of all ingress packets that match the filtering criteria with the specified CoS value.

- A port can have only one QoS policy.
- A QoS policy can be assigned to more than one port.
- QoS classifies ingress packets, but does not process egress packets. As a result, you must apply QoS policies to the ingress ports of the designated traffic flows.
- QoS policies for static port trunks or LACP trunks must be assigned to the individual ports of the trunks.
- A QoS policy can have multiple filtering criteria. For example, a QoS policy may classify traffic based on a source IP address, a VLAN ID, and a DSCP value.
- A QoS policy that has more than one filtering criterion selects traffic that matches all specified filtering criteria.

Creating a QoS Policy

To create a QoS policy, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 103.

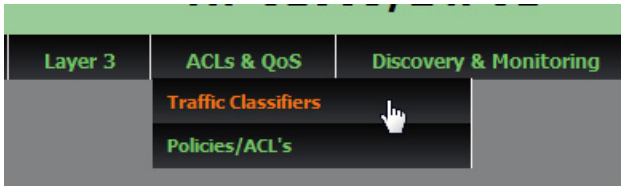


Figure 103. ACLs and QoS Tab

2. From the **ACLs & QoS** tab drop-down menu, select **Traffic Classifiers**.

   The Traffic Classifiers page is displayed. See Figure 104.

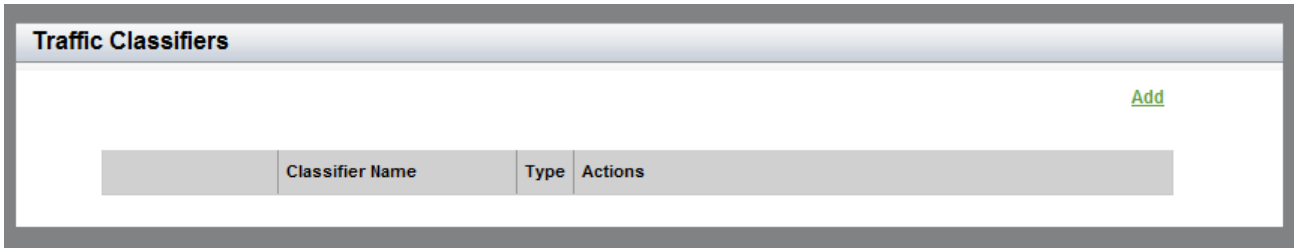


Figure 104. Traffic Classifiers Page

3. Click Add on the right above the table.

   The Traffic Classification page is displayed. See Figure 105 on page 256.

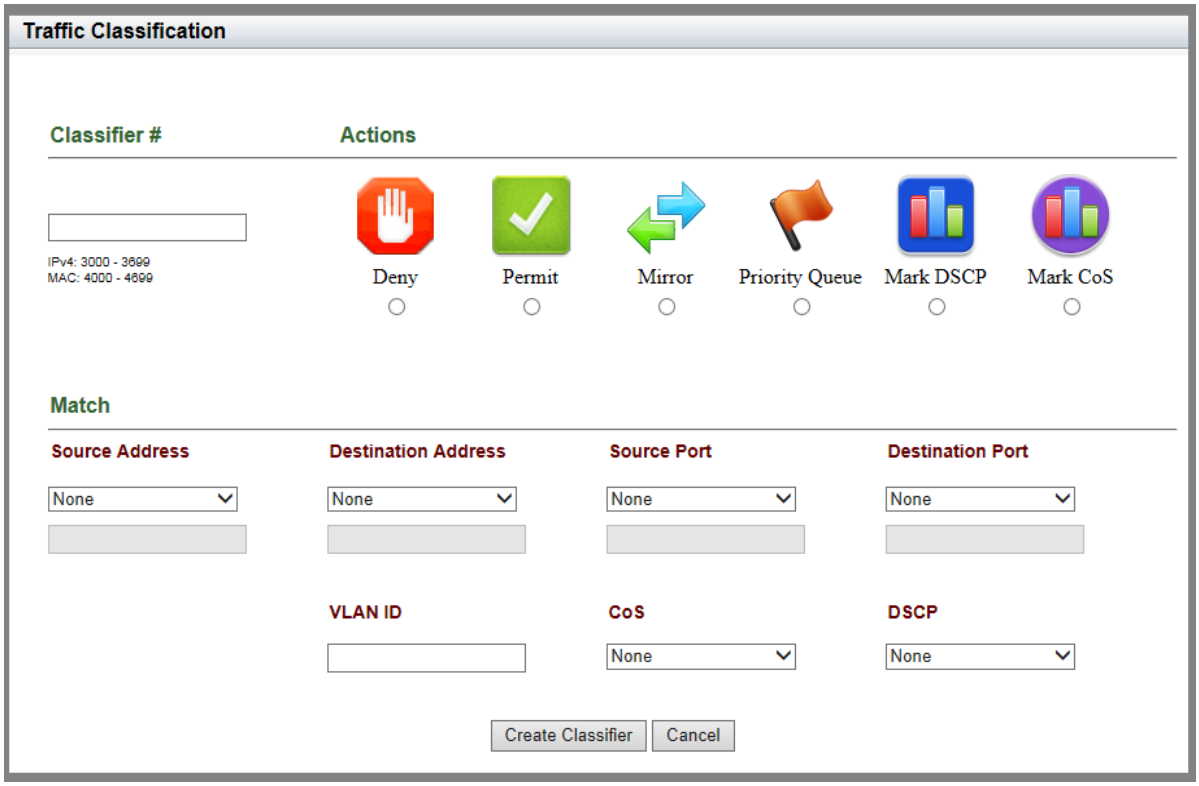


Figure 105. Traffic Classification Page

4. Enter and select the following fields as needed:

   - **Classifier #**— Enter a classifier number to identify a QoS policy. Choose a classifier number according to the following conditions:

     When specifying an IPv4 address as a filtering criterion: Choose from 3000 to 3699.

     When specifying a MAC Address as a filtering criterion: Choose from 4000 to 4699.

     When not specifying an address as a filtering criterion: Choose from 3000 to 3699 or from 4000 to 4699.

- **Actions**— Click a radio button to select an action from the following options:

  Priority Queue: Instructs ports to place all ingress packets that match the filtering criteria into a specified priority queue.

  When you select Priority Queue, a text box appears below the action icons as shown in Figure 106. Enter a priority queue number. Choose from 0 to 7.

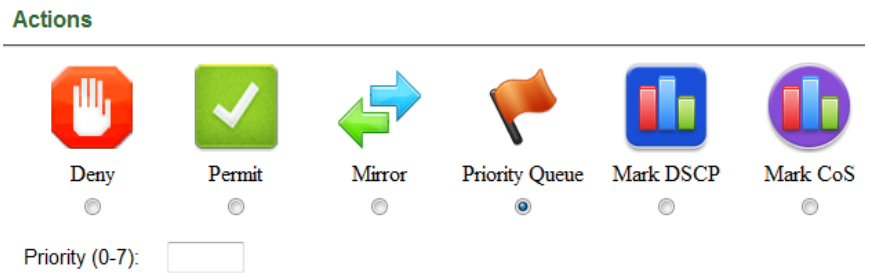


Figure 106. Text Box for Priority Queue

  Mark DSCP: Instructs ports to set the DSCP value in all ingress packets that match the filtering criteria with a specified DSCP value.

  When you select Mark DSCP, a text box appears below the action icons as shown in Figure 107. Enter a DSCP value. Choose from 0 to 63.

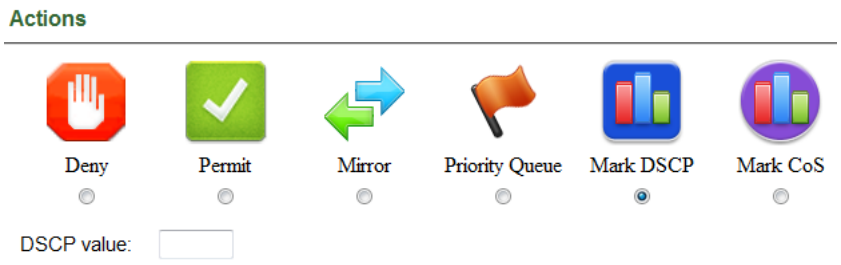


Figure 107. Text Box for DSCP

  Mark CoS: Instructs ports to set the CoS value in all ingress packets that match the filtering criteria with a specified CoS value.

  When you select Mark CoS, a text box appears below the action icons shown in Figure 108 on page 258. Enter a CoS value. Choose from 0 to 7.

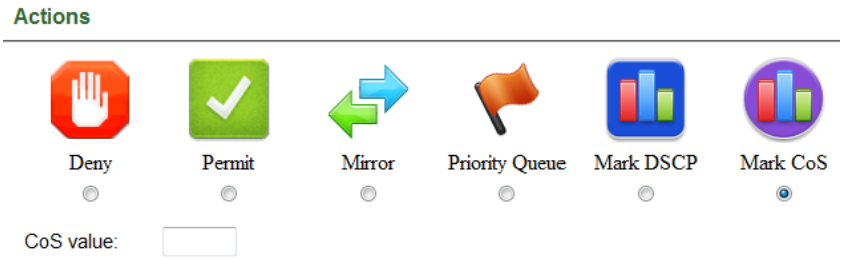


Figure 108. Text Box for CoS

Note
The action options of Deny, Permit, and Mirror are for the Access Control List (ACL) feature. For information about creating an ACL, see “Creating an ACL” on page 235.

Match

The following parameters are under the “Match” heading on the Traffic Classification Page.

Note
You can specify one or more match criteria to create a QoS policy.

- **Source Address**— Specify a source address to match ingress packets as needed. Enter one of the following:

  The keyword “any”: Matches all packets on the source address.

  IPv4 Address and mask: Enter an IPv4 source address followed by a slash (/) and a mask if you are creating an IPv4 ACL.

  MAC Address and mask: Enter a MAC source address followed by a slash (/) and a mask if you are creating a MAC ACL. The wildcard mask for MAC addresses must be either “0” (zero) or “F” to indicate the parts of MAC address to filter. “F” means anything; “0” (zero) means it has to match.

- **Destination Address**— Specify a destination address to match ingress packets as needed. Enter one of the following:

  The keyword “any”: Matches all packets on the destination address.

  IPv4 Address and mask: Enter an IPv4 source address followed by a slash (/) and a mask if you are creating an IPv4 ACL.

MAC Address and mask: Enter a MAC source address followed by a slash (/) and a mask if you are creating a MAC ACL. The wildcard mask for MAC addresses must be either "0" (zero) or "F" to indicate the parts of MAC address to filter. "F" means anything; "0" (zero) means it has to match.

- **Source Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed.
- **Destination Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed.
- **VLAN ID**— Enter a VLAN ID. Use this field if you want the QoS policy to filter tagged packets.
- **CoS**— Select a CoS value from the pull-down menu as needed. Choose from 0 to 7.
- **DSCP**— Select a DSCP value from the pull-down menu as needed. Choose from 0 to 63.

5. Click **Create Classifier**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a QoS Policy to Ports

Before assigning QoS policies to ports, QoS policies must be available on the switch. For how to create a QoS policy, see “Creating a QoS Policy” on page 255.

To assign a QoS policy to ports, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 103 on page 255.

2. From the **ACLs & QoS** tab drop-down menu, select **Policies/ACLs**.

   The Policies/ACLs page is displayed. See Figure 109.

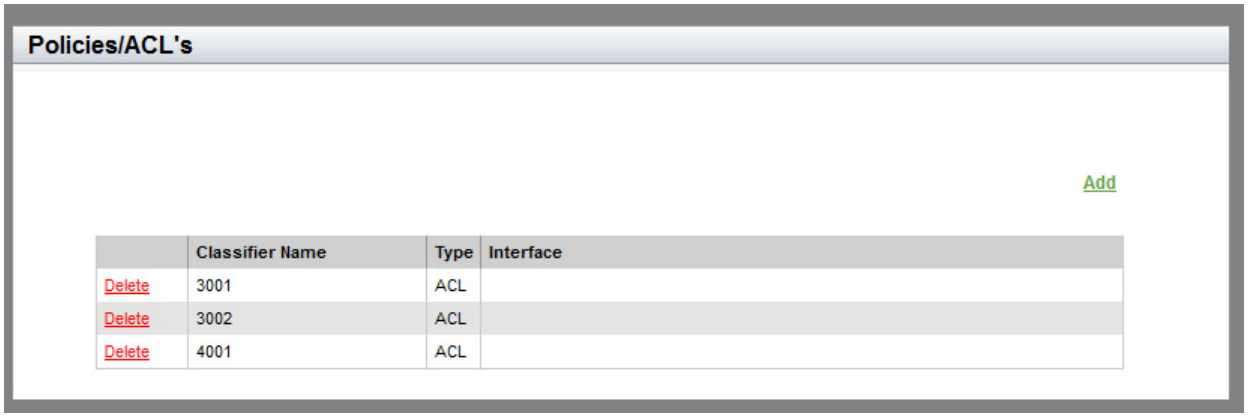


Figure 109. Policies/ACLs Page

3. Click Add on the right above the table.

   The Traffic Classifiers page is displayed. See Figure 110 on page 261.

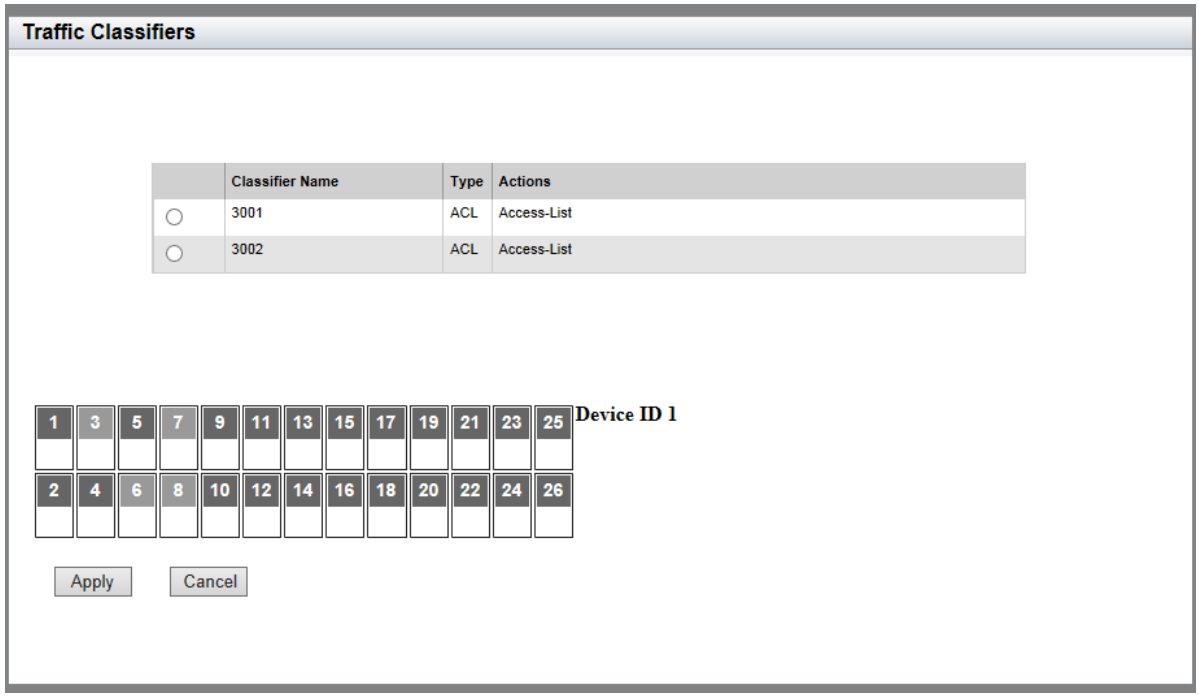


Figure 110. Traffic Classifier Page

4. Click a radio button to select a QoS policy.
5. Check one or multiple checkboxes to select ports to apply the QoS policy.
6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Displaying a List of QoS Policies

To display a list of QoS policies, do the following:

1. Hover the cursor over the **ACLs & QoS** tab.

   The **ACLs & QoS** tab is displayed. See Figure 103 on page 255.

2. From the **ACLs & QoS** tab drop-down menu, select **Traffic Classifiers**.

   The Traffic Classifiers page is displayed. See Figure 111.

