Management Software

AT-S62

Web Browser Interface User’s Guide

AT-8516F/SC, AT-8524M, AT-8524POE,
AT-8550GB and AT-8550SP LAYER 2+
FAST ETHERNET SWITCHES

VERSION 1.3.0

Allied Telesyn

PN 613-000127 Rev A

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

Table of Contents

Chapter 17

Chapter 18

Section III

Chapter 19

Chapter 25

Section VII

Chapter 26

Chapter 27

Chapter 28

Chapter 29

List of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 15

Chapter 16

Chapter 17

Chapter 18

Chapter 19

Chapter 20

Preface

This guide contains instructions on how to configure an AT-8500 Series Layer 2+ Fast Ethernet Switch using the web browser interface in the AT-S62 management software. For instructions on how to manage the switch from the menus or command line interface, refer to the *AT-S62 Menus Interface User's Guide* or *AT-S62 Command Line Interface User's Guide*. The guides are available from the Allied Telesyn web site.

For background information and guidelines on the features of the AT-8500 Series switches and the AT-S62 management software, refer to the appropriate chapter in the *AT-S62 Menus Interface User's Guide*. This guide also contains an overview of the different methods to managing a switch.

How This Guide is Organized

This manual is divided into the following sections.

Section I: Basic Operations

The chapters in this section explain how to perform basic operations on the switch using the web browser interface. Some of the operations include setting port parameters, creating port trunks, and viewing the MAC address table.

Section II: Advanced Operations

The chapters in this section explain some of the more advanced operations of the switch. Examples include using the file system and downloading and uploading files.

Section III: SNMPv3 Operations

The chapter in this section explains how to configure the switch for SNMPv3. (The instructions for SNMPv1 and SNMPv2 are in Section I, Basic Operations.)

Section IV: Spanning Tree Protocols

The chapters in this section configure the Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree Protocols.

Section V: Virtual LANs

The chapters in this section configure port-based and tagged VLANs, GVRP, and the multiple VLAN modes.

Section VI: Port Security

The chapters in this section explain the MAC address security system and 802.1x port-based access control.

Section VII: Management Security

The chapters in this section explain the management security features, such as the Secure Sockets Layer (SSL) and the Secure Shell (SSH) protocols.

⚠ **Caution**

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a "retail encryption item" in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesyn sales representative for current information on this product's export status.

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

Contacting Allied Telesyn

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

Online Support

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

Email and Telephone Support

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

Returning Products

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

To obtain a RMA number, contact Allied Telesyn's Technical Support at our web site: **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

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

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

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

Section I

Basic Operations

The chapters in this section cover a variety of basic switch features and functions. The chapters include:

- Chapter 1: Starting a Web Browser Management Session on page 19
- Chapter 2: Enhanced Stacking on page 25
- Chapter 3: Basic Switch Parameters on page 31
- Chapter 4: SNMPv1 and SNMPv2c Community Strings on page 47
- Chapter 5: Port Parameters on page 57
- Chapter 6: MAC Address Table on page 68
- Chapter 7: Static Port Trunks on page 77
- Chapter 8: Port Mirroring on page 85

Chapter 1

Starting a Web Browser Management Session

This chapter contains the procedure for starting a web browser management session on an AT-8500 Series switch. Sections in the chapter include:

Starting a Web Browser Management Session

In order for you to establish a web browser management session with an AT-8500 Series switch, there has to be at least one switch in the subnet with an IP address and whose stacking status is set to master switch. Starting a web browser management session on a master switch allows you to manage all the enhanced stacking switches that reside in the enhanced stack from the same management session.

Note
For background information on enhanced stacking, refer to *AT-S62 Menus Interface User's Guide*.

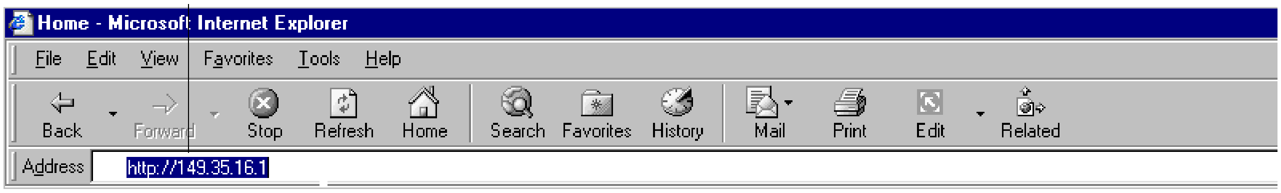
To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note
If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. In the URL field of the browser, enter the IP address of the switch you want to manage or of the master switch of the enhanced stack.

Switch's IP Address



Home - Microsoft Internet Explorer

Address http://149.35.16.1

Figure 1 Entering a Switch's IP Address in the URL Field

The AT-S62 software displays the login page, as shown in Figure 2.

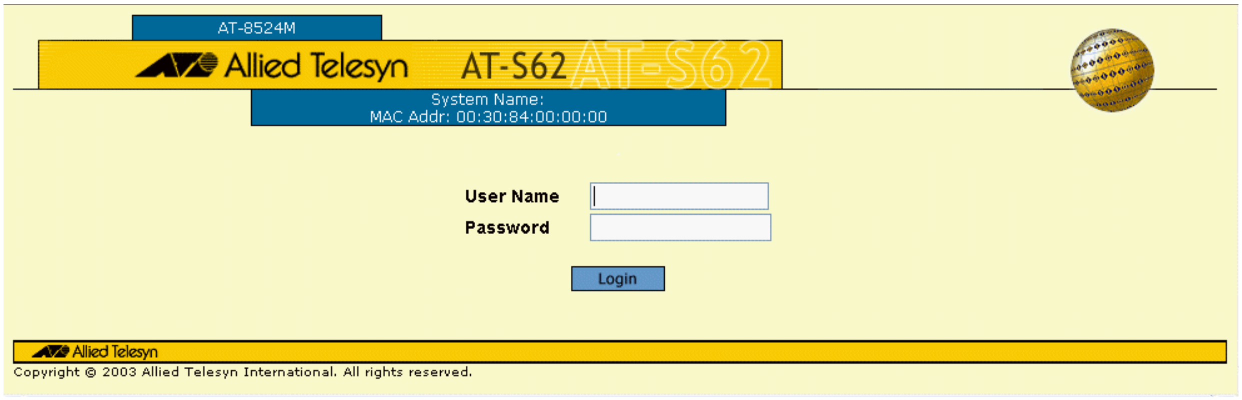

AT-8524M
Allied Telesyn AT-S62
System Name:
MAC Addr: 00:30:84:00:00:00
User Name
Password
Login
Allied Telesyn
Copyright © 2003 Allied Telesyn International. All rights reserved.

Figure 2 AT-S62 Login Page

3. Enter a user name and password. For manager access, enter "manager" as the user name. The default password is "friend". For operator access, enter "operator" as the user name. The default password is "operator". Login names and passwords are case-sensitive. (For information on the two access levels, refer to the *AT-S62 Menus Interface User's Guide*.)

   The user names cannot be changed. To change a password, refer to Configuring the Manager and Operator Passwords on page 38.

   The Home page is shown in Figure 3.

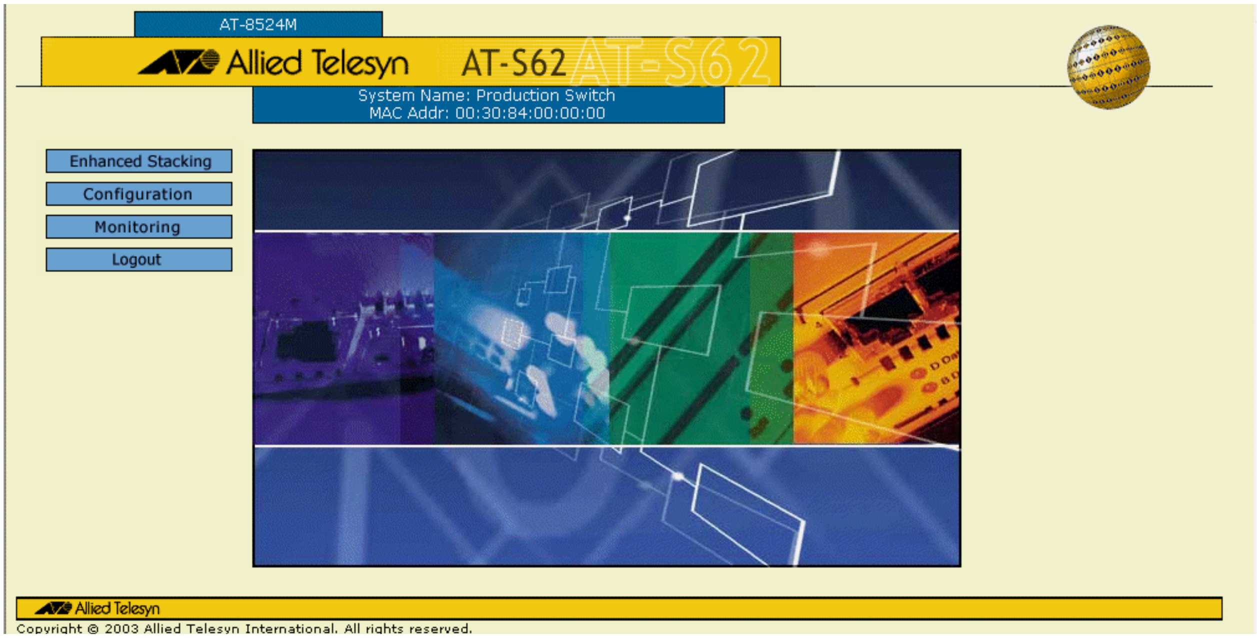

AT-8524M
Allied Telesyn AT-S62
System Name: Production Switch
MAC Addr: 00:30:84:00:00:00
Enhanced Stacking
Configuration
Monitoring
Logout
Allied Telesyn
Copyright © 2003 Allied Telesyn International. All rights reserved.

Figure 3 Home Page

The main menu is on the left side of the Home page and consists of the following selections:

❑ Enhanced Stacking

❑ Configuration

❑ Monitoring

❑ Logout

Note
The Enhanced Stacking selection is displayed only on master switches.

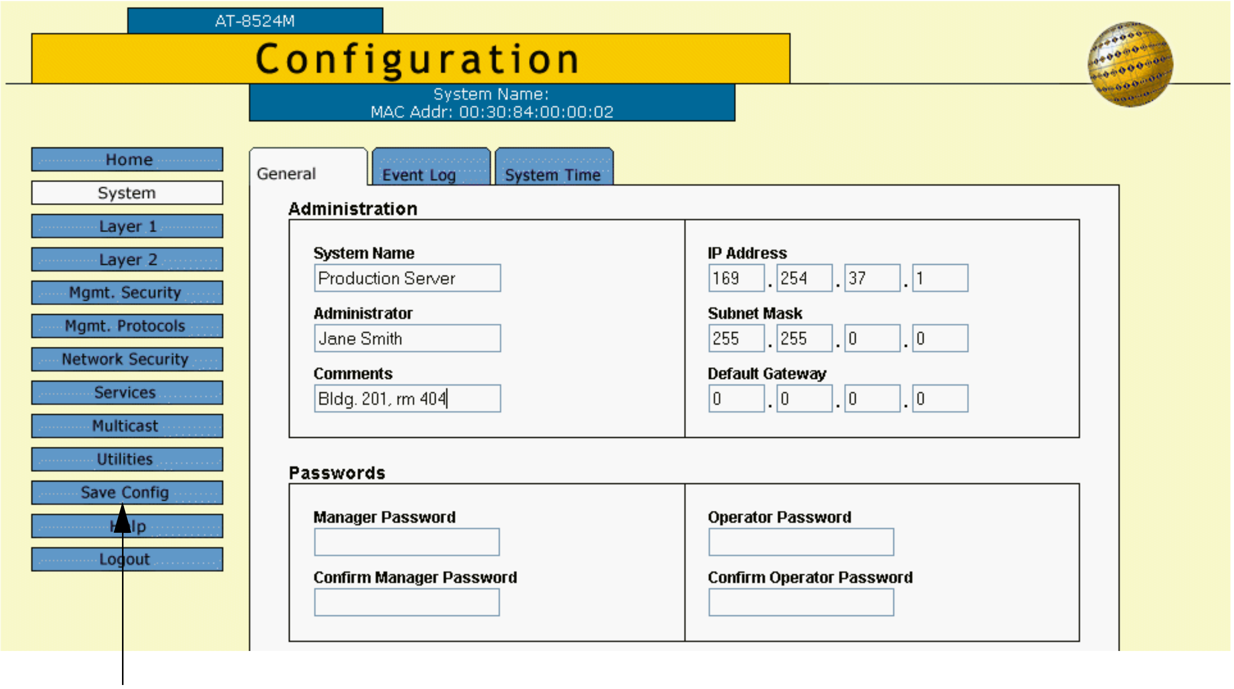
A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Browser Tools

You can use the browser tools to move around the management pages. Selecting **Back** on your browser’s toolbar returns you to the previous display. You can also use the browser’s **bookmark** feature to save the link to the switch.

Saving Your Parameter Changes

When you make a change to a switch parameter, the change is, in most cases, immediately activated as soon as you click the Apply button. However, a change to a switch parameter is initially saved only to temporary memory and will be lost the next time you reset or power cycle the unit. To permanently save a change, you must click the **Save Config** button, shown in Figure 4. This updates the switch's active configuration file. A change that is saved to the configuration file is retained even when the unit is powered off or reset. If the button is not visible in the menu, there are no changes for the switch to save.



System Name:
MAC Addr: 00:30:84:00:00:02

Administration

System Name: Production Server

Administrator: Jane Smith

Comments: Bldg. 201, rm 404

IP Address: 169 . 254 . 37 . 1

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Passwords

Manager Password:

Confirm Manager Password:

Operator Password:

Confirm Operator Password:

Save Config Button

Figure 4 Save Config Button

Quitting a Web Browser Management Session

To exit a web browser management session, select **Logout** from the main menu.

Chapter 2

Enhanced Stacking

This chapter contains the following procedures:

- ❑ Setting a Switch’s Enhanced Stacking Status on page 26
- ❑ Selecting a Switch in an Enhanced Stack on page 28
- ❑ Displaying the Enhanced Stacking Status on page 30

Note
For background information on enhanced stacking, refer to the *AT-S62 Menus Interface User’s Guide*.

Setting a Switch’s Enhanced Stacking Status

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

❑ Master - A master switch of a stack is used to manage other switches in an enhanced stack. Establishing a local or remote management session on a master switch gives you access to the other switches in the enhanced stack.

In order to manage the switches of an enhanced stack using the web browser interface, you must assign the master switch a unique IP address. You can manually assign the address or activate the BOOTP and DHCP client software on the switch so that it automatically obtains an IP address from a BOOTP or DHCP server on your network.

❑ Slave - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask. This is the default setting for an AT-8500 Series switch.

❑ Unavailable - A switch with this designation cannot be accessed through enhanced stacking. To remotely manage a switch with this designation using the web browser interface, you must assign it an IP address.

Note
The only switch whose stacking status you can change through a web browser management session is the switch on which you started the management session, typically a master switch. You cannot change the stacking status of a switch accessed through enhanced stacking. If the switch does not have an IP address and subnet mask, the only way to change its stacking status is through a local management session.

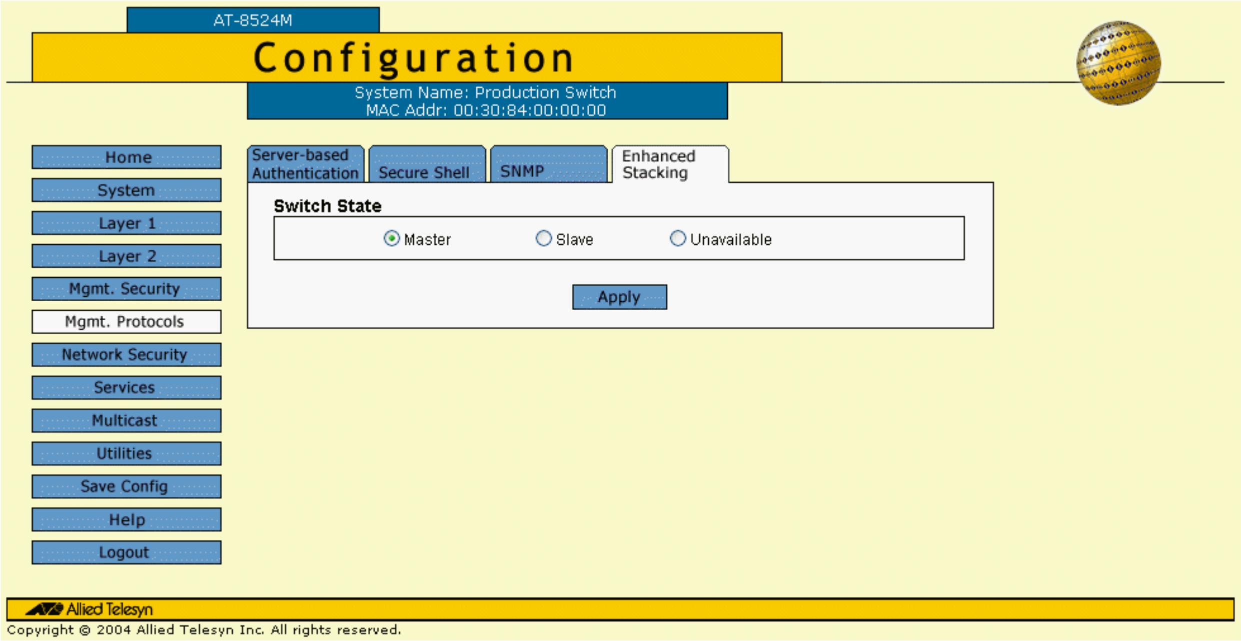
To adjust a switch’s enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **Enhanced Stacking** tab.

Note

If the window does not have an Enhanced Stacking tab, you have accessed the switch through enhanced stacking. Changing a switch's stacking status through enhanced stacking is not allowed. The only stacking status you can change remotely from a web browser management session is the switch on which you started the session.

The Enhanced Stacking tab is shown in Figure 5.


AT-8524M

Configuration

System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Switch State

● Master ○ Slave ○ Unavailable

Figure 5 Enhanced Stacking Tab

4. Click the desired enhanced stacking status for the switch. The default is Slave.

5. Click **Apply**.

   The new enhanced stacking status is immediately activated on the switch.

6. To permanently save the change, click the **Save Config** menu selection.

Selecting a Switch in an Enhanced Stack

The first thing that you should do before you perform any procedure on a switch in an enhanced stack is check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, identifying your switches is easy. The management software displays the name of the switch being managed at the top of every management window.

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

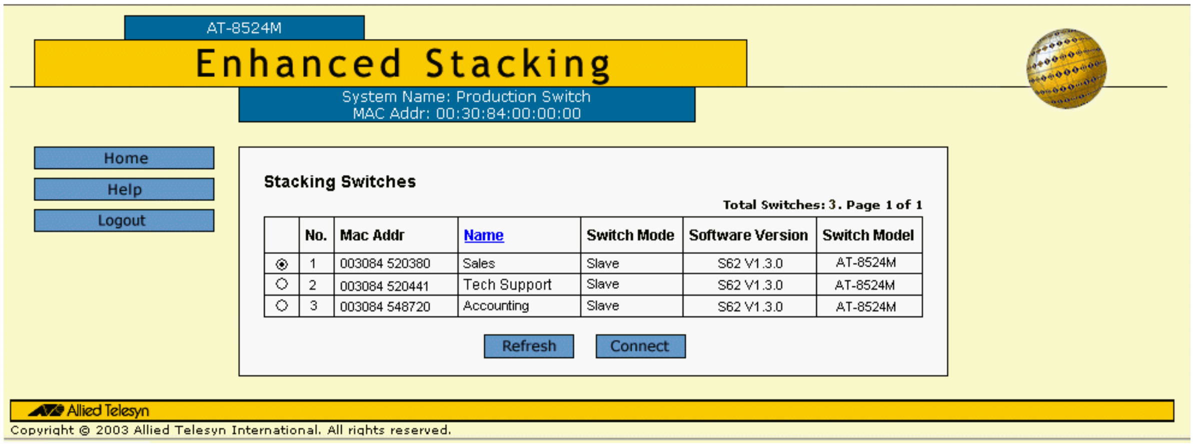
To manage a slave switch or another master switch in the same stack, you need to select it from the management software.

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

1. From the Home Page, select **Enhanced Stacking**.

Note
If the Home page does not have an Enhanced Stacking menu selection, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure.

The master switch polls the network for the slave and master enhanced stacking switches in the enhanced stack and displays a list of the switches in the Enhanced Stacking page. An example is shown in Figure 6.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Stacking Switches

Total Switches: 3. Page 1 of 1

	No.	Mac Addr	Name	Switch Mode	Software Version	Switch Model
●	1	003084 520380	Sales	Slave	S62 V1.3.0	AT-8524M
○	2	003084 520441	Tech Support	Slave	S62 V1.3.0	AT-8524M
○	3	003084 548720	Accounting	Slave	S62 V1.3.0	AT-8524M

Copyright © 2003 Allied Telesyn International. All rights reserved.

Figure 6 Enhanced Stacking Page

Note
The list does not include the master switch on which you started the management session or any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

You can refresh the list by clicking **Refresh**. This instructs the master switch to again poll the subnet for all switches.

2. To manage a switch in an enhanced stack, click the button to the left of the appropriate switch in the list. You can select only one switch at a time.

Note
If the web server on the master switch is operating in the secure HTTPS mode, you can manage only those enhanced stacking switches that are also operating HTTPS.

3. Click **Connect**.

4. Enter a user name and password for the switch when prompted.

   The Home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you finish managing a slave switch and want to manage another switch in the stack, return to the Home page of the switch and select **Disconnect** from the menu. This returns you to the Enhanced Stacking page in Figure 6 on page 28. When that page reappears, you are again addressing the master switch where you started the management session.

You can select another switch in the list to manage or, if you want to manage the master switch, return to the master switch's Home page by selecting **Home**.

Displaying the Enhanced Stacking Status

To display the enhanced stacking status of a switch, do the following:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select the **Mgmt. Protocols** menu option.
3. From the Layer 2 page, select the **Enhanced Stacking** tab.

   The information in the tab states the current enhanced stacking status of the switch as master, slave, or unavailable.

Chapter 3

Basic Switch Parameters

This chapter contains the following sections:

Configuring an IP Address and Switch Name

Note
For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8500 Series switch, refer to the *AT-S62 Menus Interface User's Guide*.

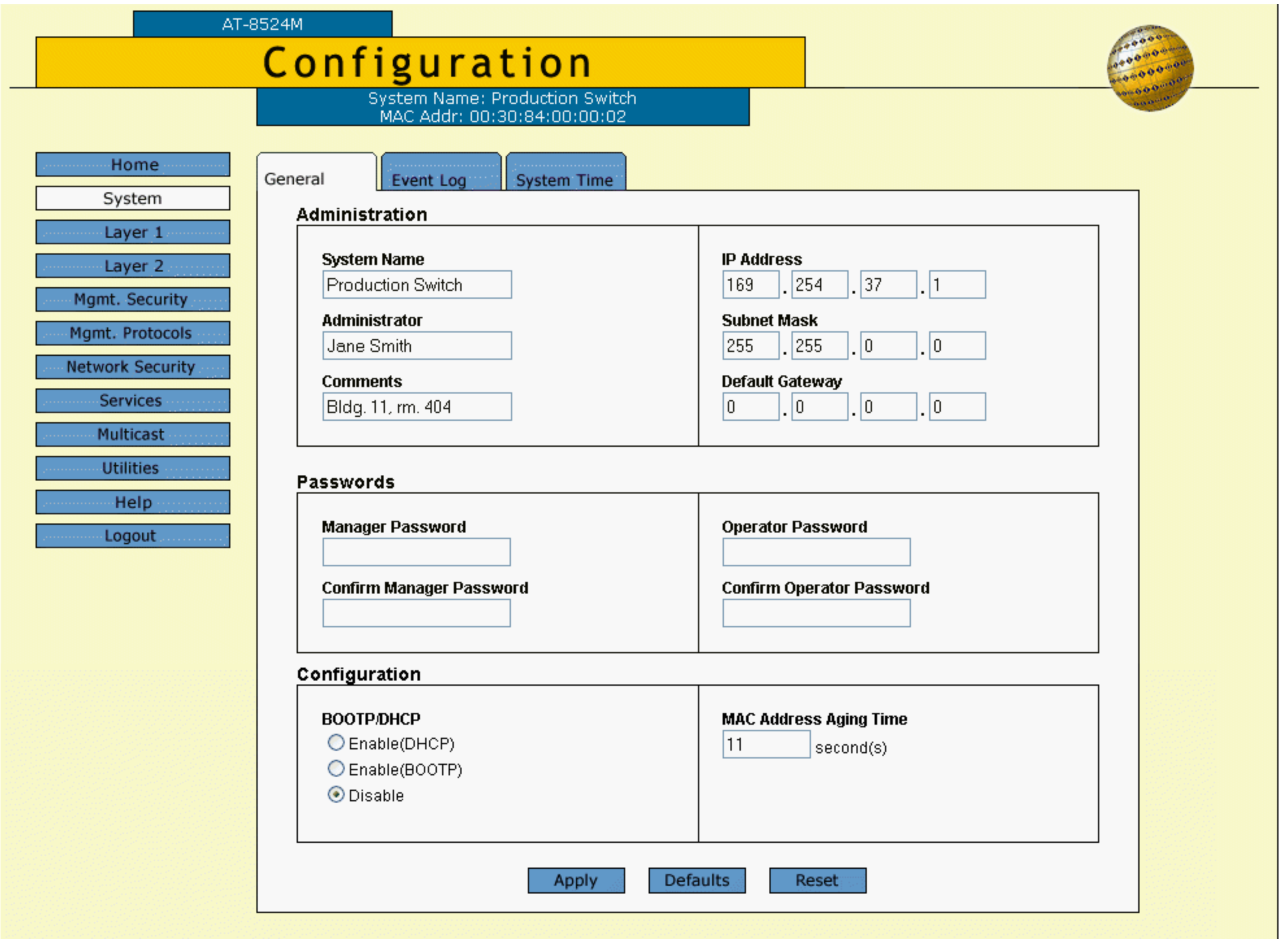
To set basic switch parameters for an AT-8500 Series switch, perform the following procedure:

1. From the Home Page, select **Configuration**.

2. Select the **System** menu option.

3. Select the **General** tab.

   The General tab is shown in Figure 7.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Administration

System Name: Production Switch

Administrator: Jane Smith

Comments: Bldg. 11, rm. 404

IP Address: 169 . 254 . 37 . 1

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Passwords

Manager Password

Confirm Manager Password

Operator Password

Confirm Operator Password

Configuration

BOOTP/DHCP
○ Enable(DHCP)
○ Enable(BOOTP)
● Disable

MAC Address Aging Time: 11 second(s)

Figure 7 General Tab

Note
This procedure describes the parameters in the Administration section of the tab. The Passwords section is described in Configuring the Manager and Operator Passwords on page 38. The DHCP/BOOTP options are described in Activating the BOOTP or DHCP Client Software on page 36. The MAC address aging time option is described in Changing the Aging Time on page 76.

Note
The Defaults button returns all parameters in this tab to their default settings. To return all switch parameters to the default values, refer to Returning the AT-S62 Software to the Factory Default Values on page 45

The Reset button resets the switch, as explained in Rebooting a Switch on page 40.

4. Change the parameters as desired.

   The parameters in the Administration section are described below:

   System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed at the top of the AT-S62 management pages and tabs. The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.

Note
Allied Telesyn recommends assigning each switch a name. Names can make it easier for you to identify the various switches when you manage them and help you avoid performing a configuration procedure on the wrong switch.

Administrator
This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 39 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

Comments
This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 39 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.

IP address
This parameter specifies the IP address of the switch. You must specify an IP address if you want the switch to function as the Master switch of an enhanced stack. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Note
Changing the IP address of a master switch will result in the loss of your remote management session. You can restart the management session using the master switch's new IP address.

Note
When setting the IP address and subnet mask of a switch accessed through enhanced stacking, such as a slave switch, you must set the subnet mask first or both IP address and subnet mask simultaneously. Your network management session will end if you set the IP address without specifying a subnet mask.

Subnet mask
This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The subnet mask must be entered in the format: xxx.xxx.xxx.xxx. The default value is 255.255.0.0.

Gateway address
This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router. The address must be entered in the format: xxx:xxx:xxx:xxx. The default value is 0.0.0.0.

5. Click the **Apply** button to activate your changes on the switch.

Note
A change to any of the above parameters is immediately activated on the switch.

A change to the IP address of a master switch will result in the loss of your remote management session. You can restart the management session using the switch's new IP address.

6. Click the **Save Config** menu option to permanently save your changes.

Activating the BOOTP or DHCP Client Software

For background information on BOOTP and DHCP, refer to the *AT-S62 Menus Interface User's Guide*.

To activate or deactivate the BOOTP or DHCP client software on the switch from a web browser management session, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **General** tab.

   The General tab is shown in Figure 7 on page 32.
4. In the BOOTP/DHCP section of the tab, click **Enable (DHCP)** to activate the DHCP client software, **Enable (BOOTP)** to activate the BOOTP client software, or **Disable** if you want to enter a static IP address for the switch or do not want to assign the switch an IP address. The default is disabled.
5. Click **Apply** to activate your change on the switch.

   Note
   If you activated the BOOTP or DHCP client software, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response. If you manually assigned the switch and IP address, that address is deleted and replaced by the IP address received from the BOOTP or DHCP server.
6. Click **Save Config** to permanently save your changes.

Displaying System Information

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

1. From the Home page, select **Monitoring**.
2. Select the **System** menu option.
3. Select the **General** tab. This tab is for viewing purposes only. You cannot change any of the values from this tab. The information in the tab is defined below:

   System Name
   The name of the switch.

   Administrator
   The name of the network administrator responsible for managing the switch.

   Comments
   The location of the switch, (for example, 4th Floor - rm 402B).

   DHCP/BOOTP
   The status of the DHCP and BOOTP client software. If enabled, the switch is obtaining its IP information from a DHCP or BOOTP server on the network.

   MAC Address Aging Timer
   The time interval an inactive dynamic MAC address can remain in the MAC address table before it is deleted.

   IP Address
   The switch's IP address.

   Subnet mask
   The switch's subnet mask.

   Default Gateway
   The IP address of a router for remote management.

   System Up Time
   The length of time since the switch was last reset or power cycled.

   Application Software
   The version number and build date of the AT-S62 software.

   Bootloader
   The version number and build date of the AT-S62 bootloader.

Configuring the Manager and Operator Passwords

There are two levels of management access on an AT-8500 Series switch: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S62 management session. The default password for manager access is "friend". The default password for operator access is "operator". Passwords are case-sensitive.

To change the manager or operator password, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **General** tab.

   The General tab is shown in Figure 7 on page 32.

4. In the Passwords section, enter the new values. The parameters are described below.

   Manager Password
   Manager Confirm Password
   These parameters are used to change the manager's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend". The password is case-sensitive.

⚠ **Caution**
You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password. Many web browsers cannot handle special characters in passwords.

   Operator Password
   Operator Confirm Password
   These parameters are used to change the operator's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator". The password is case-sensitive.

⚠ **Caution**

You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password. Many web browsers cannot handle special characters in passwords.

Note

A change to a password is immediately activated on the switch. You will be prompted for the new password the next time you log on.

5. Click **Apply** to activate your change on the switch.
6. Click **Save Config** to permanently save your change.

Rebooting a Switch

Note
Any parameters changes that have not been saved will be discarded when a system is reset. To save parameter changes, refer to Saving Your Parameter Changes on page 23.

To reboot a switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **General** tab.

   The General tab is shown in Figure 7 on page 32.

4. Click the **Reset** button.

   A confirmation prompt is displayed.

5. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

Note
The switch does not forward packets while it initializes the AT-S62 management software and loads the configuration file.

Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Setting the System Time

This procedure explains how to set the switch's date and time. Setting the system time is important if you configured the switch to send traps to your management workstations. Traps from a switch where this has not been set will not contain the correct date and time, making it difficult for you to determine when the events represented by the traps occurred.

It is also important to set the system time if you intend to use the Secure Sockets Layer (SSL) certificate feature described in Chapter 33, Public Key Infrastructure Certificates on page 651. Certificates must contain the date and time of when they were created.

There are two ways to set the switch's date and time. One method is to set it manually. There is, however, a drawback to this method. The switch loses the values when reset or power cycled. Using this method requires resetting the values whenever you reset the device.

The second method uses the Simple Network Time Protocol (SNTP). The AT-S62 management software comes with the client version of this protocol. You can configure the AT-S62 software to obtain the current date and time from an SNTP or Network Time Protocol (NTP) server located on your network or the Internet.

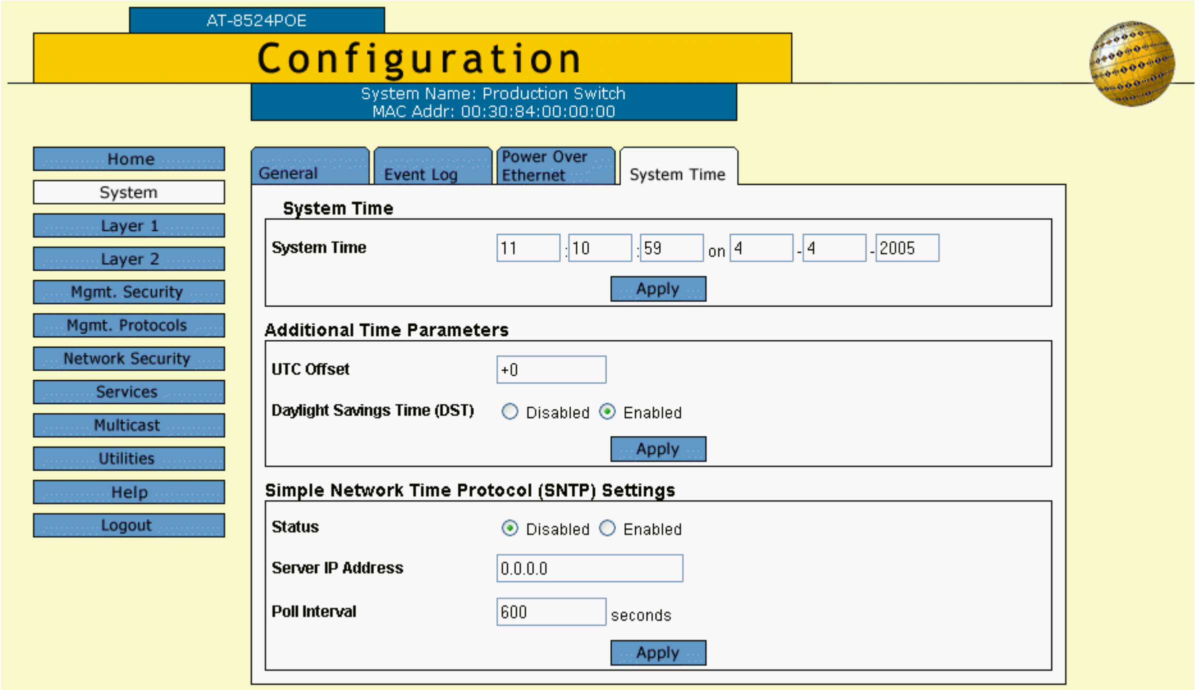
SNTP is a reduced version of the NTP. However, the SNTP client software in the AT-S62 management software is interoperable with NTP servers.

Note
The default system time on the switch is midnight, January 1, 1980.

To set the system time manually or to configure SNTP client, do the following:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select the **System** menu selection.
3. Select the **System Time** tab.

The System Time tab is shown in Figure 8.



System Time

System Time: 11 : 10 : 59 on 4 - 4 - 2005

Additional Time Parameters

UTC Offset: +0

Daylight Savings Time (DST): ○ Disabled ● Enabled

Simple Network Time Protocol (SNTP) Settings

Status: ● Disabled ○ Enabled

Server IP Address: 0.0.0.0

Poll Interval: 600 seconds

Figure 8 System Time Tab

4. To set the system time manually, do the following:

   a. In the System Time section of the tab, enter the time and date in the following format.

      hh:mm:ss dd-mm-yyyy

   b. Click **Apply**.

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

   UTC Offset
   Specifies the difference between the UTC and local time. The default is 0 hours. The range is -12 to +12 hours.

   > **Note**
   > If the switch is using DHCP, it automatically attempts to determine this value. In this case, you do not need to configure a value for the UTC Offset parameter.

   Daylight Savings Time (DST)
   Enables or disables the system's adjustment for daylight savings time. The default is enabled.

Note
The switch does not set DST automatically. If the switch is in a locale that uses DST, you must remember to enable this in April 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.

Status
Enables or disables the SNTP client on the switch. The default is disabled.

Server IP Address
Specifies the IP address of an SNTP server.

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

Poll Interval
Specifies the number of seconds the switch waits between polling the SNTP or NTP server. The default is 600 seconds. The range is from 60 to 1200 seconds.