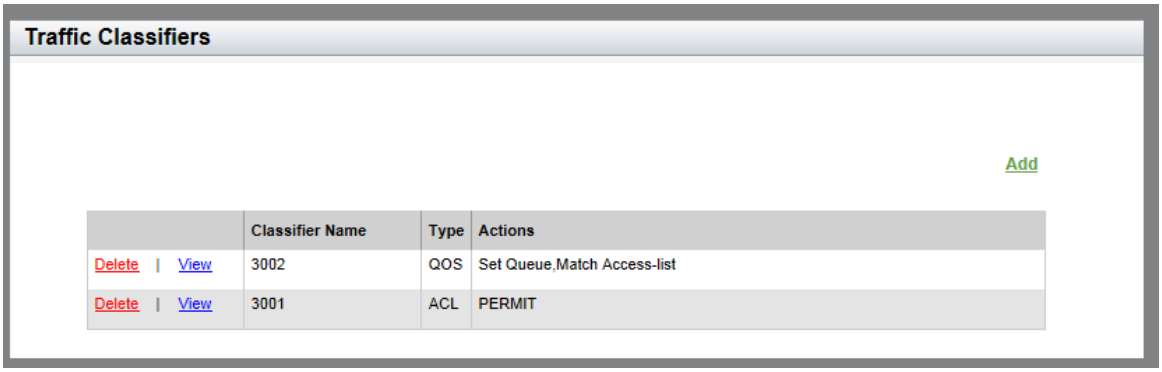


Figure 111. Traffic Classifiers Page

3. The following fields are displayed:

   - **Classifier Number**— Indicates an ACL or QoS classifier number.
   - **Type**— Indicates either ACL or QoS.
   - **Actions**— Lists actions specified to the classifier.

Note
This list includes ACLs as well as QoS policies.

Chapter 23

Setting Dynamic Routes Using RIP

The chapter provides a brief description of the RIP feature and explains how to display the RIP settings, enable RIP on a VLAN interface, change the RIP settings, delete a VLAN interface, and display RIP statistics. See the following sections:

For more information about RIP, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Routing Information Protocol (RIP)
- ❒ Routing Information Protocol (RIP) Commands

Overview

To make remote networks communicate, you must add either static routes, dynamic routes, or both. The AT-FS970M Series Management Software supports RIP as the routing protocol to add dynamic routes. By enabling RIP, the switch can learn about remote networks and add the routing information to its routing table dynamically. For information about static routes, refer to Chapter 21, “Setting Static Routes” on page 243.

Enabling RIP

Here are guidelines for enabling RIP:

- A VLAN interface must have an IP address assigned before RIP is enabled on the interface.
- To make a switch access remote networks, you must configure RIP on a VLAN interface or network that is connected to another Layer 3 device and remote networks that you want the switch to access.
- Authentication is supported only in RIP Version 2.

Note
To display the routing table that includes both dynamic routes and static routes, see “Displaying the Routing Table” on page 248.

Displaying the RIP Configuration

To check how the RIP is configured on the switch, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 112.

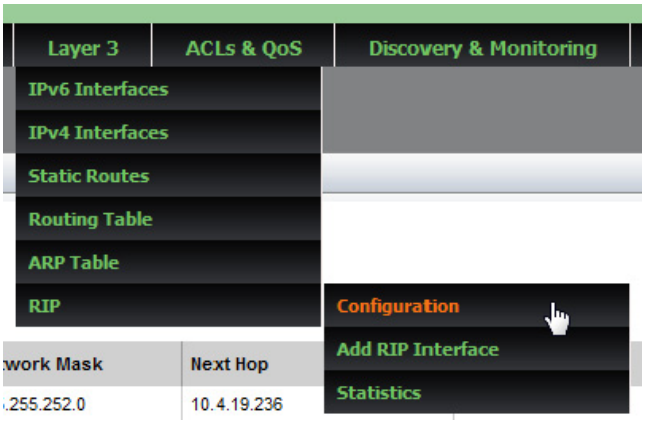


Figure 112. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, hover the cursor over **RIP**, move the cursor to the right, and select **Configuration** from the RIP drop-down menu.

   The RIP configuration page is displayed. See Figure 113.

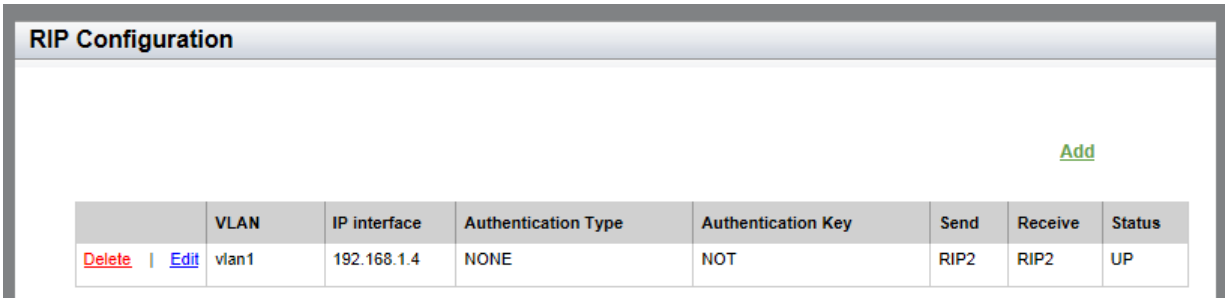


Figure 113. RIP Configuration Page

The following fields are displayed:

- **VLAN**— ID number of the VLAN. This VLAN interface receives and sends RIP packets, and the network that the VLAN belongs to is advertised through RIP.
- **IP Interface**— IP address that the VLAN interface is assigned to.

- **Authentication Type**— Authentication mode for the VLAN interface.
- **Authentication Key**— Authentication password that the VLAN interface uses to authenticate the RIP packets
- **Send**— RIP version number of the packets that the VLAN interface is specified to send.
- **Receive**— RIP version number of the packets that the VLAN interface is specified to receive.
- **Status**— Status of the VLAN interface.

Enabling RIP on a VLAN Interface

To enable RIP and connect remote networks dynamically, you must enable RIP on VLAN interfaces. When RIP is enabled on a VLAN interface, the VLAN interface sends and receives RIP packets, and the network where the VLAN belongs is advertised through RIP.

To enable RIP on a VLAN interface, you must add the VLAN to the RIP routing process by performing the following procedure:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 114.

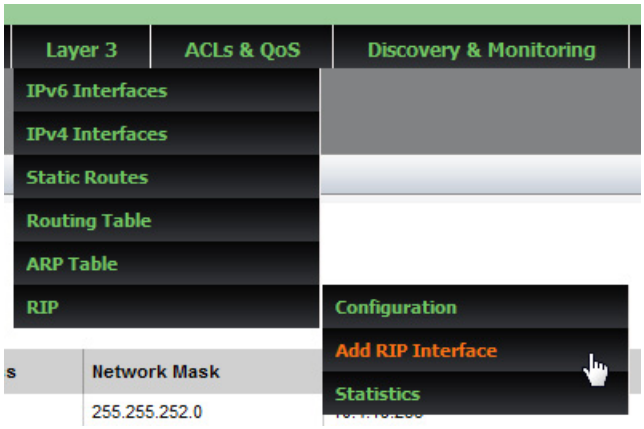


Figure 114. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, hover the cursor over **RIP**, move the cursor to the right, and select **Add RIP Interface** from the RIP drop-down menu.

   The RIP Interface page is displayed. See Figure 115 on page 268.

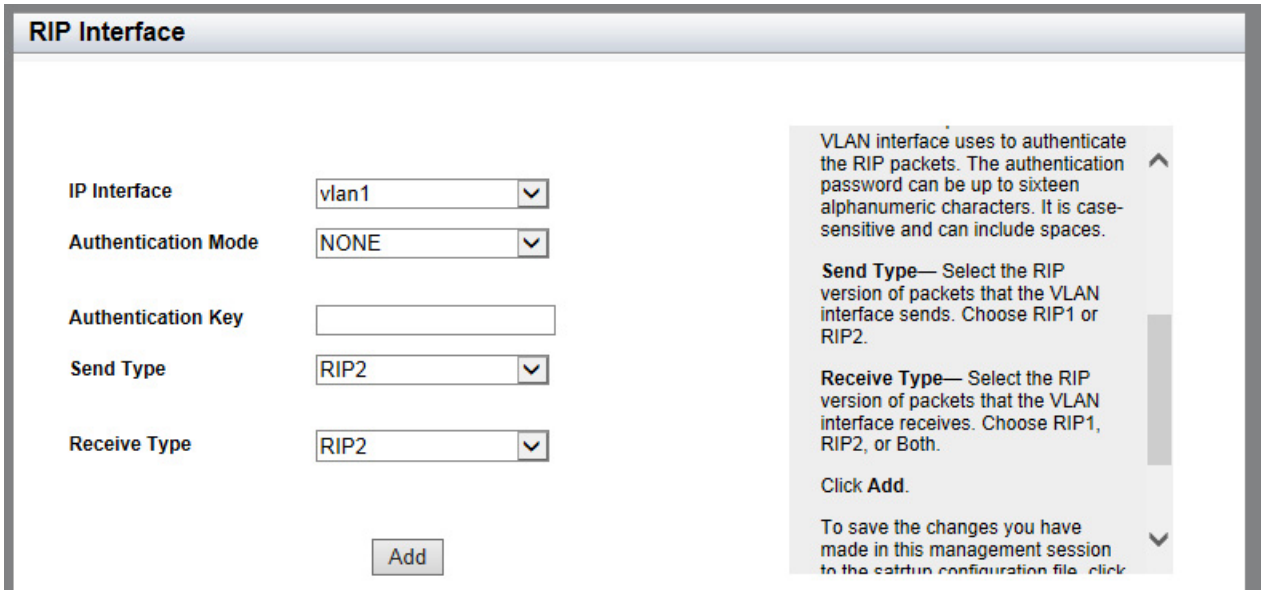


Figure 115. RIP Interface Page

3. Specify the following fields as needed:
   - **IP Interface**— Select the VLAN interface to associate with the RIP routing process. This VLAN interface receives and sends RIP packets, and the network where the VLAN belongs is advertised through RIP.
   - **Authentication Mode**— Select the authentication mode for the VLAN interface. Choose MD5, Text, or None.
   - **Authentication Key**— Enter the authentication password that the VLAN interface uses to authenticate the RIP packets. The authentication password can be up to sixteen alphanumeric characters. It is case-sensitive and can include spaces.
   - **Send Type**— Select the RIP version of packets that the VLAN interface sends. Choose RIP1, RIP2, Both, or RIP1 Compatible. RIP 1 Compatible causes version 2 RIP to broadcast, instead of multicast, the packets.
   - **Receive Type**— Select the RIP version of packets that the VLAN interface receives. Choose RIP1, RIP2, or Both.
4. Click **Add**.
5. Click **SAVE** to save your changes to the startup configuration file.

Note
There is another way to go to the RIP Interface page to enable RIP on a VLAN interface. Go to the RIP Configuration page from the RIP Configuration page shown in Figure 113 on page 265 and click **Add**. To go to the RIP Configuration page, see the procedure in "Displaying the RIP Configuration" on page 265.

Changing the RIP Settings

To change the RIP settings of the VLAN interface, perform the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 112 on page 265.

2. From the Layer 3 tab drop-down menu, hover the cursor over **RIP**, move the cursor to the right, and select **Configuration** from the RIP drop-down menu.

   The RIP Configuration page is displayed. See Figure 113 on page 265.

3. Click **Edit** next to the VLAN that you want to edit.

   The RIP Interface page is displayed. See Figure 115 on page 268.

Removing a VLAN Interface from the RIP Configuration

To remove a VLAN interface from the RIP configuration, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 112 on page 265.

2. From the Layer 3 tab drop-down menu, hover the cursor over **RIP**, move the cursor to the right, and select **Configuration** from the RIP drop-down menu.

   The RIP configuration page is displayed. See Figure 113 on page 265.

3. Click **Delete** next to the VLAN that you want to remove.

Displaying RIP Statistics

To display counters for RIP packets on the switch, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 116.

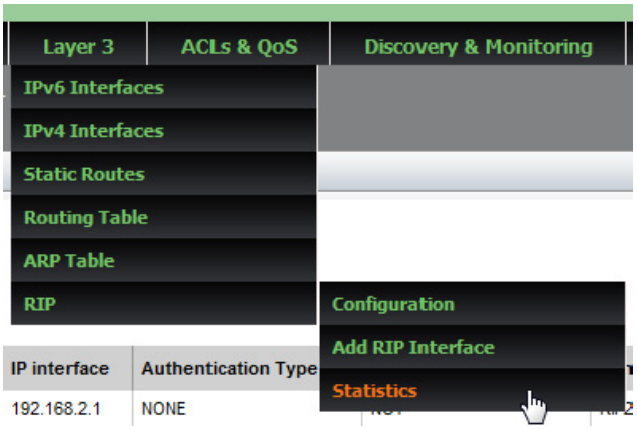


Figure 116. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, hover the cursor over **RIP**, move the cursor to the right, and select **Statistics** from the RIP drop-down menu.

   The RIP statistics page is displayed. See Figure 117.

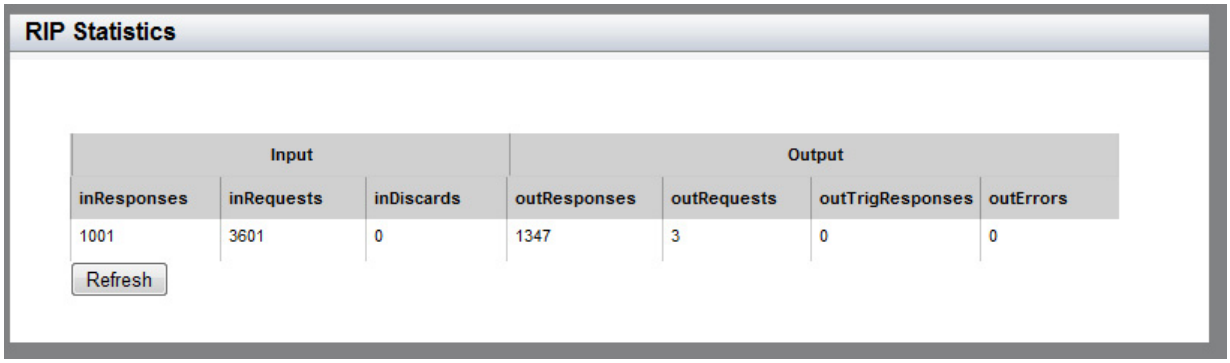


Figure 117. RIP Configuration Page

The following fields are displayed:

- **Input**— Counters displayed under these columns are for incoming RIP packets.
- **inResponses**— Number of response packets received.

- **inRequests**— Number of request packets received.
- **inDiscards**— Number of packets discarded. Packets may be discarded due to authentication failure, packet received when receive is disabled, or mismatched sequence number of a triggered acknowledgement.
- **Output**— Counters displayed under these columns are for outgoing RIP packets.
- **outResponses**— Number of response packets transmitted.
- **outRequests**— Number of request packets transmitted.
- **outTrigResponses**— Number of triggered response packets transmitted.
- **outErrors**— Number of packets with errors.

Reloading RIP Statistics

RIP statistics are constantly counting up so that the data that has been displayed in the RIP Statistics pages are not the most recent. To display the latest data possible, click on the **Refresh** button on the RIP Statistics page.

Figure 118 shows the Refresh button on the RIP Statistics page.

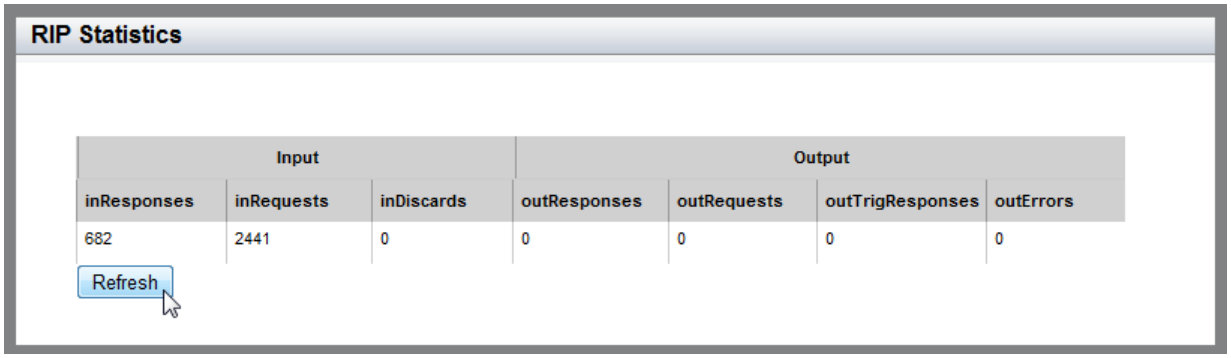


Figure 118. RIP Statistics Page with the Refresh Button

Chapter 24

Managing the ARP Table

The procedures in this chapter describe how to display the ARP table that resides on the switch, how to add static ARP entries to the table, and how to delete static ARP entries.