6. When you finish configuring the parameters, click the **Apply** buttons.

Note
If you enabled the SNTP client, the switch immediately polls the SNTP or NTP server for the current date and time. (The switch automatically polls the server whenever a change is made to any of the parameters in this menu, so long as SNTP is enabled.)

7. To permanently save your changes to the SNTP client, click **Save Config**.

Pinging a Remote System

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

To ping a network device, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select **Utilities**.
3. Select the **Ping Client** tab.

   The Ping Client tab is shown in Figure 9.

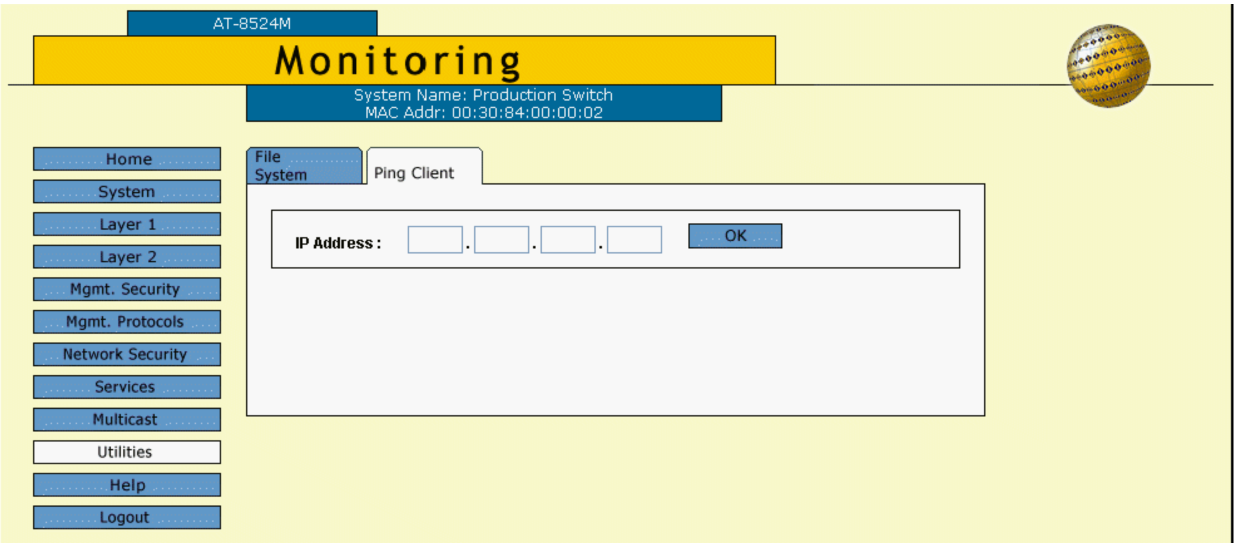


Figure 9 Ping Client Tab

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

   The results of the ping are displayed in a popup window.
6. To stop the ping, click **OK**.

Returning the AT-S62 Software to the Factory Default Values

The procedure in this section returns all AT-S62 software parameters, including IP address and subnet mask, if assigned, to their default values. Please note the following before performing this procedure:

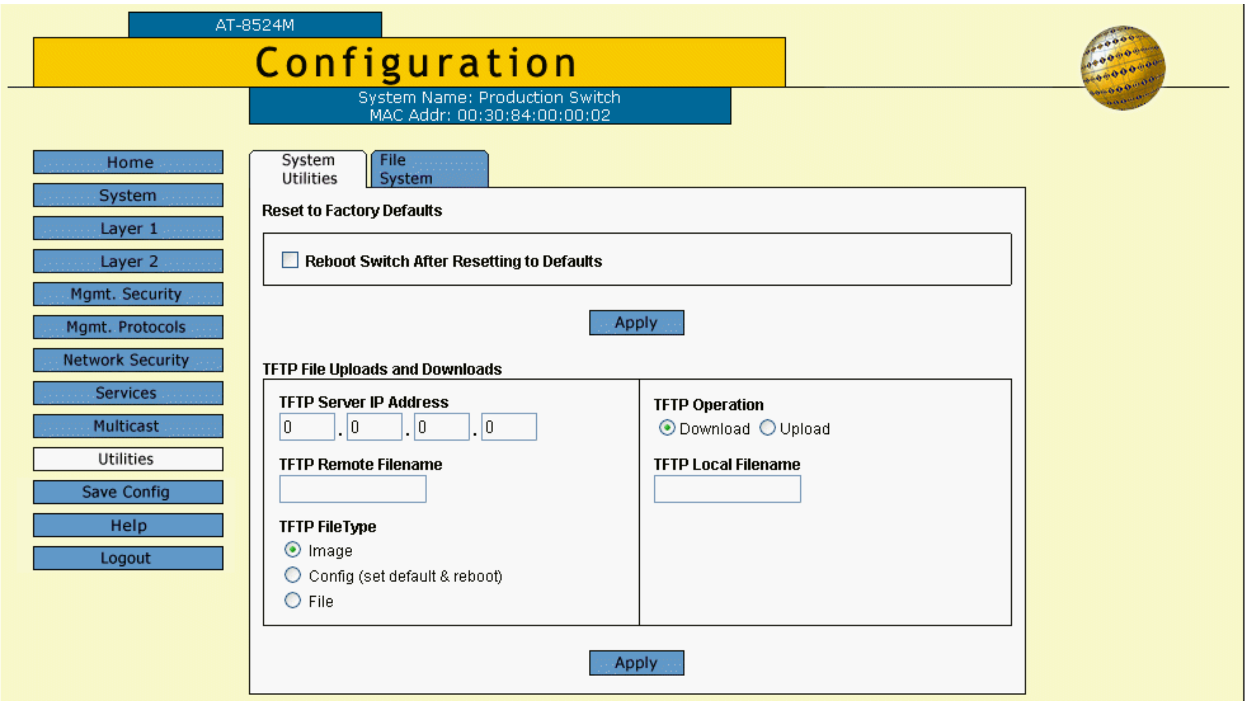
- ❑ Returning all parameter settings to their default values also deletes any port-based or tagged VLANs you created on the switch.
- ❑ This procedure retains the files in the switch's file system as well as the encryption keys stored in the key database.
- ❑ Returning a switch to its default values does not alter the contents of the active boot configuration file. To reset the file back to the default settings, you must select Save Config from the menu after the switch reboots and you have reestablished your management session. Otherwise the switch will revert back to the previous configuration the next time you reset the unit.

Note
The AT-S62 software default values can be found in Appendix A in the *AT-S62 Menus Interface User's Guide*.

To return the AT-S62 management software to the default settings, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select **Utilities** menu option.
3. Select the **System Utilities** tab.

The System Utilities tab is shown in Figure 10.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Reset to Factory Defaults

□ Reboot Switch After Resetting to Defaults

TFTP File Uploads and Downloads

TFTP Server IP Address: 0 . 0 . 0 . 0

TFTP Operation: ● Download ○ Upload

TFTP Remote Filename:

TFTP Local Filename:

TFTP FileType
● Image
○ Config (set default & reboot)
○ File

Figure 10 System Utilities Tab

The TFTP File Updates and Downloads section of the tab is explained in Chapter 10, File Downloads and Uploads on page 97.

4. Click the **Reboot Switch After Resetting to Defaults** checkbox.
5. Click **Apply**.
6. Follow the prompts.

Note
The bottom portion of the System Utilities tab is used to download and upload files from the switch. For instructions, refer to Chapter 10, File Downloads and Uploads on page 97.

Chapter 4

SNMPv1 and SNMPv2c Community Strings

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

This chapter contains the following procedures:

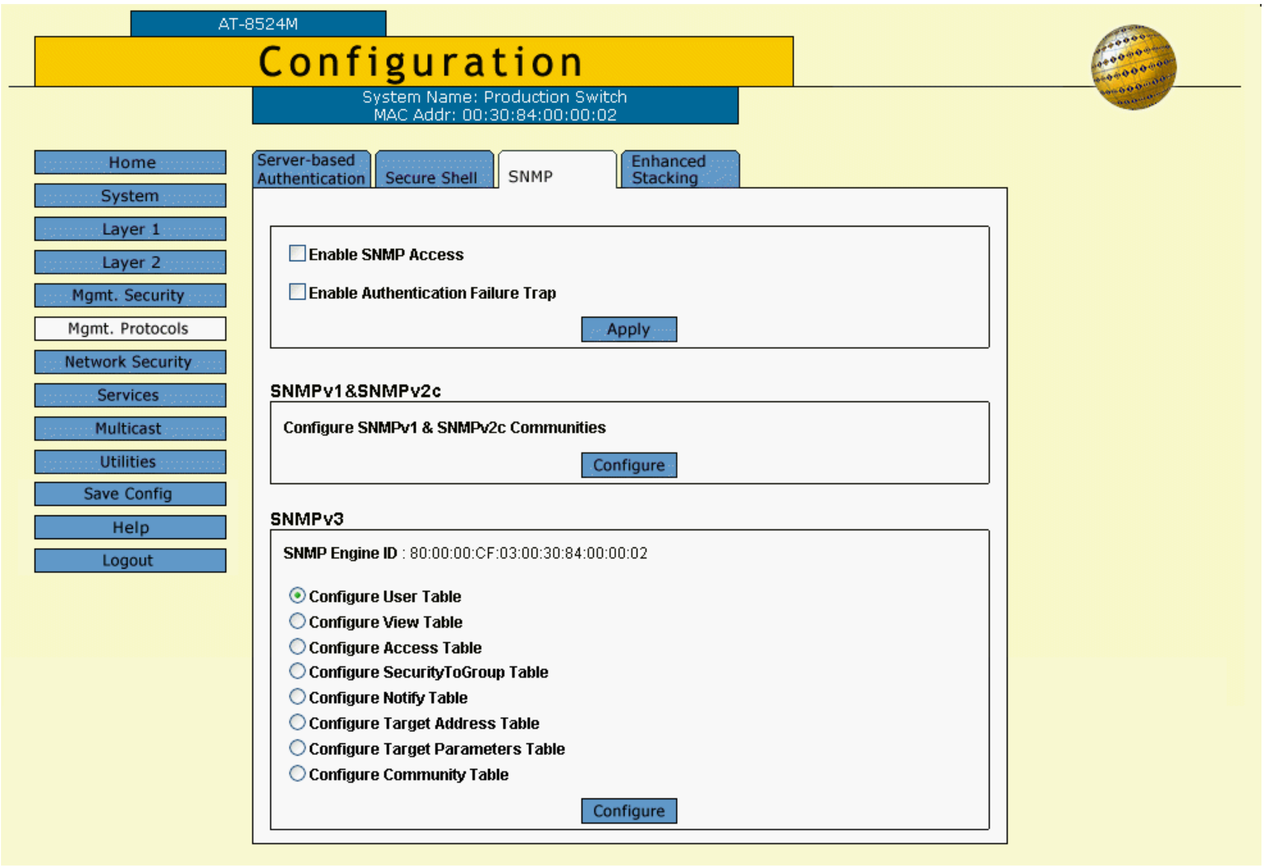
Note
For background information on SNMPv1 and SNMPv2c, refer to the *AT-S62 Menus Interface User's Guide*.

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 11.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

□ Enable SNMP Access

□ Enable Authentication Failure Trap

SNMPv1&SNMPv2c

Configure SNMPv1 & SNMPv2c Communities

SNMPv3

SNMP Engine ID : 80:00:00:CF:03:00:30:84:00:00:02

● Configure User Table
○ Configure View Table
○ Configure Access Table
○ Configure SecurityToGroup Table
○ Configure Notify Table
○ Configure Target Address Table
○ Configure Target Parameters Table
○ Configure Community Table

Figure 11 SNMP Tab (Configuration)

4. Click **Enable SNMP Access** to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management workstation. No check indicates that the feature is disabled. The default is disabled.
5. If you want the switch to send authentication failure traps, click **Enable Authentication Failure Traps**. A check in the box indicates that the switch will send the trap.
6. Click **Apply**.

A change to SNMP access is immediately activated on the switch.

7. To permanently save the changes, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

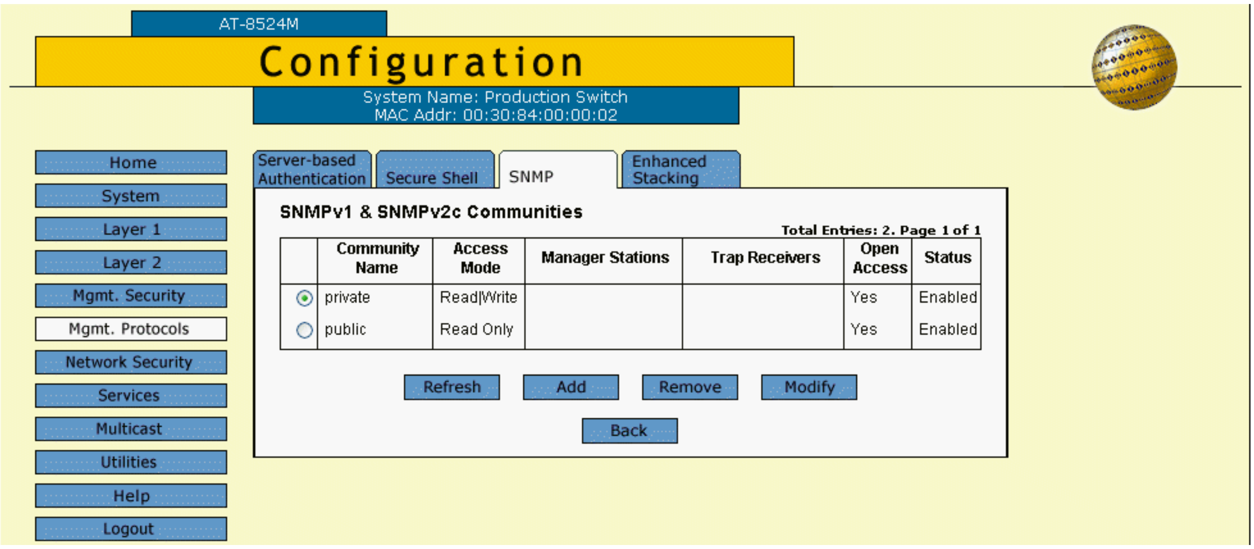
Creating a SNMPv1 or SNMPv2c Community String

To create a new SNMPv1 or SNMPv2c community string, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 11 on page 48.
4. Click **Configure** in the SNMPv1/v2c section of the tab.

   The SNMP tab for SNMPv1 and SNMPv2c community strings is shown in Figure 12.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

SNMPv1 & SNMPv2c Communities

Total Entries: 2. Page 1 of 1

	Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
●	private	Read|Write			Yes	Enabled
○	public	Read Only			Yes	Enabled

Figure 12 SNMP (SNMPv1 and SNMPv2c) Tab

The community strings already existing on the switch are displayed in the table. The columns are defined below:

Community Name
The name of a community string.

Access Mode
Whether the string's access is read/write or read only.

Manager Stations
The IP addresses of management stations that can use the community string to access the switch. This only applies if the string has a closed access status.

Trap Receivers
The IP addresses of management stations to receive SNMP traps from the switch.

Open Access

Displays the opened or closed access status of the string:

Yes - The string’s status is open, meaning any management workstation can use it.

No - The string’s status is closed, meaning only those workstations whose IP addresses have been assigned to the string can use it.

Status

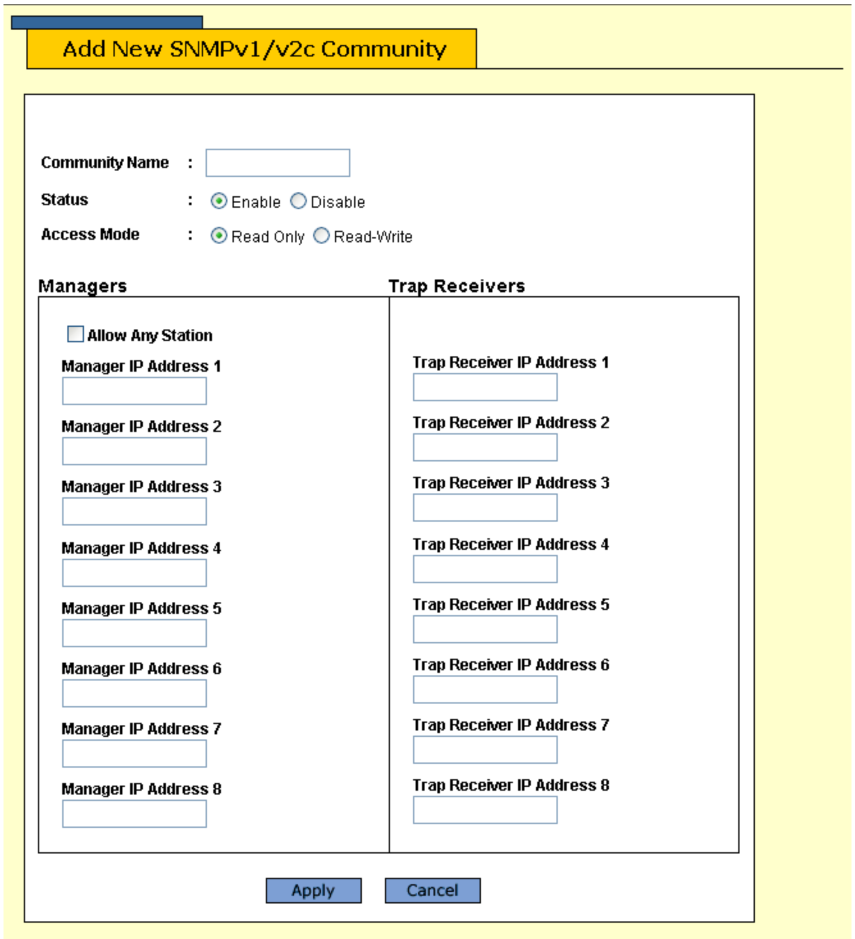
Displays whether the string is enabled or disabled. The possible settings are:

Enabled - The string can be used to access the switch.

Disabled - The string cannot be used to access the switch.

5. Click **Add**.

   The Add New SNMP Community page is shown in Figure 13.



Add New SNMPv1/v2c Community

Community Name :

Status : ● Enable ○ Disable

Access Mode : ● Read Only ○ Read-Write

Managers

□ Allow Any Station

Manager IP Address 1

Manager IP Address 2

Manager IP Address 3

Manager IP Address 4

Manager IP Address 5

Manager IP Address 6

Manager IP Address 7

Manager IP Address 8

Trap Receivers

Trap Receiver IP Address 1

Trap Receiver IP Address 2

Trap Receiver IP Address 3

Trap Receiver IP Address 4

Trap Receiver IP Address 5

Trap Receiver IP Address 6

Trap Receiver IP Address 7

Trap Receiver IP Address 8

Figure 13 Add New SNMPv1/v2c Community Page

6. In the Community Name field, enter the new community string. The name can be from one to fifteen alphanumeric characters. Spaces are allowed.
7. Use the Status option to either enable or disable the community string. A disabled community string cannot be used to access the switch. The default is enabled.
8. Use the Access Mode option to specify the access mode for the new SNMP community string. If you specify Read Only, the community string will only allow you to view the MIB objects on the switch. If you specify Read/Write, the community string will allow you to both view and change the SNMP MIB objects on the switch.
9. Use the Allow Any Station option to set the community string as opened or closed. If there is no check in the box next to the option, the community string is closed; only those workstations whose IP addresses are assigned to the community string can use it. If there is a check in the box, the string is open, meaning any SNMP management workstation can use it to access the switch.
10. If you specified the community string as closed, enter the IP addresses of up to eight management workstations in the Manager IP Address fields. These are the management workstations that can use the string.
11. If you want the switch to send traps, enter the IP addresses of up to eight trap receivers in the Trap Receiver IP Address fields.
12. Click **Apply**.

    The new community string is now available on the switch.
13. Repeat this procedure starting with step 3 to add more community strings.
14. To permanently save your changes, select the **Save Config** menu option.

Modifying a Community String

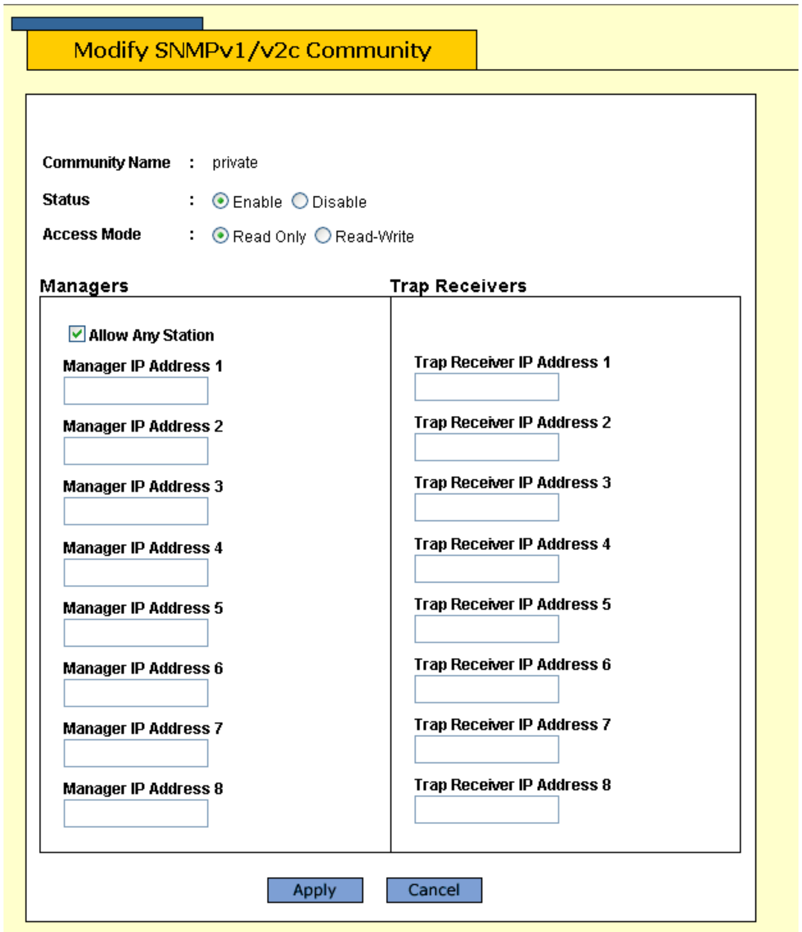
To modify a community string, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 11 on page 48.
4. Click **Configure** in the SNMPv1/v2c section of the tab

   The SNMP tab for SNMPv1 and SNMPv2c is shown in Figure 12 on page 50.
5. Click the button next to the community string you want to modify.
6. Click **Modify**.

   The Modify SNMP Community page is shown in Figure 14.


Modify SNMPv1/v2c Community

Community Name : private

Status : ● Enable ○ Disable

Access Mode : ● Read Only ○ Read-Write

☑ Allow Any Station

Managers
Trap Receivers
Manager IP Address 1
Manager IP Address 2
Manager IP Address 3
Manager IP Address 4
Manager IP Address 5
Manager IP Address 6
Manager IP Address 7
Manager IP Address 8
Trap Receiver IP Address 1
Trap Receiver IP Address 2
Trap Receiver IP Address 3
Trap Receiver IP Address 4
Trap Receiver IP Address 5
Trap Receiver IP Address 6
Trap Receiver IP Address 7
Trap Receiver IP Address 8
Apply
Cancel

Figure 14 Modify SNMPv1/v2c Community Page

Note
You cannot change the name of a community string.

7. Use the Status option to either enable or disable the community string. A disabled community string cannot be used to access the switch.

8. Use the Access Mode option to change the access mode of the community string. If you specify Read Only, the community string will only allow you to view the MIB objects on the switch. If you specify Read/Write, the community string will allow you to both view and change the SNMP MIB objects on the switch.

9. Use the Allow Any Status option to change the open and close status of the community string. If there is no check in the box next to the option, the community string is closed; only those workstations whose IP addresses are assigned to the community string can use it. If there is a check in the box, then the status is open, meaning that any SNMP management workstation can use it to access the switch.

10. If the community string as closed, enter, delete, or modify the IP addresses of up to eight management workstations in the Manager IP Address fields. These are the management workstations that can use the string.

11. If you want the switch to send traps, enter, delete, or modify the IP addresses of up to eight trap receivers in the Trap Receiver IP Address fields.

12. Click **Apply**.

    The modified community string is now available on the switch.

13. To permanently save the changes, select the **Save Config** menu option.

Deleting a Community String

To delete a community string, do the following:

1. From the Home page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 11 on page 48.
4. Click **Configure** in the SNMPv1/v2c section of the tab.

   The SNMP tab for SNMPv1 and SNMPv2c is shown in Figure 12 on page 50.
5. Click the button next to the community string you want to delete. You can select only one community string.
6. Click **Remove**.

   A confirmation prompt is displayed.
7. Click **OK**. The community string is deleted from the switch.
8. To permanently save the change, select the **Save Config** menu option.

Displaying the SNMP Status and Community Strings

To display the SNMPv1 and SNMPv2c community strings on the switch, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** menu option.
3. Select the **SNMP** tab.

   The information in the tab includes:

   SNMP Access
   Whether SNMP access is enabled or disabled.

   Authentication Failure Trap
   Whether the authentication failure trap is enabled or disabled.

4. Click **View** in the SNMPv1/v2c section of the tab.

   The information in the tab is described below:

   Community Name
   The community string.

   Access
   Whether access is read/write or read only.

   Manager Stations
   The IP addresses of the management stations that can use a community string to access the switch. This only applies if the string has a closed access status.

   Trap Receivers
   IP addresses of management stations to receive SNMP traps from the switch.

   Open Access
   Displays the opened or closed access status of the string:

   Yes - The string's status is open, meaning that any workstation can use it.

   No - The string's status is closed, meaning that only those workstations whose IP addresses have been assigned to the string can use it.

   Status
   Displays the status of the string. The possible values are:

   Enabled - The string can be used to access the switch.

   Disabled - The string cannot be used to access the switch.

Chapter 5

Port Parameters

This chapter explains how to view and change the parameter settings for the individual ports on a switch. Examples of the parameters that you can adjust include port speed and duplex mode.

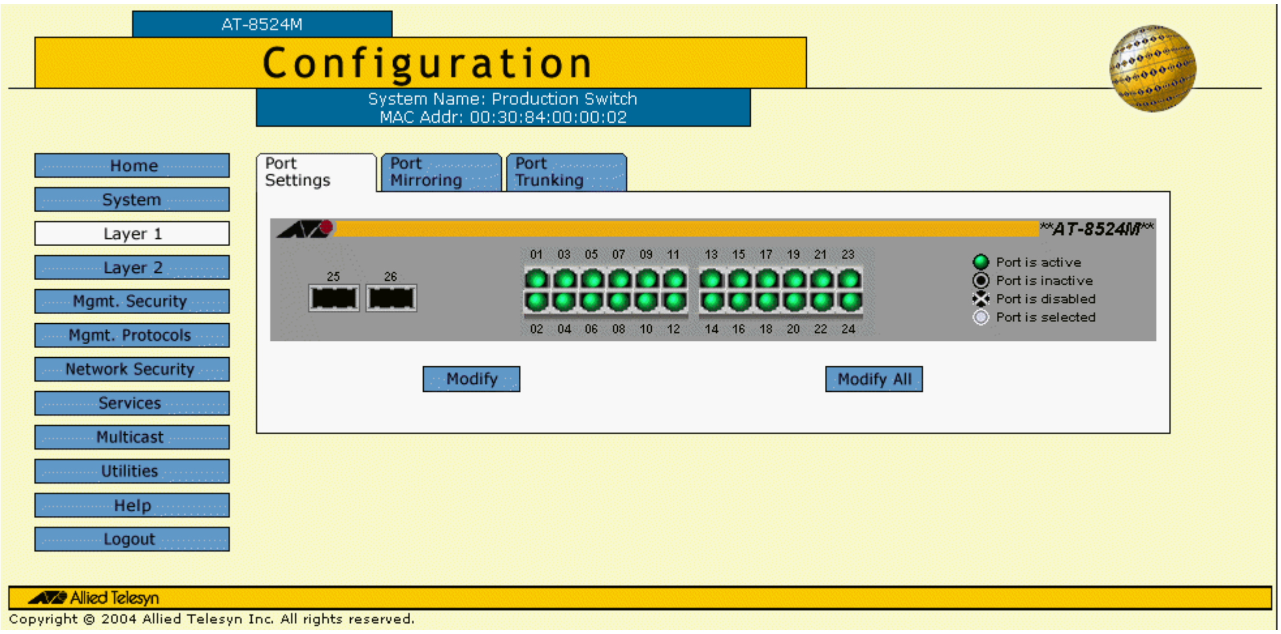
This chapter contains the following procedures:

Configuring Port Parameters

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

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Settings** tab.

   The Port Settings tab is shown in Figure 15.



AT-8524M

Configuration

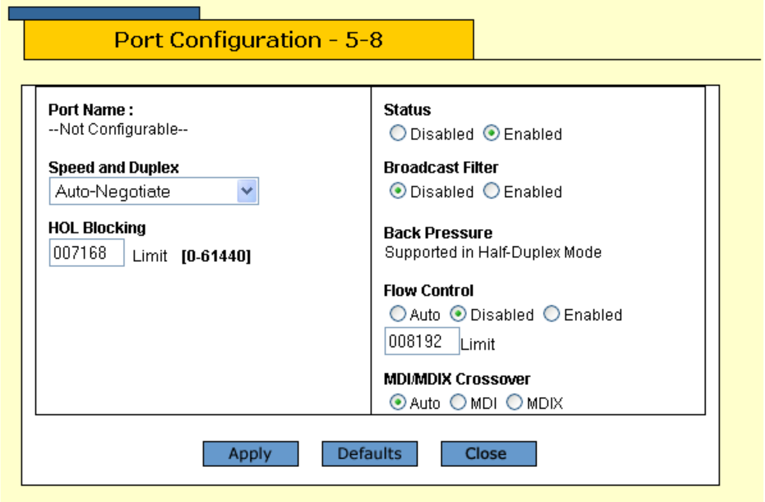
System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Copyright © 2004 Allied Telesyn Inc. All rights reserved.

Figure 15 Port Settings Tab (Configuration)

4. Click the port in the graphical switch image you want to configure. The selected port turns white. You can configure more than one port at a time. (To deselect a port, click it again.)
5. Click **Modify**. To configure all of the base ports (not including any expansion ports), click **Modify All**.

The Port Configuration page is shown Figure 16.



Port Configuration - 5-8

Port Name :
--Not Configurable--

Speed and Duplex
Auto-Negotiate

HOL Blocking
007168 Limit [0-61440]

Status
○ Disabled ● Enabled

Broadcast Filter
● Disabled ○ Enabled

Back Pressure
Supported in Half-Duplex Mode

Flow Control
○ Auto ● Disabled ○ Enabled
008192 Limit

MDI/MDIX Crossover
● Auto ○ MDI ○ MDIX

Figure 16 Port Configuration Page

Note
The Port Configuration page in the figure above is for a 10/100 Mbps twisted pair port. The page for a fiber optic port will contain a subset of the parameters.

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

The **Defaults** button returns the port settings to the default values, which are listed in Appendix A in the *AT-S62 Menus Interface User's Guide*.

6. Adjust the port parameters as needed.

The parameters are described below.

Port Name
You use this selection to assign a name to a port. The name can be from one to fifteen alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points. (You cannot assign a name when you are configuring more than one port.)

Speed and Duplex
You use this selection to configure the speed and duplex mode of a port. For a twisted pair port, you can select Auto-Negotiation or you can set its speed and duplex mode manually. For a fiber optic port, you can set the duplex mode.

If you are configuring a twisted pair port and you select Auto-Negotiation, which is the default setting, the port's speed, duplex mode, and MDI/MDI-X settings are set automatically.

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

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

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

❑ If you disable Auto-Negotiation on a port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. Consequently, if you disable Auto-Negotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Here are the possible settings for a twisted pair port:

❑ Auto: The port uses Auto-Negotiation to set both speed and duplex mode. This is the default.

❑ 10Mbps - Half Duplex

❑ 10Mbps - Full Duplex

❑ 100Mbps - Half Duplex

❑ 100Mbps - Full Duplex

Note
Ports 49R and 50R on an AT-8550GB Series switch must be set to Auto-Negotiation in order to operate at 1000Mbps. You cannot manually configure these ports to 1000Mbps.

Here are the possible settings for a fiber optic port:

❑ Half Duplex

❑ Full Duplex: This is the default setting

HOL Blocking

For a definition of Head of Line Blocking, refer to the *AT-S62 Menus Interface User's Guide*.

This parameter can prevent Head of Line Blocking from occurring on a port. The parameter sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port. The number for this value represents cells. A cell is 64 bytes. The range is 1 to 61,440 cells. The default is 7,168.

Status

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

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation.

You might also want to disable a port that is not being used to secure it from unauthorized connections.

Possible settings for this parameter are:

Enabled	The port will receive and forward packets. This is the default setting.
Disabled	The port will not receive or forward packets.

Broadcast Filter

Most frames on an Ethernet network are usually unicast frames. A unicast frame is a frame that is sent to a single destination. A node sending a unicast frame intends the frame for a particular node on the network. For example, when a node sends a file to a network server for storage, the node sends the file in unicast Ethernet frames containing the destination address of the server where the file is to be stored.

Broadcast frames are different. Broadcast frames are directed to all nodes on the network or all nodes within a particular virtual LAN. Broadcast packets can perform a variety of functions. For example, some network operating systems use broadcast frames to announce the presence of devices on a network.

The problem with broadcast frames is that too many of them traversing a network can impact network performance. The more bandwidth consumed by broadcast frames, the less available for unicast frames.

Should the performance of your network be impacted by heavy broadcast traffic, you can use this parameter to limit the number of broadcast frames forwarded by the switch and so limit the number of broadcast frames on your network.

When you activate this feature on a port, the port will discard all egress broadcast packets. That is, if the port has a broadcast packet that is intended to be sent to the end node connected to the port, the port will instead discard the packet.

It should be noted that the filtering takes place only on egress broadcast packets—packets that a port is transmitting. This filter does not apply to ingress broadcast packets.

Possible settings for this parameter are:

Enabled	The port will not transmit any broadcast frames.
Disabled	The port will transmit broadcast frames. This is the default setting.

Back Pressure
Sets backpressure on a port. This option only applies to ports operating in half-duplex mode. A switch port uses backpressure to control the flow of ingress packets.

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

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

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

The Limit field specifies the maximum number of ingress packets that a port will accept within a 1 second period before initiating backpressure. The range is 1 to 57,344. The default is 8192.

Flow Control
Sets flow control on the port. This option applies only to ports operating in full-duplex mode.

A switch port uses flow control to control the flow of ingress packets from its end node.

A port using flow control issues a special frame, referred to as a PAUSE frame, as specified in the IEEE 802.3x standard, to stop the transmission of data from an end node. When a port needs to stop an end node from transmitting data, it issues this frame. The frame instructs the end node to cease transmission. The port continues to issue PAUSE frames until it is ready again to receive data from the end node.

The default setting for flow control on a switch port is disabled.

Possible values are:

Auto - The port will use flow control if it detects that the end node is using it.

Disabled - No flow control on the port.

Enabled - Flow control is activated.

Limit - Specifies the maximum number of ingress packets that a port will receive within a 1 second period before initiating flow control. The range is 1 to 57,344 packets. The default is 8192.

MDI/MDIX Crossover
Use this selection to set the wiring configuration of the port. The configuration can be Auto, MDI, or MDI-X. The default setting is Auto.

The default Auto setting activates the auto-MDI/MDI-X feature on a port, which enables a port to configure itself automatically as MDI or MDI-X when connected to an end node. This allows you to use a straight-through twisted pair cable when connecting any type of network device to a port on the switch.

The Auto setting is only available when a port is set to Auto-Negotiate its speed and duplex mode. It is also the only setting available when a port's speed and duplex are set through Auto-Negotiation.

The auto-MDI/MDI-X feature is not available if you disable Auto-Negotiation on a port and set a port's speed and duplex mode manually. A port where Auto-Negotiation has been disabled defaults to MDI-X. Disabling Auto-Negotiation may require that you manually configure a port's MDI/MDI-X setting using this option or use a crossover cable.

7. Once you have made the desired changes, click **Apply**.

   The switch activates the parameter changes on the port.