See the following sections:

For more information about ARP, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ Address Resolution Protocol (ARP)
- ❒ Address Resolution Protocol (ARP) Commands

Overview

The Address Resolution Protocol (ARP) is used to associate an IPv4 address with a MAC address used by network nodes including the AT-FS970M switches. ARP gathers information about mapping between an IPv4 address and a MAC address and stores them in the ARP table. When the node receives a packet from the Network layer, then the node encapsulates the packet into a frame. The node looks up the ARP cache to find out the MAC address of the destination node. The ARP table is populated dynamically; however, the AT-FS970M switches allow you to add static ARP entries, which are entered manually.

ARP Table Management Guidelines

See the following list for guidelines about managing the ARP table on the AT-FS970M switches:

- The dynamic ARP entries are time-stamped and set to time out in 300 seconds.
- The dynamic ARP entries are not deleted individually and must be deleted altogether if you want to delete them before they time out.
- The switch supports up to 512 static ARP entries.
- The static ARP entries never expire. You must remove them manually as needed. You can delete them individually.

Displaying the ARP Table

To display the ARP table, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 119.

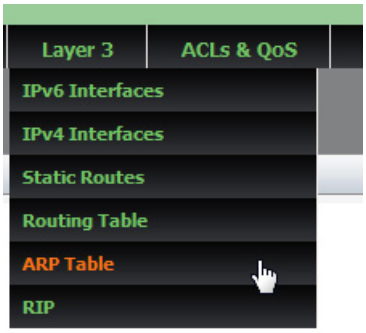


Figure 119. Layer 3 Tab

2. From the Layer 3 tab drop-down menu, select **ARP Table**.

   The ARP table is displayed. See Figure 120.

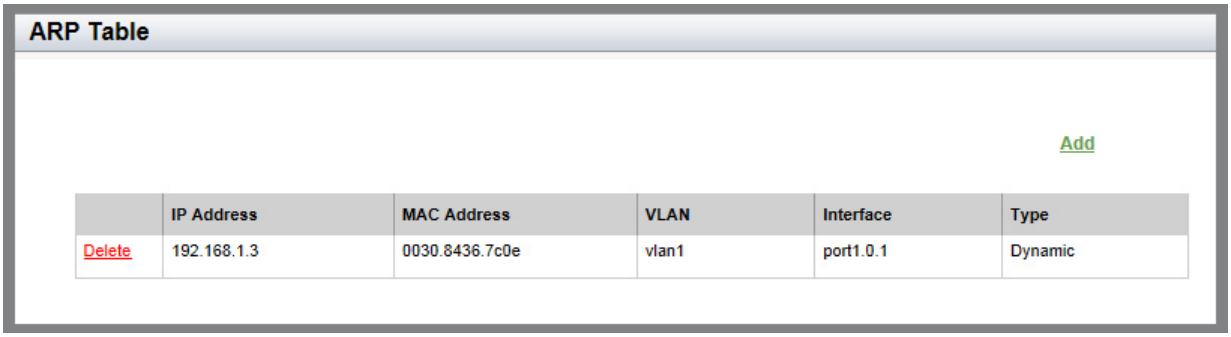


Figure 120. ARP Table Page

The following fields are displayed:

- **IP Address**— IP address of the host that is connected to the switch.
- **MAC Address**— MAC address of the host.
- **VLAN**— ID number of the VLAN where the host is a member.
- **Interface**— Port number where the host is connected.
- **Type**— Type of the ARP entry: static or dynamic.

Adding a Static ARP Entry

To add a static ARP entry, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 119 on page 277.

2. From the Layer 3 tab drop-down menu, select **ARP Table**.

   The ARP table is displayed. See Figure 120 on page 277.

3. Click **Add**.

   The Add Static ARP Page is displayed. See Figure 121.

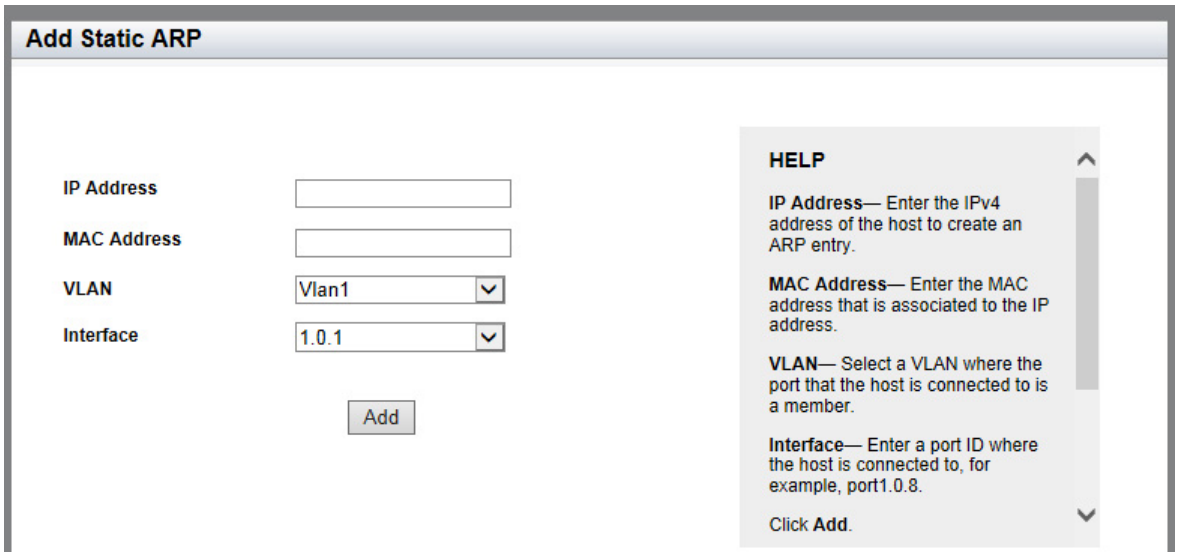


Figure 121. Add Static ARP Page

4. Enter the following settings:

   - **IP Address**— Enter the IPv4 address of the host to create an ARP entry.
   - **MAC Address**— Enter the MAC address that is associated to the IP address.
   - **VLAN**— Select a VLAN from the drop-down menu. The port is where the host is connected.
   - **Interface**— Select a port ID to where the host is connected from the drop-down menu, for example, 1.0.1.

5. Click **Add**.

6. Click **SAVE** to save your changes to the startup configuration file.

Deleting ARP Entries

To delete a static ARP entry, do the following:

1. Hover the cursor over the **Layer 3** tab.

   The Layer 3 tab is displayed. See Figure 119 on page 277.

2. From the Layer 3 tab drop-down menu, select **ARP Table**.

   The ARP table is displayed. See Figure 120 on page 277.

3. Do one of the following:

   - To clear all of the dynamic ARP entries in the ARP address table, click Clear Dynamic.
   - To delete a specific ARP entry, click Delete next to the IP address that you want to delete.

Chapter 25

LLDP and LLDP-MED

This chapter provides a brief description of the Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) features, and explains how to enable these features on the switch. See the following sections:

For more information about the LLDP and LLDP-MED features, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- LLDP and LLDP-MED
- LLDP and LLDP-MED Commands

Overview

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) allow Ethernet network devices, such as switches and routers, to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocols, and store the information that is learned about other devices. The data sent and received by LLDP and LLDP-MED are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, enabling some types of misconfiguration to be more easily detected and corrected.

LLDP is a “one hop” protocol. LLDP information can only be sent to and received by devices that are directly connected to each other or connected via a hub or repeater. Devices that are directly connected to each other are called *neighbors*. Advertised information is not forwarded on to other devices on the network. In addition, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

A single LLDPDU contains multiple TLVs. Each TLV includes a single type of information, such as its device ID, type, or management addresses, in a standardized format.

The TLVs are grouped as follows:

- Mandatory LLDP TLVs:

  Chassis ID, Port ID, and Time to Live (TTL) that are Included in an LLDPDU by default.

- Optional LLDP TLVs:

  You can select LLDP TLVs that are included in an LLDPDU. The switch sends selected TLVs along with the mandatory TLVs in an LLDPDU.

- Optional LLDP-MED TLVs:

  You can select LLDP-MED TLVs that are included in an LLDPDU. The switch sends selected TLVs along with the mandatory TLVs in an LLDPDU.

Enabling and Configuring LLDP on the Switch

To enable LLDP and set the basic LLDP configuration on the switch, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122.

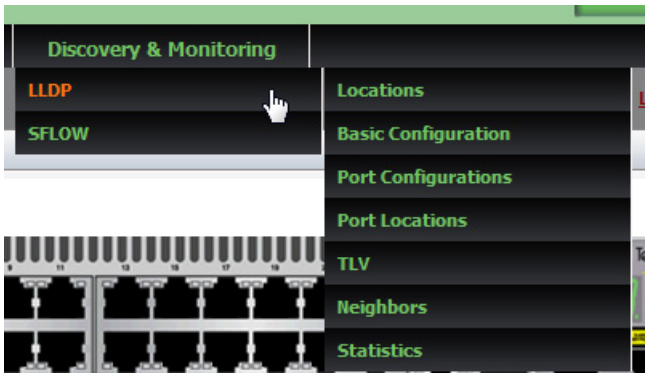


Figure 122. Discovery & Monitoring Tab

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears to the right.

3. From the LLDP tab, move the cursor to the right and select **Basic Configuration** from the drop-down menu.

   The LLDP Configuration page is displayed. See Figure 123 on page 285.

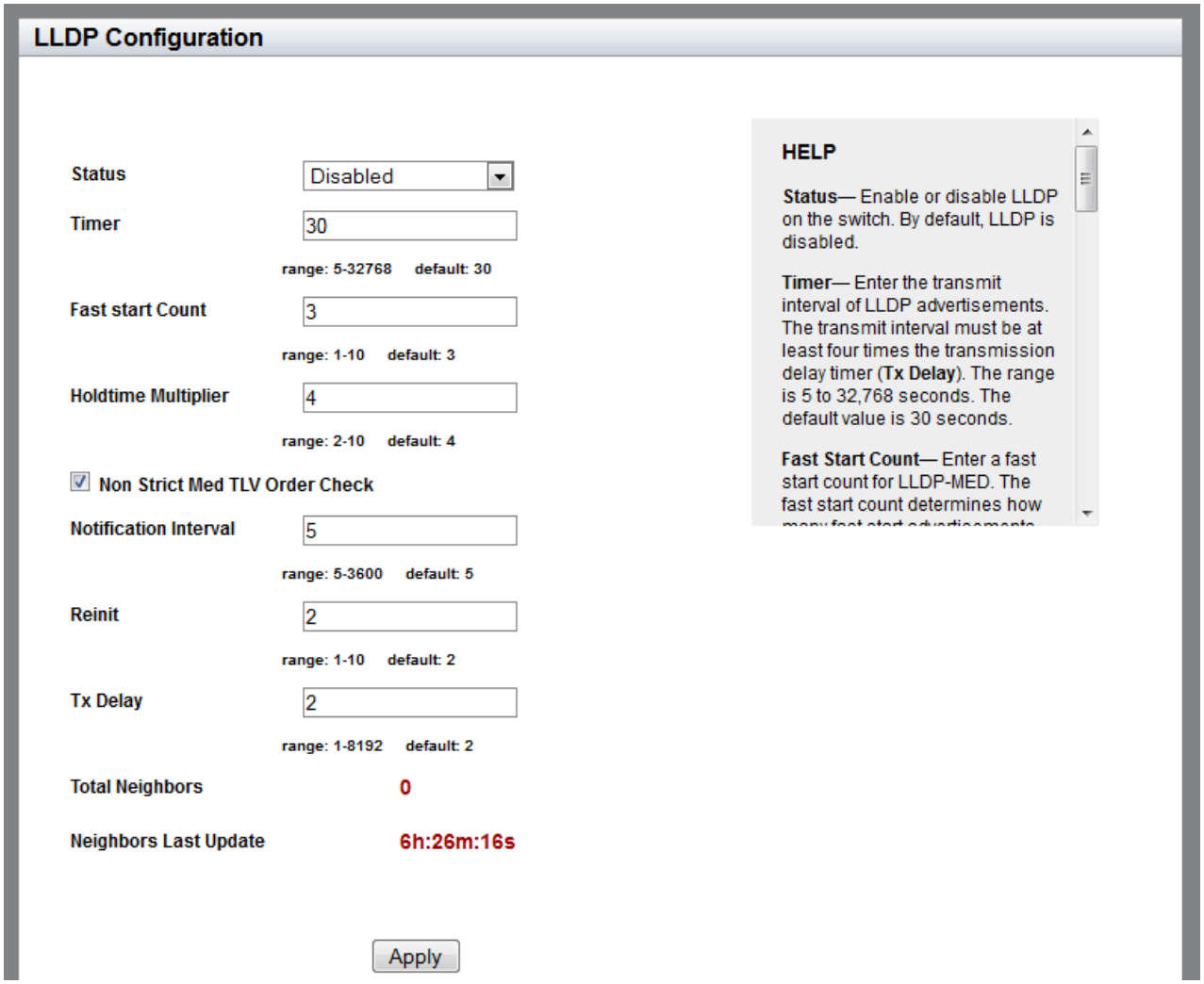


Figure 123. LLDP Configuration Page

4. Change the following fields as needed:

   - **Status**— To enable or disable LLDP on the switch, select Enabled or Disabled from the drop-down menu. By default, LLDP is disabled.
   - **Timer**— Enter the transmit interval of LLDP advertisements. The transmit interval must be at least four times the transmission delay timer (Tx Delay). The range is 5 to 32,768 seconds. The default value is 30 seconds.
   - **Fast Start Count**— Enter a fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from the port when it begins sending LLDP-MED advertisements, for instance when it detects a new LLDP-MED capable device. The range is 1 to 10. The default value is 3.

- **Holdtime Multiplier**— Enter a holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors. The range is 2 to 10. The default value is 4.
- **Non Strict Med TLV Order Check**— Check the checkbox to set the switch to accept LLDP-MED advertisements, even if the TLVs are not in the standard order, as specified in ANSI/TIA-1057. This configuration is useful if the switch is connected to devices that send LLDP-MED advertisements in which the TLVs are not in the standard order. By default, this checkbox is not selected.
- **Notification Interval**— Enter a notification interval. This is the minimum interval between LLDP SNMP notifications (traps). The range is 5 to 3,600 seconds. The default value is 5.
- **Reinit**— Enter a reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is 1 to 10 seconds. The default value is 2.
- **Tx Delay**— Enter a transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information. The range is 1 to 8192 seconds. The default value is 2.
- **Total Neighbors**— Indicates the number of LLDP neighbors the switch has discovered on all its ports.
- **Neighbors Last Update**— Indicates the time since the LLDP neighbor table was last updated.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Disabling LLDP on the Switch

To disable the LLDP feature on a switch, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears to the right.

3. From the LLDP tab, move the cursor to the right and select **Basic Configuration** from the drop-down menu.

   The LLDP Configuration page is displayed. See Figure 123 on page 285.

4. Use the pull-down menu next to the **Status** field to select "Disabled."

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Configuring LLDP on a Port

To assign LLDP to a port, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then select **Port Configurations** on the right.

   The LLDP Port Config page is displayed. See Figure 124.

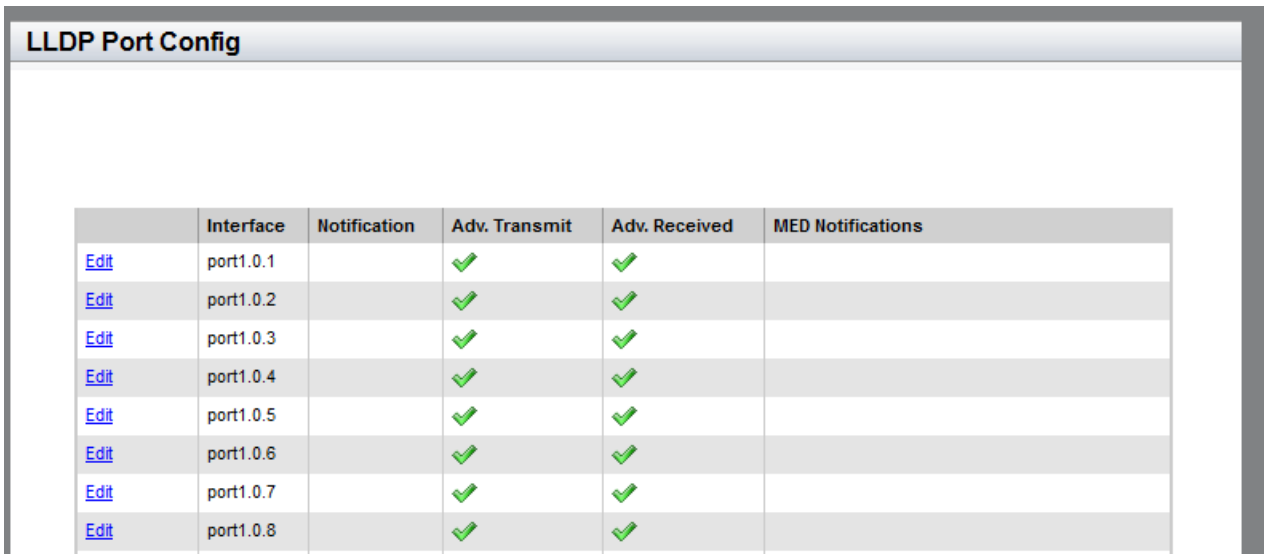


Figure 124. LLDP Port Config Page

3. Select **Edit** next to the port that you want to modify.

   The Modify LLDP Port Configuration page is displayed. See Figure 125 on page 289.

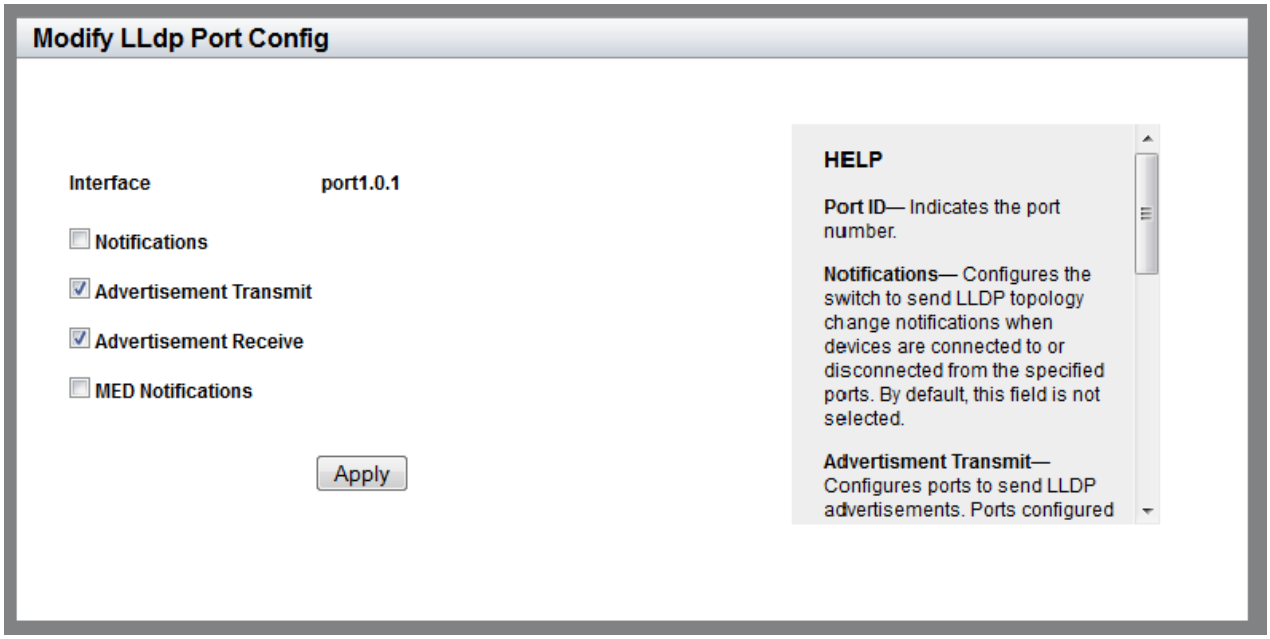


Figure 125. Modify LLDP Port Configuration Page

4. Change the settings as needed:
   - **Interface**— Indicates the port ID.
   - **Notifications**— Check the checkbox to activate the switch to send LLDP-MED topology change notifications when a device is connected to, or disconnected from, the port. By default, this field is not selected.
   - **Advertisement Transmit**— Check the checkbox to activate the port to send LLDP advertisements. A port configured to transmit LLDP advertisements sends the mandatory TLVs and any optional LLDP TLVs they have been specified to send. By default, this field is selected.
   - **Advertisement Receive**— Check the checkbox to activate the port to accept LLDP advertisements. A port configured to receive LLDP advertisements accepts all advertisements from their neighbors. By default, this field is selected.
   - **Med Notifications**— Check the checkbox to activate the switch to send LLDP-MED topology change notifications when a device is connected to, or disconnected from, the port. By default, this field is not selected.
5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Selecting LLDP TLVs on a Port

To enable LLDP TLV, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP.**

   The LLDP tab is displayed.

3. From the LLDP tab, hover over **TLV**.

   The LLDP TLV tab is displayed in Figure 126.

Figure 126. LLDP TLV Tab

4. Move your cursor to the right and select **TLV** again.

   The LLDP TLV page is displayed. See Figure 127 on page 291.

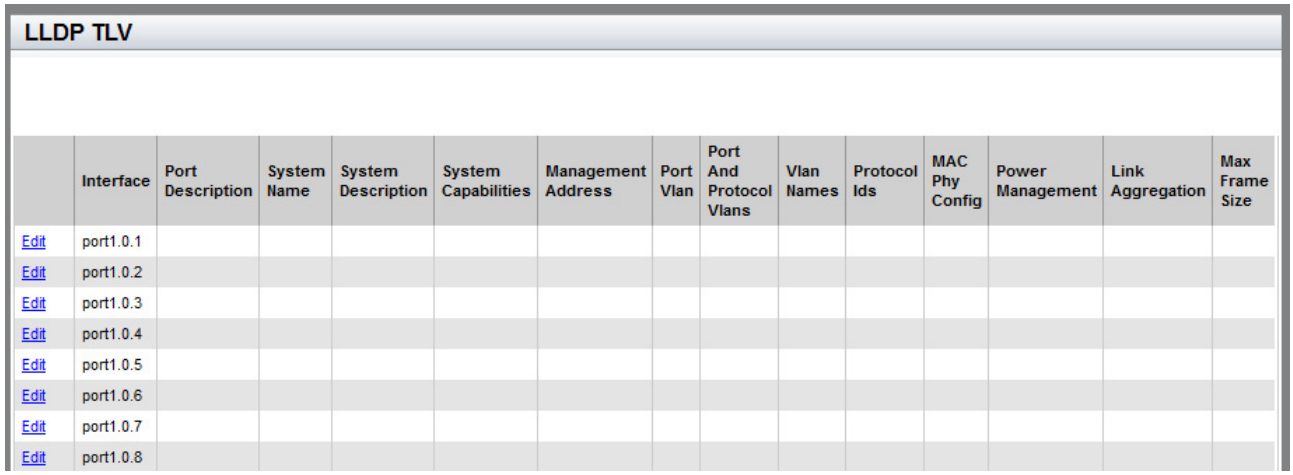


Figure 127. LLDP TLV Page

5. Click **Edit** next to the port that you want to modify.

   The Modify LLDP TLV page is displayed. See Figure 128 on page 292.

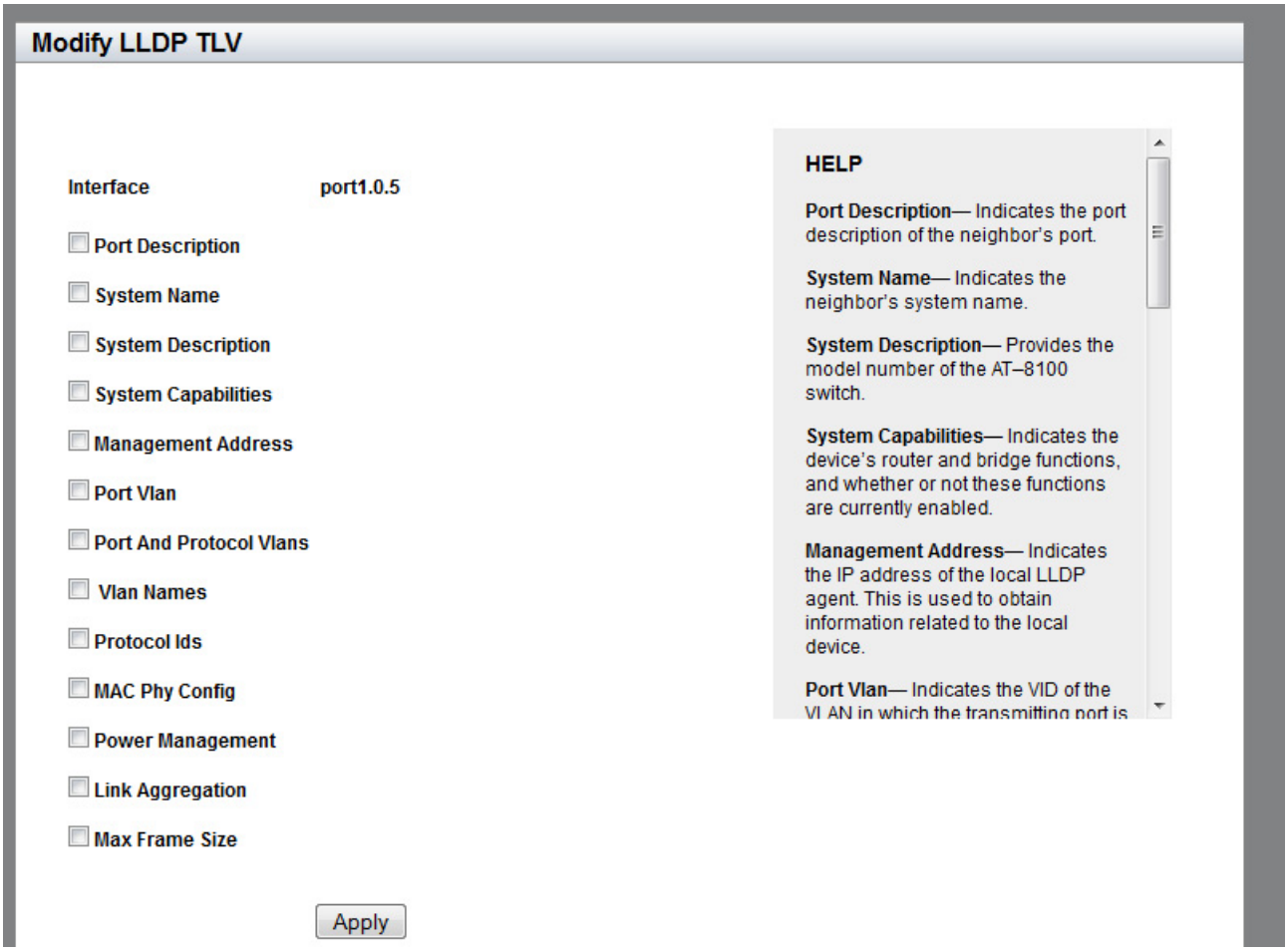


Figure 128. Modify LLDP TLV Page

6. Change the settings as needed:

   - **Interface**— Indicates the port ID.
   - **Port Description**— Check the checkbox to select the port description to be included in LLDPDUs.
   - **System Name**— Check the checkbox to select the system name to be included in LLDPDUs.
   - **System Description**— Check the checkbox to select the model number of the AT-FS970M switch to be included in LLDPDUs.
   - **System Capabilities**— Check the checkbox to include the device's capabilities, such as router or bridge, and whether or not these functions are currently enabled in LLDPDUs.

- **Management Address**— Check the checkbox to select the IP address of the local LLDP agent to be included in LLDPDUs.
- **Port VLAN**— Check the checkbox to select the VID of the untagged VLAN in which the transmitting port is a member to be included in LLDPDUs.
- **Port and Protocol VLANs**— Check the checkbox to select whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers to be included in LLDPDUs.
- **VLAN Names**— Check the checkbox to select a list of the names of the VLANs in which the transmitting port is either an untagged or tagged member to be included in LLDPDUs.
- **Protocol IDs**— Check the checkbox to select a list of protocol IDs that are accessible through the port to be included in LLDPDUs. For instance:

  - 9000 (Loopback)
  - 0026424203000000 (STP, RSTP, or MSTP)
  - 888e01 (802.1x)
  - AAAA03 (EPSR)
  - 88090101 (LACP)
  - 00540000e302 (Loop protection)
  - 0800 (IPv4)
  - 0806 (ARP)
  - 86dd (IPv6)

- **MAC Phy Config**— Check the checkbox to select the physical layer information, including the link speed, duplex mode, and Auto -Negotiation setting to be included in LLDPDUs.
- **Power Management**— Check the checkbox to select the power via MDI capabilities of the port to be included in LLDPDUs.
- **Link Aggregation**— Check the checkbox to include whether the port is capable of link aggregation and, if so, whether it is currently a member of an aggregator in LLDPDUs.
- **Max Frame Size**— Check the checkbox to include the maximum supported frame size of the port in LLDPDUs. This field is not adjustable on the switch.

7. Click **Apply**.
8. Click **SAVE** to save your changes to the startup configuration file.

Setting a Location Entry for the LLDP-MED Location TLV

You can define location information about a network device as an LLDP-MED TLV and include the TLV in an LLDPDU, which the switch sends to its neighbors. Unlike some of the other LLDP-MED LLDP TLVs, such as capabilities and network policy TLVs, which have pre-set values, a location TLV must be specified before a port sends it to the neighbors.

To include location information in LLDPDUs, you must create a location entry with the relevant location information, apply it to one or more ports on the switch, and then specify a port to include the location TLV-MED in LLDPDUs.

The procedures in this section allow you to create LLDP-MED Civic, Coordinate, and ELIN location entries. See the following:

- ❒ “Creating a Civic Location Entry” on page 294
- ❒ “Creating a Coordinate Location” on page 298
- ❒ “Creating an Emergency Location Identification Number (ELIN) Location” on page 300

Note
To apply a location entry to a port, see “Assigning LLDP Locations to a Port” on page 302. To specify a port to include a location LLPD-MED TLV, see “Selecting LLDP-MED TLVs on a Port” on page 304.

Creating a Civic Location Entry

To create an LLDP Civic Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

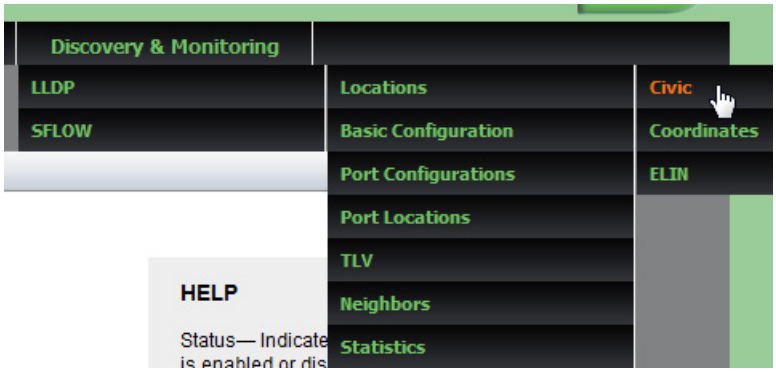


Figure 129. Locations Tab

4. From the Locations tab drop-down menu, move the cursor to the right and select **Civic**.

The LLDP Civic Location page is displayed. See Figure 130.