8. To permanently save the changes, select the **Save Config** menu option.

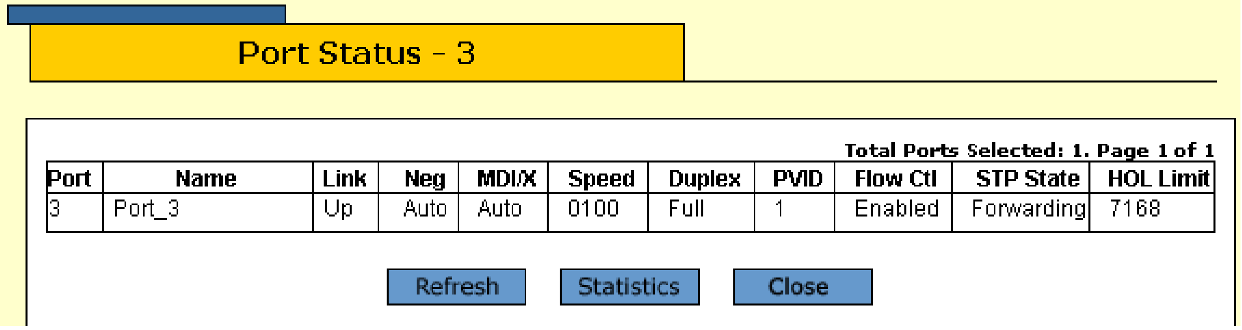
Displaying Port Status and Statistics

The procedure in this section displays the operating status of the ports on a switch and port statistics. You can view a port's operating speed, duplex mode, MDI/MDI-X configuration, and more. You can also view the operating status of any GBIC modules installed in an AT-8550GB.

To display the status or statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.
3. Select the **Port Settings** tab.
4. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
5. Click **Status** to display the port's operating status or **Statistics** to display port statistics.

   If you select port status, the Port Status page in Figure 17 is displayed.



Port Status - 3

Total Ports Selected: 1. Page 1 of 1

Port	Name	Link	Neg	MDI/X	Speed	Duplex	PVID	Flow Ctl	STP State	HOL Limit
3	Port_3	Up	Auto	Auto	0100	Full	1	Enabled	Forwarding	7168

Figure 17 Port Status Page

The information in this page is for viewing purposes only. To adjust port parameters, refer to Configuring Port Parameters on page 58.

The columns in the page are described below:

Port
The port number.

Name
The name of the port.

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

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

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

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

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

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

MDI/X
The operating configuration of the port. Possible values are MDI and MDI-X.

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

0010 - 10 Mbps

0100 - 100 Mbps

1000 - 1000 Mbps (Optional expansion ports only.)

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

PVID
The port VLAN identifier assigned to the port.

Flow Control
The port's flow control setting. Possible values are:

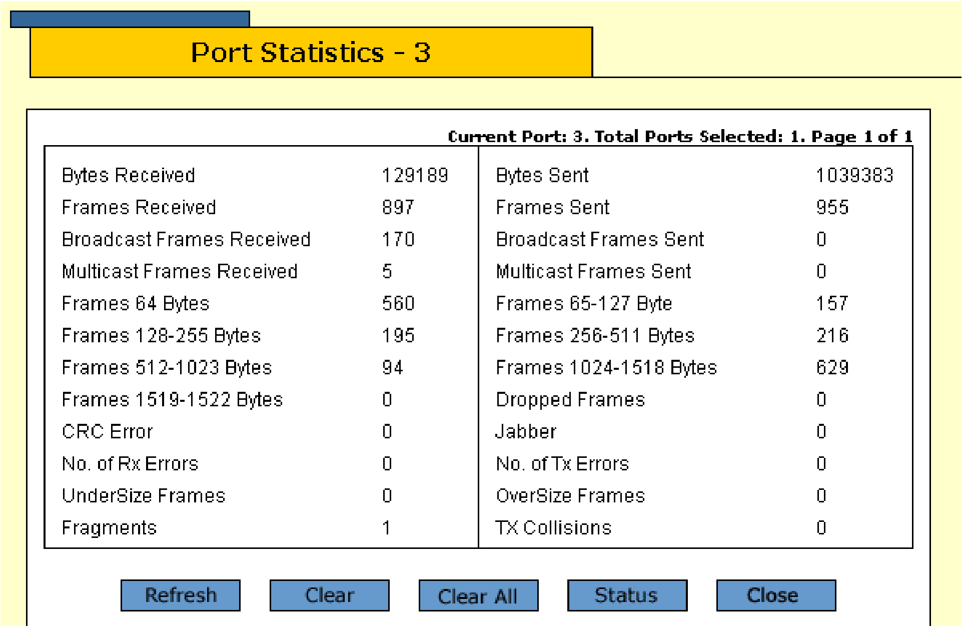
Enabled - Flow control is enabled on the port.

Disabled - Flow control is disabled on the port.

STP State
The operating status of the port. Possible values are Forwarding, Blocking, Listening, and Learning.

HOL Limit
The utilization threshold of a port's egress queue which initiates the Head of Line Blocking prevention mechanism. The number for this value represents cells. A cell is 64 bytes. The range is 1 to 61,440 cells. The default is 7,168.

If you select Statistics, the Statistics page in Figure 18 is displayed.



Port Statistics - 3

Current Port: 3. Total Ports Selected: 1. Page 1 of 1

Bytes Received	129189	Bytes Sent	1039383
Frames Received	897	Frames Sent	955
Broadcast Frames Received	170	Broadcast Frames Sent	0
Multicast Frames Received	5	Multicast Frames Sent	0
Frames 64 Bytes	560	Frames 65-127 Byte	157
Frames 128-255 Bytes	195	Frames 256-511 Bytes	216
Frames 512-1023 Bytes	94	Frames 1024-1518 Bytes	629
Frames 1519-1522 Bytes	0	Dropped Frames	0
CRC Error	0	Jabber	0
No. of Rx Errors	0	No. of Tx Errors	0
UnderSize Frames	0	OverSize Frames	0
Fragments	1	TX Collisions	0

Figure 18 Port Statistics Page

The information in this page is for viewing purposes only. The statistics are defined below:

Bytes Received
Number of bytes received on the port.

Bytes Sent
Number of bytes transmitted from the port.

Frames Received
Number of frames received on the port.

Frames Sent
Number of frames transmitted from the port.

Broadcast Frames Received
Number of broadcast frames received on the port.

Broadcast Frames Sent
Number of broadcast frames transmitted from the port.

Multicast Frames Received
Number of multicast frames received on the port.

Multicast Frames Sent
Number of multicast frames transmitted from the port.

Frames 64 Bytes
Frames 65 - 127 Bytes
Frames 128 - 255 Bytes
Frames 256 - 511 Bytes
Frames 512 - 1023 Bytes

Frames 1024 - 1518 Bytes
Frames 1519 - 1522 Bytes
Number of frames transmitted from the port, grouped by size.

Dropped Frames
The number of frames successfully received and buffered by the port, but subsequently discarded.

CRC Error
Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Jabber
Number of occurrences of corrupted data or useless signals appearing on the port.

No. of Rx Errors
Total number of frames received on the port containing errors.

Undersize Frames
Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Frames
Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received on the port.

The Clear button at the bottom of the statistics page clears all the counters for the selected port. The Clear All button clears the counters for all of the ports on the switch.

Tx Collisions
Total number of collisions detected on the port. Occurs only on ports operating in half duplex mode.

Chapter 6

MAC Address Table

This chapter contains instructions on how to view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❑ Displaying the MAC Address Table on page 69
- ❑ Adding Static Unicast and Multicast MAC Addresses on page 72
- ❑ Deleting Unicast and Multicast MAC Addresses on page 74
- ❑ Deleting All Dynamic Unicast and Multicast MAC Addresses on page 75
- ❑ Changing the Aging Time on page 76

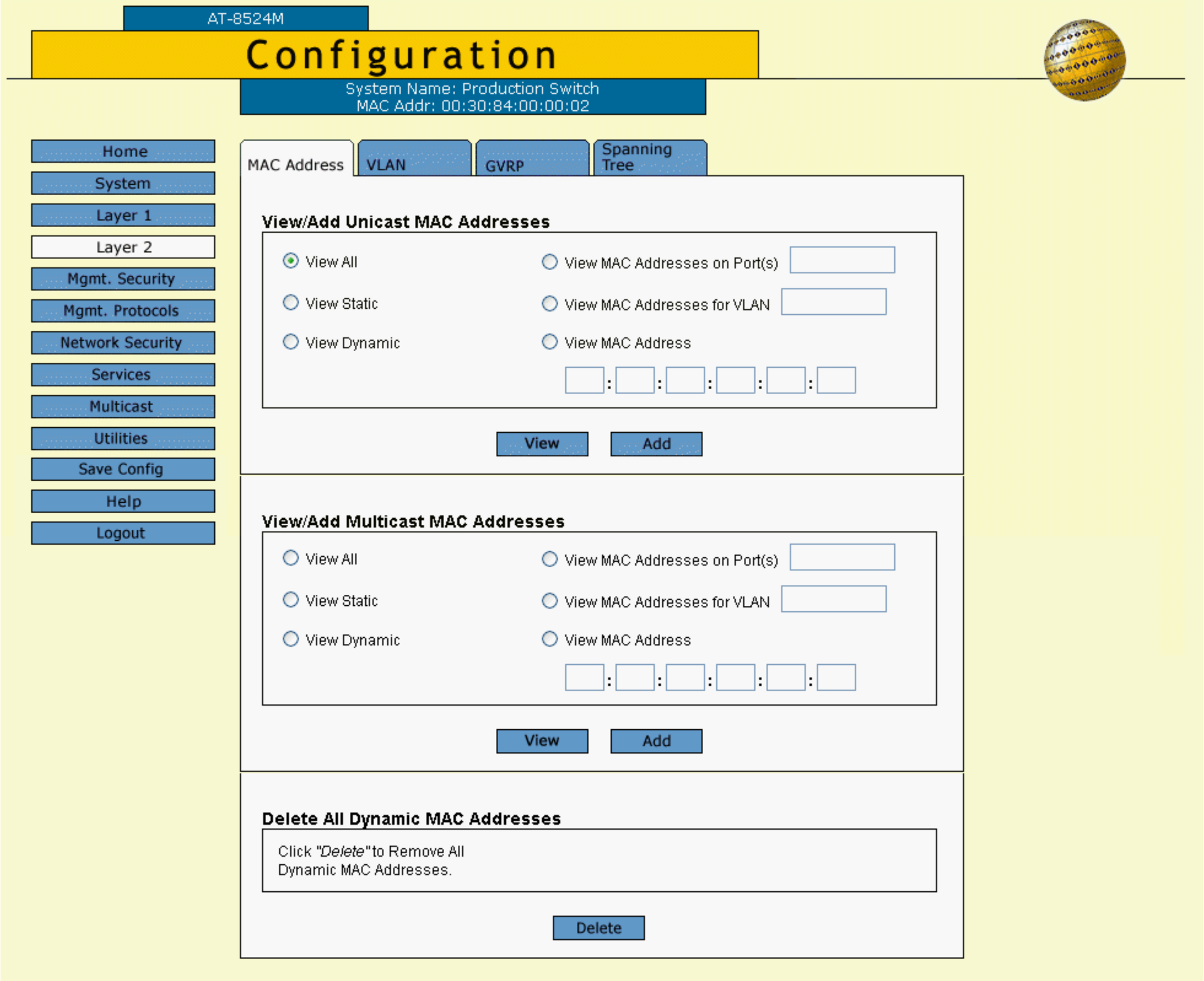
Note
For background information on the MAC address table, refer to the *AT-S62 Menus Interface User's Guide*.

Displaying the MAC Address Table

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

1. From the Home page, select either **Configuration** or **Monitoring**.
2. Select the **Layer 2** menu option.
3. Select the **MAC Address** tab.

   Figure 19 shows how the tab appears when displayed through the Configuration page. If displayed through the Monitoring page, the Add buttons and the Delete section at the bottom of the window are not included. The buttons are used to add static and multicast address to the switch as explained in Adding Static Unicast and Multicast MAC Addresses on page 72. The Delete section is used to delete all dynamic MAC addresses, as explained in Deleting All Dynamic Unicast and Multicast MAC Addresses on page 75.



View/Add Unicast MAC Addresses

● View All ○ View MAC Addresses on Port(s)

○ View Static ○ View MAC Addresses for VLAN

○ View Dynamic ○ View MAC Address

View/Add Multicast MAC Addresses

○ View All ○ View MAC Addresses on Port(s)

○ View Static ○ View MAC Addresses for VLAN

○ View Dynamic ○ View MAC Address

Delete All Dynamic MAC Addresses

Click "*Delete*"to Remove All
Dynamic MAC Addresses.

Figure 19 MAC Address Tab (Configuration)

The top section displays unicast addresses while the middle section displays multicast addresses. The options function the same in both sections, and are described below. You can select only one option at a time.

The default selection is the View All option for multicast MAC addresses. To avoid displaying the wrong MAC addresses, check to be sure that you have selected the desired unicast or multicast address option before clicking a View button.

View All
This selection displays all dynamic addresses learned on the ports of the switch and all static addresses that have been assigned to the ports.

View Static
This selection displays just the static addresses assigned to the ports on the switch.

View Dynamic
This selection displays just the dynamic addresses learned on the ports on the switch.

View MAC Addresses on Port
Displays the dynamic and static MAC addresses of a particular port. You can specify more than one port at a time.

View MAC Addresses for VLAN
Displays the static and dynamic addresses learned on the tagged and untagged ports of a specific VLAN. You specify the VLAN by entering the VLAN ID number. You can specify only one VLAN at a time.

View MAC Address
Displays the port number on which a MAC address was assigned or learned.

In some situations, you might want to know which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The procedure in this section offers an easier way. You can specify the MAC address and let the management software automatically locate the port on the switch where the device is connected.

4. After you select an option, click **View**.

   The columns in the MAC address page are defined below.

   MAC Address - The static or dynamic unicast MAC address.

   Port(s) - The port on which the address was learned or assigned. The MAC address with port “CPU” is the address of the switch.

Vlan ID - The ID number of the VLAN where the port is a member.

Type - The type of the address: static or dynamic.

Adding Static Unicast and Multicast MAC Addresses

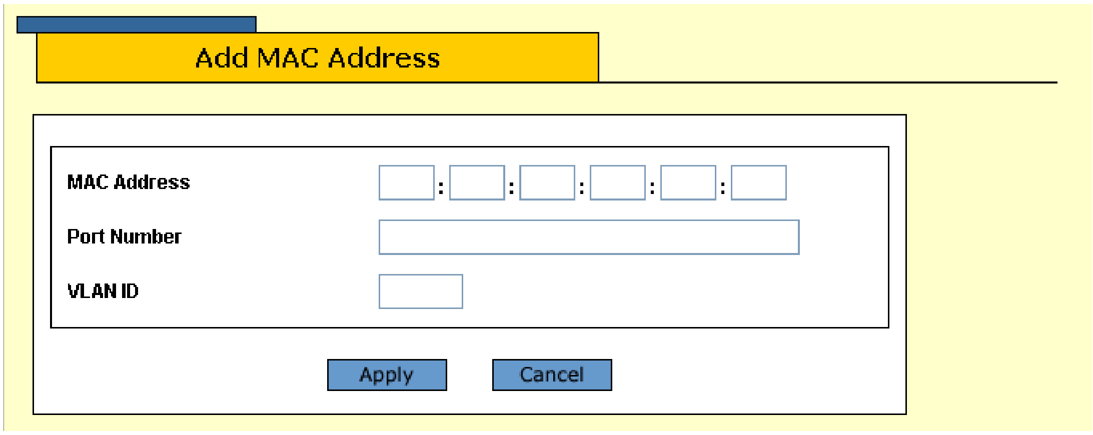
This section contains the procedure for assigning a static unicast or multicast address to a port on the switch. You can assign up to 255 static MAC addresses per port.

To add a static address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Layer 2** menu option.
3. Select the **MAC Address** tab.

   The MAC Address tab is shown in Figure 19 on page 69.
4. To add a static unicast address, in the View/Add Unicast MAC Addresses section, click **Add**. To add a static multicast address, in the View/Add Multicast MAC Addresses section, click **Add**.

   The Add MAC Address page is shown in Figure 20.



Add MAC Address

MAC Address : : : : :

Port Number

VLAN ID

Figure 20 Add MAC Address Page

5. In the MAC Address field, enter the new static unicast or multicast MAC address.
6. In the Port Number field, enter the number of the port on the switch where you want to assign the static address. If you are adding a static unicast address, you can enter only one port.

   If you are entering a static multicast address, you must specify the port when the multicast application is located as well as the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located will result in the failure of the multicast packets to be properly forwarded to the host nodes. You can specify the ports individually (e.g., 1,4,5), as a range (e.g., 11-14) or both (e.g., 15-17,22,24).

7. In the VLAN ID field, enter the VLAN ID where the port is a member.
8. Click **Apply**.
9. Repeat this procedure to add other static addresses to the switch.
10. To permanently save the change, select the **Save Config** menu option.

Deleting Unicast and Multicast MAC Addresses

To delete a specific static or dynamic unicast or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Layer 2** menu option.
3. Select the **MAC Address** tab.

   The MAC Address tab is shown in Figure 19 on page 69.
4. Display the MAC addresses on the switch by selecting one of the options. For instructions, refer to Displaying the MAC Address Table on page 69.
5. Click on the button next to the MAC address you want to delete from the switch.
6. Click **Remove**.

   Note
   You cannot delete the switch's MAC (CPU) address, an STP BPDU MAC address, or a broadcast address.

7. To permanently save the change, select the **Save Config** menu option.

Deleting All Dynamic Unicast and Multicast MAC Addresses

To delete all dynamic unicast and multicast MAC addresses from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. Select the **MAC Address** tab.

   The MAC Address tab is shown in Figure 19 on page 69.
4. Click **Delete** in the Delete All Dynamic MAC Addresses section.

   The switch deletes all dynamic MAC addresses from its table and begins to learn new addresses as packets arrive on the ports.

Changing the Aging Time

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

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **General** tab.

   The General tab is shown in Figure 7 on page 32.

4. In the Configuration section of the tab, enter a new value in seconds for the MAC Address Aging Time. The range is 0 to 1048575 seconds. The default is 300 seconds (5 minutes). The value 0 (zero) disables the aging timer. When disabled, no dynamic addresses are deleted from the table, even addresses that belong to inactive nodes.
5. Click **Apply**.
6. To permanently save the change, select the **Save Config** menu option.

Chapter 7
Static Port Trunks

This chapter contains the procedure for creating, modifying, or deleting a static port trunk from a web browser management session.

Sections in this chapter include:

Note
For background information and guidelines on static port trunks, refer to the *AT-S62 Menus Interface User's Guide*.

Creating a Static Port Trunk

This section contains the procedure for creating a static port trunk on the switch. Be sure to review the static port trunk guidelines in the *AT-S62 Menus Interface User's Guide* before performing the procedure.

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

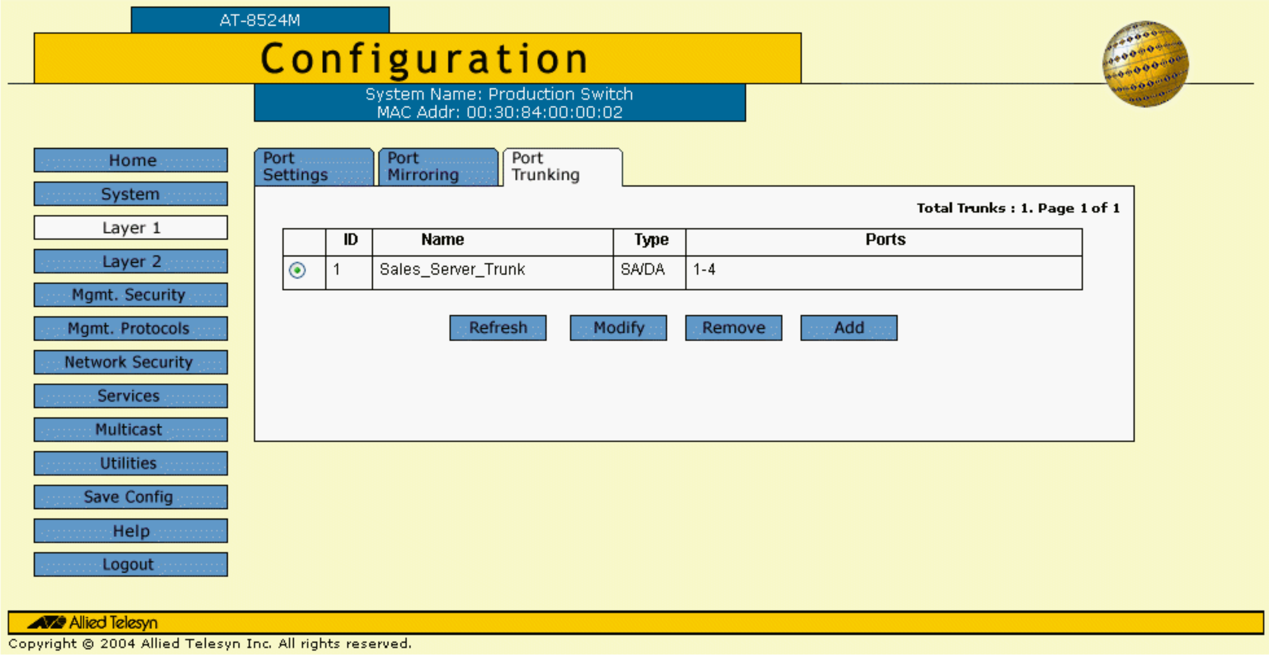
Note
Before you create a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port that will be a part of the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S62 management software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

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

To create a static port trunk, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select **Layer 1**.
3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 21.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Total Trunks : 1. Page 1 of 1

	ID	Name	Type	Ports
●	1	Sales_Server_Trunk	SA/DA	1-4

Copyright © 2004 Allied Telesyn Inc. All rights reserved.

Figure 21 Port Trunking Tab

This tab lists the existing trunks. Columns in the tab are defined below:

ID
The ID number of the trunk.

Name
The name of the trunk.

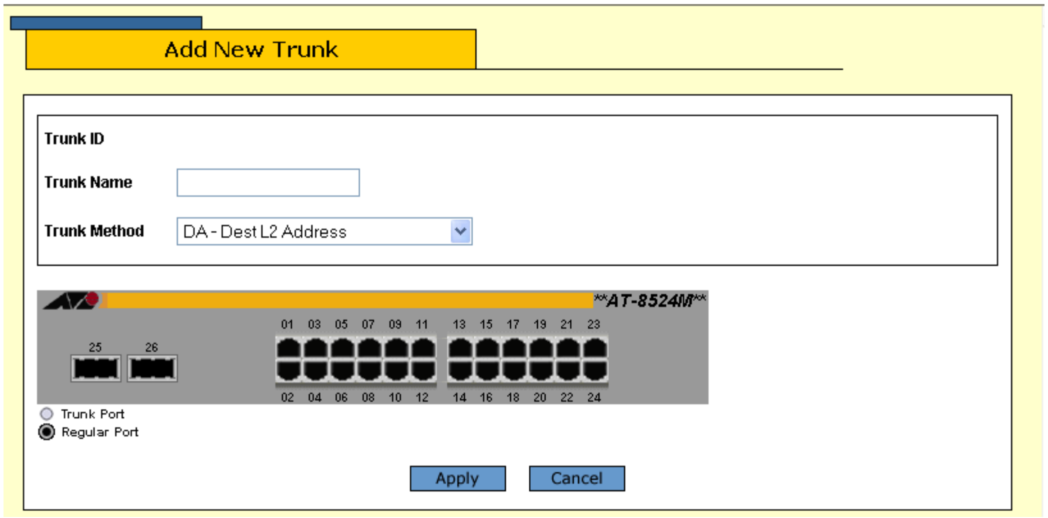
Type
The load distribution method:

- □ SA - Source MAC address (Layer 2)
- □ DA - Destination MAC address (Layer 2)
- □ SA/DA - Source MAC address /destination MAC address (Layer 2)
- □ SI - Source IP address (Layer 3)
- □ DI - Destination IP address (Layer 3)
- □ SI/DI - Source IP address /destination IP address (Layer 3)

Ports
The ports of the trunk.

4. Click **Add**.

The Add New Trunk page is shown in Figure 22.



Add New Trunk

Trunk ID

Trunk Name

Trunk Method DA - Dest L2 Address

○ Trunk Port
● Regular Port

Figure 22 Add New Trunk Page

5. In the Trunk Name field, enter a name for the port trunk. The name can be up to sixteen alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must be given a unique name.
6. From the Trunk Method list, select a distribution method. Options are:
   - ❑ SA - Source MAC address (Layer 2)
   - ❑ DA - Destination MAC address (Layer 2)
   - ❑ SA/DA - Source MAC address /destination MAC address (Layer 2)
   - ❑ SI - Source IP address (Layer 3)
   - ❑ DI - Destination IP address (Layer 3)
   - ❑ SI/DI - Source IP address /destination IP address (Layer 3)
7. Click the ports that will make up the port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.
8. Click **Apply**. The new port trunk is now active on the switch.
9. To permanently save the change, click the **Save Config** menu option.
10. Configure the ports on the remote switch for port trunking.
11. Connect the cables to the ports of the trunk on the switch.

    The port trunk is ready for network operations.

Modifying a Static Port Trunk

This section contains the procedure for modifying a static port trunk on the switch. You can change the name of a trunk and the ports that constitute the trunk. You cannot change the load distribute method. Be sure to review the static trunk guidelines in the *AT-S62 Menus Interface User's Guide* before performing the procedure.

⚠ **Caution**

If you will be adding or removing ports from the trunk, you should disconnect all data cables from the ports of the trunk on the switch before performing the procedure. Adding or removing ports from a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

Note the following before performing this procedure:

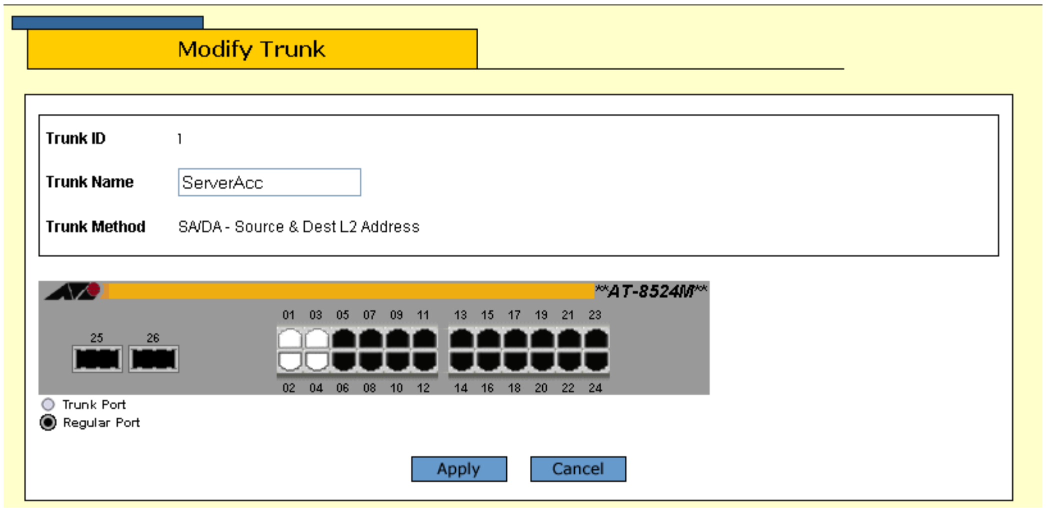
- ❑ If you are adding a port and the port will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you should check to see if its settings are appropriate prior to adding it.
- ❑ If you are adding a port and the port will not be the lowest numbered port in the trunk, its settings will be changed to match the settings of the existing ports in the trunk.
- ❑ If you are adding a port to a trunk, you should check to be sure that the new port is an untagged member of the same VLAN as the other trunk ports. A trunk cannot contain ports that are untagged members of different VLANs.

To modify a port trunk, do the following:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select **Layer 1**.
3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 21 on page 79.
4. Click the button next to the port trunk you want to modify and click **Modify**.

An example of the Modify Trunk page is shown in Figure 23.



Modify Trunk

Trunk ID 1

Trunk Name ServerAcc

Trunk Method SA/DA - Source & Dest L2 Address

○ Trunk Port
● Regular Port

Figure 23 Modify Trunk Page

Note
You cannot change the Trunk ID number or the load distribution method of a port trunk.

5. To change the name of the trunk, click the Trunk Name field and modify the name as needed. The name can be up to sixteen alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

6. To add or remove ports from a trunk, click the ports in the graphical image of the switch. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.

7. Click **Apply**.

   Changes to a port trunk are immediately activated on the switch.

8. To permanently save the change, click the **Save Config** menu option.

9. Reconnect the cables to the ports of the trunk.

Deleting a Static Port Trunk

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

To delete a static port trunk from the switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select **Layer 1**.
3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 21 on page 79.
4. Click the button next to the static port trunk you want to delete and click **Remove**.

   The port trunk is deleted from the switch.
5. To permanently save the change, click the **Save Config** menu option.

Displaying the Static Port Trunks

To display the static port trunks on the switch, do the following:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** menu option.
3. Select the **Port Trunking** tab.

   The Port Trunking tab displays the following information:

   ID
   The ID number of the trunk.

   Name
   The name of the trunk.

   Type
   The load distribution method:

   ❑ SA - Source MAC address (Layer 2)

   ❑ DA - Destination MAC address (Layer 2)

   ❑ SA/DA - Source/destination MAC address (Layer 2)

   ❑ SI - Source IP address (Layer 3)

   ❑ DI - Destination IP address (Layer 3)

   ❑ SI/DI - Source/destination IP address (Layer 3)

   Ports
   The ports of the trunk.

Chapter 8

Port Mirroring

This chapter contains the procedure for creating or deleting a port mirror. Sections in the chapter include:

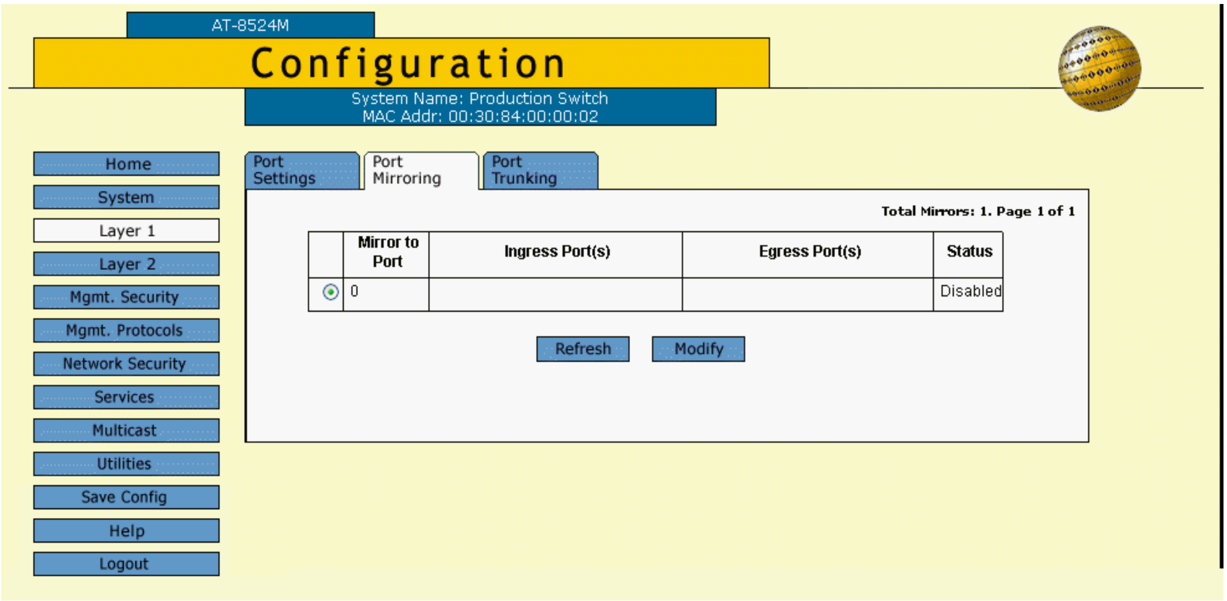
Note
For background information and guidelines on port mirroring, refer to the *AT-S62 Menus Interface User's Guide*.

Creating a Port Mirror

To create or delete a port mirror, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select **Layer 1**.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 24.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Total Mirrors: 1. Page 1 of 1

	Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
⦿	0			Disabled

Figure 24 Port Mirroring Tab (Configuration)

This tab displays any port mirror already existing on the switch. The columns are defined below:

Mirror to Port
This is the destination port where the traffic will be copied to and where the network analyzer will be located. There can be only one destination port. A 0 (zero) in this column indicates there is no port mirror on the switch.

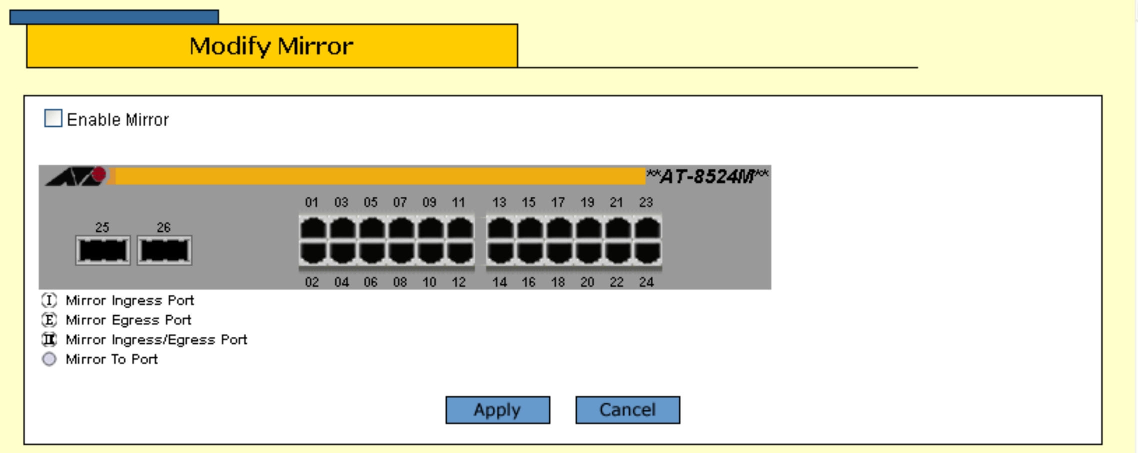
Ingress Port(s)
This column lists the source ports whose ingress traffic is mirrored to the destination port.

Egress Port(s)
This column lists the source ports whose egress traffic is mirrored to the destination port.

Status
This column contains the status of the mirroring feature. If enabled, traffic is being copied to the destination port. If disabled, no traffic is being mirrored.

4. Click **Modify**.

   The Modify Mirror page is shown in Figure 25.



Modify Mirror

□ Enable Mirror

(I) Mirror Ingress Port
(E) Mirror Egress Port
(IE) Mirror Ingress/Egress Port
○ Mirror To Port

Figure 25 Modify Mirror Page

5. Click the ports of the port mirror. Clicking a port toggles it through the possible settings, which are shown here:

   □ The destination (mirror) port. There can be only one destination port.

   I A source port. The port’s ingress traffic will be mirrored to the destination port.

   E A source port. The port’s egress traffic will be mirrored to the destination port.

   IE A source port. The port’s ingress and egress traffic will be mirrored to the destination port.

   You can mirror one port, a few ports, or all of the ports on the switch, with the exception, of course, of the destination port.

Figure 26 shows an example of the Modify Mirror page configured for a port mirror. The egress traffic on Ports 11 and 12 is mirrored to the destination Port 5.

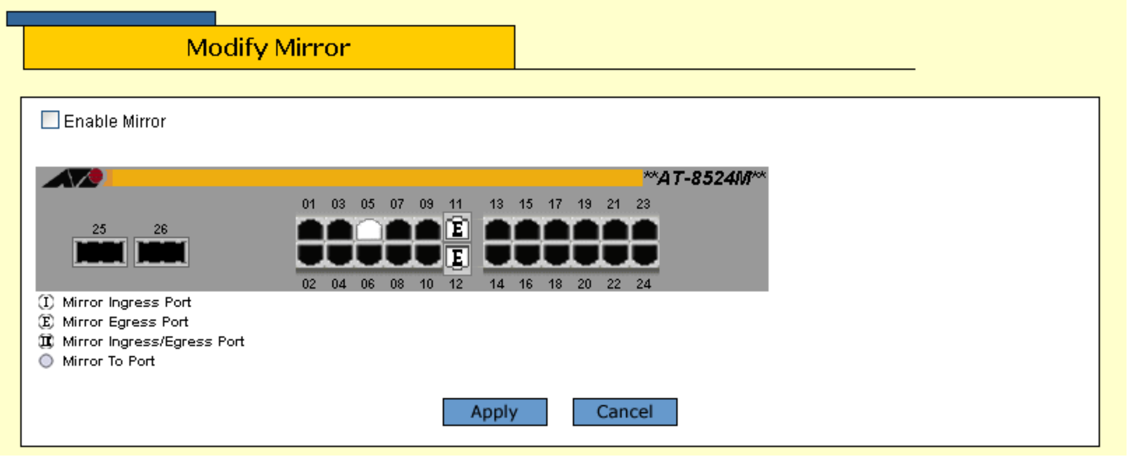


Figure 26 Example of a Modify Mirror Page

6. After selecting the destination and source ports, click the **Enable Mirror** check box.

7. Click **Apply**.

   The port mirror is now active on the switch. You can connect a data analyzer to the destination port to monitor the traffic on the source ports.