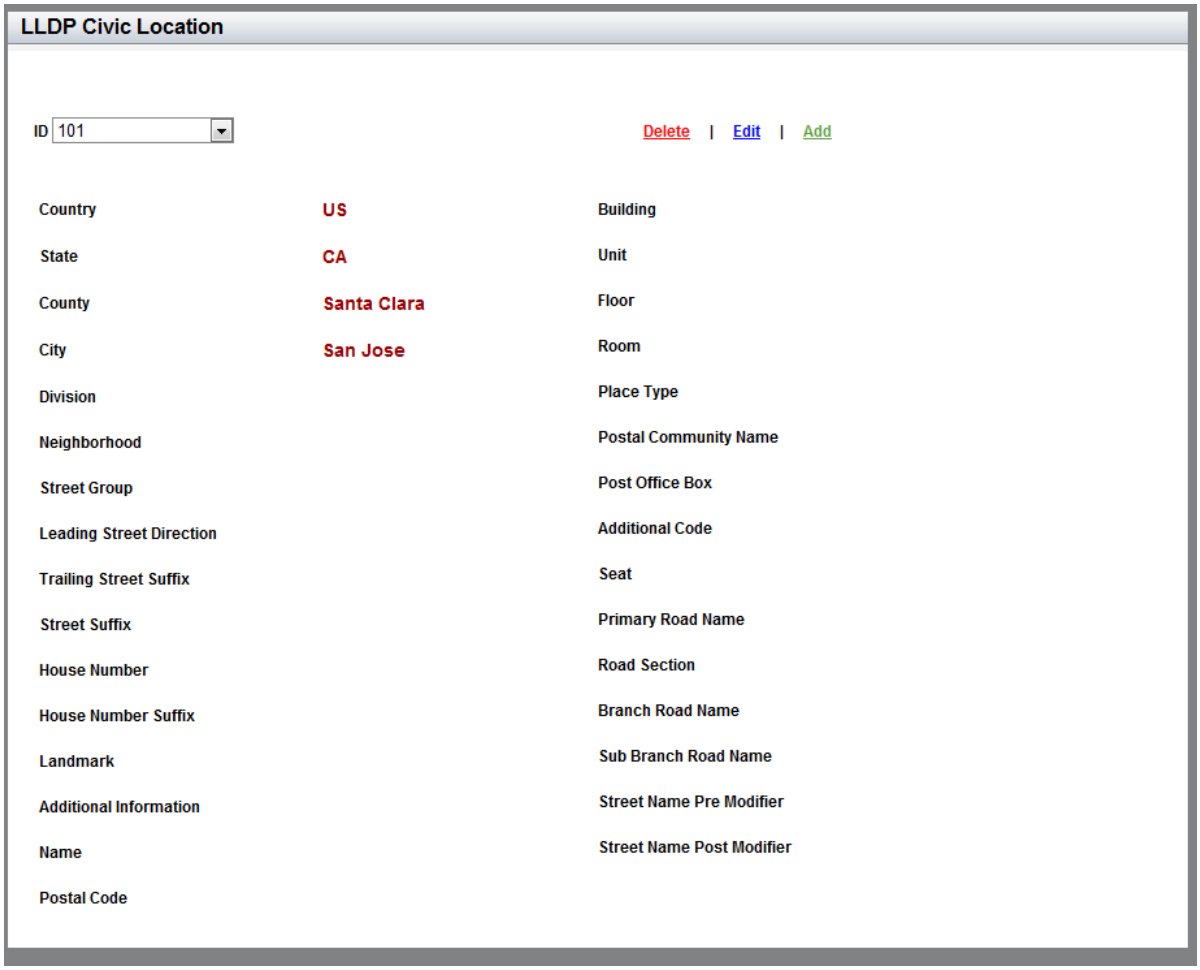


Figure 130. LLDP Civic Location Page

5. Click **Add**.

   The Add LLDP Civic Location Page is displayed. See Figure 131.

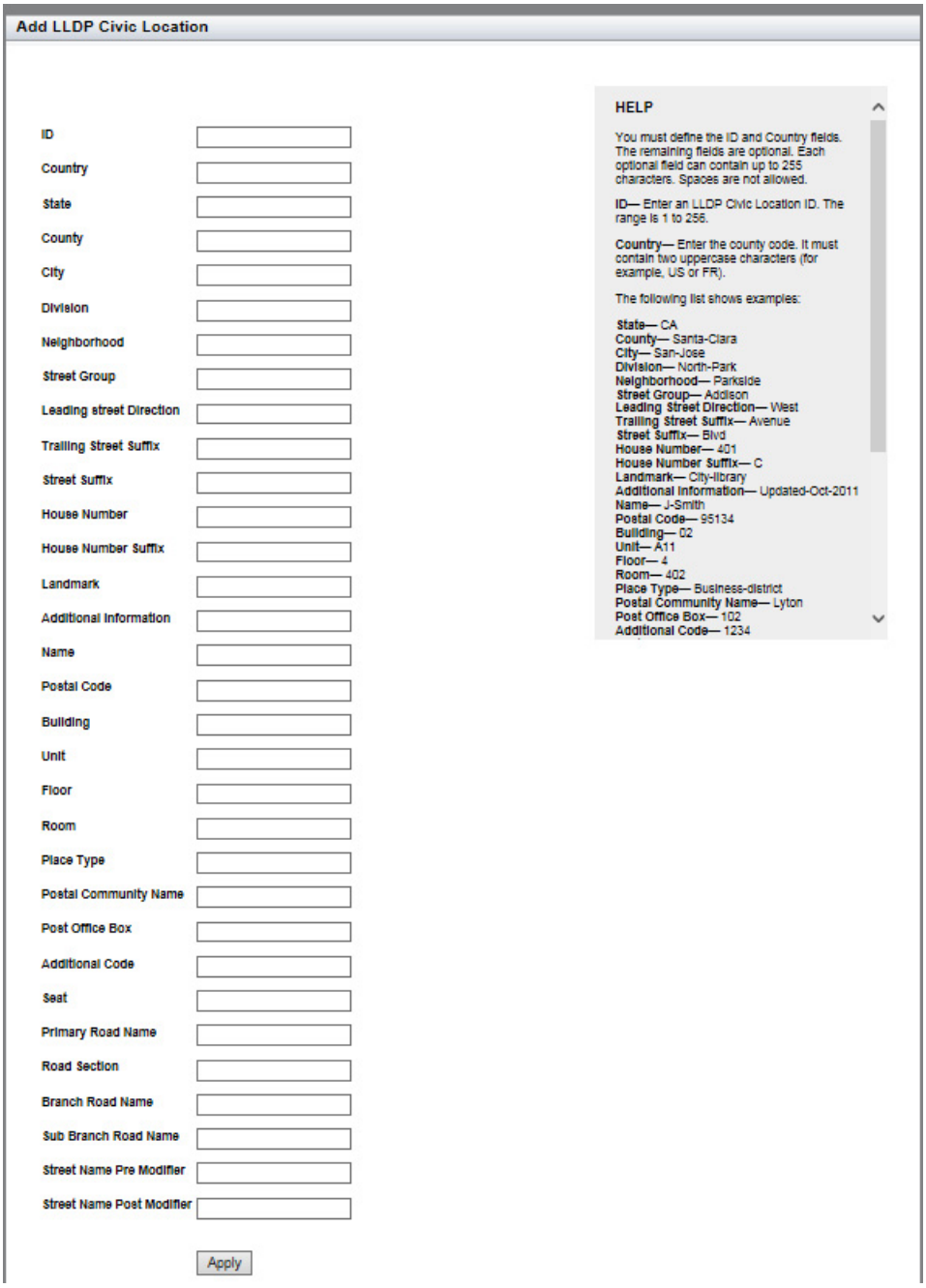


Figure 131. LLDP Civic Location Page— Add

6. Enter the **ID** and **Country** fields:

- **ID**— Enter an LLDP Civic Location ID. The range is 1 to 256. (This range is separate from the ranges for coordinate and ELIN entries.)
- **Country**— Enter the county code. It must contain two uppercase characters (for example, US or FR).

Note
You must define the ID and Country fields. The remaining fields are optional.

7. Enter the ID and the following fields as needed:

Note
Each field can contain up to 255 characters. Spaces are not allowed.

The following list shows examples:

- **Country**— USA
- **State**— CA
- **County**— Santa-Clara
- **City**— San-Jose
- **Division**— North-Park
- **Neighborhood**— Parkside
- **Street Group**— Addison
- **Leading Street Direction**— West
- **Trailing Street Suffix**— Avenue
- **Street Suffix**— Blvd
- **House Number**— 401
- **House Number Suffix**— C
- **Landmark**— City-library
- **Additional Information**— Updated-Oct-2011
- **Name**— J-Smith
- **Postal Code**— 95134
- **Building**— 02
- **Unit**— A11
- **Floor**— 4
- **Room**— 402
- **Place Type**— Business-district
- **Postal Community Name**— Lyton
- **Post Office Box**— 102

- **Additional Code**— 1234
- **Seat**— cube-411a
- **Primary Road Name**— Zanker
- **Road Section**— North
- **Branch Road Name**— State-Lane
- **Sub Branch Road Name**— Boulder-Creek-Avenue
- **Street Name Pre Modifier**— West
- **Street Name Post Modifier**— Div

8. Click **Apply**.
9. Click **SAVE** to save your changes to the startup configuration file.

Creating a Coordinate Location

To create an LLDP Coordinate Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

4. From the Locations tab drop-down menu, move the cursor to the right and select **Coordinates**.

   The LLDP Coordinate Location List page is displayed. See Figure 132.

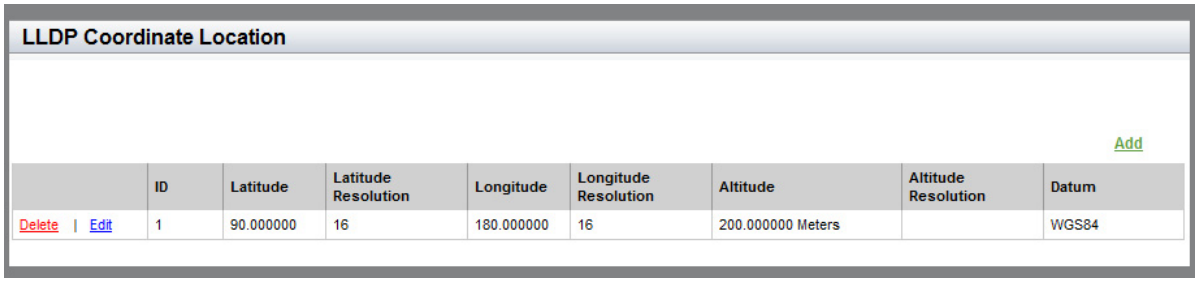


Figure 132. LLDP Coordinate Location List Page

5. From the LLDP Coordinate Location page, click Add.

The LLDP Coordinate Location page is displayed. See Figure 133.

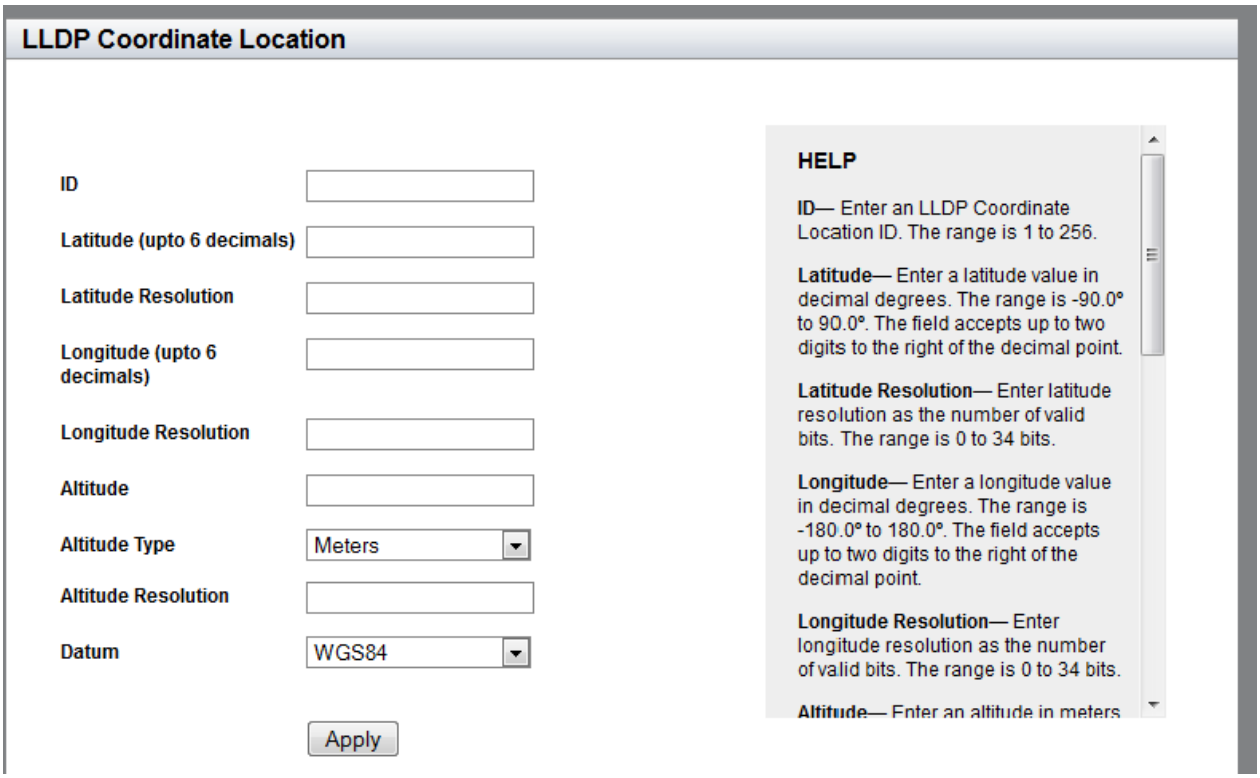


Figure 133. LLDP Coordinate Location Page— Add

6. Specify the following fields as needed:

   - **ID**— Enter an LLDP Coordinate Location ID. The range is 1 to 256. (This range is separate from the ranges for civic and ELIN entries.)
   - **Latitude**— Enter a latitude value in decimal degrees. The range is -90.0º to 90.0º. The field accepts up to two digits to the right of the decimal point.
   - **Latitude Resolution**— Enter latitude resolution as the number of valid bits. The range is 0 to 34.
   - **Longitude**— Enter a longitude value in decimal degrees. The range is -180.0º to 180.0º. The field accepts up to two digits to the right of the decimal point.
   - **Longitude Resolution**— Enter longitude resolution as the number of valid bits. The range is 0 to 34.
   - **Altitude**— Enter an altitude in meters or floors. For the altitude in meters, the range is -2097151.0 to 2097151.0 meters. The parameter accepts up to eight digits to the right of the decimal point. For altitude in the number of floors, the range is -2097151.0 to 2097151.0. Use the **Altitude Type** field to specify meters or floors.

- **Altitude Type**— Choose between meters and floors.
- **Altitude Resolution**— Enter altitude resolution as the number of valid bits. The range is 0 to 30.
- **Datum**— Select the geodetic system (or datum) of the coordinates. Choose one of the following:

  WGS84: World Geodetic System 1984

  NAD83_NAVD: North American vertical datum 1983

  NAD83_MLLW: Mean lower low water datum 1983

7. Click **Apply**.

Creating an Emergency Location Identification Number (ELIN) Location

The ELIN TLV specifies the location of a network device by its Emergency Location Identifier Number (ELIN).

To create an LLDP ELIN location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

4. From the Locations tab drop-down menu, move the cursor to the right and select **ELIN**.

   The LLDP ELIN Location List page is displayed. See Figure 134.