8. To permanently save the change, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

Modifying or Disabling a Port Mirror

To modify a port mirror, you perform the same procedure that you did to create it, as explained in Creating a Port Mirror on page 86. But before modifying it, you should first disable it using the Enable Mirror option in the Modify Mirror page. Once you have made the necessary modifications, enable the mirror again and click **Apply**.

To permanently save the change, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

Deleting a Port Mirror

To delete a port mirror so that you can use the destination port for normal network operations, perform the procedure Creating a Port Mirror on page 86. Disable the port mirror using the Enable Mirror option and then click the destination port to change it from white to black. Once black, the port is available for normal network operations. Then click **Apply**.

To permanently save the change, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

Displaying the Port Mirror

To display the port mirror, do the following:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The information in the tab is described below:

   Mirror to Port
   The destination port where the traffic is copied to and where the network analyzer is located.

   Ingress Port(s)
   The source ports whose ingress traffic is mirrored to the destination port.

   Egress Port(s)
   The source ports whose egress traffic is mirrored to the destination port.

   Status
   The status of the mirroring feature. If enabled, traffic is being copied to the destination port. If disabled, no traffic is being mirrored.

Section II

Advanced Operations

The chapters in this section explain how to manage an AT-8524M switch from a local or Telnet management session. The chapters include:

Chapter 9
File System

This chapter contains instructions on how to display the files stored in the switch’s file system and select a new active boot configuration file. This chapter contains the following procedure:

❑ Viewing System Files or Changing the Active Configuration File on page 94

Note
For background information on the file system and boot configuration files, refer to the *AT-S62 Menus Interface User’s Guide*.

Viewing System Files or Changing the Active Configuration File

This procedure displays the files stored in the switch's file system. This procedure also explains how to change the active boot configuration file on the switch. The active boot configuration file is used by the switch to configure its operating parameters whenever the unit is reset or power cycled. The active boot file is also the file that is updated whenever you select the Save Config option.

Note the following before performing this procedure:

- ❑ You cannot create a new configuration file from a web browser management session. That function must be performed from a local, Telnet, or SSH session.
- ❑ You cannot copy, rename, delete, or view the contents of files in the file system from a web browser management session. Those tasks must be performed from a local, Telnet, or SSH session.

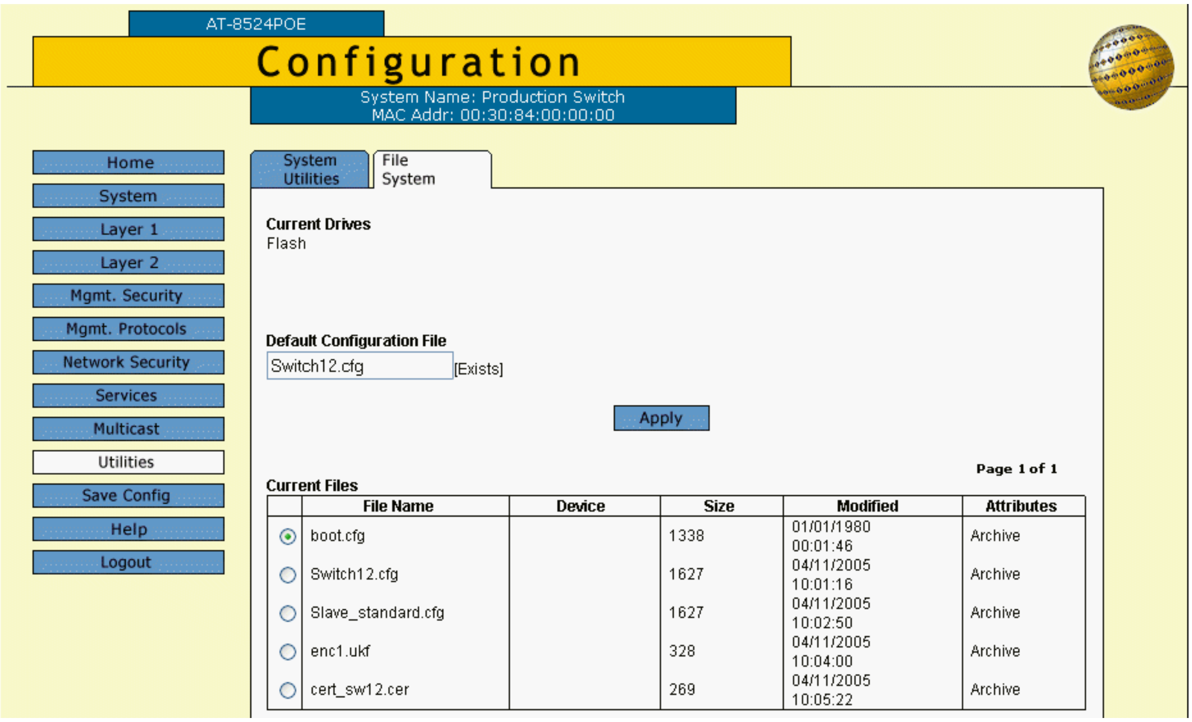
To change the active boot configuration file or to view system files, perform the following procedure:

1. From the Home Page, select **Configuration** or **Monitoring**.

   To change the active boot configuration file, select Configuration.

2. From the Configuration or Monitoring menu, select the **Utilities** menu option.
3. Select the **File System** tab.

The File System tab is shown in Figure 27.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Current Drives
Flash

Default Configuration File
Switch12.cfg [Exists]

Page 1 of 1

Current Files

	File Name	Device	Size	Modified	Attributes
●	boot.cfg		1338	01/01/1980 00:01:46	Archive
○	Switch12.cfg		1627	04/11/2005 10:01:16	Archive
○	Slave_standard.cfg		1627	04/11/2005 10:02:50	Archive
○	enc1.ukf		328	04/11/2005 10:04:00	Archive
○	cert_sw12.cer		269	04/11/2005 10:05:22	Archive

Figure 27 File System Tab

The information in the tab is defined below:

Current Drive

Specifies the location of the file system. The AT-8500 Series switch has just one file system, located in flash memory. This will always indicate Flash. This cannot be changed.

Default Configuration File

Specifies the filename of the active configuration file. The switch uses this file to configure its operating parameters whenever it is reset or power cycled. The active boot file is also the file that is updated whenever you select the Save Config option.

Current Files

Lists the files stored in the file system. The columns are defined here:

File Name - The name of the system file.

Device - The storage location of the file. This column will be empty for all files on an AT-8500 Series switch.

Size - The size of the file in kilobytes.

Modified - The date the file was created or last modified.

Attributes - This can be any of the following:

- ❑ Normal
- ❑ Read Only
- ❑ Hidden
- ❑ System
- ❑ Volume
- ❑ Directory
- ❑ Archive
- ❑ Invalid

4. To change the active boot configuration file, enter the name of the file in the Default Configuration Field field. The file must already exist in the file system. You can select a configuration file that you created on the switch or that you downloaded onto the switch from another switch.

> **Note**
> You cannot create a new boot configuration file from the web browser interface.

5. Click **Apply**.

   The switch checks to be sure that the file exists and then displays the file name with “Exists” following it, meaning that the switch found the file. The file has now been designated as the new active boot configuration file for the switch.

   If the switch could not locate the file, the name of the previous boot configuration file is displayed again. Repeat steps 4 and 5, being sure to enter the name correctly.

6. Do one of the following:

   - ❑ To configure the switch using the parameter settings in this boot configuration file, do **not** select Save Config. Instead, reset or power cycle the switch.
   - ❑ To overwrite the settings in the configuration file with the switch’s current operating settings, select **Save Config**.

Chapter 10

File Downloads and Uploads

This chapter contains the procedure for downloading a new AT-S62 image file onto the switch from a web browser management session. This chapter also contains procedures for uploading and downloading system files, such as a boot configuration file, from the file system in the switch. This chapter contains the following section:

Downloading a File

This procedure explains how to download a file from a TFTP server on your network to the switch using the web browser interface. You can download any of the following files:

- ❑ AT-S62 image file
- ❑ Boot configuration file
- ❑ Public key
- ❑ CA certificate

Note
The public key and CA certificate are only supported on the version of AT-S62 management software that features SSL, PKI, and SSH security.

⚠ **Caution**
Installing a new AT-S62 image file will invoke a switch reset. Some network traffic may be lost.

Note the following before you begin this procedure:

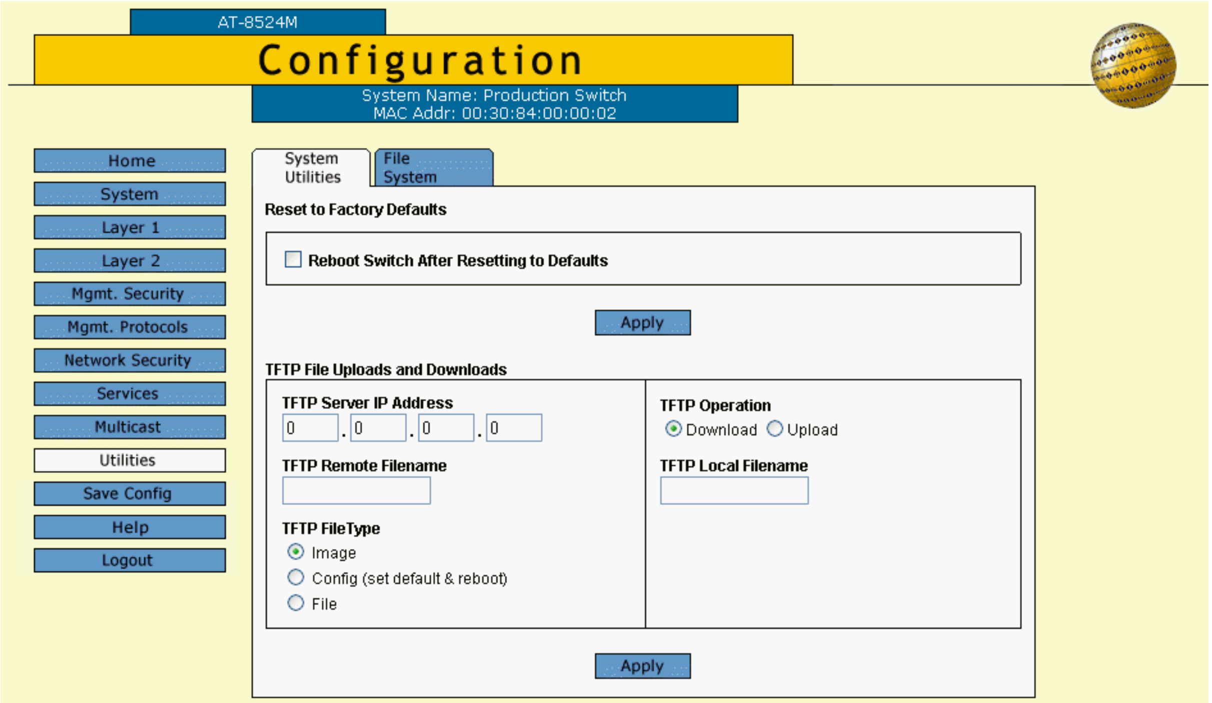
- ❑ You must use TFTP to download a file from a web browser management session.
- ❑ There must be a node on your network that has TFTP server software.
- ❑ The file to be downloaded must be stored on the TFTP server node.
- ❑ You should start the TFTP server before you begin the download procedure.
- ❑ The AT-S62 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- ❑ Installing a new AT-S62 software image does not change the current configuration of a switch (for instance, IP address, subnet mask, and virtual LANs).
- ❑ The switch on which you are downloading the file must have an IP address and subnet mask, such as a master switch of an enhanced stack. You cannot use TFTP on a slave switch, since that type of switch typically does not have an IP address. Rather, you would need to perform the download from a local management session

of the switch using Xmodem or, alternatively, switch to switch. For instructions, refer to the *AT-S62 Menus Interface User’s Guide*.

To download a file, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Utilities** menu option.
3. Select the **System Utilities** tab.

   The System Utilities tab is shown in Figure 28.



Reset to Factory Defaults

□ Reboot Switch After Resetting to Defaults

TFTP File Uploads and Downloads

TFTP Server IP Address: 0 . 0 . 0 . 0

TFTP Operation: ● Download ○ Upload

TFTP Remote Filename:

TFTP Local Filename:

TFTP FileType:
● Image
○ Config (set default & reboot)
○ File

Figure 28 System Utilities Tab

> **Note**
> The top portion of the tab returns the switch to its factory default settings. For instructions, refer to Returning the AT-S62 Software to the Factory Default Values on page 45.

4. In the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
5. In the TFTP Operation field, click **Download**.
6. In the TFTP Remote Filename field, enter the filename of the file on the TFTP server to be downloaded to the switch.

7. In the TFTP Local Filename field, enter a name for the file. This is the name that the switch will store the file as in its file system. If you are downloading the AT-S62 image file, enter "ats62.img" as the filename.

8. In the TFTP File Type, select one of the following:

   ❑ Image - Select this option to download a new AT-S62 image file.

   ❑ Config (set default and reboot) - Select this option to download a configuration file that is to be designated as the active boot configuration file on the switch.

   ❑ File - Select this option to download a CA certificate or a configuration file that you do not want designated as the active boot configuration file.

9. Click **Apply**.

   The management software will notify you once the download is complete.

⚠ **Caution**

If you are downloading a system image file, the switch must decompress it and write it to flash after it has been downloaded. This can require one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file. Once the file has been decompressed, the switch automatically resets. Your web browser management session will end. To continue managing the switch, you must reestablish the management session.

Note

If you downloaded a configuration file using the Config selection, the switch automatically designates it as the active configuration file and resets.

Uploading a File

This procedure explains how to upload a file from the switch's file system to a TFTP server on your network using the web browser interface. You can upload any of the following files:

- ❑ Boot configuration file
- ❑ Public encryption key
- ❑ CA certificate
- ❑ CA enrollment request
- ❑ Event log file

Note
The public key, CA certificate, and CA enrollment request are only supported on the version of AT-S62 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- ❑ You must use TFTP to upload a file using a web browser management session.
- ❑ There must be a node on your network that contains the TFTP server software.
- ❑ You should start the TFTP server before you begin the upload procedure.
- ❑ The switch from which you are uploading a file must have an IP address and subnet mask, such as a master switch of an enhanced stack. You cannot use TFTP on a slave switch, since that type of switch typically does not have an IP address. Rather, you would need to perform the upload from a local management session of the switch using Xmodem. For instructions, refer to the *AT-S62 Menus Interface User's Guide*.

To upload a file, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Utilities** menu option.
3. Select the **System Utilities** tab.

   The System Utilities tab is shown in Figure 28 on page 99.

Note
The top portion of the tab returns the switch to its factory default settings. For instructions, refer to Returning the AT-S62 Software to the Factory Default Values on page 45.

4. In the TFTP Server IP Address field, enter the IP address of the network node with the TFTP server software.

5. In the TFTP Operation field, click **Upload**.

6. In the TFTP Remote Filename field, enter a name for the file. This is the name that the file will be stored as on the TFTP server.

7. In the TFTP Local Filename field, enter the name of the file in the switch's file system that you want to upload to the TFTP server.

Note
The TFTP File Type options are not used when uploading a file.

8. Click **Apply**.

   The management software notifies you once the upload is complete.

Chapter 11

Event Log and Syslog Servers

This chapter describes the event log and syslog servers. Sections in the chapter include:

- ❑ Managing the Event Log on page 104
- ❑ Managing Syslog Server Definitions on page 112

Note
For background information on the event log and syslog server definitions, refer to the *AT-S62 Menus Interface User's Guide*.

Managing the Event Log

The event log contains event messages that are generated by a switch. These events can provide vital information about network activity on an AT-8500 Series switch that can help you identify and solve network problems. The information includes the time and date when an event occurred, the event's severity, the AT-S62 module that generated the event, and an event description.

The following procedures explain how to view the events in the event log as well as how to enable or disable the log. Procedures include:

❑ Enabling or Disabling the Event Log on page 104

❑ Displaying the Event Log on page 106

❑ Modifying the Event Log Full Action on page 110

❑ Saving the Event Log on page 111

❑ Clearing the Event Log on page 111

Enabling or Disabling the Event Log

This procedure explains how to enable or disable the event log on the switch. If you disable the log, the AT-S62 management software will not store events in its log and will not send events to any syslog servers you might have defined. The default setting for the event log is enabled.

The event log, even when disabled, will log all AT-S62 initialization events that occur whenever the switch is reset or power cycled. Any switch events that occur after AT-S62 initialization are entered into the log only if it is enabled.

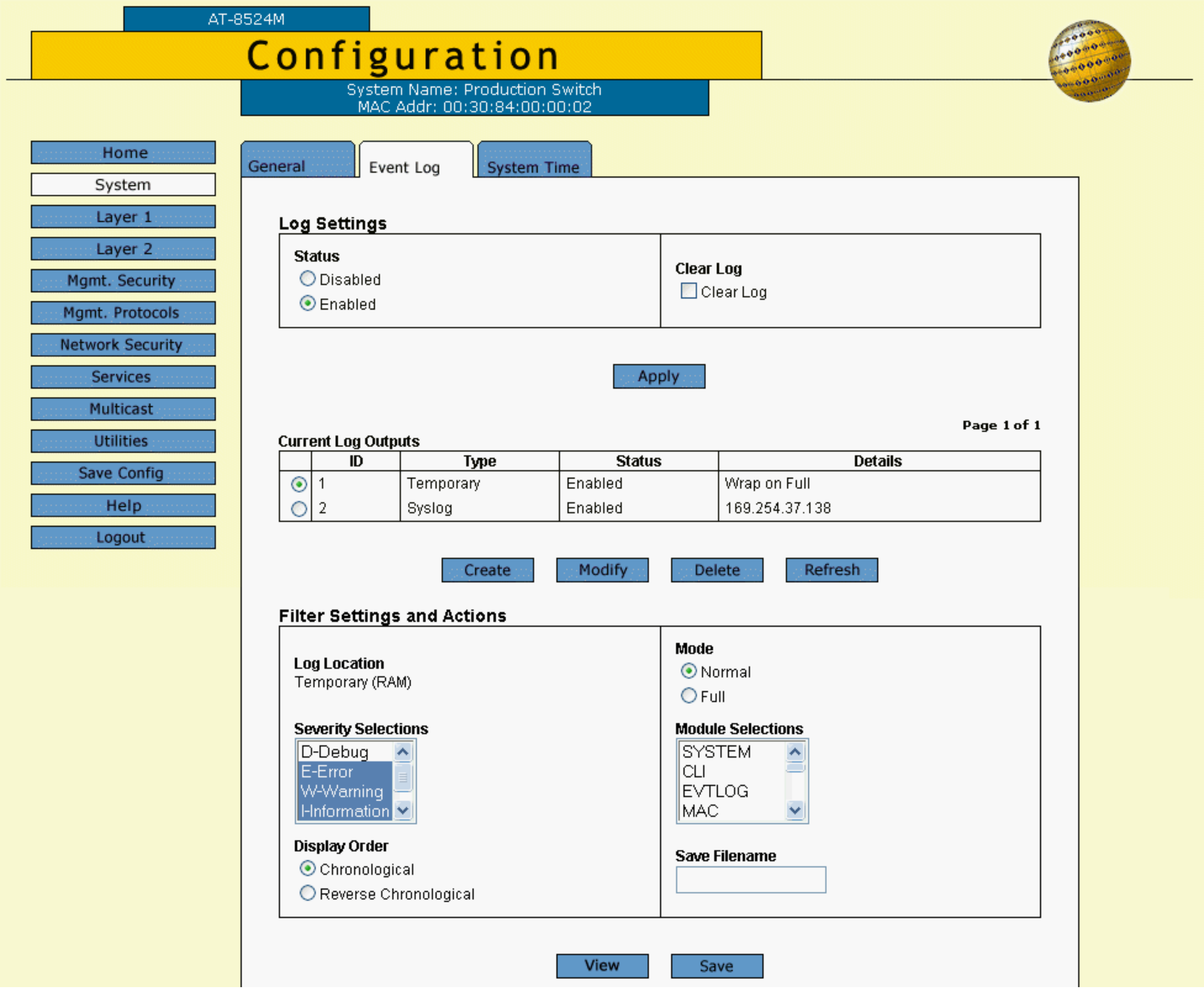
Note
Allied Telesyn recommends setting the switch's date and time if you enable the event log. Otherwise, the entries entered in the log and sent to a syslog server will not have the correct date and time. For instructions, refer to Setting the System Time on page 41.

To enable or disable the event log on a switch, do the following:

To enable or disable the event log, do the following:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.

The Event Log tab is shown in Figure 29.



Log Settings

Status
○ Disabled
● Enabled

Clear Log
□ Clear Log

Page 1 of 1

Current Log Outputs

	ID	Type	Status	Details
●	1	Temporary	Enabled	Wrap on Full
○	2	Syslog	Enabled	169.254.37.138

Filter Settings and Actions

Log Location
Temporary (RAM)

Severity Selections
D-Debug
E-Error
W-Warning
I-Information

Display Order
● Chronological
○ Reverse Chronological

Mode
● Normal
○ Full

Module Selections
SYSTEM
CLI
EVTLOG
MAC

Save Filename

Figure 29 Event Log Tab

4. For Status in Log Settings, click either **Disable** or **Enable**. If you enable the log, the switch immediately begins to add events in the log and send events to defined syslog servers. The default is enabled.

5. Click **Apply**.

6. To permanently save the change, select the **Save Config** menu selection.

   To display the events in the log, go to the next procedure.

Displaying the Event Log

To view the event log, do the following:

1. From the Home Page, click either **Configuration** or **Monitoring**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
4. Configure the following options:

   Severity Selections
   Displays events of a selected severity. Event severity is a predefined value assigned to an event according to its potential impact on switch operation. There are four severity levels, as defined in Table 1. The default is informational, error, and warning. You can specify more than one severity (for example, E,W).

Table 1 Event Log Severity Levels

Value	Severity Level	Description
ALL	-	Selects all severity levels
E	Error	Switch operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for Technical Support and Software Development.

   Display Order
   Controls the order of the events in the log. Choices are Chronological, which displays the events in the order oldest to newest, and Reverse Chronological, which displays the events newest to oldest. The default is Chronological.

   Mode
   Controls the format of the event log. Choices are Normal, which displays the time, module, severity, and description for each event, and Full, which displays the same information as Normal, plus filename, line number, and event ID. The default is Normal.

   Module Selections
   Displays events of a selected AT-S62 module. The AT-S62 management software consists of a number of modules, each responsible for a different part of switch operation. You can instruct the switch to display only those events that apply to selected modules. The default is ALL, which displays the events for

all modules. You can display more than one module at a time by holding down the Shift key when making a selection. The modules are defined in Table 2.

Table 2 AT-S62 Modules

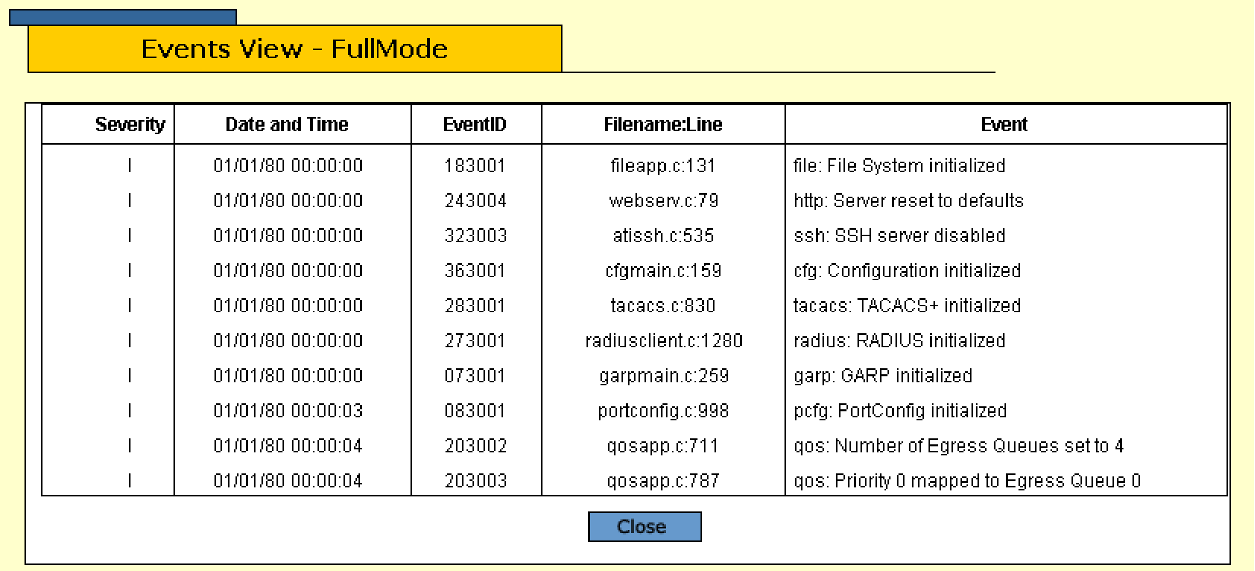
Module Name	Description
ALL	All modules
ACL	Access control list
CFG	Configuration files
CLASSIFIER	ACL and QoS policy classifiers
CLI	Command line interface commands
DOS	Denial of service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	Switch IP configuration, DHCP, and BOOTP
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
PACCESS	802.1x port-based access control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
POE	Power over Ethernet (AT-8524POE switch only)
PSEC	Port security (MAC address-based)

Table 2 AT-S62 Modules

Module Name	**Description**
PTRUNK	Port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
Telnet	Telnet
TFTP	TFTP
Time	SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

5. Once you have set the log filters, click **View**.

Figure 30 shows an example of the event log in the Full display mode. The Normal display mode does not include the Filename, Line Number, and Event ID items.



Severity	Date and Time	EventID	Filename:Line	Event
I	01/01/80 00:00:00	183001	fileapp.c:131	file: File System initialized
I	01/01/80 00:00:00	243004	webserv.c:79	http: Server reset to defaults
I	01/01/80 00:00:00	323003	atissh.c:535	ssh: SSH server disabled
I	01/01/80 00:00:00	363001	cfgmain.c:159	cfg: Configuration initialized
I	01/01/80 00:00:00	283001	tacacs.c:830	tacacs: TACACS+ initialized
I	01/01/80 00:00:00	273001	radiusclient.c:1280	radius: RADIUS initialized
I	01/01/80 00:00:00	073001	garpmain.c:259	garp: GARP initialized
I	01/01/80 00:00:03	083001	portconfig.c:998	pcfg: PortConfig initialized
I	01/01/80 00:00:04	203002	qosapp.c:711	qos: Number of Egress Queues set to 4
I	01/01/80 00:00:04	203003	qosapp.c:787	qos: Priority 0 mapped to Egress Queue 0

Figure 30 Event Log Example

The columns in the log are described below:

❑ S (Severity) - The event's severity. Table 1 on page 106 defines the different severity levels.

❑ Date/Time - The date and time the event occurred.

❑ Event ID - A unique number that identifies the event. (Displayed only in the Full display mode.)

❑ Filename:Line - The subpart of the AT-S62 module and the line number that generated the event. (Displayed only in the Full display mode.)

❑ Event - The module within the AT-S62 software that generated the event followed by a brief description of the event. For a list of the AT-S62 modules, see Table 2 on page 107.

Modifying the Event Log Full Action

This procedure explains how to control what the log will do once it reaches its maximum capacity of 4,000 events. You have two options. The first is to have the switch delete the oldest entries as it adds new entries to the log. The second is to have the switch stop adding entries, so as to preserve the existing log contents.

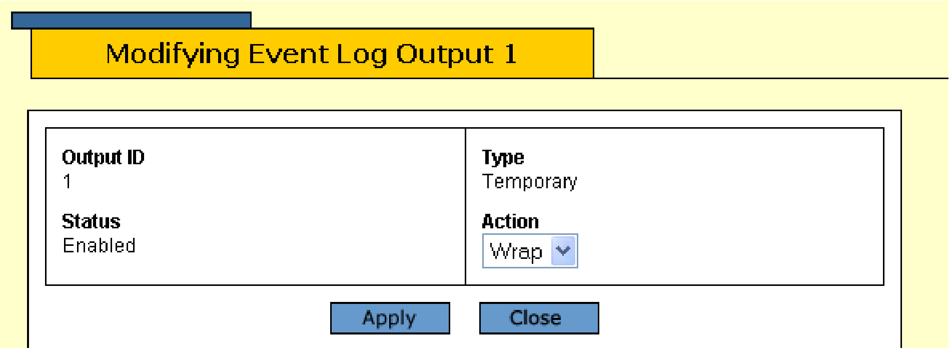
This procedure is only relevant when viewing the event log through a local or remote management session. If you defined syslog servers, the switch continues to send events to a syslog server even when the log is full.

To configure the event log, do the following procedure:

1. From the Home Page, click either **Configuration**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
4. Under Current Log Outputs, select Output 1, Temporary, and click **Modify**.

   The Modifying Event Log Output 1 window is shown in Figure 31.



Modifying Event Log Output 1

Output ID
1

Status
Enabled

Type
Temporary

Action
Wrap

Figure 31 Modifying Event Log Output 1 Window

5. Using the Action pull-down menu, select one of the following:

   Wrap
   The switch deletes the oldest entries as it adds new entries.

   Halt
   The switch stops adding entries when the log reaches maximum capacity of 4,000 entries.
6. Click **Apply**.
7. To permanently save the change, select the **Save Config** menu selection.

Saving the Event Log

You can save the current events in the log as a file in the file system, from where you can view it or download it to your management workstation. To save the current events, do the following:

1. From the Home Page, click either **Configuration**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
4. In the Filter Settings and Actions section of the tab, adjust the settings to indicate which events you want to save to the file. For information on the settings, refer to Displaying the Event Log on page 106.
5. In the Save Filename field, enter a name for the file. The name can be up to 16 alphanumeric characters, followed by a 3 letter extension. The extension should be ".log".
6. Click **Save**.

   The selected events are immediately saved to the file system. For instructions on how to upload the file to a TFTP server, refer to Uploading a File on page 101.

Clearing the Event Log

To clear all events from the log, perform the following procedure:

1. From the Home Page, click **Configuration**.
2. From the System page, select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
3. In Log Settings, click **Clear Log**.
4. Click **Apply**.

   The log, if enabled, immediately begins to learn new events.

Managing Syslog Server Definitions

You can configure the switch to send its events to a syslog server. A syslog server can store the events of many network devices simultaneously. Storing network events on a syslog server can make managing your network easier since you need only go to one site to see all of the events.

Here are the guidelines to observe when using this feature:

❑ You can define up to 19 syslog servers.

❑ The event log on the switch must be enabled in order for the switch to send events. For instructions, refer to Enabling or Disabling the Event Log on page 104.

❑ The switch must have an IP address and subnet mask. This rule applies to slave switches, which typically do not have an IP address, as well as master switches. If you want a slave switch to send its events to a syslog server, you must assign it an IP address and a subnet mask.

❑ The syslog server must communicate with the switch through the switch's management VLAN. The AT-S62 management software uses the management VLAN to watch for and transmit management packets. The default management VLAN is Default_VLAN. For background information on the management VLAN, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring the switch to send its events to a syslog server involves creating a syslog server definition. The definition contains the IP address of the syslog server along with other information, such as what types of messages you want the switch to send.

This section contains the following procedures:

❑ Creating a Syslog Server Definition on page 113

❑ Modifying a Syslog Server Definition on page 117

❑ Deleting a Syslog Server Definition on page 117

❑ Viewing a Syslog Server Definition on page 118

Creating a Syslog Server Definition

To create a syslog server definition, perform the following procedure:

1. From the Home Page, click **Configuration**.

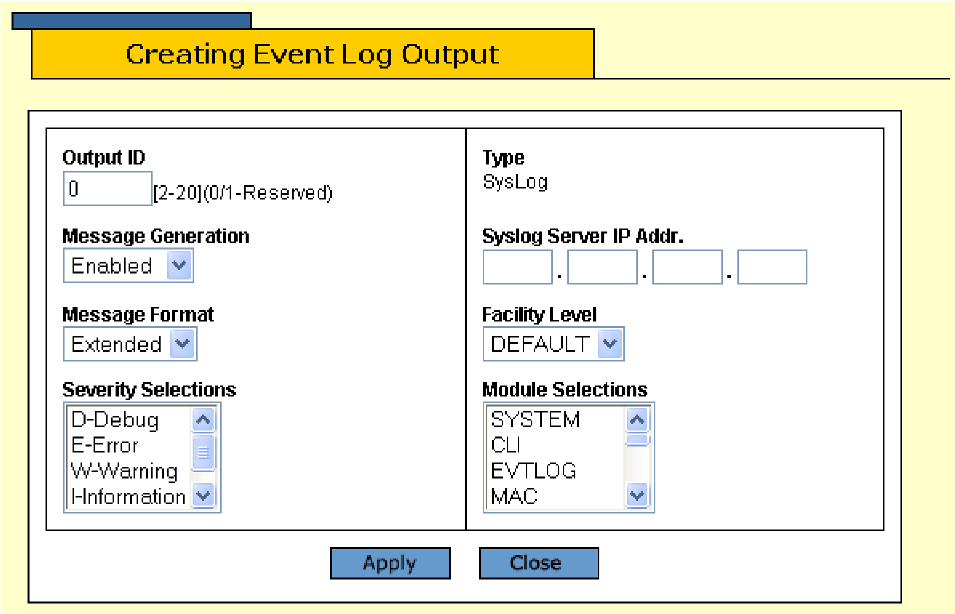
2. Select the **System** menu selection.

3. The **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.

4. In the Current Log Outputs section of the tab, click **Create**.

   The Creating Event Log Output Window is shown in Figure 32.



Output ID: 0 [2-20](0/1-Reserved)
Message Generation: Enabled
Message Format: Extended
Severity Selections: D-Debug, E-Error, W-Warning, I-Information
Type: SysLog
Syslog Server IP Addr.: . . .
Facility Level: DEFAULT
Module Selections: SYSTEM, CLI, EVTLOG, MAC

Figure 32 Creating Event Log Output Window

5. Configure the parameters as needed. The parameters are defined here:

   Output ID
   The ID number for the syslog server definition. The definition will be identified in the Configure Log Outputs menu by this number. The range is 2 to 20. The default is the next available number. You cannot use a number that is already assigned.

   Message Generation
   This enables and disables the syslog server definition. If set to disabled, which is the default, the switch does not send events to the syslog server. When enabled, the switch sends events. The default is disabled.

   Message Format
   The information sent with each event. Choices are:

   ❑ Normal - sends the severity, module, and description.

❑ Extended - sends the same as Normal, plus the date, time, and switch’s IP address. This is the default.

Severity Selections
The severity of events to be sent by the switch to the syslog server. Event severity is a predefined value assigned to an event by the switch according to its possible impact on the switch’s operation. You can use this parameter to configure the switch to send only those events that match one or more severity levels. There are four severity levels, as defined in Table 1 on page 106. The default is informational, error, and warning. To select more than one severity level, hold down the Ctrl key when making your selections.

Type
The type of output. There is only one supported value, Syslog. This setting cannot be changed.

Syslog Server IP Addr.
The IP address of the syslog server.

Facility Level
The facility level to be added to the entries by the switch when it sends them to the syslog server. You can use the facility level to add a numerical code to the entries as they are transmitted to help you group entries on the syslog server according to the management module or switch that produced them. This can help you determine which entries belong to which units when a syslog server is collecting events from several difference network devices. You can specify only one facility level.

There are two approaches to using this parameter. The first is to use the DEFAULT setting. At this setting, the code is based on the functional groupings defined in the RFC 3164 standard. The codes that are applicable to the AT-S62 management software and its modules are shown in Table 3.

Table 3 Applicable RFC 3164 Numerical Code and AT-S62 Module Mappings

Numerical Code	RFC 3164 Facility	AT-S62 Module
4	Security and authorization messages	Security modules: - PSEC - PACCESS - ENCO - PKI - SSH - SSL - MGMTACL - DOS Authentication modules: - SYSTEM - RADIUS - TACACS+
9	Clock daemon	Time- based modules: - TIME (system time and SNTP) - RTC
22	Local use 6	Physical interface and data link modules: - PCFG - PMIRR - PTRUNK - STP - VLAN
23	Local use 7	SYSTEM events related to major exceptions.
16	Local use 0	All other modules and events.

For example, the setting of DEFAULT assigns all port mirroring events a code of 22 and all encryption key events a code of 4.

Your other option is to assign all events from a switch the same numerical code using one of the following facility level settings:

❑ LOCAL1

❑ LOCAL2

❑ LOCAL3

❑ LOCAL4

❑ LOCAL5

❑ LOCAL6

❑ LOCAL7

Each setting represents a predefined RFC 3164 numerical code. The code mappings are listed in Table 4.

Table 4 Numerical Code and Facility Level Mappings

Numerical Code	Facility Level Setting
17	LOCAL1
18	LOCAL2
19	LOCAL3
20	LOCAL4
21	LOCAL5
22	LOCAL6
23	LOCAL7

For example, selecting LOCAL2 as the facility level assigns the numerical code of 18 to all events sent to the syslog server by the switch.