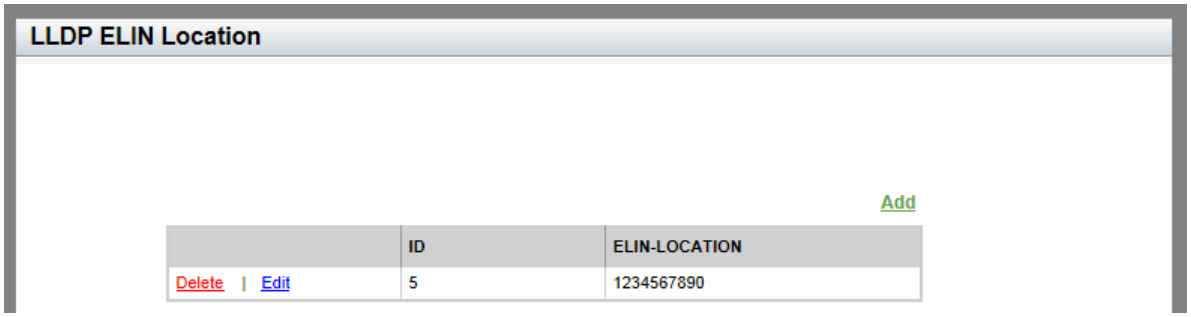


Figure 134. LLDP ELIN Location List Page

5. From the LLDP ELIN Location page, click Add.

The LLDP ELIN Location page is displayed. See Figure 135.

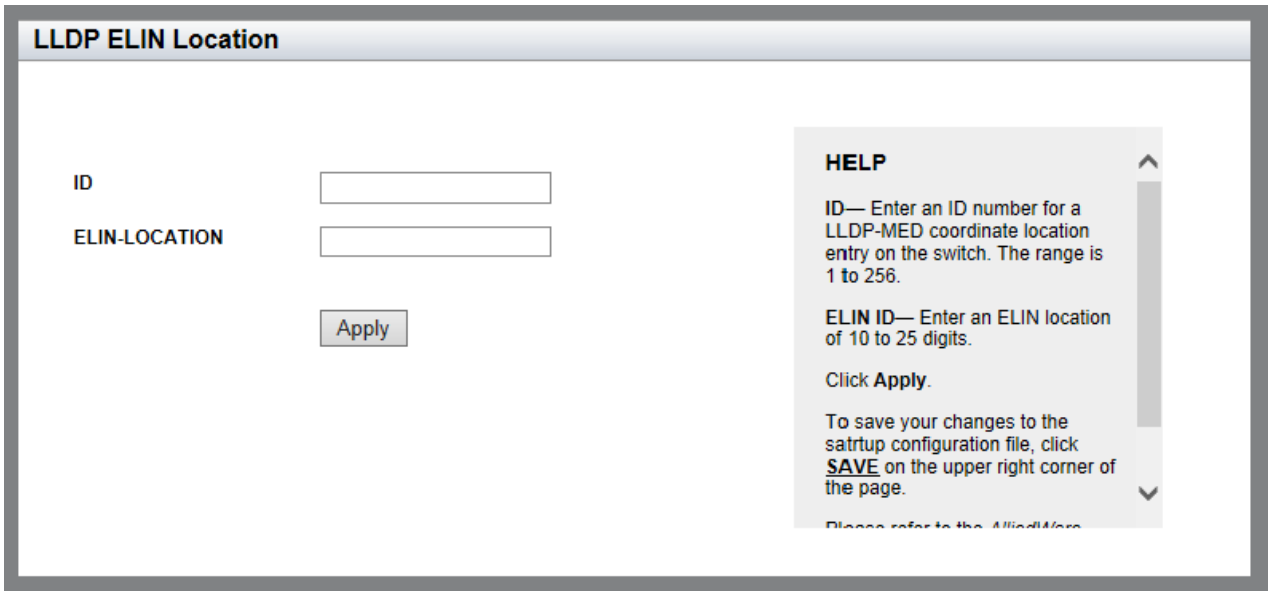


Figure 135. LLDP ELIN Location Page

6. Enter values in the following fields:
   - **ID**— Enter an ID number for an LLDP-MED coordinate location entry on the switch. The range is 1 to 256. (This range is separate from the ranges for civic and coordinate entries.)
   - **ELIN-LOCATION**— Enter an ELIN location of 10 to 25 digits.
7. Click **Apply**.
8. Click **SAVE** to save your changes to the startup configuration file.

Assigning LLDP Locations to a Port

Use a Civic, Coordinate, or ELIN location ID port location to assign to a port. You must create these location IDs *before* you assign a port location to a port. For instructions to create location IDs, see “Setting a Location Entry for the LLDP-MED Location TLV” on page 294.

To set an LLDP port location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then select **Port Locations** on the right.

   The LLDP Port Location page is displayed. See Figure 136.

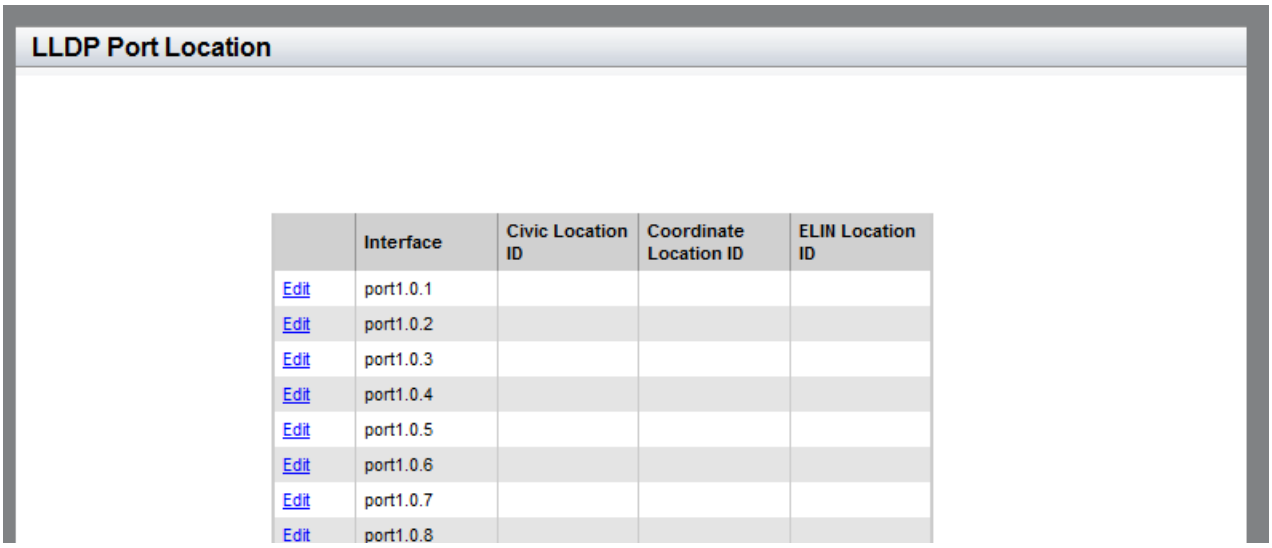


Figure 136. LLDP Port Location Page

3. Click **Edit** next to the port that you want to modify.

   The Modify LLDP Port Location page is displayed. See Figure 137 on page 303.

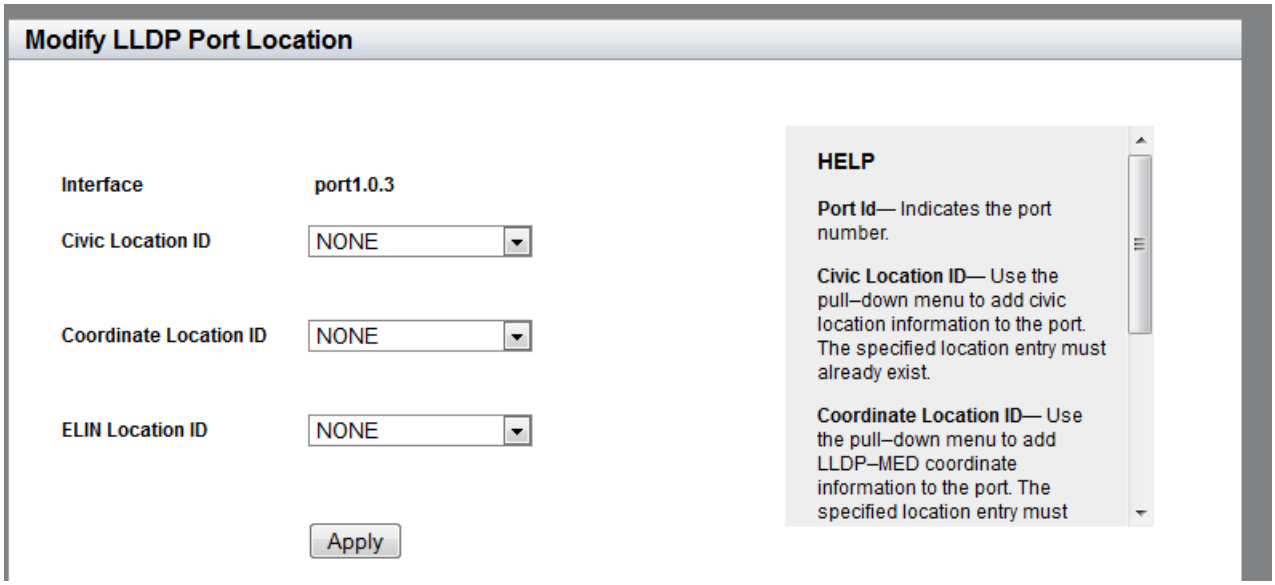


Figure 137. Modify LLDP Port Location Page

4. Select values in the fields as needed:
   - **Interface** — Indicates the port ID.
   - **Civic Location ID**— Select a Civic Location ID from the pull-down menu. By default, none is selected.
   - **Coordinate Location ID**— Select a Coordinate Location ID from the pull-down menu. By default, none is selected.
   - **ELIN Location ID**— Select an ELIN Location ID from the pull-down menu. By default, none is selected.
5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Selecting LLDP-MED TLVs on a Port

To enable LLDP-MED TLV, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then hover over **TLV**.

   The LLDP TLV tab is displayed. See Figure 126 on page 290.

3. From the LLDP TLV tab, select **TLV-MED** on the right

   The LLDP-MED TLV page is displayed. See Figure 138.

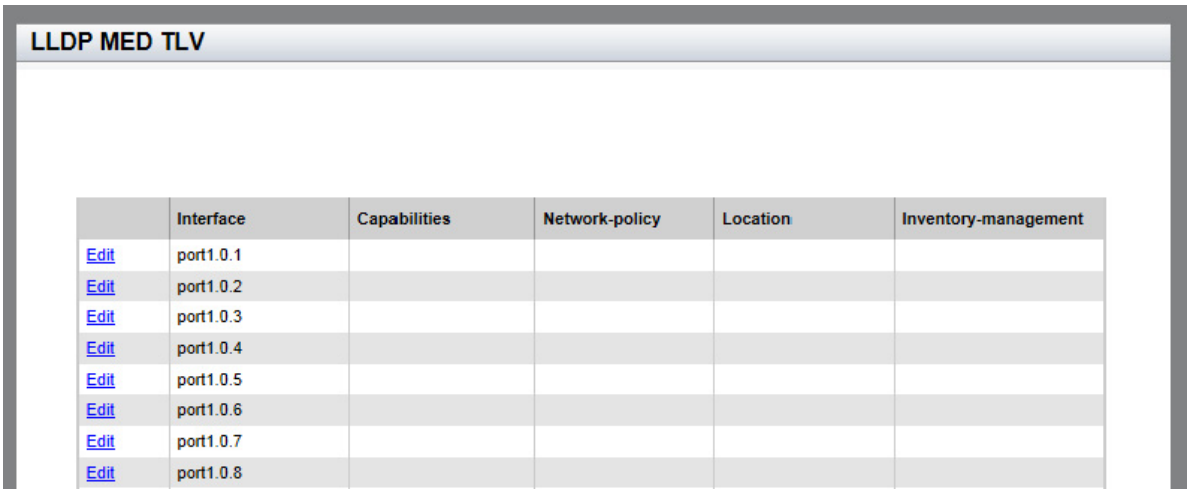


Figure 138. LLDP-MED TLV Page

4. Click **Edit** next to the port that you want to modify.

   The Modify LLDP-MED TLV page is displayed. See Figure 139 on page 305.

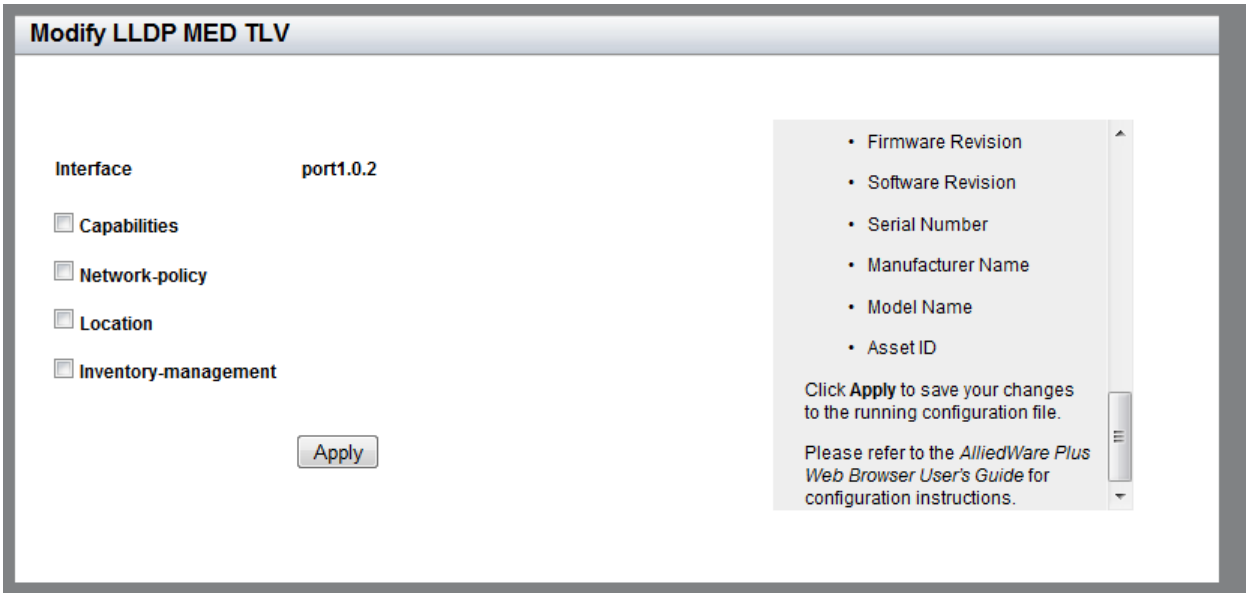


Figure 139. Modify LLDP-MED TLV Page

5. Change the fields as needed:

   - **Interface**— Indicates the port ID.
   - **Capabilities**— Check the checkbox to select the capabilities to be included in LLDPDUs.
   - **Network-policy**— Check the checkbox to select the network policy TLV to be included in LLDPDUs. The network policy TLV includes the network policy information specified on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:

     - Voice VLAN ID
     - Voice VLAN Class of Service (CoS) priority
     - Voice VLAN Diffserv Code Point (DSCP)

   - **Location**— Check the checkbox to select the location TLV to be included in LLDPDUs. The location TLV is in one or more of the following formats:

     - Civic location
     - Coordinate location
     - Emergency Location Identification Number (ELIN)

- **Inventory-management**— Check the checkbox to select the current hardware and the software information to be included in LLDPDUs. This information is identical on every port on the switch:
  - Hardware Revision
  - Firmware Revision
  - Software Revision
  - Serial Number
  - Manufacturer Name
  - Model Name
  - Asset ID

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Displaying LLDP Neighbor Information

To display LLDP Statistical information, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**, move the cursor to the right, and then select **Neighbors**.

   The LLDP Neighbors Information page is displayed. See Figure 140.