Module Selections
The originating module of the events to be sent to the syslog server. The AT-S62 management software consists of a number of modules, each responsible for a different part of switch operation. You can use this parameter to instruct the switch to send only those events that originated from selected modules. The default is ALL, which sends the events from all modules. The modules are defined in Table 2 on page 107. To select more than one module, hold down the Ctrl key when making your selections.

6. After configuring the syslog server definition, click **Apply**.

   The switch adds the new syslog server definition to the Event Log tab and immediately begins to send events to the server if you enabled the Message Generation option.

7. To permanently save the change, click the **Save Config** menu selection.

Modifying a Syslog Server Definition

To modify a syslog server definition, perform the following procedure:

1. From the Home Page, click **Configuration**.
2. Select the **System** menu selection.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
4. In the Current Log Outputs section of the tab, click the syslog entry you want to modify and click **Modify**.

   The Modify Event Log Output window for the selected syslog definition is displayed.
5. Configure the parameter settings as needed. For descriptions of the parameters, refer to Creating a Syslog Server Definition on page 113.
6. After you finish configuring the parameters, click **Apply**.

   Changes to a syslog definition are immediately activated on the switch.
7. To permanently save the change, click the **Save Config** menu selection.

Deleting a Syslog Server Definition

To delete a syslog server definition, perform the following procedure:

1. From the Home Page, click **Configuration**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 29 on page 105.
4. In the Current Log Outputs section of the tab, click the syslog definition you want to delete and click **Delete**.

   The selected syslog definition is immediately deleted from the switch.
5. To permanently save the change, click the **Save Config** menu selection.

Viewing a Syslog Server Definition

To view the parameter settings of a syslog server definition, perform the following procedure:

1. From the Home Page, click **Monitoring**.
2. Select the **System** menu option.
3. Select the **Event Log** tab.
4. In the Current Log Outputs section of the tab, click the syslog definition you want to view and click **View**.

   The switch displays the parameter settings of the selected syslog definition. For descriptions of the settings, refer to Creating a Syslog Server Definition on page 113.

Chapter 12

Classifiers

A classifier defines a traffic flow. You use classifiers with access control lists to filter ingress traffic on a port. You can also use classifiers with Quality of Service policies to regulate different traffic flows that pass through a switch.

This chapter contains the following sections:

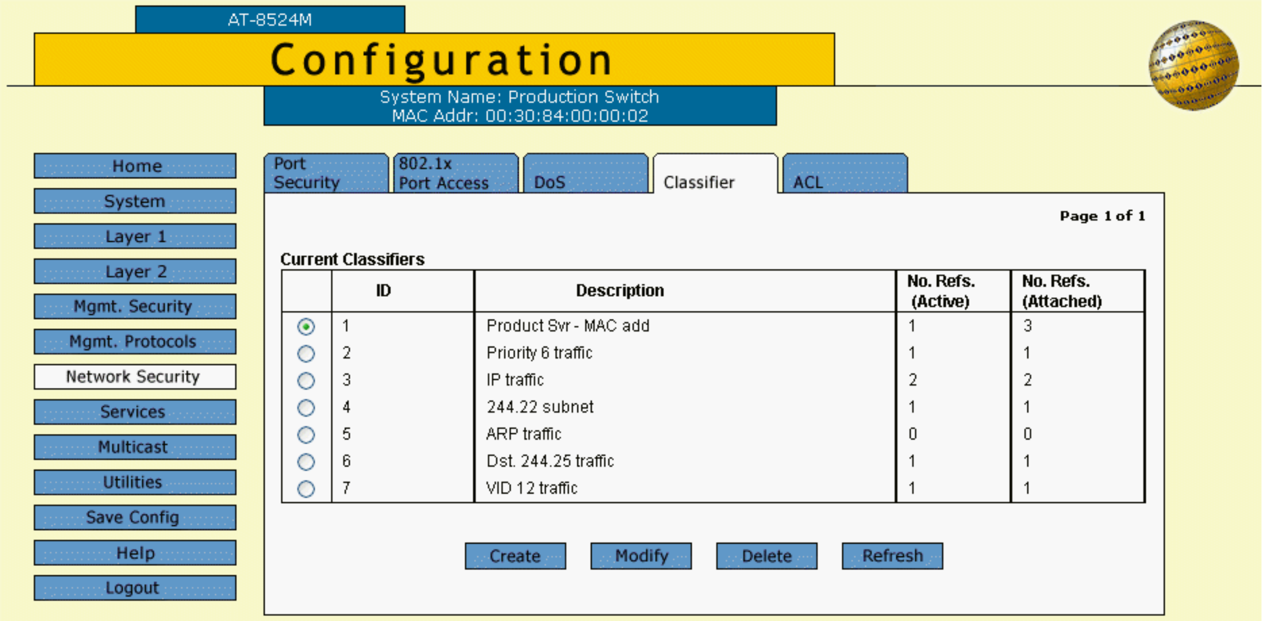
Note
For background information and guidelines on classifiers, refer to the *AT-S62 Menus Interface User's Guide*.

Creating a Classifier

To create a new classifier, perform the following procedure:

5. From the Home Page, select **Configuration**.
6. Select the **Network Security** or **Services** menu selection. (The Classifier tab is accessible from both menu selections.)
7. Select the **Classifier** tab.

   An example of the Classifier tab is shown in Figure 33.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Current Classifiers

	ID	Description	No. Refs. (Active)	No. Refs. (Attached)
●	1	Product Svr - MAC add	1	3
○	2	Priority 6 traffic	1	1
○	3	IP traffic	2	2
○	4	244.22 subnet	1	1
○	5	ARP traffic	0	0
○	6	Dst. 244.25 traffic	1	1
○	7	VID 12 traffic	1	1

Figure 33 Classifier Tab (Configuration)

The tab lists the current classifiers on the switch. The columns are defined here:

ID
The ID number of the classifier.

Description
A description of the classifier.

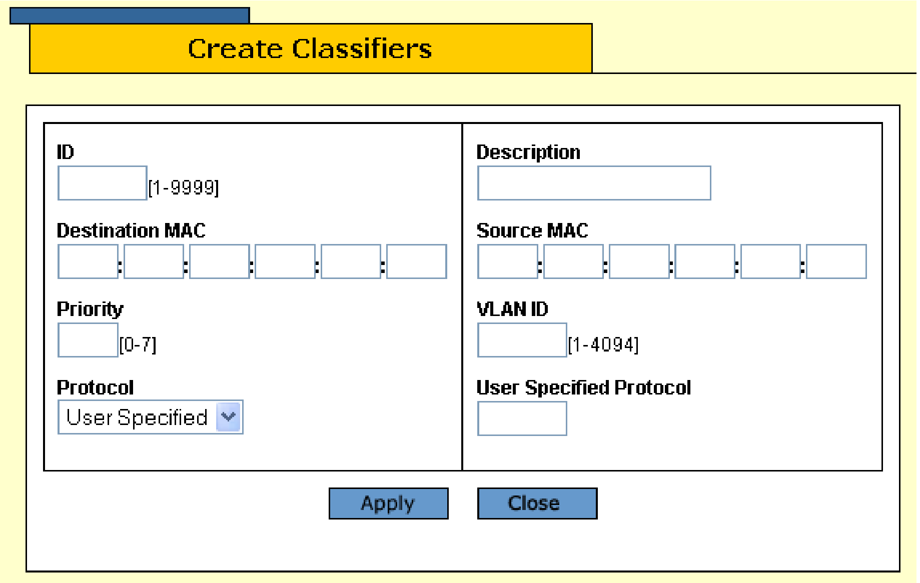
No. Refs. (Active)
The number of active ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch port.

No. Refs. (Attached)
The number of active and inactive ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS is

assigned to a switch port, while an inactive ACL or QoS policy is currently not assigned to any port. If this column is 0 (zero), the classifier is not assigned to any ACLs or policies, active or inactive.

8. To create a new classifier, click **Create**.

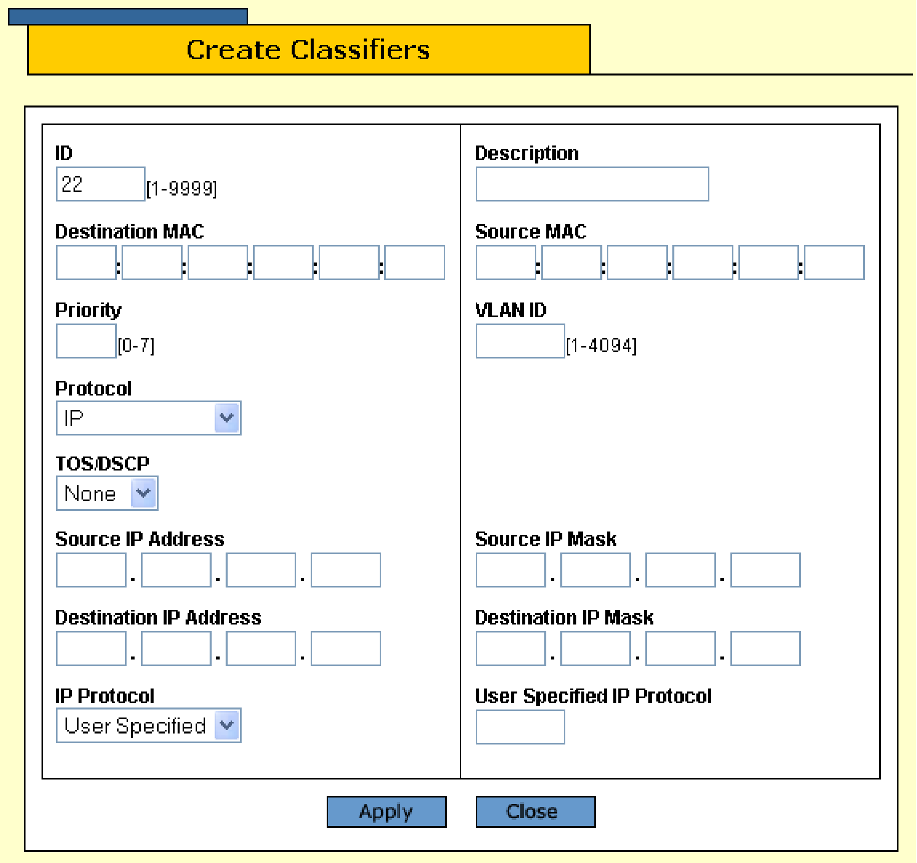
   The Create Classifier page is shown in Figure 34.



Protocol: User Specified

Figure 34 Create Classifier Page

Some of the variables and settings display additional selections. For example, selecting IP as the Protocol displays the selections shown in Figure 35.



Create Classifiers

ID: 22 [1-9999]

Description

Destination MAC

Source MAC

Priority [0-7]

VLAN ID [1-4094]

Protocol: IP

TOS/DSCP: None

Source IP Address

Source IP Mask

Destination IP Address

Destination IP Mask

IP Protocol: User Specified

User Specified IP Protocol

Figure 35 Create Classifier Page - IP Protocol

9. Configure the parameters as needed. They are defined here:

ID
Specifies an ID number for the classifier. Every classifier on the switch must have a unique ID number. The range is 1 to 9999. This parameter is required.

Description
Specifies a description for the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed.

Destination MAC
Defines a traffic flow by its destination MAC address.

Source MAC
Defines a traffic flow by its source MAC address.

Priority
Defines a traffic flow by the user priority level in tagged Ethernet frames. The range is 0 to 7.

VLAN ID

Defines a traffic flow of tagged packets by its VLAN ID number. The range is 1 to 4094.

Protocol

Defines a traffic flow as one of the following Layer 2 protocols:

❑ User Specified

❑ IP

❑ ARP

❑ RARP

User Specified Protocol

Defines a traffic flow of a Layer 2 protocol by its protocol number. The number can be entered in either decimal or hexadecimal format. For the latter, precede the number with "0x". To use this parameter, the Protocol parameter must be set to User Specified.

TOS/DSCP

Defines a traffic flow by its Type of Service or DSCP value. To set this parameter, the Protocol parameter must be set to IP. Options are:

❑ TOS (Type of Service)

❑ DSCP

TOS

Defines a traffic flow by its Type of Service value. The range is 0 to 7. To set this value, the TOS/DSCP parameter must be set to TOS.

DSCP

Defines a traffic flow by its DSCP value. The range is 0 to 63. To set this value, the TOS/DSCP parameter must be set to DSCP.

IP Protocol

Defines a traffic flow of a Layer 3 protocol. Options are:

❑ User Specified

❑ TCP

❑ UDP

❑ ICMP

❑ IGMP

User Specified IP Protocol

Defines a traffic flow of a Layer 3 protocol by its protocol number. The number can be entered in either decimal or hexadecimal format. If you use the latter, precede the number with “0x”. To set this parameter, the IP Protocol parameter must be set to User Specified.

Source IP Address
Source IP Mask
Defines a traffic flow by a source IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask “255.255.255.0”.

Destination IP Address
Destination IP Mask
Defines a traffic flow by its destination IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask “255.255.255.0”.

TCP Source Port
Defines a traffic flow by source TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Destination Port
Defines a traffic flow by destination TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Flags
Defines a traffic flow by TCP flag. To set this parameter, IP Protocol must be set to TCP. Options are

❑ URG - Urgent

❑ ACK - Acknowledgement

❑ RST - Reset

❑ PSH - Push

❑ SYN - Synchronization

❑ FIN - Finish

UDP Source Port
Defines a traffic flow by source UDP port. To set this parameter, IP Protocol must be set to UDP.

UDP Destination Port
Defines a traffic flow by a destination UDP port. To set this parameter, IP Protocol must be set to UDP.

User Specified Protocol
Defines a traffic flow by a protocol other than one of those listed in the Protocol or IP Protocol list. To set this parameter, Protocol must be set to User Specified. Alternatively, you can set this parameter is IP Protocol is set to User Specified.

10. After you have finished configuring the necessary parameters, click **Apply**.
11. To permanently save your changes, select the **Save Config** menu selection.

Modifying a Classifier

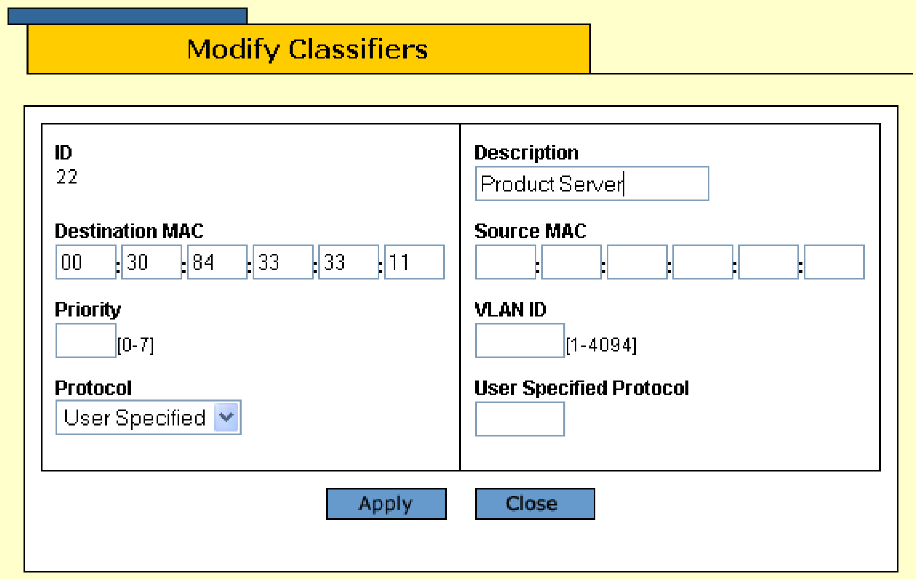
This procedure explains how to modify a classifier. If the classifier you want to modify is currently assigned to an active ACL or QoS policy, you must first remove the port assignments from the ACL or policy before you can modify the classifier. Once you have finished modifying the classifier, you can reassign the ports again to the ACL or QoS policy.

To modify a classifier, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Network Security** or **Services** menu selection. (The Classifier tab is accessible from both menu selections.)
3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 33 on page 120.
4. Click the dialog circle next to the classifier you want to modify and click **Modify**. You can modify only one classifier at a time.

   An example of the Modify Classifier page is shown in Figure 36.



ID
22

Description
Product Server

Destination MAC
00 : 30 : 84 : 33 : 33 : 11

Source MAC
: : : : :

Priority
[0-7]

VLAN ID
[1-4094]

Protocol
User Specified

User Specified Protocol

Figure 36 Modify Classifier Page

5. Modify the parameters as necessary. For definitions of the parameter, refer to Creating a Classifier on page 120.
6. After you have finished modifying the parameters, click **Apply**.

   The modifications are immediately implemented in the classifier.
7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Classifier

This procedure explains how to delete a classifier. If the classifier you want to delete is currently assigned to an ACL or QoS policy, you must first remove it from the ACL or policy.

To delete a classifier, perform the following procedure:

1. From the home page, select **Configuration**.
2. Select the **Network Security** or **Services** menu selection. (The Classifier tab is accessible from both menu selections.)
3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 33 on page 120.
4. Click the button next to the ID number of the classifier you want to delete and click **Delete**.
5. To permanently save your changes, select the **Save Config** menu selection.

Displaying the Classifiers

To display the classifiers on a switch, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select either the **Network Security** or **Services** menu selection. (The Classifier tab is accessible from both menu selections.)
3. Select the **Classifiers** tab.

   This tab lists the classifiers currently existing on the switch. The columns are defined here:

   ID
   The ID of the classifier.

   Description
   A description of the classifier.

   No. Refs. (Active)
   The number of active ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS policy is assigned to a switch port.

   No. Refs. (Attached)
   The number of active and inactive ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS is assigned to a switch port, while an inactive ACL or QoS is currently not assigned to any port.
4. To display detailed information about a classifier, select the button next to the classifier and click **View**.

   For definitions of the parameters, refer to Creating a Classifier on page 120.
5. Click **Close** to close the page.

Chapter 13

Access Control Lists

An access control list (ACL) is used to filter ingress traffic on a port. Traffic is defined by the classifiers assigned to the ACL.

This chapter contains the following sections:

- Creating an Access Control List on page 130
- Modifying an Access Control List on page 133
- Deleting an Access Control List on page 135
- Displaying the Access Control Lists on page 136

Note
For background information and guidelines on access control lists, refer to the *AT-S62 Menus Interface User's Guide*.

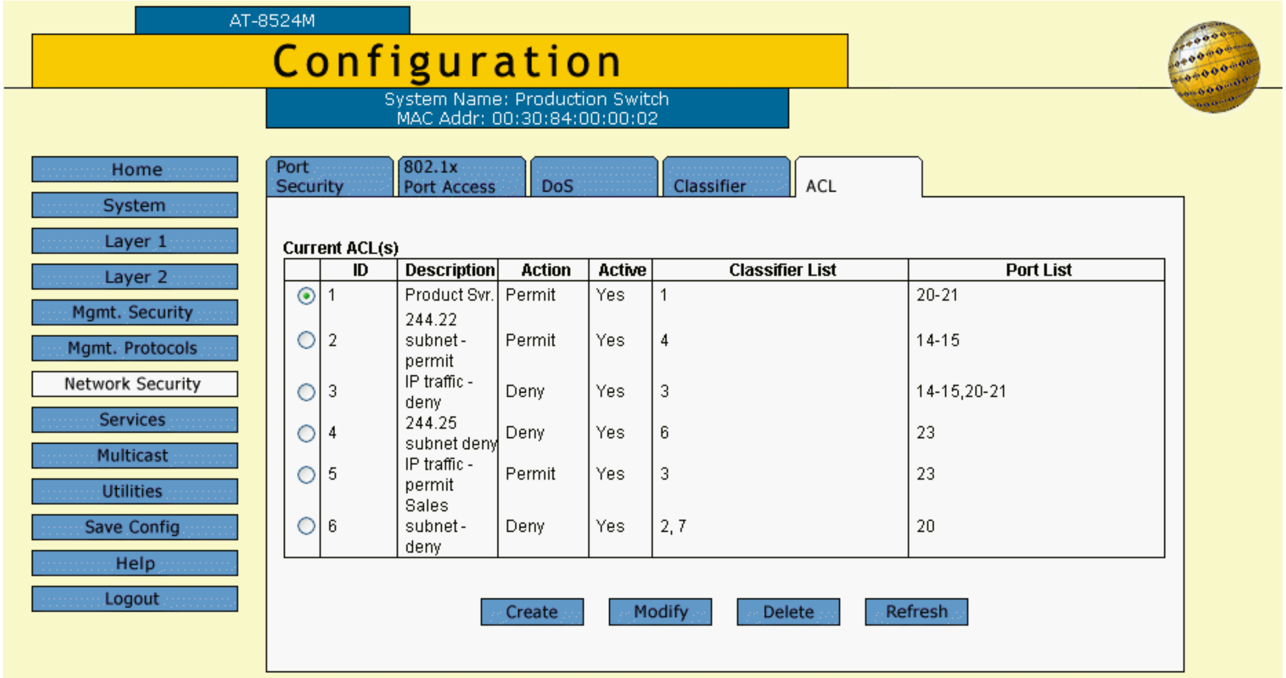
Creating an Access Control List

This procedure explains how to create an ACL. It is a good idea before performing this procedure to jot down on paper the ID number(s) of the classifier(s) you want to assign to the ACL and the action of the ACL, which is either Permit or Deny. An action of Permit instructs the port to accept packets from the defined traffic flow of the classifier, while an action of Deny discards the packets. Having this information handy will make it easier for you to perform the procedure. To view the classifier ID numbers and specifications, refer to Displaying the Classifiers on page 128.

To create an access control list, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Network Security** menu selection.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 37.



AT-8524M

Configuration

System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Current ACL(s)

	ID	Description	Action	Active	Classifier List	Port List
●	1	Product Svr.	Permit	Yes	1	20-21
○	2	244.22 subnet-permit	Permit	Yes	4	14-15
○	3	IP traffic - deny	Deny	Yes	3	14-15,20-21
○	4	244.25 subnet deny	Deny	Yes	6	23
○	5	IP traffic - permit	Permit	Yes	3	23
○	6	Sales subnet - deny	Deny	Yes	2, 7	20

Figure 37 ACL Tab (Configuration)

The tab lists the access control lists that currently exist on the switch. The columns in the table are defined here:

ID
The ID number of the ACL.

Description
A description of the ACL.

Action
The action of the ACL. An action of Permit means the ACL accepts packets that match the traffic flows defined by the classifiers. An action of Deny means that the ACL discards ingress packets that match the defined traffic flows, provided that the packets do not also meet the criteria of a Permit ACL. (A Permit ACL overrides a Deny ACL.)

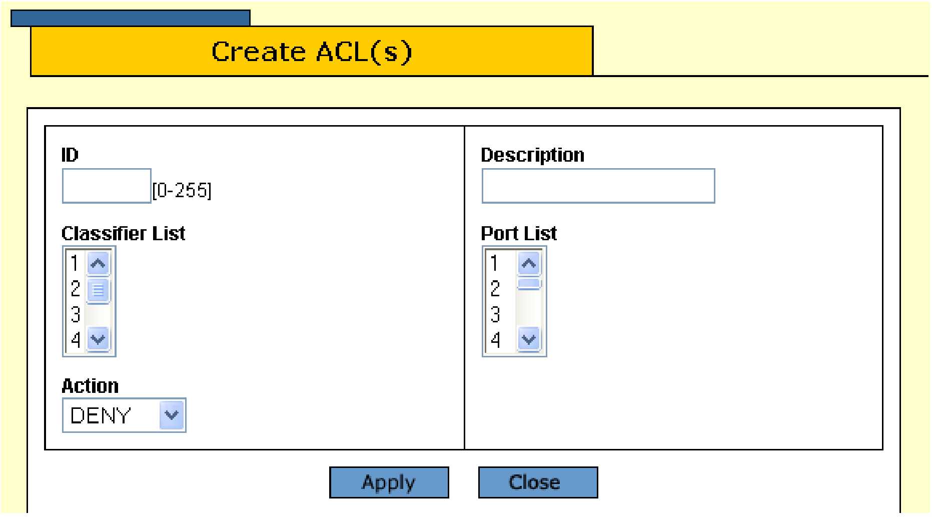
Active
The status of the ACL. A status of Yes means that the ACL is assigned to at least one port on the switch. A status of No means the ACL is not assigned to any ports and so is inactive

Classifier List
The classifiers assigned to the ACL.

Port List
The ports assigned to the ACL.

4. To create a new ACL, click **Create**.

   The Create ACLs page is shown in Figure 38.



Create ACL(s)

ID [0-255]

Description

Classifier List

Port List

Action DENY

Figure 38 Create ACLs Page

5. Configure the following parameters:

ID
Use this field to enter an ID number for the ACL. Every ACL on the switch must have a unique ID number. The range is 0 to 255.

Classifier List
Use this list to select the classifier you want to assign to this ACL. You can assign more than one classifier to an ACL. To select multiple classifiers, hold down the Ctrl key while making your

selections. To view the classifiers on a switch, refer to Displaying the Classifiers on page 128. An ACL must have at least one classifier.

Action
Use this menu to specify the action of the ACL. Deny, which is the default, discards ingress packets that match the defined traffic flow of the classifier. Permit accepts the packets. The default is Deny.

Description
Use this field to enter a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces. A description is optional.

Port List
Use this list to specify the port where you want to assign the ACL. You can assign an ACL to more than one port. To select multiple ports, hold down the Ctrl key while making your selections. You do not have to assign an ACL to a port when you initially create it. However, an ACL that is not assigned to any port is considered inactive.

6. After you have finished configuring the parameters, click **Apply**.

   The new ACL is immediately activated on the specified ports. If you did not specify any ports for the ACL, the ACL is created but remains inactive until you assign it to a port.

7. To permanently save your changes, select the **Save Config** menu selection.

Modifying an Access Control List

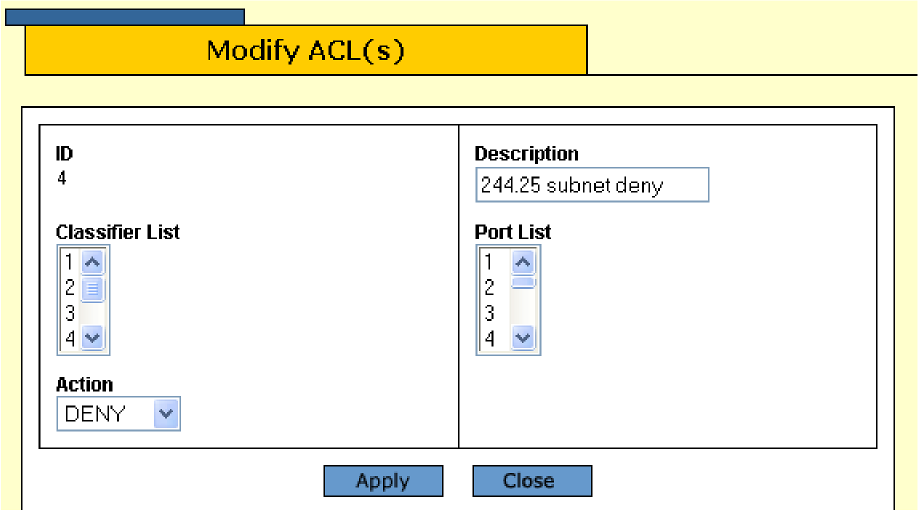
To modify an ACL, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Network Security** menu selection.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 37 on page 130.

4. Click the dialog circle next to the ID number of the ACL you want to modify and click **Modify**. You can modify only one ACL at a time.

   The Modify ACLs page is shown in Figure 39.



ID
4

Description
244.25 subnet deny

Action
DENY

Figure 39 Modify ACLs Page

5. Configure the following parameters as necessary:

   ID
   The ID number of the ACL. You cannot change this value.

   Classifier List
   Use this list to select the classifier you want to assign to this ACL. You can assign more than one classifier to an ACL. To select multiple classifiers, hold down the Ctrl key while making your selections. To view the classifiers, refer to Displaying the Classifiers on page 128. An ACL must have at least one classifier.

   Action
   Use this menu to specify the action of the ACL. Deny, which is the default, discards ingress packets that match the defined traffic flow of the classifier. Permit accepts the packets. The default is Deny.

Description
Use this field to enter a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces. Entering a description is optional.

Port List
Use this list to specify the port where you want to assign the ACL. You can assign an ACL to more than one port. To select multiple ports, hold down the Ctrl key while making your selections. To remove the ACL from its current port assignments without assigning it to any new ports, hold down the Ctrl key while deselecting the currently assigned ports. An ACL that is not assigned to any port is considered inactive.

6. Click **Apply.**

   Changes to the ACL are immediately implemented on the switch.

7. To permanently save your changes, select the **Save Config** menu selection.

Deleting an Access Control List

To delete an ACL, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Network Security** menu selection.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 37 on page 130.
4. Click the dialog circle next to the ID number of the ACL you want to delete and click **Delete**. You can delete only one ACL at a time. The ACL is immediately deleted.
5. To permanently save your changes, select the **Save Config** menu selection.

Displaying the Access Control Lists

To display the current ACLs on the switch, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select the **Network Security** menu selection.
3. Select the **ACL** tab.

   The ACL tab displays a table of the currently configured ACLs that contains the following columns of information:

   ID
   The ID number of the ACL.

   Description
   A description of the ACL.

   Action
   The action of the ACL. An action of Permit means the ACL accepts packets that match the traffic flows defined by the classifiers. An action of Deny means that the ACL discards ingress packets that match the defined traffic flows, provided that the packets do not also meet the criteria of a Permit ACL. (A Permit ACL overrides a Deny ACL.)

   Active
   The status of the ACL. A status of Yes means that the ACL is assigned to at least one port on the switch. A status of No means the ACL is not assigned to any ports and therefore is inactive.

   Classifier List
   The classifiers assigned to the ACL.

   Port List
   The ports assigned to the ACL.

4. To view the same information for each ACL, click the dialog circle next to the ACL and click **View.**
5. Click **Close**.

Chapter 14

Quality of Service

This chapter contains instructions on how to configure Quality of Service (QoS). This chapter contains the following procedures:

- ❑ Managing Flow Groups on page 138
- ❑ Managing Traffic Classes on page 144
- ❑ Managing Policies on page 151

Note
For background information and guidelines on QoS, refer to the *AT-S62 Menus Interface User's Guide*.

Managing Flow Groups

Flow groups are groups of classifiers that group together similar traffic flows. This section contains the following procedures:

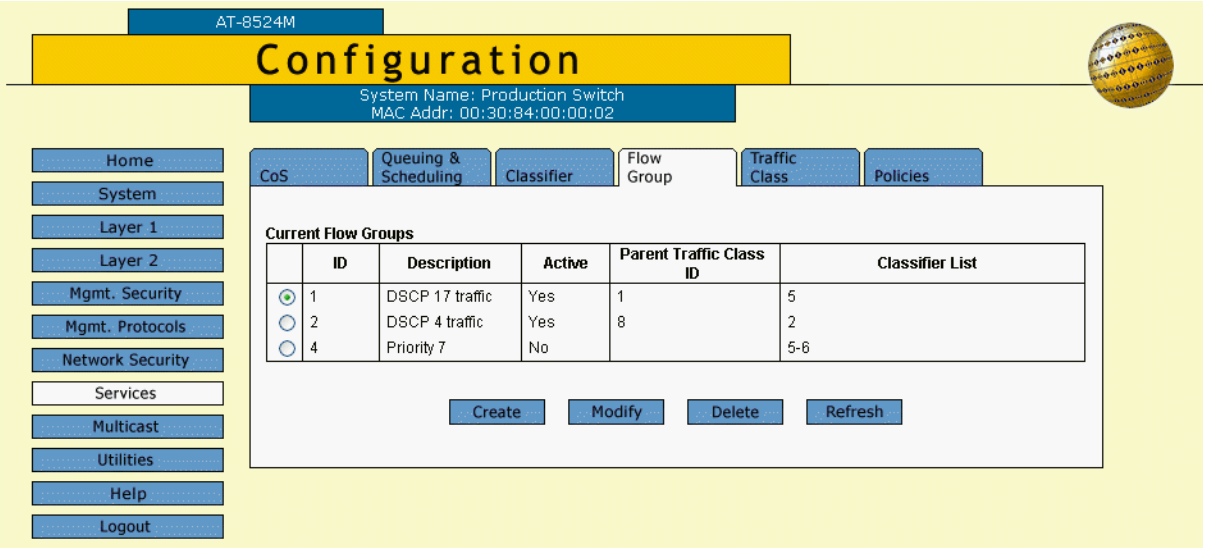
- ❑ Creating a Flow Group on page 138
- ❑ Modifying a Flow Group on page 140
- ❑ Deleting a Flow Group on page 142
- ❑ Displaying Flow Groups on page 142

Creating a Flow Group

To create a flow group, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 40.



Current Flow Groups

	ID	Description	Active	Parent Traffic Class ID	Classifier List
●	1	DSCP 17 traffic	Yes	1	5
○	2	DSCP 4 traffic	Yes	8	2
○	4	Priority 7	No		5-6

Figure 40 Flow Group Tab (Configuration)

The columns in the tab are defined here:

ID
The ID number of the flow group.

Description
The flow group description.

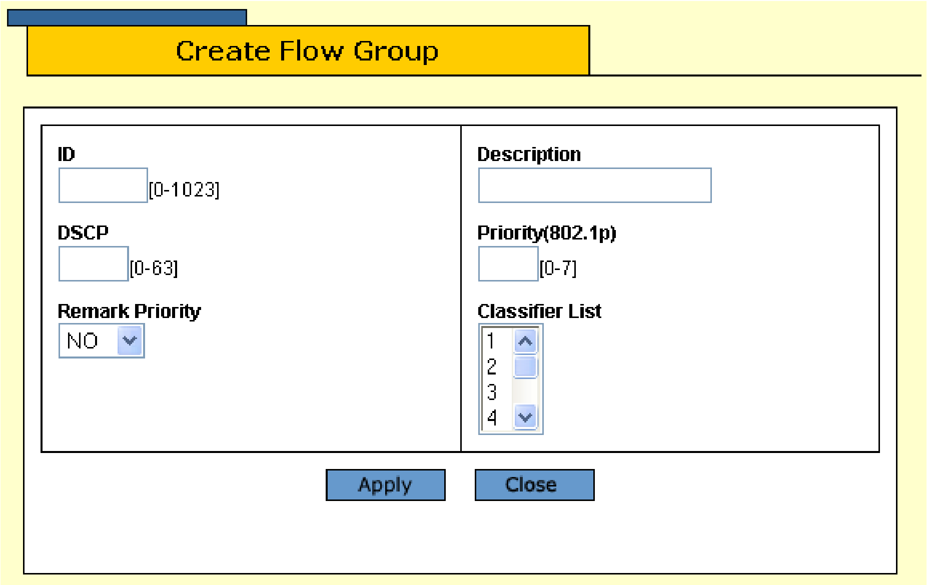
Active
The active status of the flow group. A flow group is deemed active if it is part of a policy that is assigned to a switch port. A flow group is considered inactive if it is not a part of any policies or if the policies have not been assigned to any ports.

Parent Traffic Class ID
The traffic class to which the flow group is assigned.

Classifier List
The classifiers assigned to the flow group.

4. Click **Create**.

   The Create Flow Group page is shown in Figure 41.



Create Flow Group

ID [0-1023]

DSCP [0-63]

Remark Priority: NO

Description

Priority(802.1p) [0-7]

Classifier List: 1, 2, 3, 4

Figure 41 Create Flow Group Page

5. Configure the following parameters as necessary:

ID
Specifies the ID number for this flow group. A flow group must be assigned a unique ID number. The range is 0 to 1023.

DSCP
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description
Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

Priority (802.1p)
Specifies a new user priority value for the packets. The range is 0 to 7. If you specify a new user priority value here and in Traffic Class, the value here overrides the value in Traffic Class. If you want the packets to retain the new value when they exit the switch, change Remark Priority to Yes.

Classifier List
The classifiers to be assigned to the flow group. The specified classifiers must already exist. To select more than one classifier, hold down the Ctrl key when making your selections.

6. Click **Apply**.

   The management software creates the new flow group.

7. To permanently save your changes, select the **Save Config** menu selection.

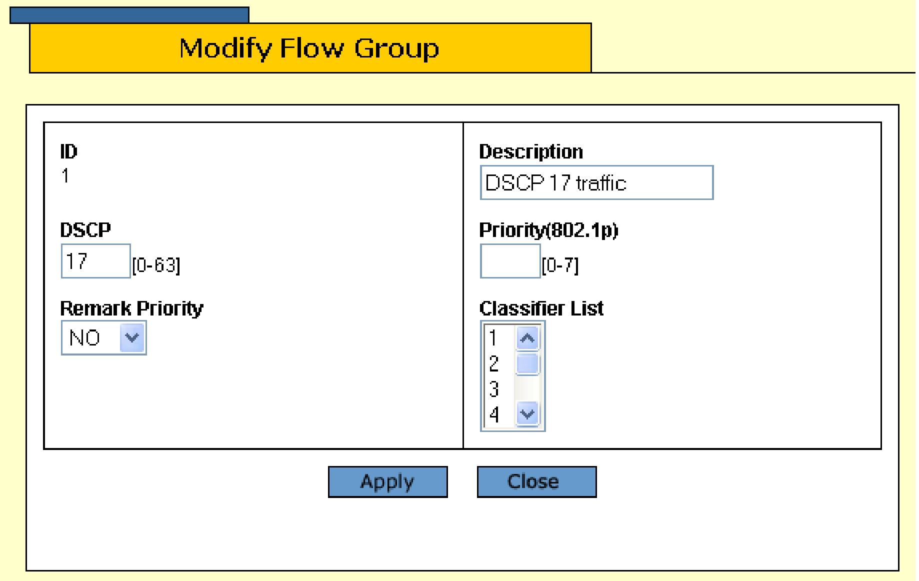
Modifying a Flow Group

This procedure explains how to modify an existing flow group. If the flow group is already part of a QoS policy that is assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can modify the flow group. You can reassign the ports back to the policy after you have finished modifying the flow group.

To modify a flow group, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Flow Group** tab.
4. Click the dialog circle next to the flow group you want to modify and click **Modify**. You can modify only one flow group at a time.

The Modify Flow Group page is shown in Figure 42.


Modify Flow Group

ID
1

DSCP
17 [0-63]

Remark Priority
NO

Description
DSCP 17 traffic

Priority(802.1p)
[0-7]

Classifier List
1
2
3
4

Figure 42 Modify Flow Group Page

5. Configure the following parameters as necessary:

ID
Specifies the ID number for this flow group. You cannot change this value.

DSCP
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description
Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

Priority (802.1p)
Specifies a new user priority value for the packets. The range is 0 to 7. If you specify a new user priority value here and in Traffic Class, the value here overrides the value in Traffic Class. If you want the packets to retain the new value when they exit the switch, change Remark Priority to Yes.

Classifier List
The classifier to be assigned to the flow group. The specified classifier must already exist. You can assign more than one classifier to a flow group. To assign multiple classifiers, hold down the Ctrl key when making your selections.

6. Click **Apply**.

   The changes are immediately applied to the flow group.

7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Flow Group

This procedure explains how to delete a flow group. If the flow group that you want to delete is already part of a QoS policy that is assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can delete the flow group. You can reassign the ports back to the policy after you have deleted the flow group.

To delete a flow group, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 40 on page 138.

4. Select the flow group you want to delete and click **Delete**.

   The flow group is deleted from the switch.

Displaying Flow Groups

To display the flow groups on a switch, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select the **Services** menu selection.
3. Select the **Flow Group** tab.

   The Flow Group tab displays the currently configured flow groups in a table that contains the following columns of information:

   ID
   The ID number for the flow group.

   Description
   The flow group description.

Active
The active status of the flow group. A flow group is deemed active if it is part of a policy that is assigned to a switch port. A flow group is considered inactive if it is not connected to any policies or if the policies have not been assigned to any ports.

Parent Traffic Class ID
The traffic class to which the flow group is assigned.

Classifier List
The classifiers assigned to the flow group.

4. To display detailed information about a flow group, select the flow group and click **View**.

   The View Flow Group page displays the following information:

   ID
   The ID number for this flow group.

   Description
   The flow group description.

   DSCP
   The replacement value to write into the DSCP (TOS) field of the packets.

   Priority
   The new user priority value for the packets.

   Remark Priority
   Replaces the user priority value in the packets with the new value specified in the Priority parameter.

   Classifier List
   The classifiers assigned to the flow group.

5. Click **Close**.

Managing Traffic Classes

Traffic classes consist of a set of QoS parameters and a group of QoS flow groups. This section contains the following procedures:

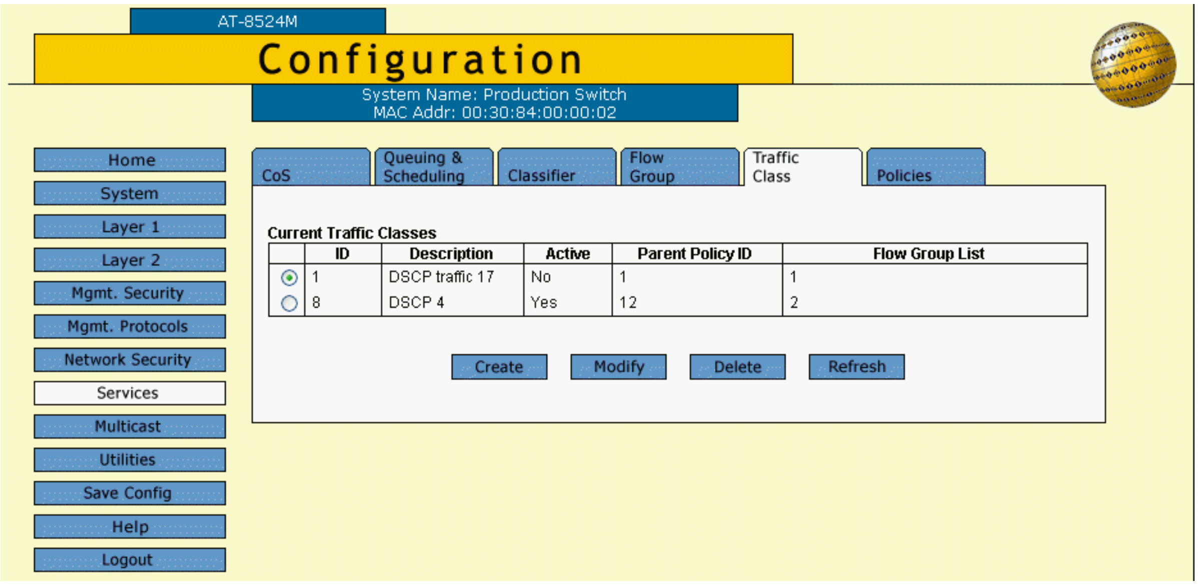
- ❑ “Creating a Traffic Class,” next
- ❑ Modifying a Traffic Class on page 148
- ❑ Deleting a Traffic Class on page 149
- ❑ Displaying the Traffic Classes on page 150

Creating a Traffic Class

To create a traffic class, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 43.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Current Traffic Classes

	ID	Description	Active	Parent Policy ID	Flow Group List
●	1	DSCP traffic 17	No	1	1
○	8	DSCP 4	Yes	12	2

Figure 43 Traffic Class Tab

The columns in the tab are defined here:

ID
The ID of the traffic class.

Description
A description of the traffic class.

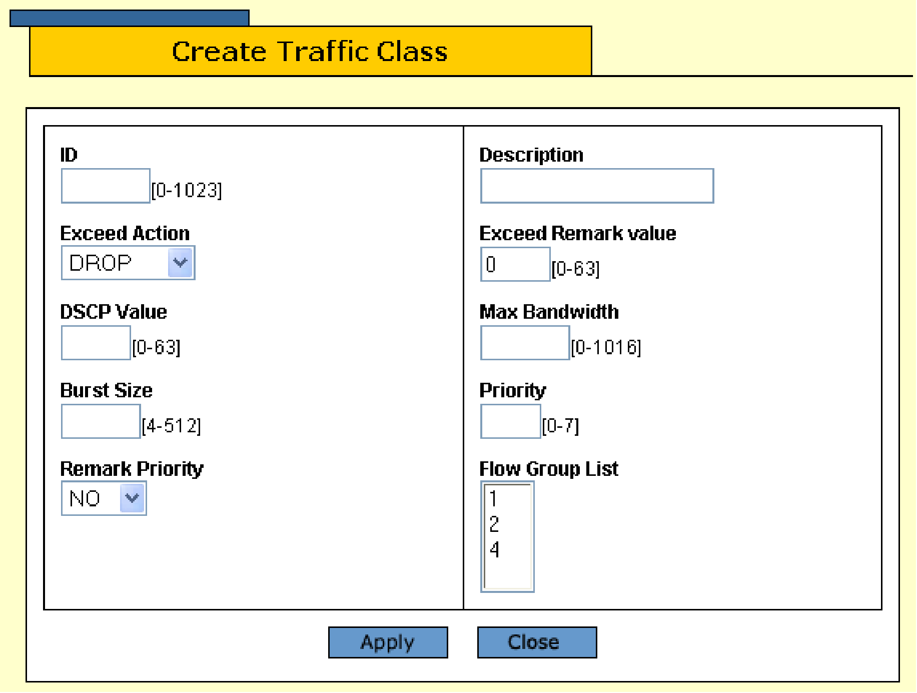
Active
Whether or not this traffic class is active on the switch. An active traffic class is part of a policy that is assigned to one or more switch ports. An inactive traffic class is not assigned to any policies or to policies that are not assigned to switch ports.

Parent Policy ID
The QoS policies to which the traffic class is assigned.

Flow Group List
The flow groups assigned to this traffic class.

4. To create a new traffic class, click **Create**.

The Create Traffic Class page is shown in Figure 44.



Create Traffic Class

ID [0-1023]

Description

Exceed Action: DROP

Exceed Remark value: 0 [0-63]

DSCP Value [0-63]

Max Bandwidth [0-1016]

Burst Size [4-512]

Priority [0-7]

Remark Priority: NO

Flow Group List: 1, 2, 4

Figure 44 Create Traffic Class Page

5. Configure the following parameters:

ID
Specifies an ID number for the traffic class. Each traffic class on the switch must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.

Exceed Action
Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth, specified in option 6. There are two possible exceed actions, drop and remark. If drop is selected,

traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified in Exceed Remark Value. The default is drop.

DSCP
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.

Burst Size
Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps.

The token bucket is used in situations where you set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded.

Tokens are added to the bucket at the same rate as the traffic class’ maximum bandwidth, set with option 6, Max Bandwidth. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at the same rate.

If the amount of traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic is discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added.

Note
To use this parameter you must specify a maximum bandwidth using the Max Bandwidth parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.

Description
Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Remark Value
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

Max Bandwidth
Specifies the maximum bandwidth available to the traffic class. The range is 0 to 1016 Mbps.

This parameter determines the maximum rate at which the ingress port accepts packets belonging to this traffic class before either dropping or remarking occurs, depending on the Exceed Action parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified.

The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).

Note
If this option is set to 0 (zero), all traffic that matches that traffic class is dropped. However, a access control list can be created to match the traffic that is marked for dropping, or a subset of it, and given an action of permit, to override this. This functionality can be used to discard all but a certain type of traffic.

Priority
Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of four Class of Service (CoS) queues based on the priority value.

If you want the packets to retain the new value when they exit the switch, change the Remark Priority parameter to Yes.

If you specify a new user priority value here and in Flow Group, the value in Flow Group overwrites the value here.

Flow Group List
The flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. After you have configured the necessary parameters, click **Apply**.

   The new traffic class is created on the switch.

7. To permanently save your changes, select the **Save Config** menu selection.

Modifying a Traffic Class

This procedure explains how to modify an existing traffic class. If the traffic class you want to modify is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can modify the traffic class. You can reassign the ports back to the policy after you have finished modifying the traffic class.

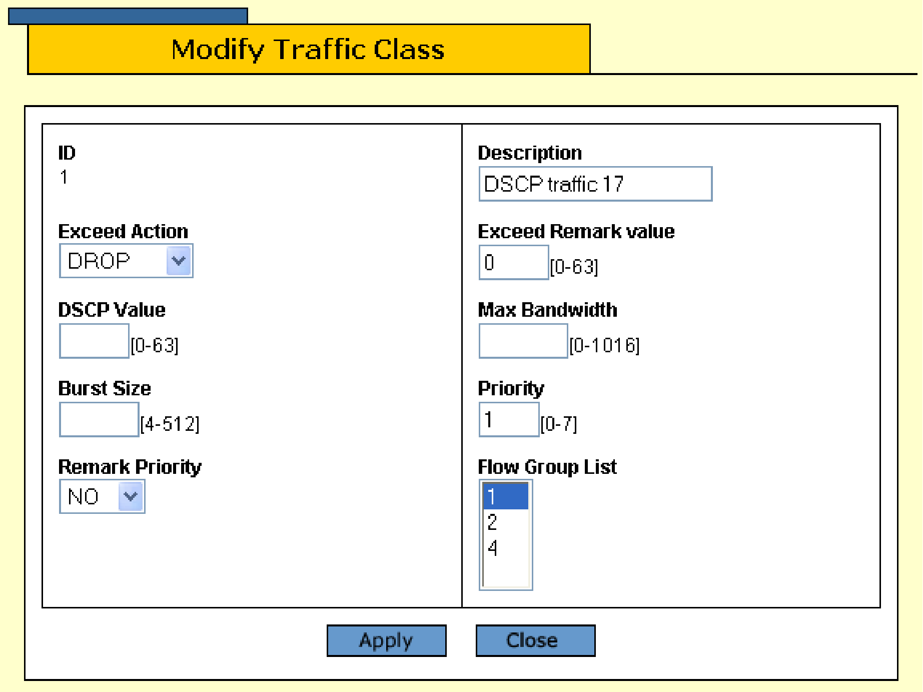
To modify a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 43 on page 144

4. Select the traffic class you want to modify and click **Modify**.

The Modify Traffic Class page is shown in Figure 45.



Modify Traffic Class

ID
1

Description
DSCP traffic 17

Exceed Action
DROP

Exceed Remark value
0 [0-63]

DSCP Value
[0-63]

Max Bandwidth
[0-1016]

Burst Size
[4-512]

Priority
1 [0-7]

Remark Priority
NO

Flow Group List
1
2
4

Figure 45 Modify Traffic Class Page

5. Configure the following parameters as necessary. For descriptions of the parameters, refer to Creating a Traffic Class on page 144.
6. Click **Apply**.

   The changes are immediately implemented in the traffic class.
7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Traffic Class

This procedure explains how to delete a traffic class. If the traffic class you want to delete is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can delete the traffic class. You can reassign the ports back to the policy after you have deleted the traffic class.

To delete a traffic class, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 43 on page 144
4. Select the traffic class you want to delete and click **Delete**.

   The traffic class is deleted from the switch.

Displaying the Traffic Classes

To display the traffic classes, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Services**.
3. Select the **Traffic Class** tab.

   The Traffic Class tab displays the currently configured flow groups in a table that contains the following columns of information:

   The columns in the tab are defined here:

   ID
   The ID of the traffic class.

   Description
   A description of the traffic class.

   Active
   Whether or not this traffic class is active on the switch. An active traffic class is part of a policy that is assigned to one or more switch ports. An inactive traffic class is not assigned to any policies or to policies that are not assigned to switch ports.

   Parent Policy ID
   The QoS policies to which the traffic class is assigned.

   Flow Group List
   The flow groups assigned to this traffic class.
4. To display detailed information about a traffic class, select the traffic class and click **View**.

   For definitions of the parameters, refer to Creating a Traffic Class on page 144.
5. Click **Close**.

Managing Policies

QoS policies consist of a collection of user-defined traffic classes. This section contains the following procedures:

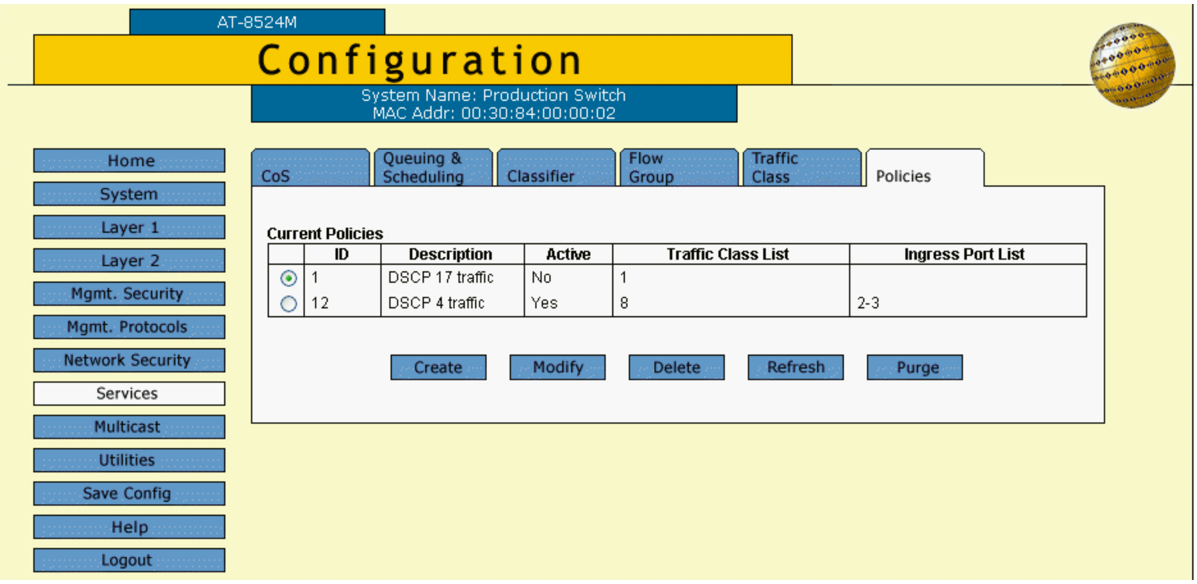
- ❑ Creating a Policy on page 151
- ❑ Modifying a Policy on page 154
- ❑ Deleting a Policy on page 154
- ❑ Displaying Policies on page 155

Creating a Policy

To create a policy, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 46.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Current Policies

	ID	Description	Active	Traffic Class List	Ingress Port List
●	1	DSCP 17 traffic	No	1	
○	12	DSCP 4 traffic	Yes	8	2-3

Figure 46 Policies Tab (Configuration)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID
The ID of the policy.

Description
A description of the policy.

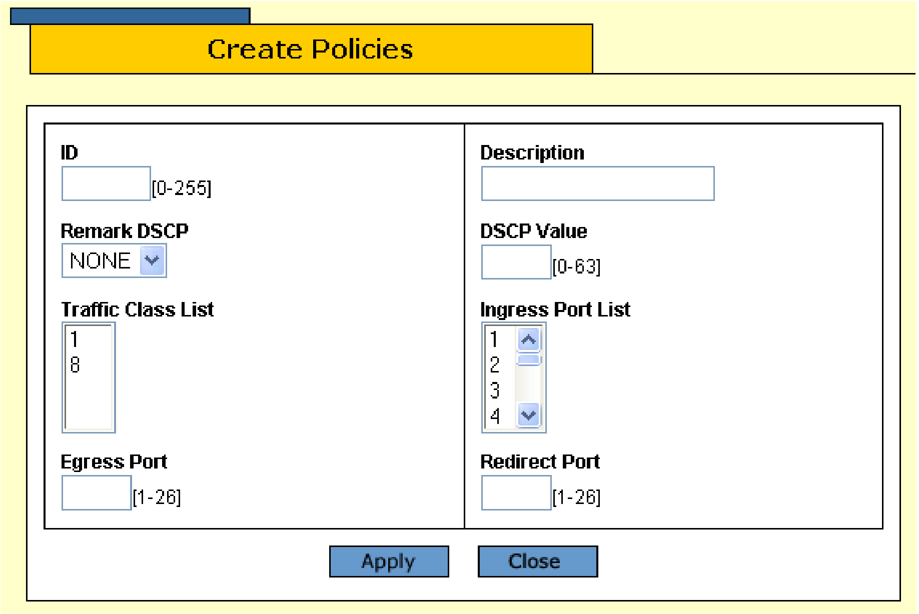
Active
Whether or not this policy is active on the switch. An active policy is assigned to one or more switch ports. An inactive policy is not assigned to any switch ports.

Traffic Class List
The traffic classes assigned to the policy.

Ingress Port List
The ingress ports to which the policy is assigned.

4. Click **Create**.

   The Create Policy page is shown in Figure 47.



Create Policies

ID [0-255]

Description

Remark DSCP NONE

DSCP Value [0-63]

Traffic Class List
1
8

Ingress Port List
1
2
3
4

Egress Port [1-26]

Redirect Port [1-26]

Figure 47 Create Policy Page

5. Configure the following parameters as necessary:

   ID
   Specifies an ID number for the policy. Every policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.

   Description
   Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

   Remark DSCP
   Specifies the conditions under which the ingress DSCP value is overwritten. Select one of the following options from the list:

   None - Disables this function.

   All - All packets are remarked.

DSCP Value
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.

Traffic Class List
Specifies the traffic class to be assigned to the policy. The traffic class must already exist. A policy can have more than one traffic class. To select more than one traffic class, hold down the Ctrl key when making your selections.

Ingress Port List
Specifies the ingress port to which the policy is to be assigned. A policy can be assigned to more than one port. To select more than one port, hold down the Ctrl key when you make your selections. A port can be an ingress port of only one policy at a time.

Egress Port
Specifies the egress port to which the policy is to be assigned. You can enter only one egress port. The egress port must be within the same port block as the ingress ports. On switches with 24 ports (plus uplinks), ports 1-26 form a port block. On switches with 48 ports (plus uplinks), ports 1-24 and 49 form one port block and ports 25-48 and 50 form a second port block.

A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.

Redirect Port
Specifies a port to where the traffic is to be redirected. Traffic that matches the defined traffic flow is redirected to the specified port. You can specify only one port.

6. Click **Apply**.
7. To permanently save your changes, select the **Save Config** menu selection.

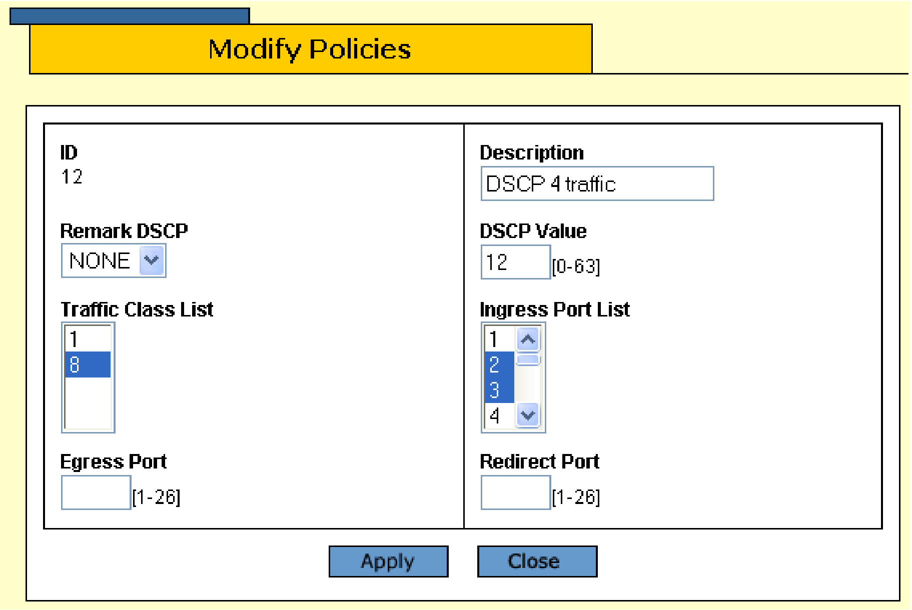
Modifying a Policy

To modify a policy, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 46 on page 151.
4. Select the policy to modify from the list and click **Modify**.

   The Modify Policy page is shown in Figure 48.



ID
12

Description
DSCP 4 traffic

Remark DSCP
NONE

DSCP Value
12 [0-63]

Traffic Class List
1
8

Ingress Port List
1
2
3
4

Egress Port
[1-26]

Redirect Port
[1-26]

Figure 48 Modify Policy Page

5. Modify the parameters as necessary. For definitions of the parameters, refer to Creating a Policy on page 151. You cannot change the ID number of a policy.
6. After you are finished modifying the parameters, click **Apply**.
7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Policy

To delete a policy, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Services** menu selection.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 46 on page 151.
4. Do one of the following:

- ❑ To delete just one policy, select the policy from the list and click **Delete**.
- ❑ To delete all the policies, click **Purge**.

Displaying Policies

To display the policies, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. Select the **Services** menu selection.
3. Select the **Policies** tab.

   The Policies tab displays the existing policies in a table that contains the following columns of information:

   ID
   The ID of the policy.

   Description
   A description of the policy.

   Active
   Whether or not this policy is active on the switch. An active policy is assigned to one or more switch ports. An inactive policy is not assigned to any switch ports.

   Traffic Class List
   The traffic classes assigned to the policy.

   Ingress Port List
   The ingress ports to which the policy is assigned.

4. To view the details of a specific policy, select the policy and click **View**.

   The descriptions of the parameters, refer to Creating a Policy on page 151.

5. Click **Close**.

Chapter 15

Class of Service

This chapter contains instructions on how to configure Class of Service (CoS). This chapter contains the following procedure:

Note
For background information on CoS, refer to the *AT-S62 Menus Interface User’s Guide*.

Configuring CoS

This procedure explains how to change the egress queue used to handle untagged ingress packets on a port. This procedure can also be used to override the priority levels in tagged ingress packets.

To configure CoS, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select the **Services** menu option.
3. Select the **CoS** tab.

   The CoS tab is shown in Figure 49.

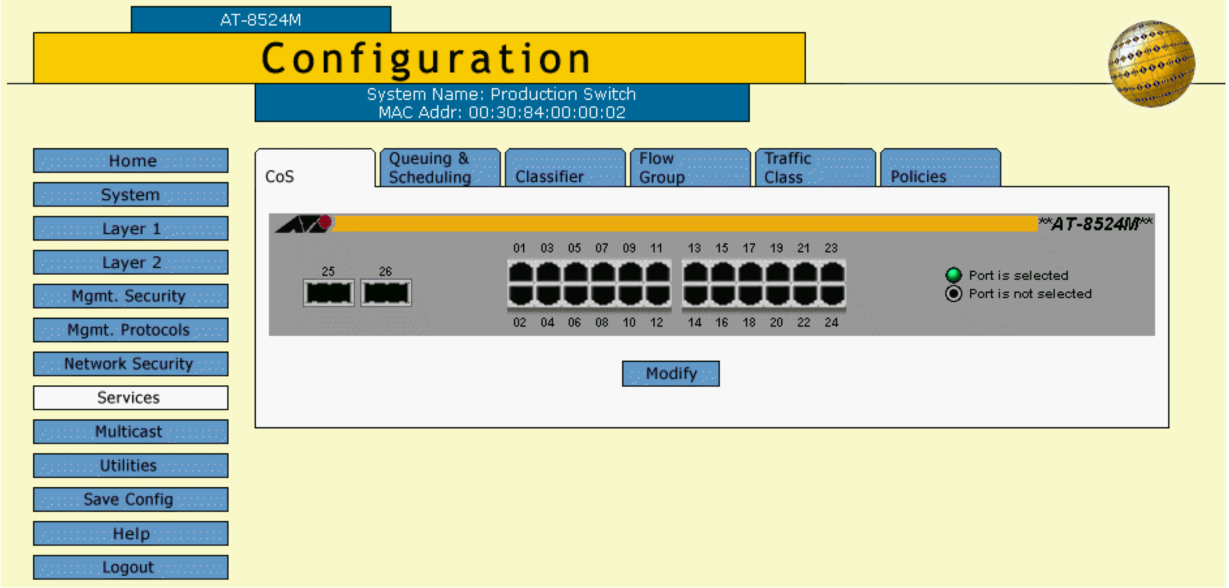
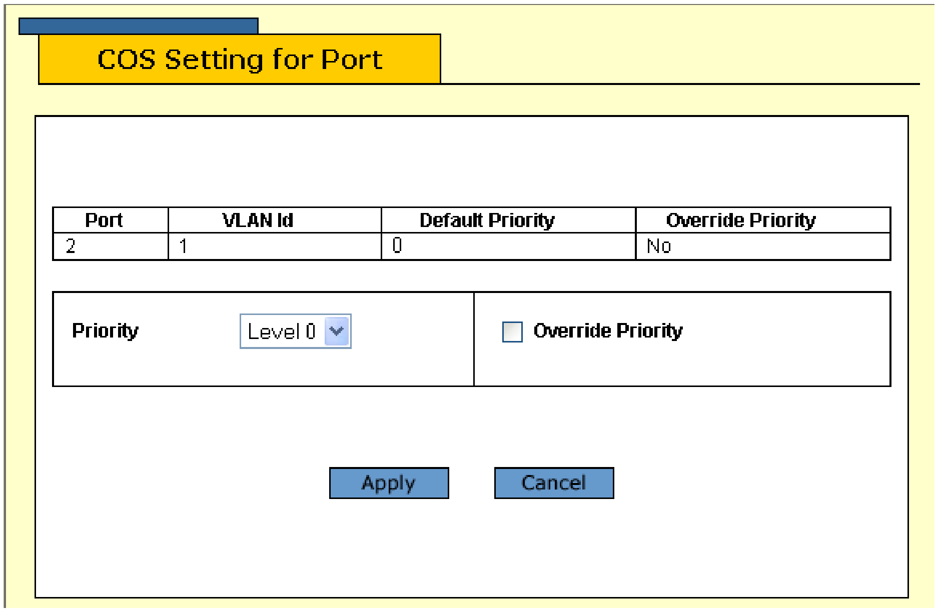


Figure 49 CoS Tab

4. Click the port where you want to configure CoS. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)
5. Click **Modify**.

The CoS Setting for Port page is shown in Figure 50.



COS Setting for Port

Port	VLAN Id	Default Priority	Override Priority
2	1	0	No

Priority Level 0

□ Override Priority

Figure 50 CoS Setting for Port Page

6. Use the Priority list to select a value from Level 1 to Level 7 that corresponds to the egress queue where you want all untagged ingress frames received on the port to be stored. For example, if you select Level 4, all untagged packets received on the port will be stored in egress queue Q2 of the egress port. The default is Level 0, which corresponds to Q0. (If you perform Step 6 and override the priority level in tagged packets, the selected egress queue is also used to store all tagged packets.)

7. If you are configuring a tagged port and you want the port to ignore the priority tag in egress tagged frames, click the **Override Priorit**y option. A check in the box indicates this feature is activated. All tagged frames will be directed to the egress queue specified in Step 6.

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

The default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.

8. Click **Apply**.

Configuration changes are immediately activated on the switch.

9. To permanently save the change, click the **Save Config** menu option.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, shown in Table 5. This is set at the switch level.

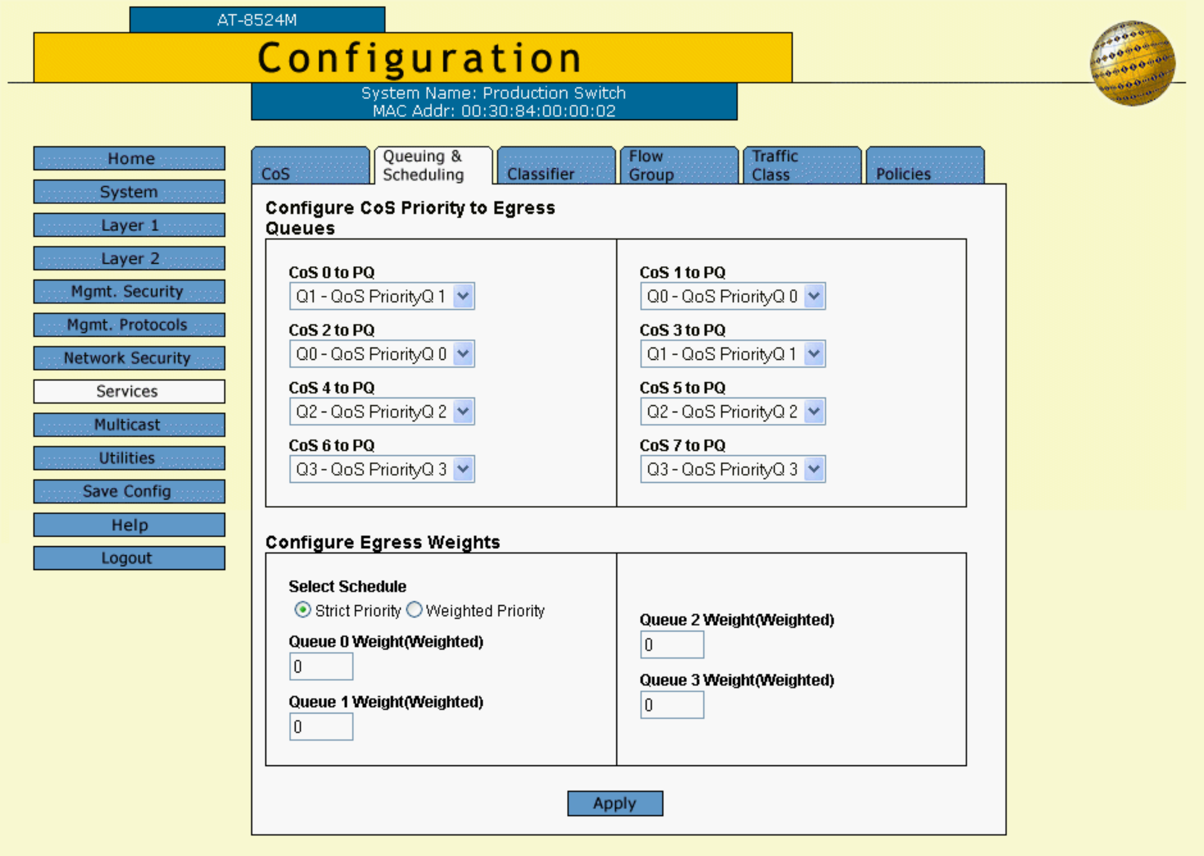
Table 5 Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0
2	Q0
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

To change the mappings, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select the **Services** menu option.
3. Select the **Queuing and Scheduling** tab.

The Scheduling tab is shown in Figure 51.



Configure CoS Priority to Egress Queues

CoS 0 to PQ: Q1 - QoS PriorityQ 1	CoS 1 to PQ: Q0 - QoS PriorityQ 0
CoS 2 to PQ: Q0 - QoS PriorityQ 0	CoS 3 to PQ: Q1 - QoS PriorityQ 1
CoS 4 to PQ: Q2 - QoS PriorityQ 2	CoS 5 to PQ: Q2 - QoS PriorityQ 2
CoS 6 to PQ: Q3 - QoS PriorityQ 3	CoS 7 to PQ: Q3 - QoS PriorityQ 3

Configure Egress Weights

Select Schedule
● Strict Priority ○ Weighted Priority

Queue 0 Weight(Weighted): 0

Queue 1 Weight(Weighted): 0

Queue 2 Weight(Weighted): 0

Queue 3 Weight(Weighted): 0

Figure 51 Queuing and Scheduling Tab

Note
The Configure Egress Weights section in the tab is explained in the next procedure, Configuring Egress Scheduling on page 161.

4. In the Configure CoS Queues to Egress Queues section of the tab, click the list for a CoS priority whose queue assignment you want to change and select the new queue.

   For example, to direct all tagged packets with a CoS priority level of 5 to egress queue Q3, you would use the list in **CoS 5 to PQ** and select **Q3 - QoS PriorityQ 3.**

5. If desired, repeat Step 4 to change the egress queue assignments of other CoS priorities.
6. Click **Apply**.
7. To permanently save the change, click the **Save Config** menu option.

Configuring Egress Scheduling

This procedure explains how to select and configure a scheduling method for QoS. Scheduling determines the order in which the ports handle packets in their egress queues. For an explanation of the two scheduling methods, refer to the *AT-S62 Menus Interface User's Guide*. Scheduling is set at the switch level. You cannot set this at the port level.

To change scheduling, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, select the **Services** menu option.
3. Select the **Queuing & Scheduling** tab.

   The Scheduling tab is shown in Figure 51 on page 160.

   Note
   The Configure CoS Queues to Egress Queues section in the tab is explained in the previous procedure Mapping CoS Priorities to Egress Queues on page 159.

4. To select a scheduling method, click either **Strict Priority** or **Weighted Priority** in the Configure Egress Weights section of the tab. The default is Strict Priority.

   Skip the next step if you select Strict Priority. Queue weights do not apply to Strict Priority scheduling.

5. If you selected Weighted Priority, use the Queue # Weight fields to specify for each queue the number of packets you want a port to transmit before it goes to the next queue.

   Leaving the default value of 1 for each queue results in all egress queues being given the same priority.

6. Click **Apply**.
7. To permanently save the change, click the **Save Config** menu option.

Displaying the CoS Settings

To display the CoS settings, do the following:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Services** menu option.
3. Select the **CoS** tab.
4. Click the port whose CoS settings you want to view. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)
5. Click **View**. The CoS Setting for Port page is shown for the selected port.

   The page displays the following information:

   Port
   The port number.

   VLAN Id
   The VLAN of which the port is a member.

   Default Priority
   The default priority level for this port.

   Override Priority
   Whether or not the default priority should be overridden.

Displaying QoS Queuing and Scheduling

To display QoS queuing and scheduling, do the following:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Services** menu option.
3. Select the **Queuing & Scheduling** tab.

   The upper section of the tab displays the CoS priority to egress queue assignments. The lower half displays the egress weight settings. For an explanation of the information in this window, refer to Mapping CoS Priorities to Egress Queues on page 159 and Configuring Egress Scheduling on page 161.

Chapter 16

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch.