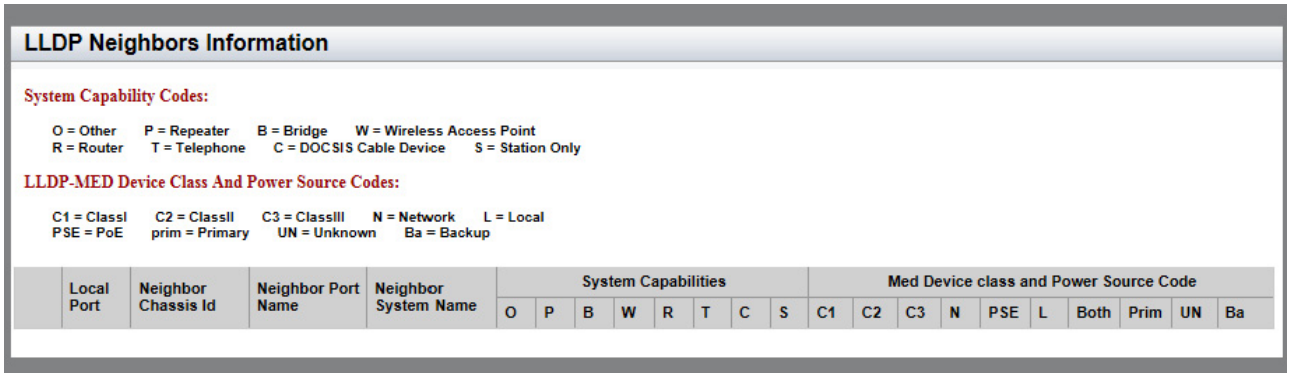


Figure 140. LLDP Neighbors Information Page

The following fields are displayed:

- **Local Port**— Port ID.
- **Neighbor Chassis ID**— ID number of the neighbor's chassis.
- **Neighbor Port Name**— Neighbor's port number that sent the information.
- **Neighbor System Name**— Neighbor's system name.
- **System Capabilities**— Capabilities that are supported and enabled on the neighbor. The System Capabilities codes are:

  O = Other

  P = Repeater

  B = Bridge

  W = Wireless Access Point

  R = Router

  T = Telephone

C = Cable Device

S = Station only

- **Med Device class and Power Source code**— Indicates whether or not the MED device Classes I through III are supported. Power Source code indicates the current power source which is either the Primary Power Source or the Backup Power Source. The codes are:

  C1 = Class I

  C2 = Class II

  C3 = Class III

  N = Network

  PSE = PoE

  L = Local

  Both = Both primary and backup

  Prim = Primary

  UN = Unknown

  Ba = Backup

Displaying LLDP Statistics

To display LLDP Statistics, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

3. From the LLDP tab, move the cursor to the right and select **Statistics**.

   The LLDP Statistics page is displayed with the Port Statistics tab selected automatically. See Figure 141.

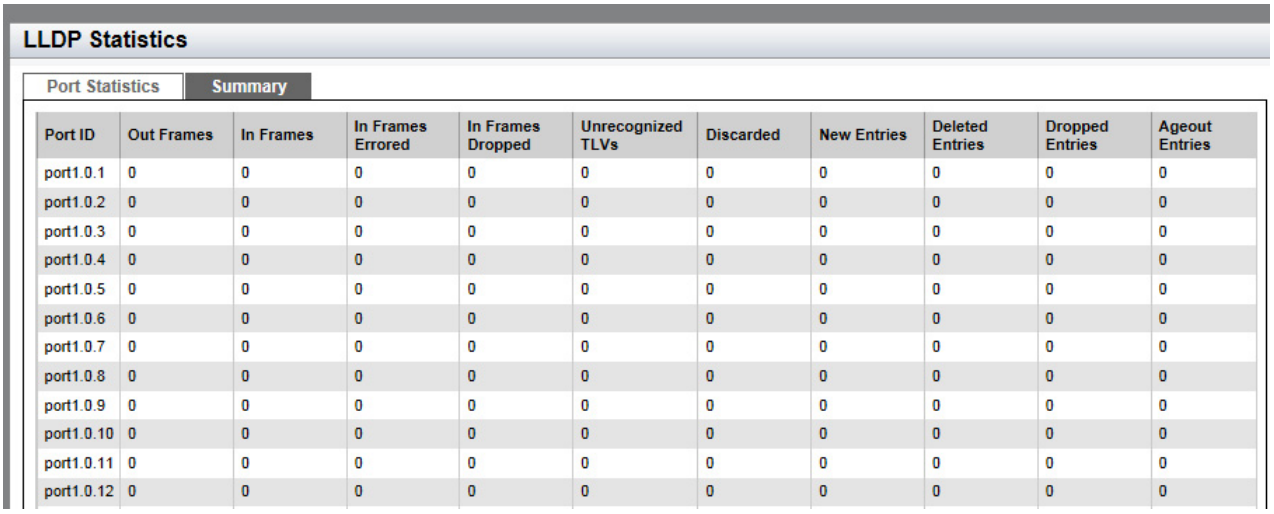


Figure 141. LLDP Statistics Page with Port Statistics Tab

The following fields are displayed:

- **Port ID**— Port ID.
- **Out Frames**— Number of LLDPDU frames transmitted.
- **In Frames**— Number of LLDPDU frames received.
- **In Frames Errored**— Number of invalid LLDPDU frames received.
- **In Frames Dropped**— Number of LLDPDU frames received and discarded.
- **Unrecognized TLVs**— Number of LLDP TLVs received that were unrecognized, but the TLV types were in the range of reserved TLV types.
- **Discarded**— Number of discarded TLVs.

- **New Entries**— Number of times the information advertised by neighbors has been inserted into the neighbor table.
- **Deleted Entries**— Number of times the information advertised by neighbors has been removed from the neighbor table.
- **Dropped Entries**— Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
- **Ageout Entries**— Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

4. Select the **Summary** tab.

The LLDP Statistics Summary page is displayed. See Figure 142.

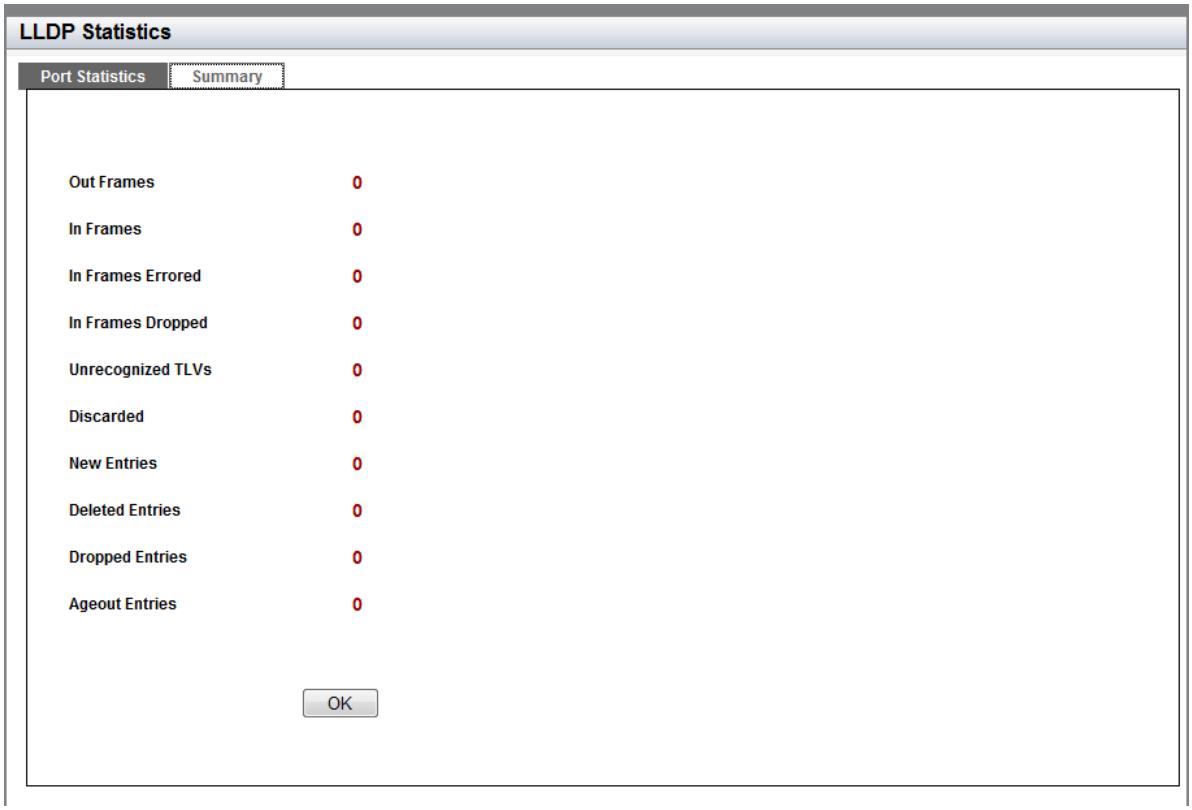


Figure 142. LLDP Statistics Page with Summary Tab

The fields are described in step 3. These fields list the statistics for all of the ports.

5. Click **OK** to return to the LLDP Statistics Page with the Port Statistics Tab selected.

Displaying Location Entries

To display the LLDP Civic, Coordinate, and ELIN locations, use the following procedures:

- "Displaying Civic Locations" on page 311
- "Displaying Coordinate Locations" on page 312
- "Displaying ELIN Locations" on page 313

For information about creating LLDP locations, see "Enabling and Configuring LLDP on the Switch" on page 284.

Displaying Civic Locations

To display a Civic Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

4. From the Locations tab, move the cursor to the right and select **Civic**.

   The LLDP Civic Location page is displayed. See Figure 131 on page 296.

   The following fields are displayed:

   - **ID**
   - **Country**
   - **State**
   - **County**
   - **City**
   - **Division**
   - **Neighborhood**
   - **Street Group**
   - **Leading Street Direction**
   - **Trailing Street Suffix**
   - **Street Suffix**

- ❒ **House Number**
- ❒ **House Number Suffix**
- ❒ **Landmark**
- ❒ **Additional Information**
- ❒ **Name**
- ❒ **Postal Code**
- ❒ **Building**
- ❒ **Unit**
- ❒ **Floor**
- ❒ **Room**
- ❒ **Place Type**
- ❒ **Postal Community Name**
- ❒ **Post Office Box**
- ❒ **Additional Code**
- ❒ **Seat**
- ❒ **Primary Road Name**
- ❒ **Road Section**
- ❒ **Branch Road Name**
- ❒ **Sub Branch Road Name**
- ❒ **Street Name Pre Modifier**
- ❒ **Street Name Post Modifier**

Displaying Coordinate Locations

To display a Coordinate Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

4. From the Locations tab, move the cursor to the right and select **Coordinates**.

   The LLDP Coordinate Location page is displayed. See Figure 133 on page 299.

The following fields are displayed:

- **ID**— LLDP Coordinate Location ID.
- **Latitude**— Latitude value in decimal degrees.
- **Latitude Resolution**— Latitude resolution as the number of valid bits.
- **Longitude**— Longitude value in decimal degrees.
- **Longitude Resolution**— Longitude resolution as the number of valid bits.
- **Altitude**— Altitude in meters or floors.
- **Altitude Resolution**— Altitude resolution as the number of valid bits.
- **Datum**— Geodetic system (or datum) of the coordinates. The datum codes are:

  WGS84: World Geodetic System 1984

  NAD83-MLLW: Mean lower low water datum 1983

  NAD83-NAVD: North American vertical datum 1983

Displaying ELIN Locations

To display an LLDP ELIN location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

   The Locations tab is displayed. See Figure 129 on page 295.

4. From the Locations tab, move the cursor to the right and select **ELIN**.

   The LLDP ELIN Location page is displayed. See Figure 135 on page 301.

   The following fields are displayed:

   - **ID**— ID number for an LLDP-MED coordinate location entry on the switch.
   - **Elin LOCATION**— ELIN of 10 to 25 digits.

Displaying LLDP and LLDP-MED Settings

To display the LLDP and LLDP-MED settings, use the following procedures:

For information about configuring LLDP and LLDP-MED, see “Assigning LLDP Locations to a Port” on page 302.

Displaying the Basic LLDP Configuration

To display the basic LLDP configuration, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears to the right.

3. From the LLDP tab, select **Basic Configuration**.

   The LLDP Configuration page is displayed. See Figure 123 on page 285.

   The following fields are displayed:

   - ❒ **Status**— Indicates whether LLDP is enabled or disabled on the switch.
   - ❒ **Timer**— Transmit interval.
   - ❒ **Fast Start Count**— Fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it begins sending LLDP-MED advertisements from a port, for instance, when it detects a new LLDP-MED capable device.
   - ❒ **Holdtime Multiplier**— Holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors.
   - ❒ **Non Strict Med TLV Order Check**— Indicates whether the switch accepts LLDP-MED advertisements when the TLVs are not in the standard order, as specified in ANSI/TIA-1057.

- **Notification Interval**— Notification interval. This is the minimum interval between LLDP SNMP notifications (traps).
- **Reinit**— Reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized.
- **Tx Delay**— Transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information.
- **Total Neighbors**— Number of LLDP neighbors the switch has discovered on all its ports.
- **Neighbors Last Update**— Time since the LLDP neighbor table was last updated.

Displaying LLDP Port Assignments

To display LLDP port assignments, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**, move the cursor to the right and then select **Port Configurations**.

   The LLDP Port Config page is displayed. See Figure 124 on page 288.

   The following fields are displayed:

   - **Interface**— Port ID.
   - **Notification**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports.
   - **Adv. Transmit**— Indicates whether the port sends LLDP advertisements. Ports configured to transmit LLDP advertisements send the mandatory TLVs and any optional LLDP TLVs they have been specified to send.
   - **Adv. Receive**— Indicates whether the port accepts LLDP advertisements. Ports configured to receive LLDP advertisements accept all advertisements from their neighbors.
   - **MED Notifications**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports.

Displaying Port Locations

To display the LLDP port locations, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and select **Port Locations**.

   The LLDP Port Location page is displayed. See Figure 136 on page 302.

   The following fields are displayed.

   - **Interface**— Port ID.
   - **Civic Location ID**— Civic location ID.
   - **Coordinate Location ID**— Coordinate location ID.
   - **ELIN Location ID**— ELIN location ID.

Displaying LLDP TLV

To display the LLDP TLV settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

   The LLDP tab is displayed.

3. From the LLDP tab, hover over **TLV**.

   The LLDP TLV tab is displayed in Figure 126 on page 290.

4. From the LLDP TLV tab, select **TLV** again.

   The LLDP TLV page is displayed. See Figure 127 on page 291.

   The following fields are displayed:

   - **Interface**— Port ID.
   - **Port Description**— Port description of the neighbor's port.
   - **System Name**— Neighbor's system name.
   - **System Description**— Model number of the AT-FS970M switch.

- **System Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
- **Management Address**— IP address of the local LLDP agent. This is used to obtain information related to the local device.
- **Port VLAN**— VID of the VLAN in which the transmitting port is an untagged member.
- **Port and Protocol VLANs**— Indicates whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers. This field is not supported on the AT-FS970M switches.
- **VLAN Names**— Lists the names of the VLANs in which the transmitting port is either an untagged or tagged member.
- **Protocol IDs**— List of protocols that are accessible through the port, for instance:

  - 9000 (Loopback)
  - 0026424203000000 (STP, RSTP, or MSTP)
  - 888e01 (802.1x)
  - AAAA03 (EPSR)
  - 88090101 (LACP)
  - 00540000e302 (Loop protection)
  - 0800 (IPv4)
  - 0806 (ARP)
  - 86dd (IPv6)

- **MAC Phy Config**— Speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
- **Power Management**— Power via MDI capabilities of the port.
- **Link Aggregation**— Indicates whether the port is capable of link aggregation and, if so, whether or not it is currently a member of an aggregator.
- **Max Frame Size**— Maximum supported frame size the port can send. This field is not adjustable on the switch.

Displaying LLDP-MED TLV

To display LLDP-MED TLV settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 122 on page 284.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then hover over **TLV**.

   The LLDP TLV tab is displayed. See Figure 126 on page 290.

3. From the LLDP TLV tab, move the cursor to the right and select **TLV-MED**.

   The LLDP-Med TLV page is displayed. See Figure 138 on page 304.

   The following fields are displayed:

   - **Interface**— Port ID.
   - **Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
   - **Network-policy**— Network policy information specified on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:
     - Voice VLAN ID
     - Voice VLAN Class of Service (CoS) priority
     - Voice VLAN Diffserv Code Point (DSCP)
   - **Location**— Location information specified for the port, in one or more of the following formats:
     - Civic location
     - Coordinate location
     - Emergency Location Identification Number (ELIN)
   - **Inventory-management**— Current hardware platform and the software version, identical on every port on the switch:
     - Hardware Revision
     - Firmware Revision
     - Software Revision
     - Serial Number
     - Manufacturer Name

- Model Name
- Asset ID

Chapter 26
sFlow

This chapter provides a brief description of the sFlow feature and explains how to enable this feature on the switch.