Sections in the chapter include:

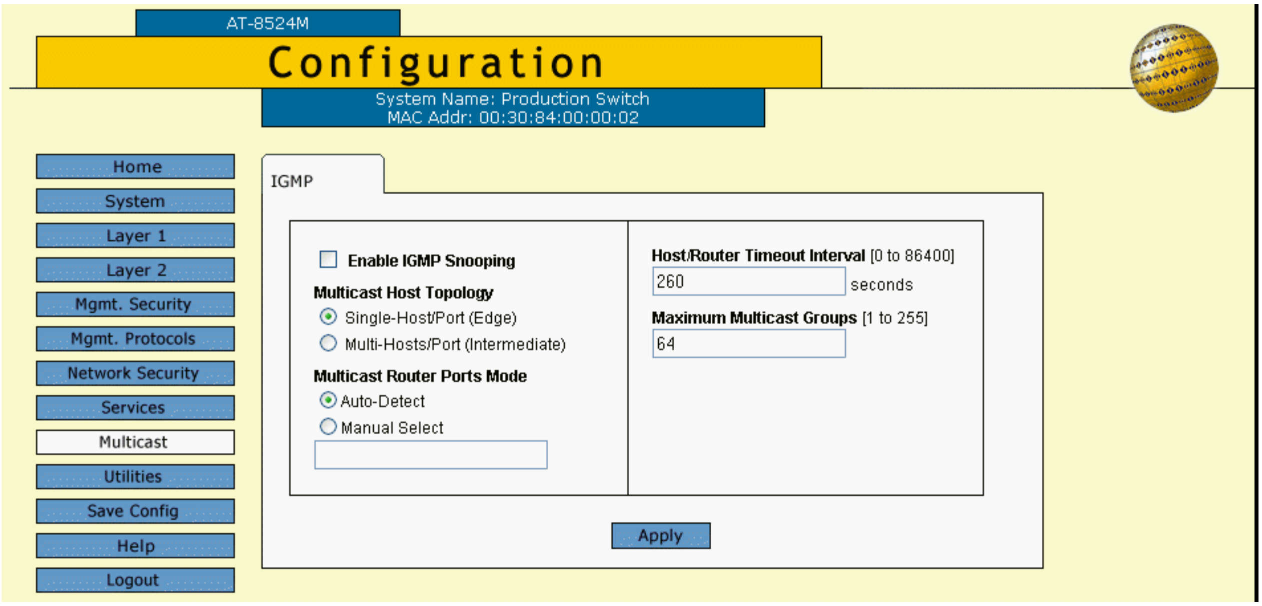
Note
For background information on IGMP snooping, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management session, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Multicast** menu option.

   The IGMP tab is shown in Figure 52.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

□ Enable IGMP Snooping

Multicast Host Topology
● Single-Host/Port (Edge)
○ Multi-Hosts/Port (Intermediate)

Multicast Router Ports Mode
● Auto-Detect
○ Manual Select

Host/Router Timeout Interval [0 to 86400]
260 seconds

Maximum Multicast Groups [1 to 255]
64

Figure 52 IGMP Tab (Configuration)

3. Adjust the IGMP parameters as necessary.

   The parameters are explained below:

   Enable IGMP Snooping
   Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

   Multicast Host Topology
   Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

   The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times-out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Multicast Router Ports Mode
Specifies whether the router ports will be determined automatically or if you will enter them manually. If you want the switch to determine the ports automatically, select Auto-Detect, which is the default. To enter them yourself, click Manual Select and enter the ports in the field.

Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

A value of 0 disables the timer. A switch with a disabled timer never times out inactive host nodes or multicast routers.

Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

4. After setting the IGMP snooping parameters, click **Apply**.
5. To permanently save the change, click the **Save Config** menu option.

Displaying a List of Host Nodes and Multicast Routers

You can use the AT-S62 software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. To view host nodes and multicast routers, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Multicast** menu option.

   The IGMP tab is displayed. For an explanation of the information in this tab, refer to the previous procedure.
3. To view the multicast addresses and the host nodes, click **View Multicast Host List** and then click **View**. To view the multicast routers, click **View Multicast Router List** and then click **View**.

   Viewing a list of host nodes opens a page containing the following information. The information in the page is for viewing purposes only.

   Multicast Group
   The multicast address of the group.

   VLAN ID
   The VID of the VLAN in which the port is an untagged member.

   Member Port
   The port(s) on the switch to which one or more host nodes of the multicast group are connected.

   Host IP
   The IP address(es) of the host node(s) connected to the port.

   Status
   The status of the host node. Status can be:

   ❑ Active - The host node is an active member of the group.

   ❑ Left Group - The host node recently left the group.

   Viewing a list of multicast routers displays a page containing the following information. The information in the page is for viewing purposes only.

   Port
   The port on the switch where the multicast router is connected.

   VLAN ID
   The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the port on the router.

Chapter 17
Denial of Service Defense

This chapter contains instructions on how to configure the Denial of Service defense feature on the switch. The sections include:

Note
For background information and guidelines on the Denial of Service defense feature, refer to the *AT-S62 Menus Interface User's Guide*. Be sure to read the overview before implementing a DoS defense. Some defense mechanisms are CPU intensive and can impact switch behavior.

Configuring Denial of Service Attack Defense

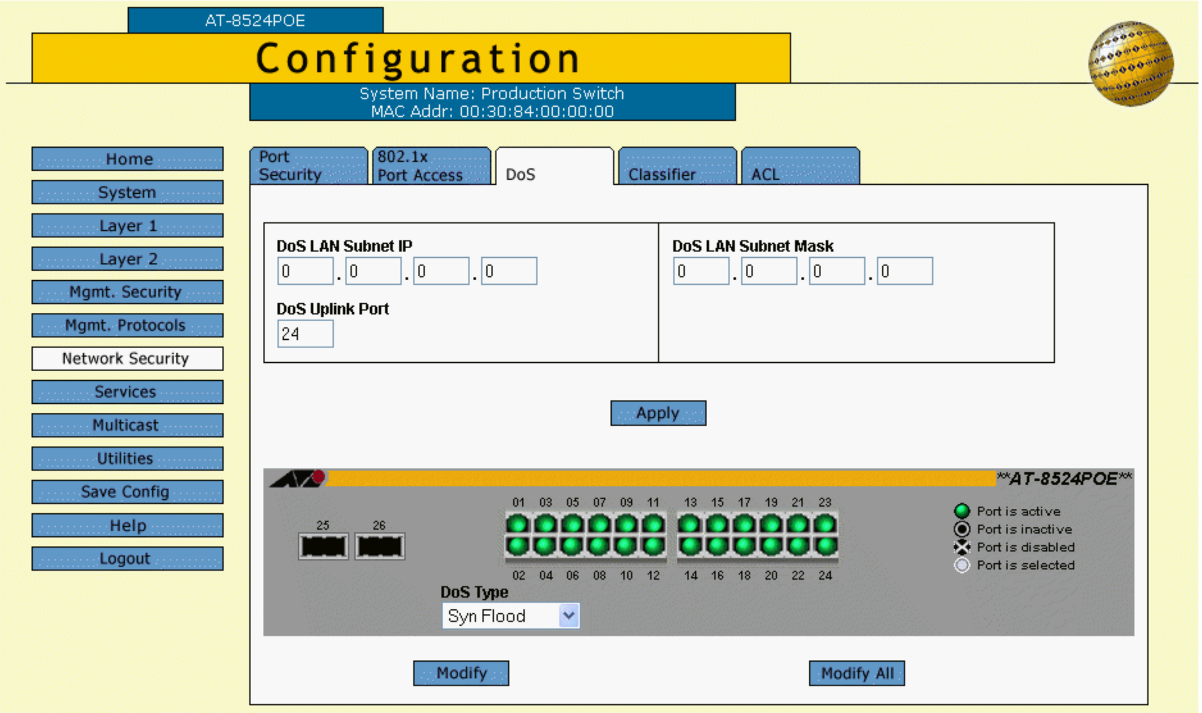
To configure the ports on the switch for a Denial of Service defense, perform the following procedure:

1. From the Home Page, select **Configuration**.

2. From the Configuration menu, select **Security**.

3. Select the **DoS** tab.

   The DoS tab is shown in Figure 53.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

DoS LAN Subnet IP: 0 . 0 . 0 . 0

DoS LAN Subnet Mask: 0 . 0 . 0 . 0

DoS Uplink Port: 24

DoS Type: Syn Flood

Figure 53 DoS Tab

4. If you are implementing the SMURF or Land defense, you must provide an IP address and mask for your LAN. To accomplish this, do the following steps. Otherwise, skip ahead to Step 5.

   a. In the DoS LAN Subnet IP field, enter the IP address of one of the devices connected to the switch, preferably the lowest IP address.

b. In the DoS Subnet Mask field, enter the LAN's mask. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The mask would be 0.0.0.63.

c. If you are activating the Land defense, in the DoS Uplink Port field enter the number of the port connected to the device (e.g., DSL router) that leads outside your network. You can specify only one uplink port. The default is the highest numbered existing port in the switch. For example, the default uplink port for an AT-8524M switch with no installed expansion modules would be Port 24.

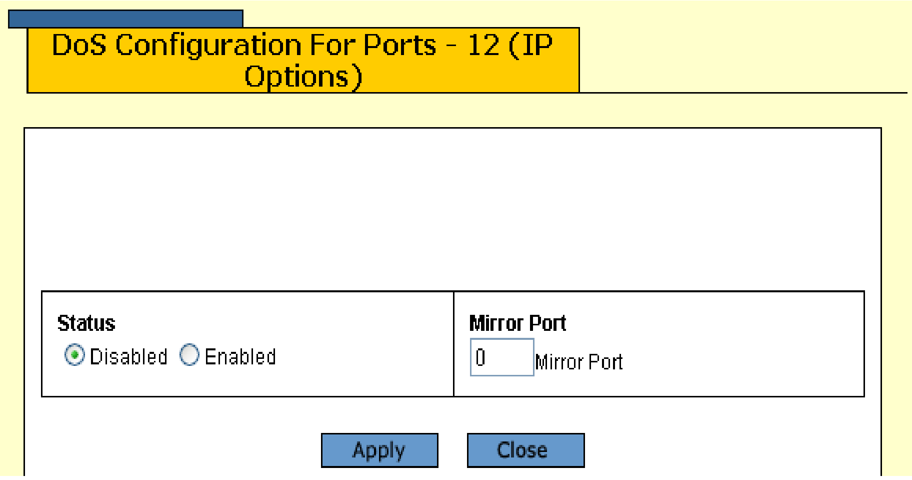
5. Click the ports in the switch image where you want to enable or disable a defense mechanism. A selected port turns white. To deselect a port, click it again. You can select more than one port at a time.

6. Using the DoS Type list, select the Denial of Service defense you want to either enable or disable on the ports. Your choices are:

   - ❑ Syn Flood attack
   - ❑ Smurf attack
   - ❑ Land attack
   - ❑ Tear drop attack
   - ❑ Ping of death attack
   - ❑ IP Options

7. Click **Modify**. To configure all the ports, click **Modify All**.

   The DoS Configuration page opens, as shown in Figure 54.



DoS Configuration For Ports - 12 (IP Options)

Status
● Disabled ○ Enabled

Mirror Port
0 Mirror Port

Figure 54 DoS Configuration Page

8. Adjust the settings as needed. The parameters are described below.

   Status
   Enables or disables the DoS on the selected ports.

   Mirror Port
   This option applies to Land, Tear Drop, Ping of Death, and IP Options. You can use this option to copy invalid traffic to another port on the switch. You can specify only one mirror port. Specifying a mirror port is not required.

9. Click **Apply**.

   The defense is immediately activated or deactivated on the ports.

10. To permanently save your changes, select the **Save Config** menu selection.

Displaying the DoS Settings

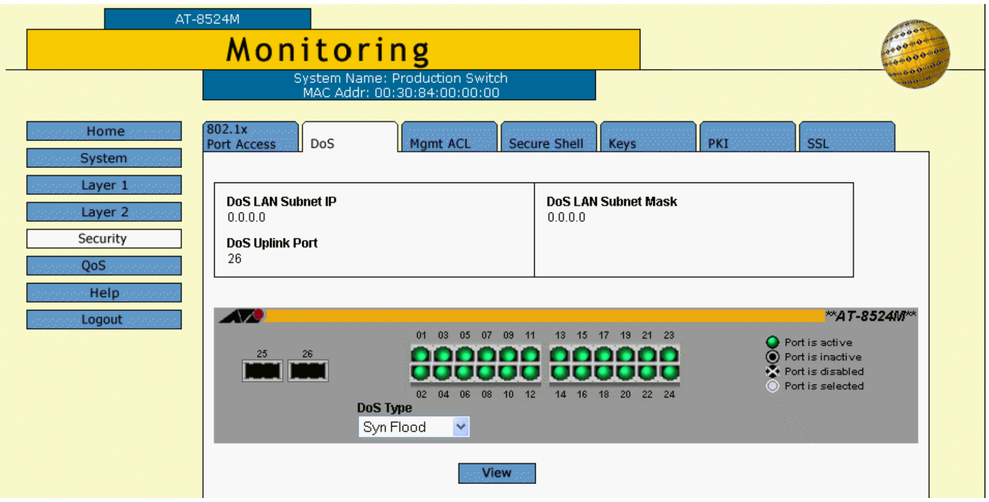
To display the DoS settings, do the following:

1. From the Home page, select **Monitoring**.

2. From the Monitoring menu, select the **Security** option.

3. Select the **DoS** tab.

   The DoS tab is shown in Figure 55.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

DoS LAN Subnet IP
0.0.0.0

DoS LAN Subnet Mask
0.0.0.0

DoS Uplink Port
26

DoS Type
Syn Flood

Figure 55 DoS Tab (Monitoring)

4. Click the port whose DoS settings you want to view. You can select more than one port at a time.

5. Using the DoS Type list, select the type of Denial of Service defense whose settings you want to view.

6. Click **View**.

Chapter 18

Power Over Ethernet

This chapter contains the procedures for configuring Power over Ethernet (PoE) for an AT-8524POE switch. Sections in the chapter include:

Note
PoE only applies to the AT-8524POE switch. For background information on PoE, refer to the *AT-S62 Menus Interface User's Guide*.

Setting the PoE Threshold

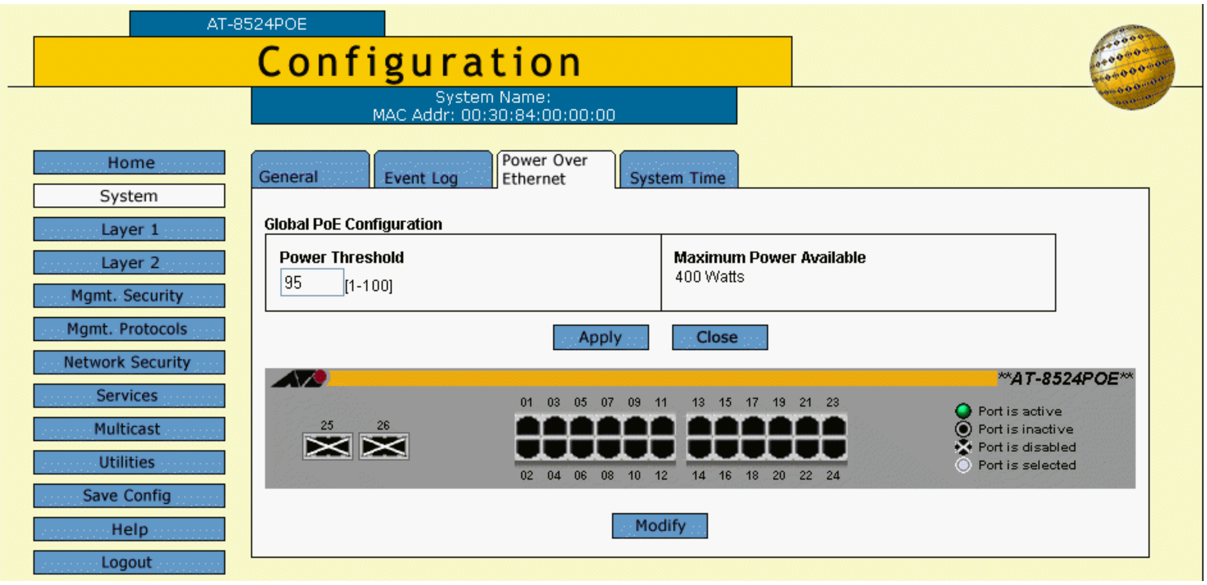
The PoE threshold is a percentage of the total maximum PoE power on the switch, which for the AT-8524POE switch is 400 W. If the total power requirements of the powered devices exceed this threshold, the switch sends an SNMP trap to your management workstation and enters an event in the event log. At the default setting of 95%, the threshold is exceeded when the PoE devices require more than 380 W, which is 95% of 400 W. The threshold is adjustable. Of course, for your management workstations to receive traps from the switch, you must configure SNMP on the switch by specifying the IP addresses of the workstations.

To configure the PoE threshold, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Power Over Ethernet** tab.

Note
The Power Over Ethernet tab only appears for AT-8524POE switches.

The Power Over Ethernet tab is shown in Figure 56.



Global PoE Configuration

Power Threshold
95 [1-100]

Maximum Power Available
400 Watts

Figure 56 Power Over Ethernet Tab

The Maximum Available Power field displays the maximum amount of PoE available from the switch for the powered devices connected to its ports. This value is 400W for the AT-8524POE switch. This value cannot be changed.

4. In the Power Threshold field, enter the new threshold value as a percentage of the total available PoE power on the switch. As an example, to configure the switch to enter an event in the event log and send an SNMP trap when power consumption exceeds 300 W, you would enter 75, for 75%.

5. Click **Apply**.

   The new threshold is immediately activated on the switch.

6. To permanently save the change, select the **Save Config** menu selection.

Configuring PoE Port Settings

This procedure enables and disables PoE on a port. This procedure also sets a port's priority level and its maximum power usage.

The default setting for PoE on a port is enabled. You do not have to disable PoE on ports that are connected to non-powered devices (that is, devices that receive their power from another power source). A port connected to a network node that is not a powered device functions as a regular Ethernet port, without PoE. The PoE feature remains activated on the port but no power is delivered to the device.

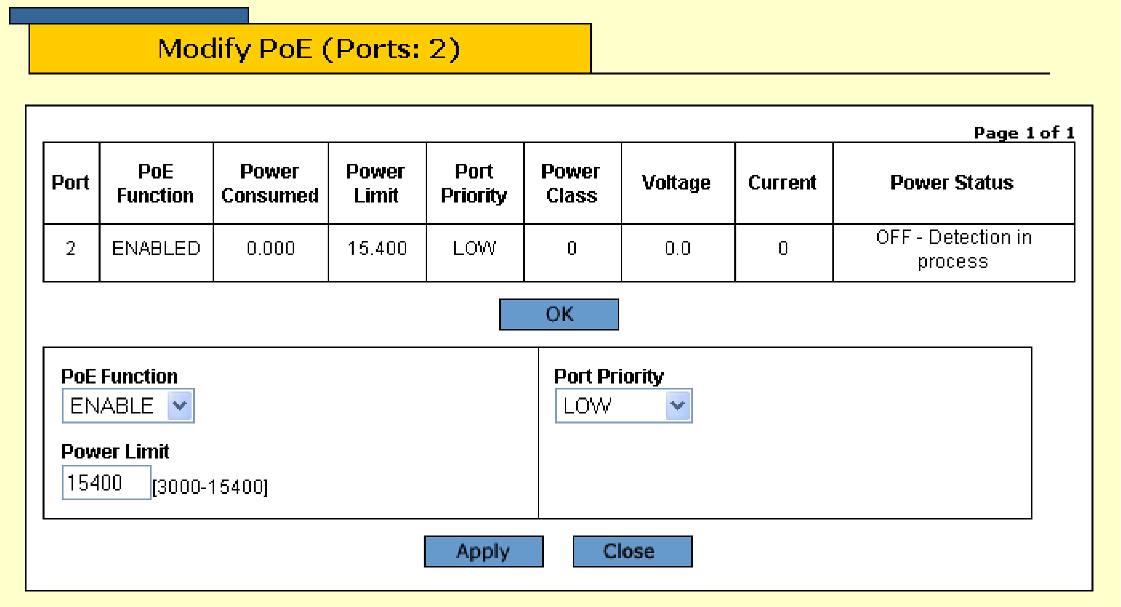
To configure PoE port settings, do the following:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Power Over Ethernet** tab.

> **Note**
> The Power Over Ethernet tab appears only for AT-8524POE switches.

4. In the graphic image of the switch, click the port you want to configure. A selected port turns white. You can configure more than one port at a time.
5. Click **Modify**.

   The PoE Port Configuration menu is shown in Figure 57.



Modify PoE (Ports: 2)

Page 1 of 1

Port	PoE Function	Power Consumed	Power Limit	Port Priority	Power Class	Voltage	Current	Power Status
2	ENABLED	0.000	15.400	LOW	0	0.0	0	OFF - Detection in process

PoE Function: ENABLE

Power Limit: 15400 [3000-15400]

Port Priority: LOW

Figure 57 PoE Port Configuration Page

The top portion of the page displays the PoE operating status of the selected ports. The columns are defined here:

Port
Port number.

PoE Function
Whether PoE is enabled or disabled on the port. The default setting is enabled.

Power Consumed
The amount of power in milliwatts currently consumed by the powered device connected to the port. If the port is not connected to a powered device, this value will be 0 (zero).

Power Limit
The maximum amount of power allowed by the port for the device. The default is 15,400 milliwatts (15.4 W).

Power Priority
The port priority. This can be Critical, High, or Low. The default is Low.

Power Class
The IEEE 802.3af class of the device.

Voltage
The voltage being delivered to the powered device

Current
The current drawn by the powered device.

Power Status
Whether power is being supplied to the device. Status will be one of the following:

ON: Power is being supplied to a powered device.

OFF - Disabled by user: PoE is disabled on the port.

Off - Detection in process: PoE is enabled on the port, but either no device is connected to the port or the device is not a powered device.

6. To enable or disable PoE on a port, set PoE Function to either **Enable** or **Disable**. The default is enabled.

7. To change a port's priority, set Power Priority to **Critical**, **High**, or **Low**. A port can belong to only one priority level at a time. The default is Low.

8. To change the maximum amount of power the port can supply to the device, enter a new value in the Power Limit field. The value is entered in milliwatts. The default value is 15,400 mW. The range is 3,000 to 15,400 mW.

9. After you finish setting the PoE parameters, click **Apply**.

   Changes to a port's PoE settings are immediately activated on the switch.

10. To permanently save the changes, select the **Save Config** menu selection.

Displaying PoE Status and Settings

Use this procedure to display PoE status and settings at the switch and port level.

To display PoE information, do the following:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Power Over Ethernet** tab.

> **Note**
> The Power Over Ethernet tab appears only for AT-8524POE switches.

The fields in the window are defined here:

Power Threshold
A percentage of the total PoE power on the switch which, when exceeded, causes the switch to enter an event in the event log and send an SNMP trap to the management workstations. As an example, at the default setting of 95%, the threshold is exceeded whenever the total power requirements of the powered devices exceed 380 W, which is 95% of 400 W, the maximum total PoE on an AT-8524POE switch.

Maximum Available
The maximum amount of PoE available from the switch for the powered devices connected to its ports. This value is 400W for the AT-8524POE switch.

To view the PoE settings of the individual ports, click a port in the the graphic switch image and click **View**. You can select more than one port at a time.

The columns in the window are defined here:

Port
Port number.

PoE Function
Whether PoE is enabled or disabled on the port. The default setting is enabled.

Power Consumed
The amount of power in milliwatts currently consumed by the powered device connected to the port. If the port is not connected to a powered device, this value will be 0 (zero).

Power Limit
The maximum amount of power allowed by the port for the device. The default is 15,400 milliwatts (15.4 W).

Power Priority
The port priority. This can be Critical, High, or Low. The default is Low.

Power Class
The IEEE 802.3af class of the device.

Voltage
The voltage being delivered to the powered device

Current
The current drawn by the powered device.

Power Status
Whether power is being supplied to the device. Status will be one of the following:

ON: Power is being supplied to a powered device.

OFF - Disabled by user: PoE is disabled on the port.

Off - Detection in process: PoE is enabled on the port, but the device connected to the port is not a powered device.

4. Click **Close**.

Section III

SNMPv3 Operations

This section contains the following chapter:

Chapter 19

SNMPv3 Protocol

This chapter provides the following procedures for configuring basic switch parameters using a web browser management session:

Note
For background information on SNMPv3, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to configure the SNMPv3 tables. To enable a manager to access the SNMPv3 protocol on the switch, you need to enable the SNMP protocol. See the following procedures:

- ❑ Enabling the SNMP Protocol on page 186
- ❑ Configuring the SNMPv3 User Table on page 188
- ❑ Configuring the SNMPv3 View Table on page 195
- ❑ Configuring the SNMPv3 Access Table on page 201
- ❑ Configuring the SNMPv3 SecurityToGroup Table on page 208
- ❑ Configuring the SNMPv3 Notify Table on page 213
- ❑ Configuring the SNMPv3 Target Address Table on page 218
- ❑ Configuring the SNMPv3 Target Parameters Table on page 224
- ❑ Configuring the SNMPv3 Community Table on page 231

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with the SNMPv1 or an SNMPv2c protocol. Allied Telesyn does not recommend this configuration.

For reference information about the SNMPv3 protocol, refer to the *AT-S62 Menus Interface User's Guide*.

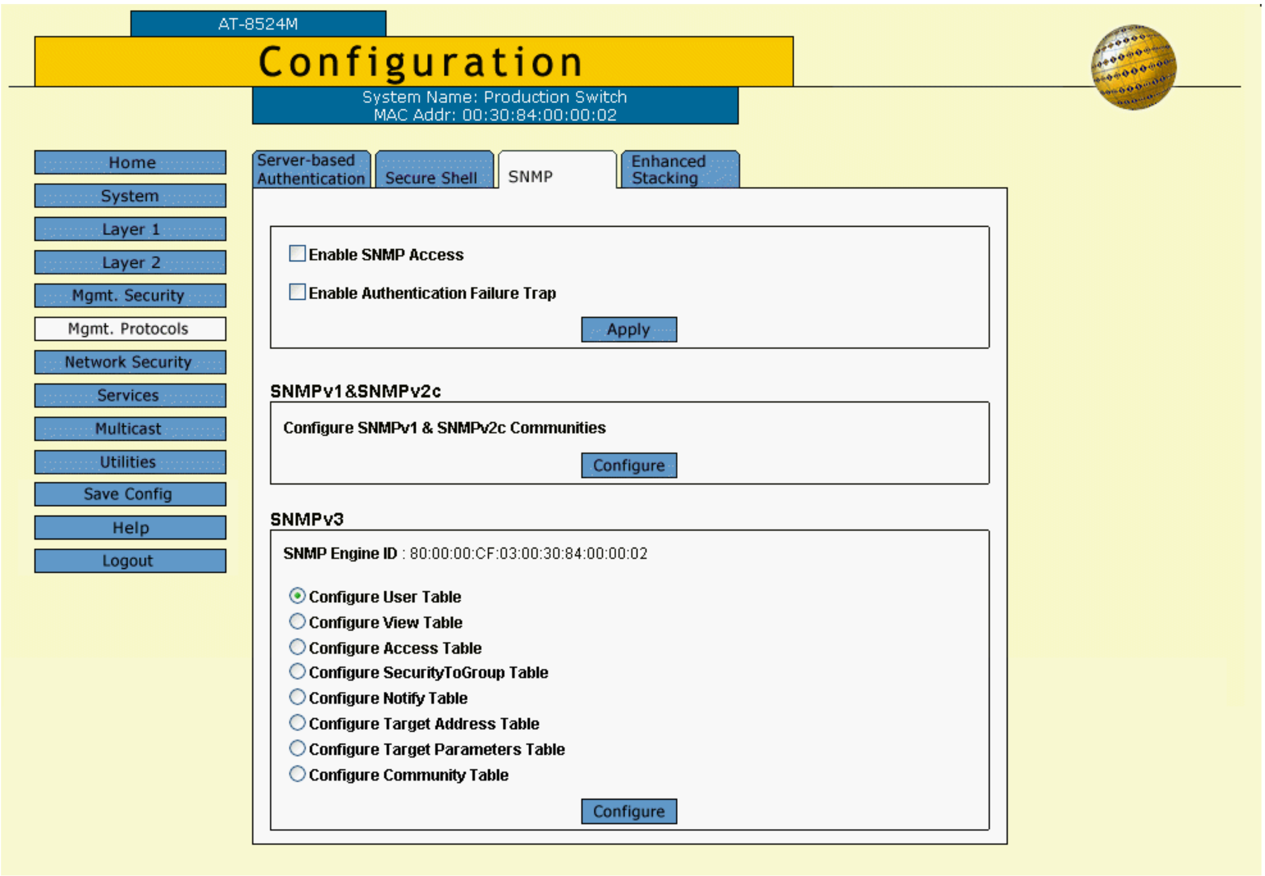
Enabling the SNMP Protocol

In order to allow an NMS (an SNMP manager) to access the switch, you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a request message, you need to enable authentication failure traps. This section provides a procedure to accomplish both of these tasks.

To enable SNMP access and authentication failure traps, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

☐ Enable SNMP Access

☐ Enable Authentication Failure Trap

SNMPv1&SNMPv2c

Configure SNMPv1 & SNMPv2c Communities

SNMPv3

SNMP Engine ID : 80:00:00:CF:03:00:30:84:00:00:02

● Configure User Table
○ Configure View Table
○ Configure Access Table
○ Configure SecurityToGroup Table
○ Configure Notify Table
○ Configure Target Address Table
○ Configure Target Parameters Table
○ Configure Community Table

Figure 58 SNMP Tab

4. To enable SNMP Access, click the box next to Enable SNMP Access.

   Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note
If the check box in the Enable SNMP Access box is empty, the switch cannot be managed through SNMP. This is the default.

5. To enable authentication failure traps to be sent on behalf of the switch, click the box next to Enable Authentication Failure Trap.
6. Click **Apply** to update the User Table.
7. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 User Table

You can create, delete, and modify an SNMPv3 User Table entry. See the following procedures:

❑ Creating a User Table Entry on page 188

❑ Deleting a User Table Entry on page 191

❑ Modifying a User Table Entry on page 191

For reference information about the SNMPv3 User Table, refer to the *AT-S62 Menus Interface User's Guide*..

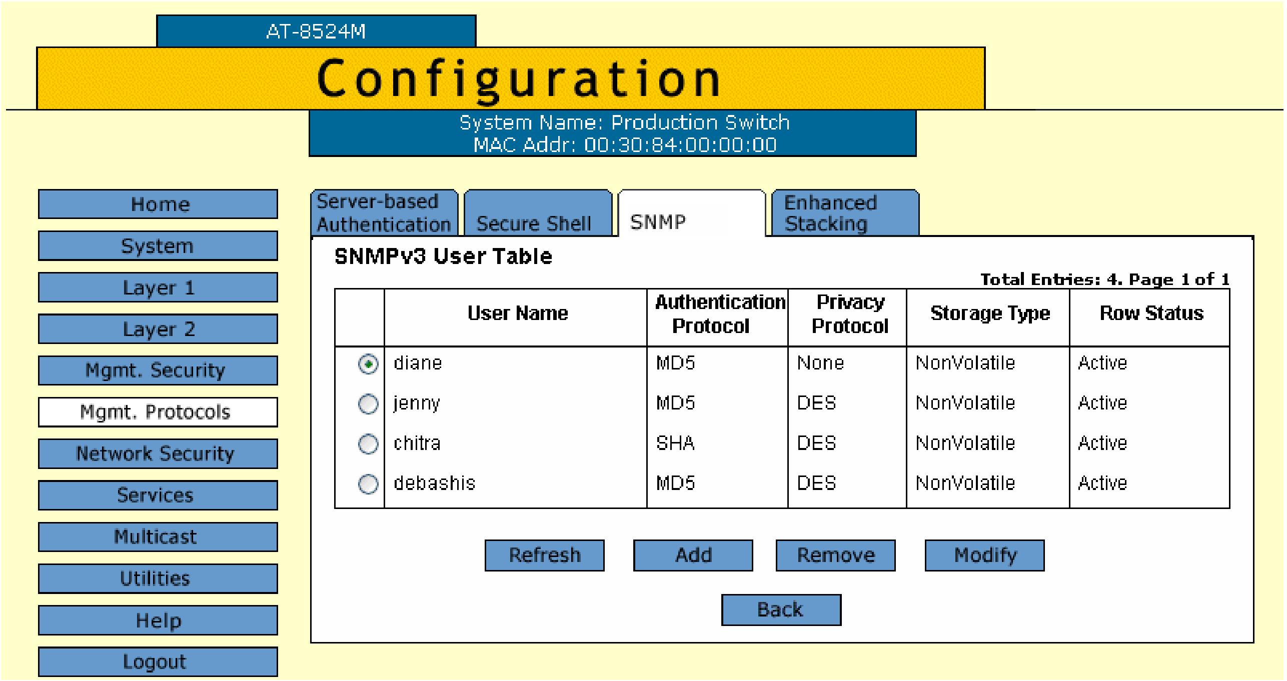
Creating a User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 User Table Page is shown in Figure 59.



SNMPv3 User Table

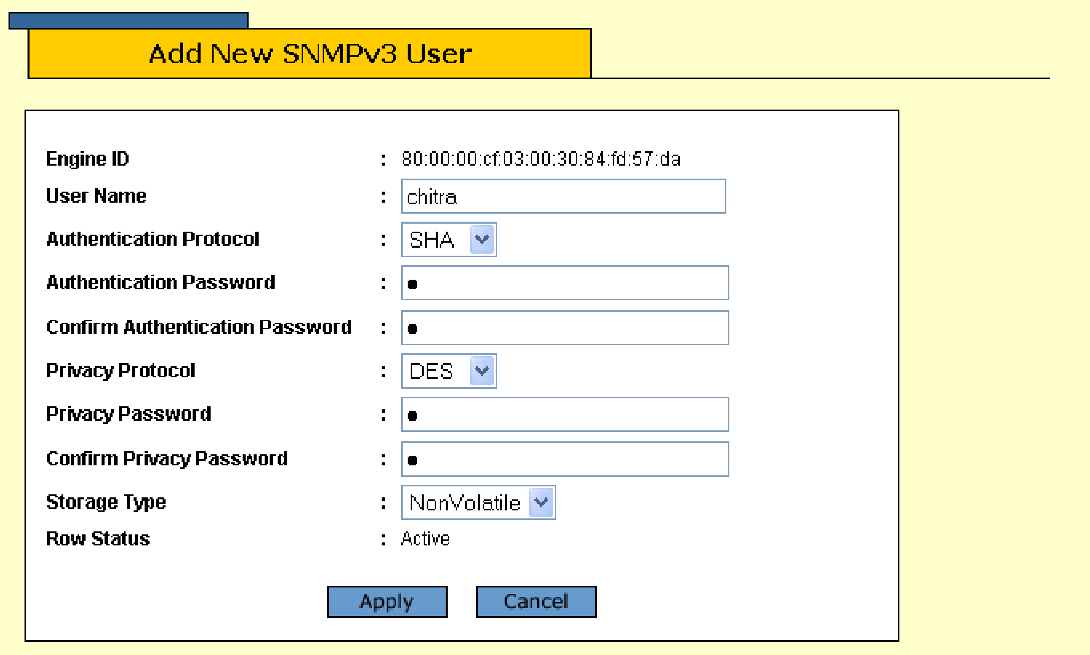
Total Entries: 4. Page 1 of 1

	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status
●	diane	MD5	None	NonVolatile	Active
○	jenny	MD5	DES	NonVolatile	Active
○	chitra	SHA	DES	NonVolatile	Active
○	debashis	MD5	DES	NonVolatile	Active

Figure 59 SNMPv3 User Table Page

5. Click the **Add** button to add a new SNMPv3 User Table entry.

   The Add New SNMPv3 User Page is shown in Figure 60



Add New SNMPv3 User

Engine ID	:	80:00:00:cf:03:00:30:84:fd:57:da
User Name	:	chitra
Authentication Protocol	:	SHA
Authentication Password	:	●
Confirm Authentication Password	:	●
Privacy Protocol	:	DES
Privacy Password	:	●
Confirm Privacy Password	:	●
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 60 Add New SNMPv3 User Page

6. In the User Name field, enter a name, or logon id, that consists of up to 32 alphanumeric characters

7. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users are authenticated with the MD5 authentication protocol after a message is received. With this selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. With this selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

8. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

9. In the Confirm Authentication Password field, re-enter the authentication password.

Note
If you have the AT-S60 software version 2.1.0 that does not contain the encryption features, then the Privacy Protocol field is read-only field and it is set to None.

Note
You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

10. In the Privacy Protocol field, enter one of the following options:

    DES
    Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

    None
    Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

11. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

12. In the Confirm Privacy Password field, re-enter the privacy password.

13. In the Storage Type field, enter one of the following storage options for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the User Table to the configuration file. After making changes to an User Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the User Table to the configuration file. After making changes to an User Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

14. Click **Apply** to update the SNMPv3 User Table.
15. To save your changes, select the **Save Config** menu selection.