See the following sections:

For more information about the sFlow feature, see the following chapters in the *AT-FS970M Series Version 2.3.1.0 Management Software Command Line Interface User’s Guide*:

- ❒ sFlow Agent
- ❒ sFlow Agent Commands

Overview

The sFlow agent allows the switch to gather data about the traffic on the ports and to send the data to sFlow collectors on your network for analysis. You can use the information to monitor the performance of your network or identify traffic bottlenecks.

The sFlow agent can gather two types of information about the traffic on the ports of the switch:

- Ingress packet samples
- Packet counters

Ingress Packet Samples

The sFlow agent can capture ingress packets on ports and send copies of the packets to sFlow collectors on your network for analysis. Depending on the capabilities of the collectors, packets can be scrutinized for source and destination MAC or IP addresses, protocol type, length, and so forth.

Packet sampling is activated by specifying sampling rates on the ports. This value defines the number of ingress packets from which the agent samples one packet. For example, a sampling rate of 1000 on a port prompts the agent to send one packet from every 1000 ingress packets to the designated sFlow collector. Different ports can have different rates.

Packet Counters

The agent can also gather and send data to a collector about overall information regarding the status and performance of the ports, such as speeds and status, and the statistics from the packet counters. The counters contain the number and types of ingress and egress packets handled by the ports since the switch or the counters were last reset. The agent can gather and send the following port status and counter information to a collector on your network:

- Port number
- Port type
- Speed
- Direction
- Status
- Number of ingress and egress octets
- Number of ingress and egress unicast packets
- Number of ingress and egress multicast packets
- Number of ingress and egress broadcast packets
- Number of ingress and egress discarded packets
- Number of ingress and egress packets with errors
- Number of ingress packets with unknown protocols

To configure the agent to forward these port statistics to the collectors, you have to specify polling rates, which define the maximum amount of time permitted between successive queries of the counters of a port by the agent.

Different ports can have different polling rates. Ports to which critical network devices are connected can be assigned low polling rates, so that the information on the collector is kept up-to-date. Ports connected to less critical devices can be assigned higher polling rates.

To increase its efficiency, the agent can send port status and counter information before the polling interval of a port times out. For example, if you define a polling interval of five minutes for a port, the agent, depending on its internal dynamics, may send the information to the collector before five minutes have actually elapsed.

sFlow Collectors

The sFlow agent on the switch can send port performance data to an sFlow collector on your network. The performance data from each port can be sent to one collector.

Guidelines

Here are the guidelines for the sFlow agent:

- You can specify just one sFlow collector.
- The sFlow collectors must be members of the same subnet as the management IP address of the switch, or must have access to it through routers or other Layer 3 devices.
- If the sFlow collectors are not a member of the same subnet as the management IP address of the switch, the switch must have a default gateway that specifies the first hop to reaching the collectors' subnet. For instructions, refer to Chapter 19, "Setting IPv4 and IPv6 Addresses" on page 215.
- The sFlow feature is not dependent on SNMP. You do not have to enable or configure SNMP on the switch to use the sFlow feature. In addition, you cannot use sFlow collectors to configure or manage SNMP.
- Configure sFlow in the following sequence: First, specify the sFlow collector. Next, set the polling interval and sample rate. Finally, enable sFlow globally.

Specifying an sFlow Collector

Use this procedure to specify the IP address and the UDP port of an sFlow collector on your network. The packet sampling data and the packet counters are sent by the switch to the collector specified. You can specify only one collector.

To select the Collector tab from the sFlow page, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 143.

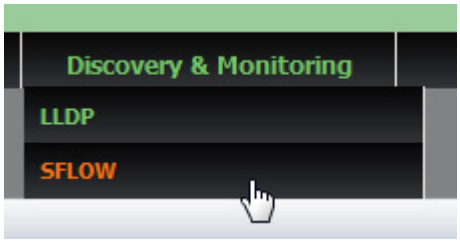


Figure 143. Discovery & Monitoring Tab

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

   The sFlow page is displayed with the Port Configurations tab selected. See Figure 144.

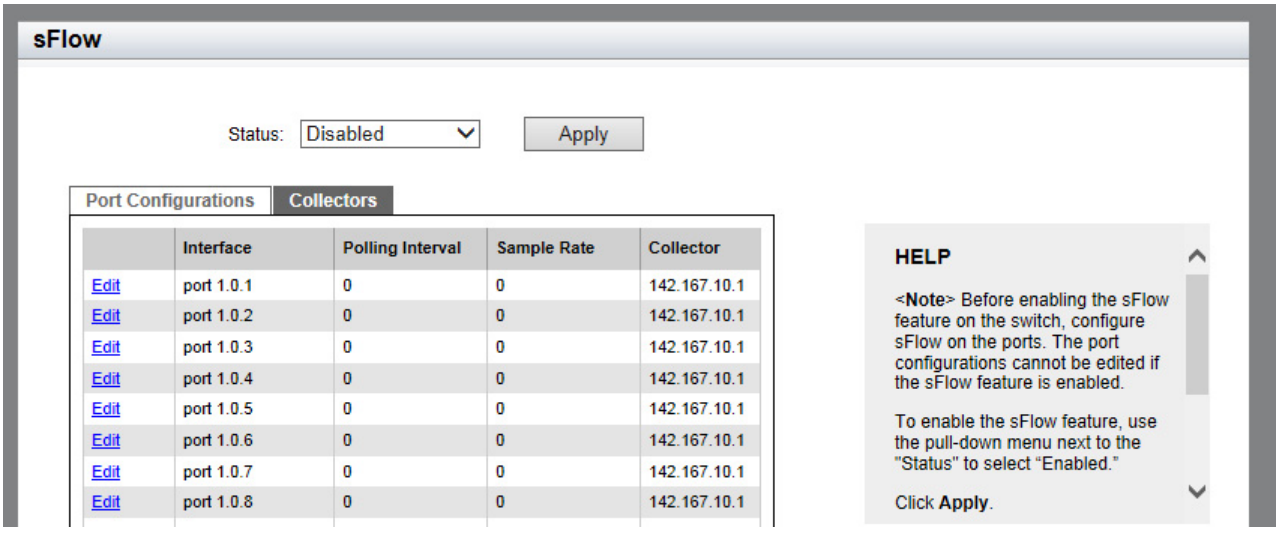


Figure 144. sFlow Page with the Port Configurations Tab

3. From the sFlow page, select the **Collector** tab.

The sFlow page is displayed with the Collector Tab selected. See Figure 145.

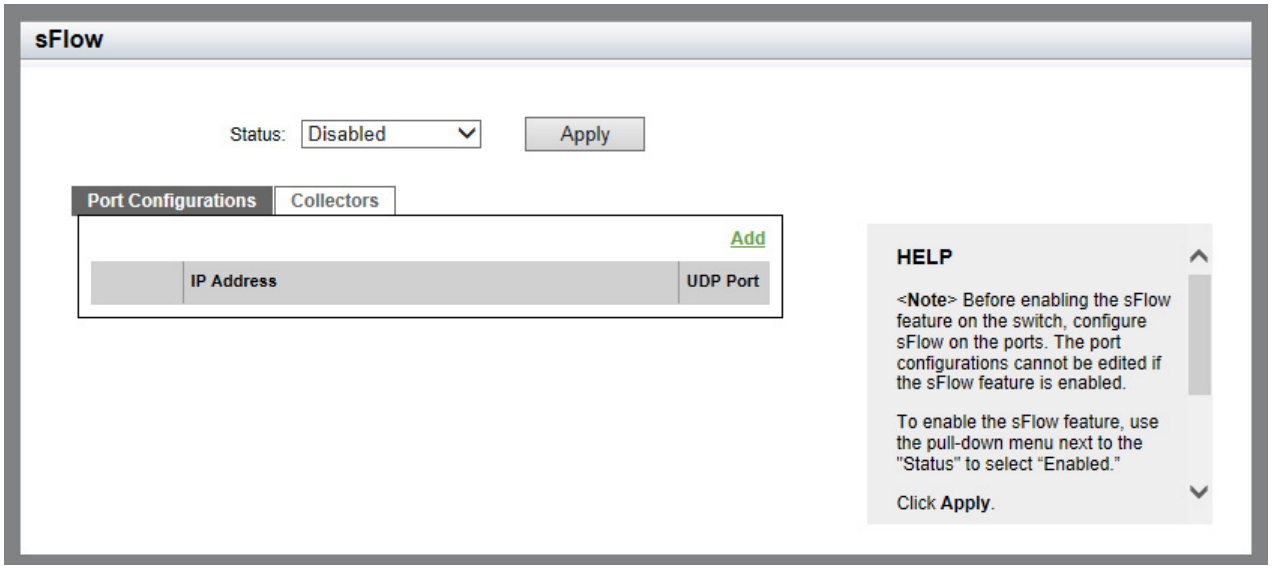


Figure 145. sFlow Page with Collectors Tab

4. Click **Add**.

   The sFlow Collector page is displayed. See Figure 146.

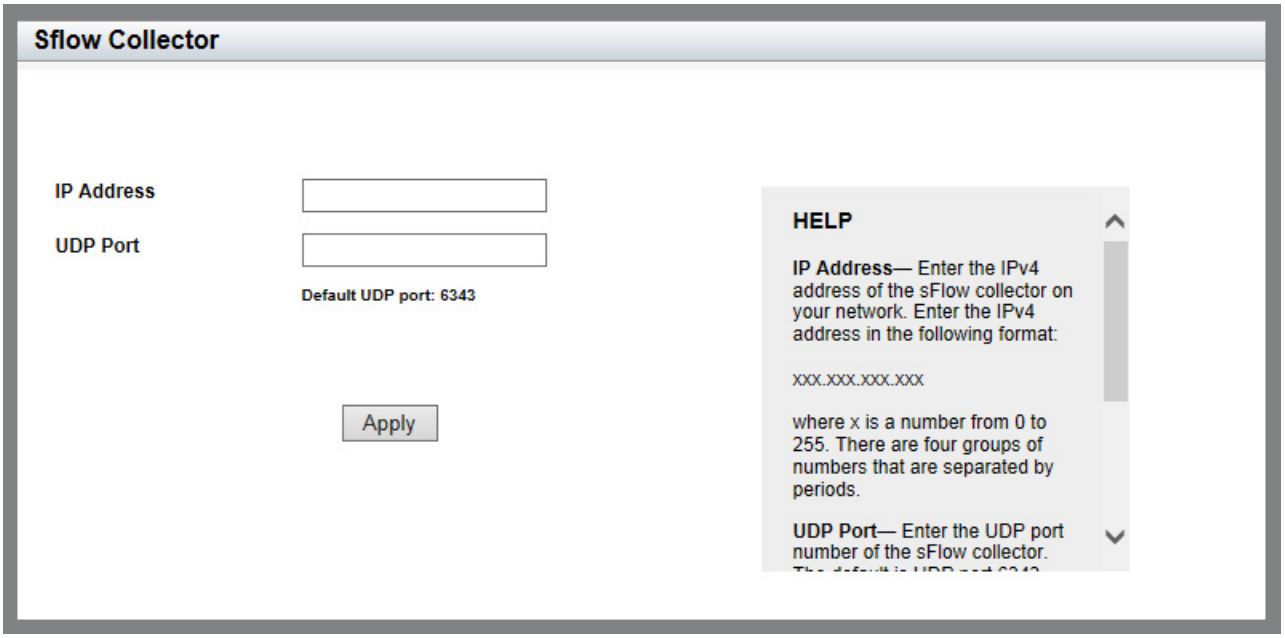


Figure 146. sFlow Collector Page

5. Enter the following fields:

- **IP Address**— IPv4 address of the sFlow collector on your network. Enter the IPv4 address in the following format:

  xxx.xxx.xxx.xxx

  where xxx is a number from 0 to 255. There are four groups of numbers that are separated by periods.

- **UDP Port**— UDP port number of the sFlow collector. The default is UDP port 6343.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Configuring sFlow on a Port

To configure the sFlow feature on a port, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 143 on page 324.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

   The sFlow page is displayed with the Port Configurations tab selected. See Figure 144 on page 324.

3. Click Edit next to the port that you want to modify.

The sFlow Port Modify page is displayed. See Figure 147.

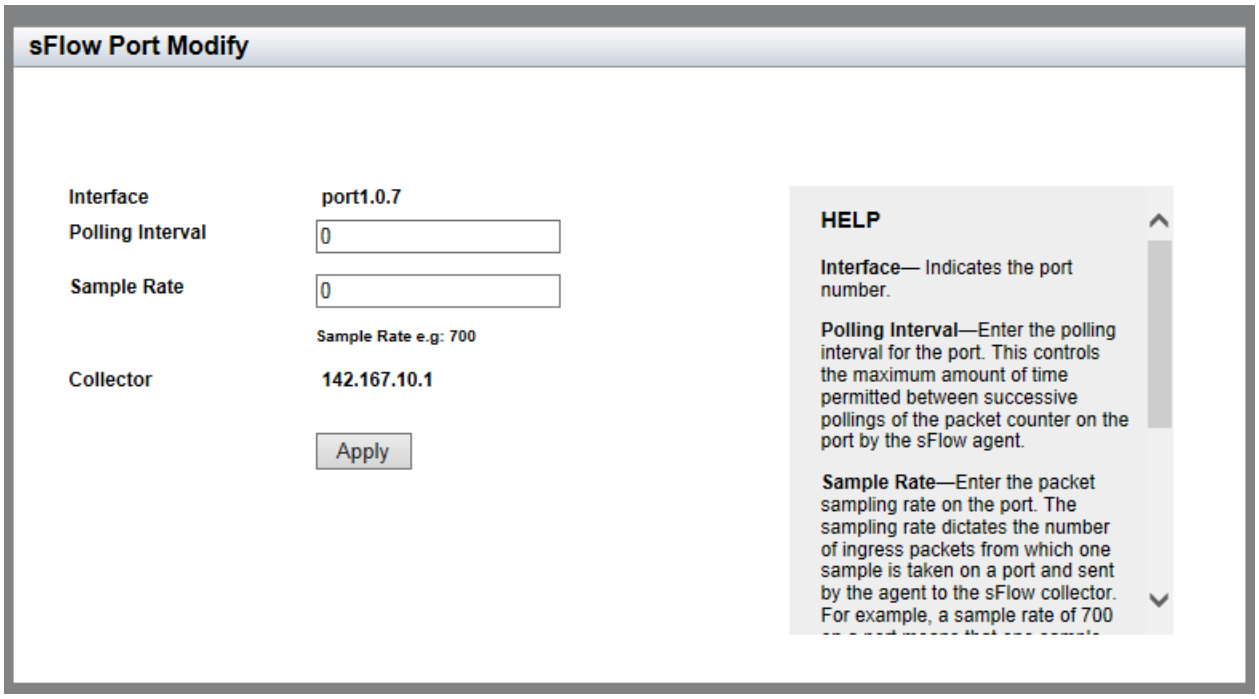


Figure 147. sFlow Port Modify Page

4. Change the following fields as needed:
   - **Interface**— Indicates the port ID. You cannot change this parameter on this page.
   - **Polling Interval**— Enter the polling interval for the port. This controls the maximum amount of time permitted between successive pollings of the packet counter on the port by the sFlow agent.
   - **Sample Rate**— Enter the packet sampling rate on the port. The sampling rate dictates the number of ingress packets from which one sample is taken on a port and sent by the agent to the sFlow collector. For example, a sample rate of 700 on a port means that one sample packet is taken for every 700 ingress packets. The possible values are 0 and 256 to 16,441,700 packets. Entering the value 0 disables packet sampling.
5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Enabling sFlow on the Switch

Before enabling the sFlow feature on the switch, you must configure sFlow on the ports. The port configurations cannot be edited if the sFlow feature is enabled. For how to configure sFlow on the ports, see "Configuring sFlow on a Port" on page 327.

To enable the sFlow feature on a switch, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 143 on page 324.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

   The sFlow page is displayed with the Port Configurations tab selected. See Figure 144 on page 324.

3. Use the pull-down menu next to the **Status** field to select "Enabled."

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Displaying the sFlow Settings

To display the sFlow settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

   The **Discovery & Monitoring** tab is displayed. See Figure 143 on page 324.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

   The sFlow page is displayed with the Port Configurations tab selected. See Figure 144 on page 324.