Deleting a User Table Entry

To delete an entry in the SNMPv3 User Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure**.

   The SNMPv3 User Table Page is shown in Figure 59 on page 188.
5. Click the circle next to the User Table entry that you want to delete. Then click **Remove**.

   A warning message is displayed. Click OK to remove the User Table entry.
6. To save your changes, select the **Save Config** menu selection.

Modifying a User Table Entry

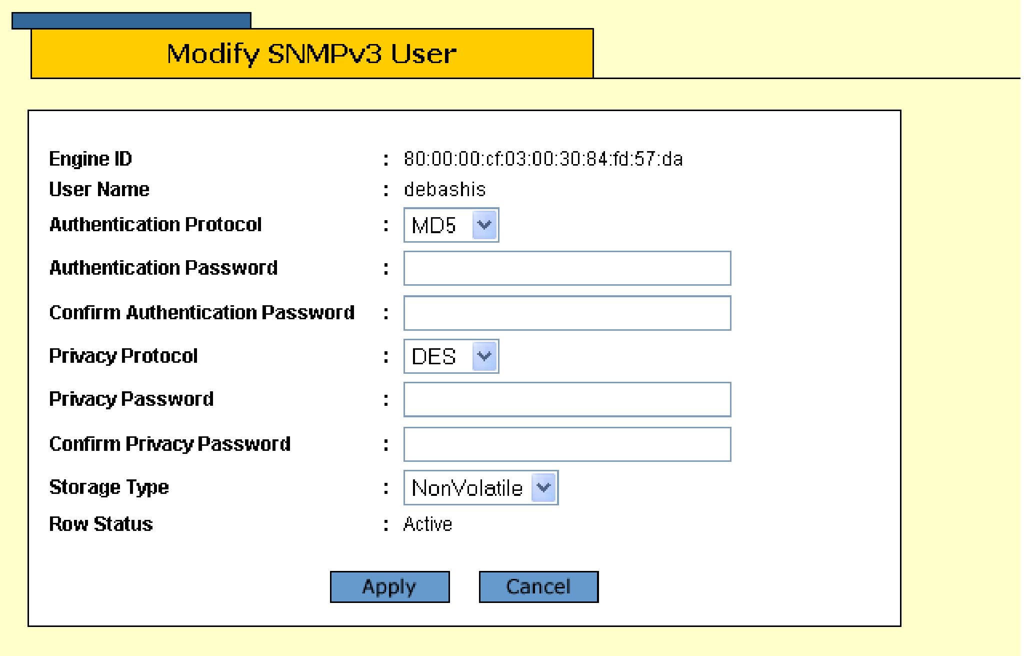
To modify an entry SNMPv3 User Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure**.

   The SNMPv3 User Table Page is shown in Figure 59 on page 188.
5. To modify an SNMPv3 User Table entry, click the circle next to the SNMPv3 user that you want to change. Then click **Modify**.

The Modify SNMPv3 User Page is shown in Figure 61.



Modify SNMPv3 User

Engine ID	:	80:00:00:cf:03:00:30:84:fd:57:da
User Name	:	debashis
Authentication Protocol	:	MD5
Authentication Password	:	
Confirm Authentication Password	:	
Privacy Protocol	:	DES
Privacy Password	:	
Confirm Privacy Password	:	
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 61 Modify SNMPv3 User Page

6. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users are authenticated with the MD5 authentication protocol after a message is received. With this selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. With this selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note
When you change the Authentication Protocol field, you must reenter the authentication password. In addition, if the Privacy Protocol is set to DES and you change Authentication Protocol, then you must reenter the Privacy Password.

7. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

8. In the Confirm Authentication Password field, re-enter the authentication password.

Note
If you have the AT-S60 software version 2.1.0 that does not contain the encryption features, then the Privacy Protocol field is read-only field and it is set to None.

Note
You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

9. In the Privacy Protocol field, enter one of the following options:

   DES
   Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

   None
   Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

10. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

11. In the Confirm Privacy Password field, re-enter the privacy password.

12. In the Storage Type field, enter one of the following storage options for this User Table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table to the configuration file. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the SNMPv3 User Table to the configuration file. After making changes to an SNMPv3 User Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.
14. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 View Table

You can create, delete, and modify an SNMPv3 View Table entry. See the following procedures:

- □ Creating a View Table Entry on page 195
- □ Deleting a View Table Entry on page 198
- □ Modifying a View Table Entry on page 199

For reference information about the SNMPv3 View Table, see Configuring the SNMPv3 View Table on page 195.

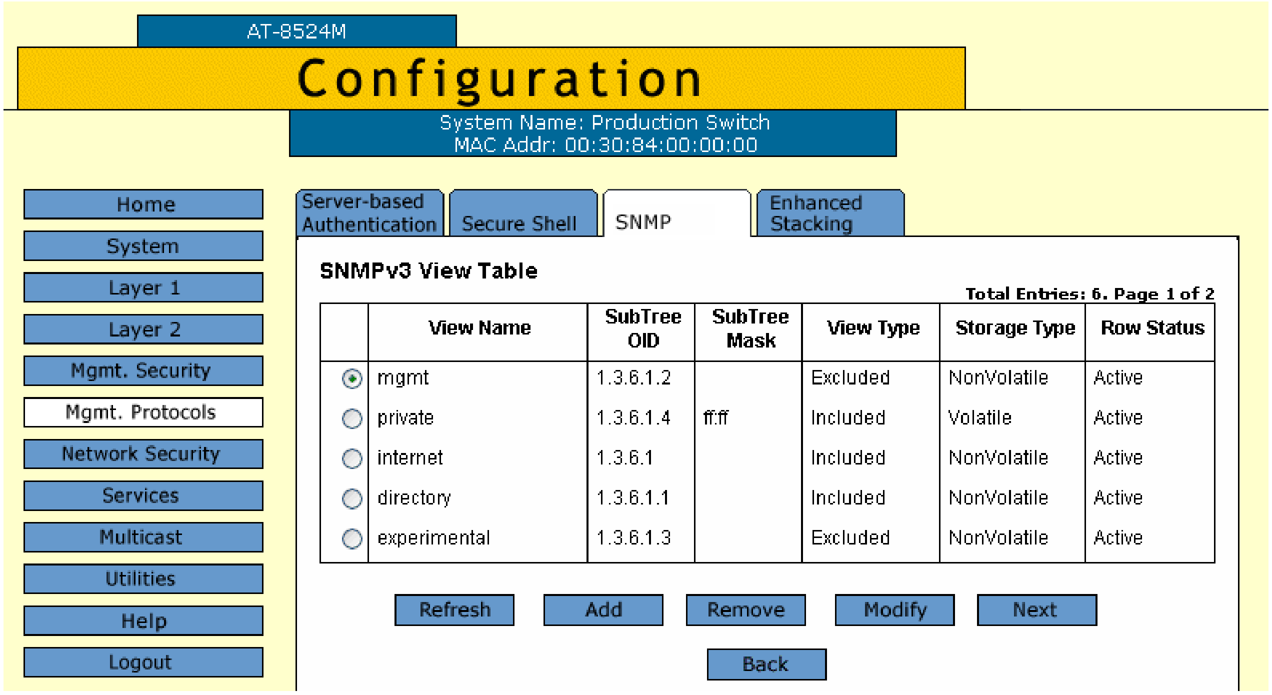
Creating a View Table Entry

To create an entry in the SNMPv3 View Table entry, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 View Table Page is shown in Figure 62.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

SNMPv3 View Table

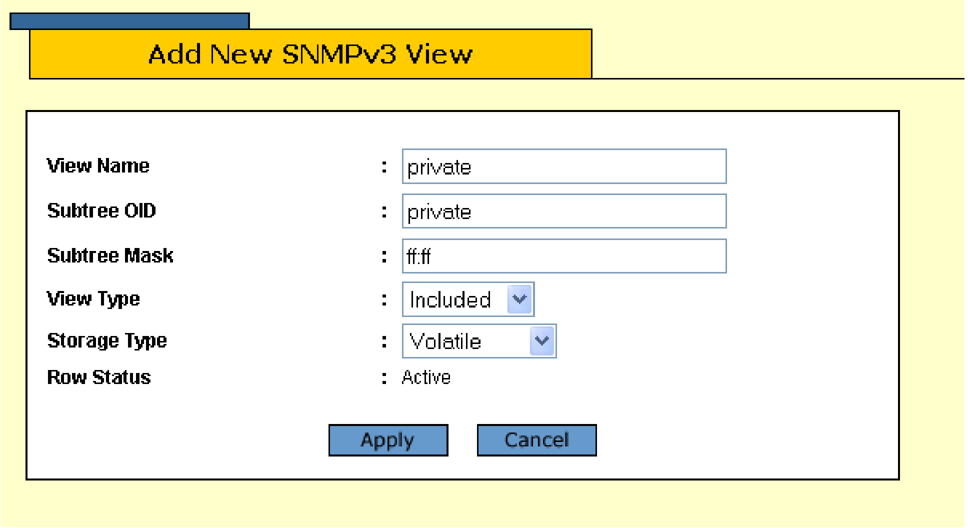
Total Entries: 6. Page 1 of 2

	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
●	mgmt	1.3.6.1.2		Excluded	NonVolatile	Active
○	private	1.3.6.1.4	ff:ff	Included	Volatile	Active
○	internet	1.3.6.1		Included	NonVolatile	Active
○	directory	1.3.6.1.1		Included	NonVolatile	Active
○	experimental	1.3.6.1.3		Excluded	NonVolatile	Active

Figure 62 SNMPv3 View Table Page

5. To create a new SNMPv3 View Table entry click **Add**.

   The Add New SNMPv3 View Page is shown in Figure 63.



Add New SNMPv3 View

View Name	:	private
Subtree OID	:	private
Subtree Mask	:	ff:ff
View Type	:	Included
Storage Type	:	Volatile
Row Status	:	Active

Figure 63 Add New SNMPv3 View Page

6. In the View Name field, enter a descriptive name of this view.

   Assign a name that reflects the subtree OID, for example, “internet.” Enter a unique name of up to 32 alphanumeric characters.

Note
The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use the default value for an SNMPv3 View Table entry.

7. In the Subtree OID field, enter a subtree that this view will or will not be permitted to display.

   You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:

   ```
   1.3.6.1.2.1.6
   ```

   The text format is for TCP/IP is:

   ```
   tcp
   ```

8. In the Subtree Mask field, enter a subtree mask in hexidecimal format.

   This is an optional parameter that is used to further refine the value in the View Subtree parameter. This parameter is in binary format.

The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

9. In the View Type field, enter one of the following view types:

   Included
   Enter this value to permit the user to see the subtree specified above.

   Excluded
   Enter this value to not permit the user to see the subtree specified above.

10. In the Storage Type field, enter a storage type for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the View Table to the configuration file. After making changes to a View Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the View Table to the configuration file. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 View Table.

12. To save your changes, select the **Save Config** menu selection.

Deleting a View Table Entry

To delete an entry in the SNMPv3 View Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure**.
5. The SNMPv3 View Table Page is shown in Figure 62 on page 195.
6. Click the circle next to the View Table entry that you want to delete. Then click **Remove**.

   A warning message is displayed. Click OK to remove the View Table entry.
7. To save your changes, select the **Save Config** menu selection.

Modifying a View Table Entry

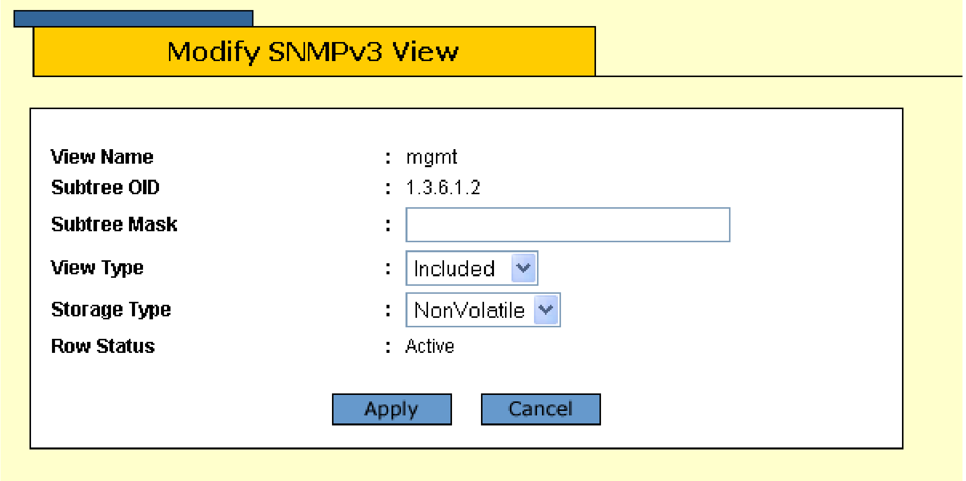
To modify an entry in the SNMPv3 View Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 View Table Page is shown in Figure 62 on page 195.
5. To modify an SNMPv3 View Table entry, click the circle next to the SNMPv3 View Table entry that you want to change. Then click **Modify**.

   The Modify SNMPv3 View Page is shown in Figure 64.



Modify SNMPv3 View

View Name	:	mgmt
Subtree OID	:	1.3.6.1.2
Subtree Mask	:	
View Type	:	Included
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 64 Modify SNMPv3 View Page

6. In the Subtree Mask field, enter a subtree mask in hexidecimal format.

   This is an optional parameter that is used to further refine the value in the View Subtree parameter. This parameter is in binary format.

   The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

7. In the View Type field, enter one of the following view types:

   Included
   Enter this value to permit the View Name to see the subtree specified above.

   Excluded
   Enter this value to not permit the View Name to see the subtree specified above.

8. In the Storage Type field, enter a storage type for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the View Table to the configuration file. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

   Note
   The Row Status parameter is a read-only field in the web interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 View Table.

10. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 Access Table

You can create, delete, and modify an SNMPv3 Access Table entry. See the following procedures:

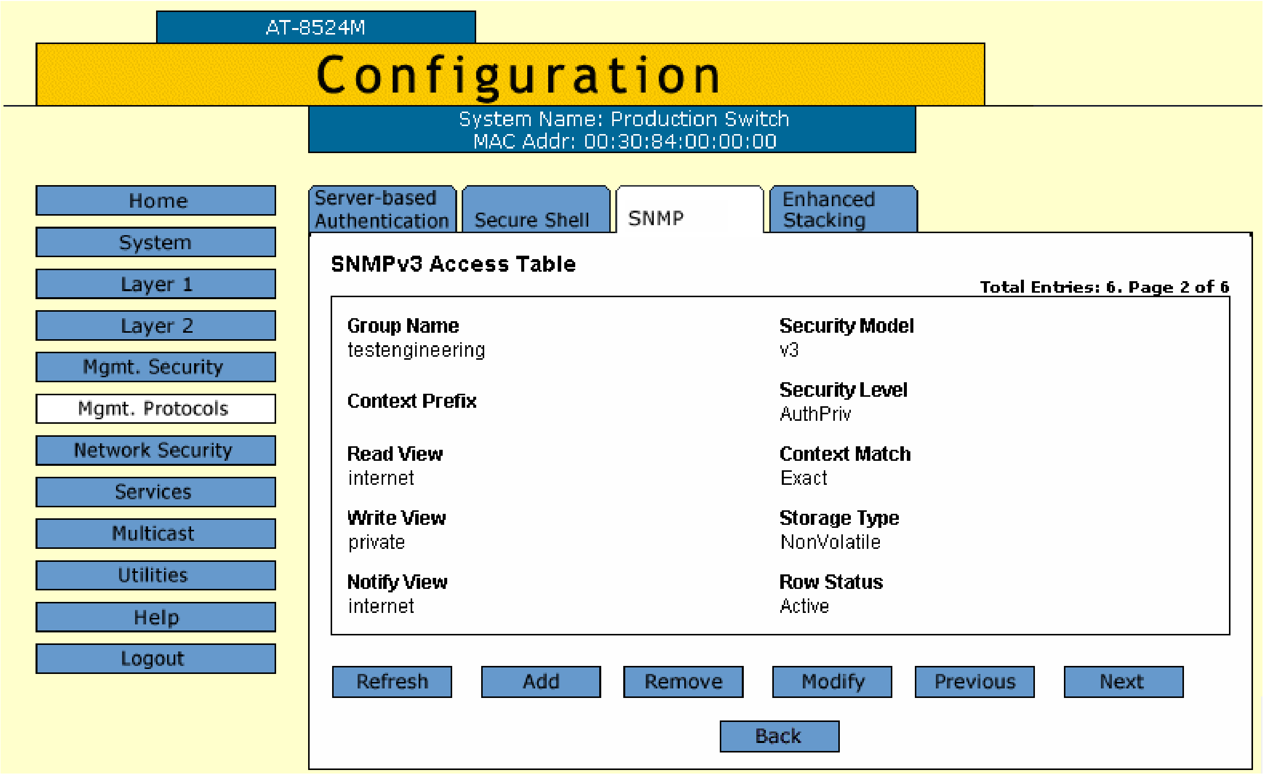
- ❑ Creating an Access Table on page 201
- ❑ Deleting an Access Table Entry on page 204
- ❑ Modifying an Access Table Entry on page 206

For reference information about the SNMPv3 Access Table, see Configuring the SNMPv3 Access Table on page 201.

Creating an Access Table

To create an entry in the SNMPv3 Access Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab. The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page. The SNMPv3 Access Table Page is shown in Figure 65.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

SNMPv3 Access Table

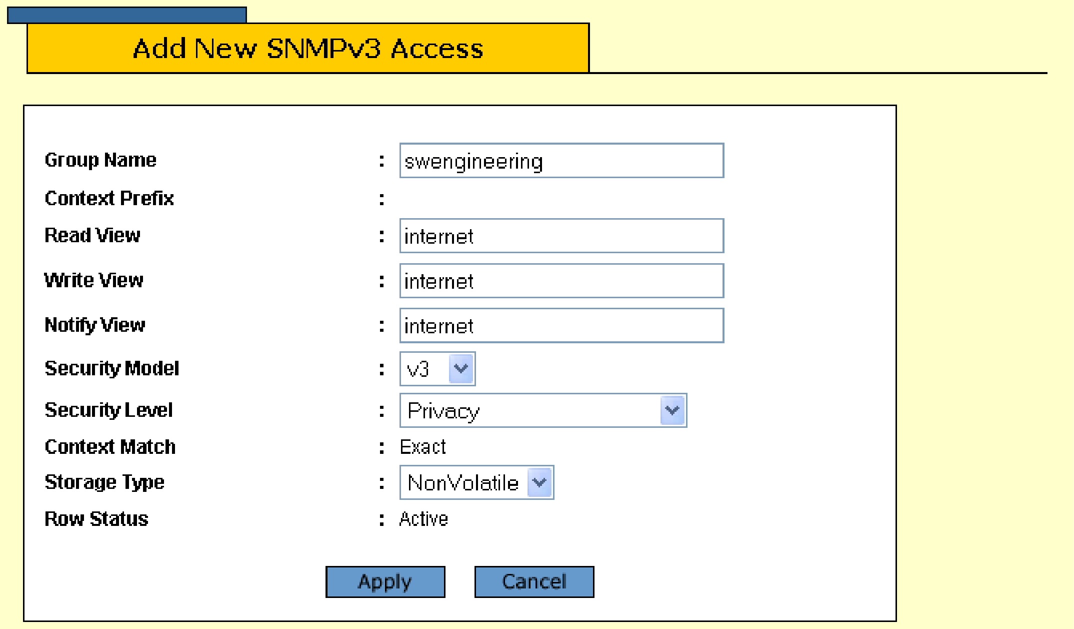
Total Entries: 6. Page 2 of 6

Group Name testengineering	**Security Model** v3
Context Prefix	**Security Level** AuthPriv
Read View internet	**Context Match** Exact
Write View private	**Storage Type** NonVolatile
Notify View internet	**Row Status** Active

Figure 65 SNMPv3 Access Table Page

5. To create an SNMPv3 Access Table entry, click **Add**.

   The Add New SNMPv3 Access Page is shown in Figure 66.



Add New SNMPv3 Access

Group Name	:	swengineering
Context Prefix	:	
Read View	:	internet
Write View	:	internet
Notify View	:	internet
Security Model	:	v3
Security Level	:	Privacy
Context Match	:	Exact
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 66 Add New SNMPv3 Access Page

6. In the Group Name field, enter a descriptive name of the group.

   The Group Name can consist of up to 32 alphanumeric characters.

   You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, a unique group name makes it easier for you to tell the groups apart.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   ❑ defaultV1GroupReadOnly

   ❑ defaultV1GroupReadWrite

   ❑ defaultV2cGroupReadOnly

   ❑ defaultV2cGroupReadWrite

Note
The Context Prefix field is a read only field. The Context Prefix field is always set to null.

7. In the Read View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

8. In the Write View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

9. In the Notify View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

10. In the Security Model field, enter an SNMP protocol.

    Select one of the following SNMP protocols as the Security Model for this Group Name.

    v1
    Select this value to associate the Group Name with the SNMPv1 protocol.

    v2c
    Select this value to associate the Group Name with the SNMPv2c protocol.

    v3
    Select this value to associate the Group Name with the SNMPv3 protocol.

11. In the Security Level field, enter a security level.

    Select one of the following security levels:

    No Authentication/Privacy
    This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate users and you do not want to encrypt messages using a privacy protocol. This option provides the least security.

    Note
    If you have selected SNMPv1 or SNMPv2c, NoAuthenticationNoPrivacy is the only security level you can select.

    Authentication
    This option permits an authentication protocol, but not a privacy protocol. Select this security level if you want to authenticate

SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

> **Note**
> The Context Match field is a read only field. The Context Match field is always set to Exact.

12. In the Storage Type field, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

> **Note**
> The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

13. Click **Apply** to update the SNMPv3 Access Table.
14. To save your changes, select the **Save Config** menu selection.

Deleting an Access Table Entry

To delete an entry in the SNMPv3 Access Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

    The SNMP Tab is shown in Figure 58 on page 186.

4. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Access Table Page is shown in Figure 65 on page 201.

5. Display the Access Table entry that you want to delete.

   Click **Next** or **Previous** to display an entry.

6. Click **Remove**.

   A warning message is displayed. Click OK to remove the Access Table entry.

7. To save your changes, select the **Save Config** menu selection.

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table, perform the following procedure.

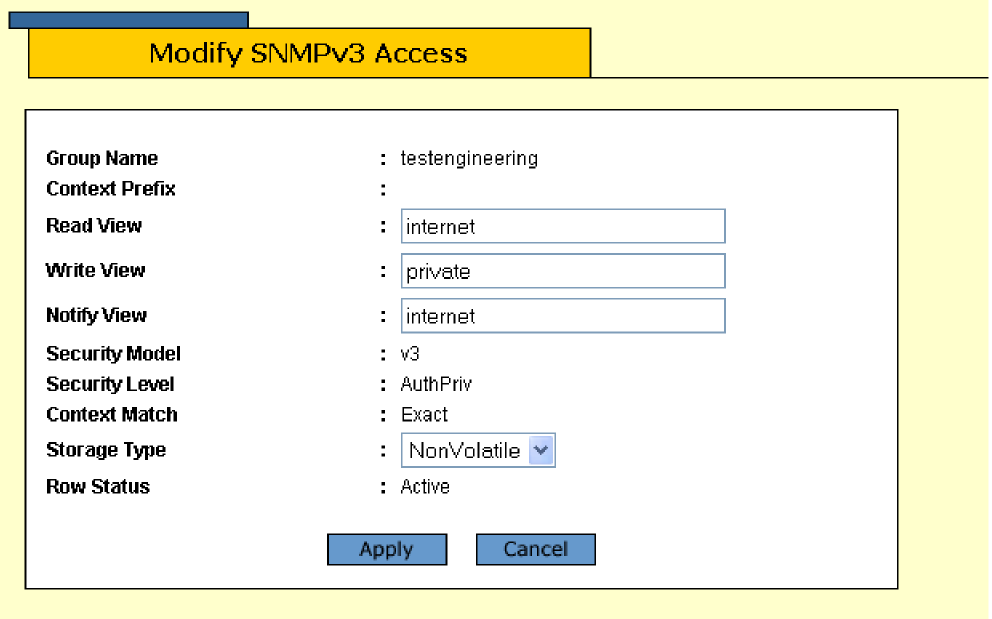
1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Access Table Page is shown in Figure 65 on page 201.
5. Display the Access Table entry that you want to change.

   Click **Next** or **Previous** to display an entry.
6. Click **Modify**.

   The Modify SNMPv3 Access Page is shown in Figure 67.



Modify SNMPv3 Access

Group Name	:	testengineering
Context Prefix	:	
Read View	:	internet
Write View	:	private
Notify View	:	internet
Security Model	:	v3
Security Level	:	AuthPriv
Context Match	:	Exact
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 67 Modify SNMPv3 Access Page

Note
The Context Prefix field is a read-only field. The Context Prefix field is always set to null.

7. In the Read View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

8. In the Write View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

9. In the Notify View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

Note
The Context Match field is a read only field. The Context Match field is always set to Exact.

10. In the Storage Type field, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the Access Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Access Table.

12. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 SecurityToGroup Table

You can create, delete, and modify an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- ❑ Creating a SecurityToGroup Table Entry on page 208
- ❑ Deleting a SecurityToGroup Table Entry on page 210
- ❑ Modifying a SecurityToGroup Table Entry on page 211

For reference information about the SNMPv3Configuring the SNMPv3 SecurityToGroup Table on page 208.

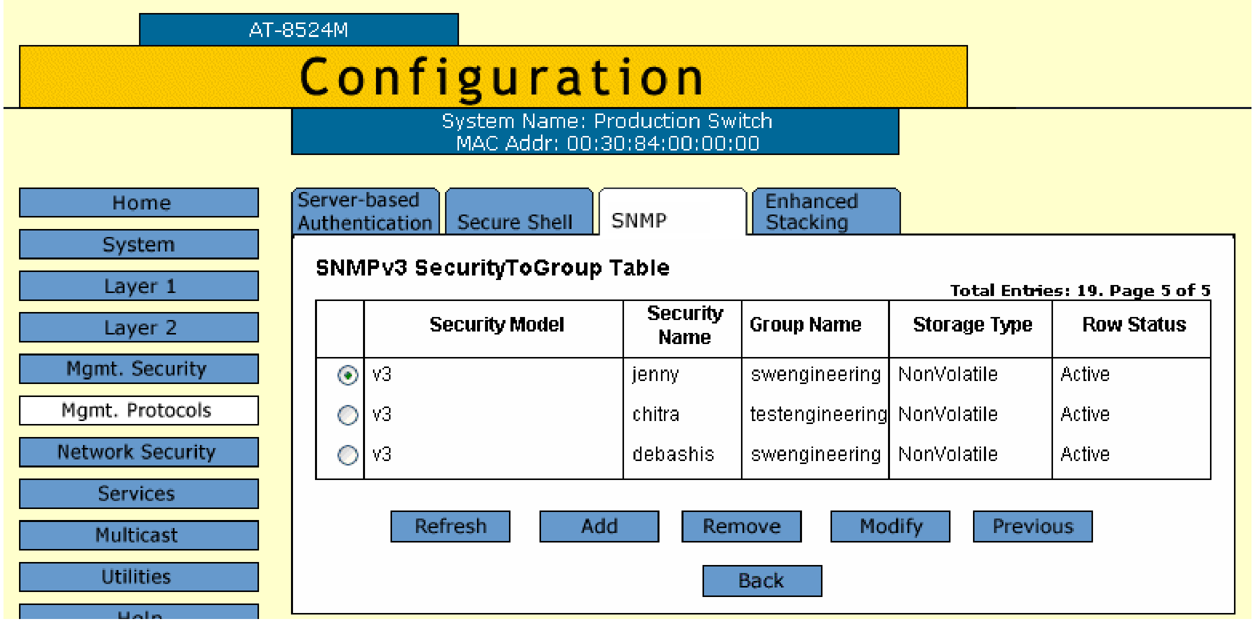
Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 SecurityToGroup Table Page is shown in Figure 68.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

SNMPv3 SecurityToGroup Table

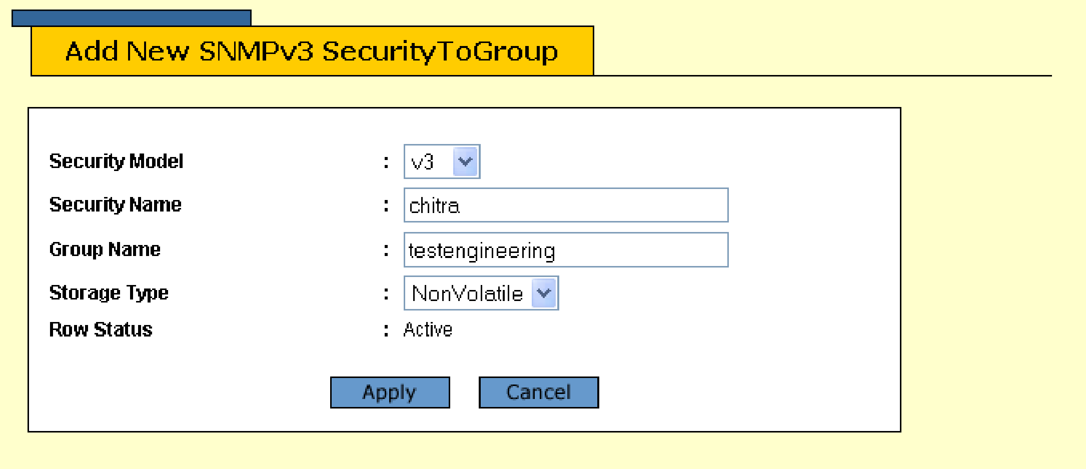
Total Entries: 19. Page 5 of 5

	Security Model	Security Name	Group Name	Storage Type	Row Status
●	v3	jenny	swengineering	NonVolatile	Active
○	v3	chitra	testengineering	NonVolatile	Active
○	v3	debashis	swengineering	NonVolatile	Active

Figure 68 SNMPv3 SecurityToGroup Table Page

5. To create an SNMPv3 SecurityToGroup Table entry, click **Add**.

   The Add New SNMPv3 SecurityToGroup Page is shown in Figure 69.



Add New SNMPv3 SecurityToGroup

Security Model	:	v3
Security Name	:	chitra
Group Name	:	testengineering
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 69 Add New SNMPv3 SecurityToGroup Page

6. In the Security Model field, select the SNMP protocol that was configured for this User Name.

   Choose from the following:

   v1
   Select this value to associate the User Name with the SNMPv1 protocol.

   v2c
   Select this value to associate the User Name with the SNMPv2c protocol.

   v3
   Select this value to associate the User Name with the SNMPv3 protocol.

7. In the Security Name field, enter the User Name that you want to associate with a group.

   Enter a User Name that you configured in Creating a User Table Entry on page 188.

8. In the Group Name field, enter a Group Name that you configured in the Access Table.

   See Creating an Access Table on page 201.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- ❑ defaultV1GroupReadOnly
- ❑ defaultV1GroupReadWrite
- ❑ defaultV2cGroupReadOnly
- ❑ defaultV2cGroupReadWrite

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

> **Note**
> The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 SecurityToGroup Table.
11. To save your changes, select the **Save Config** menu selection.

Deleting a SecurityToGroup Table Entry

To delete an entry SNMPv3 SecurityToGroup Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 SecurityToGroup Table Page is shown in Figure 68 on page 208.

5. Click the circle next to the SecurityToGroup Table entry that you want to delete. Then click **Remove**.

   A warning message is displayed. Click OK to remove the SNMPv3 SecurityToGroup Table entry.

6. To save your changes, select the **Save Config** menu selection.

Modifying a SecurityToGroup Table Entry

To modify an entry SNMPv3 SecurityToGroup Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

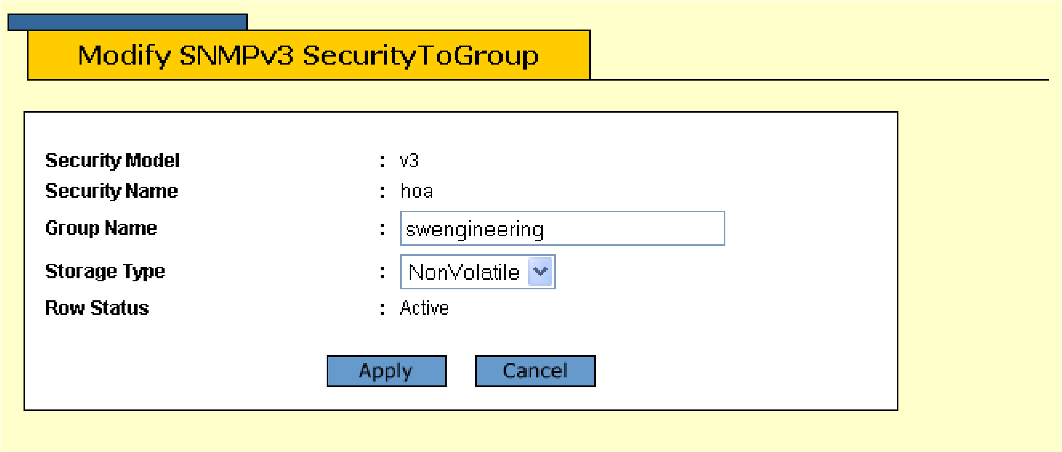
   The SNMP Tab is shown in Figure 58 on page 186.

4. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 SecurityToGroup Table Page is shown in Figure 68 on page 208.

5. Click the circle next to the SecurityToGroup Table entry that you want to change. Then click **Modify**.

   The Modify SNMPv3 SecurityToGroup Page is shown in Figure 70.



Modify SNMPv3 SecurityToGroup

Security Model	:	v3
Security Name	:	hoa
Group Name	:	swengineering
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 70 Modify SNMPv3 SecurityToGroup Page

6. In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

   See Creating an Access Table on page 201.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

❑ defaultV1GroupReadOnly

❑ defaultV1GroupReadWrite

❑ defaultV2cGroupReadOnly

❑ defaultV2cGroupReadWrite

7. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

   Note
   The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 SecurityToGroup Table.

9. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 Notify Table

You can create, delete, and modify an SNMPv3 Notify Table entry. See the following procedures:

- ❑ Creating a Notify Table Entry on page 213
- ❑ Deleting a Notify Table Entry on page 215
- ❑ Modifying a Notify Table Entry on page 216

For reference information about the SNMPv3 Notify Table, see Configuring the SNMPv3 Notify Table on page 213.

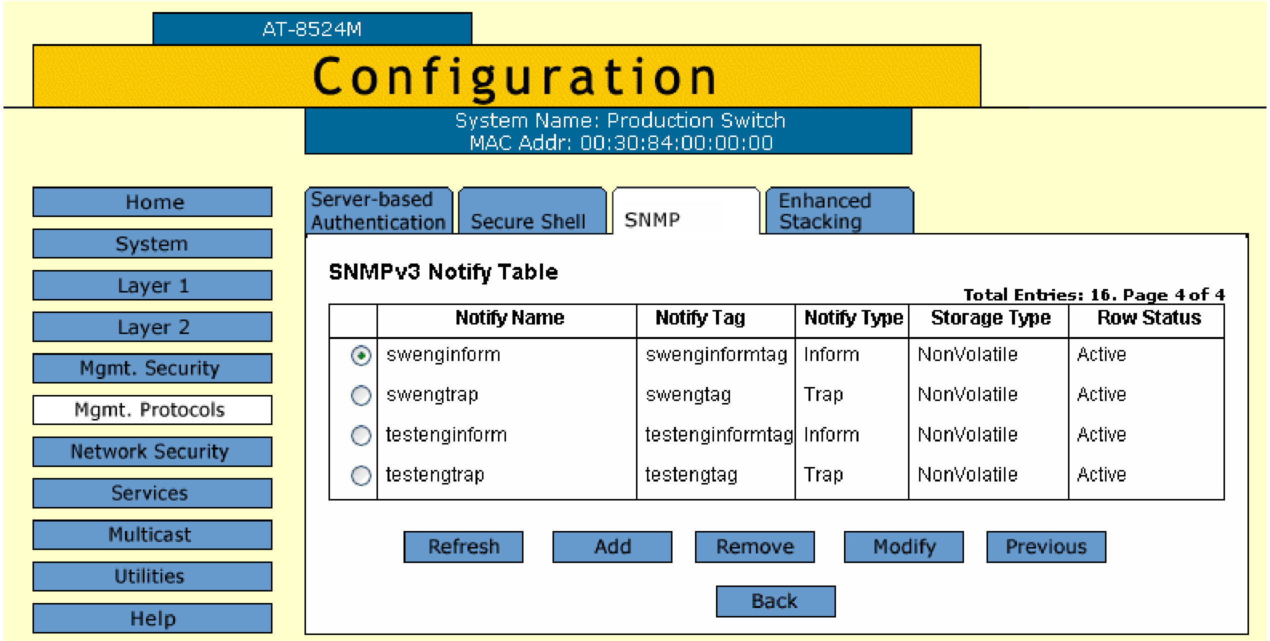
Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Notify Table Page is shown in Figure 71.



SNMPv3 Notify Table

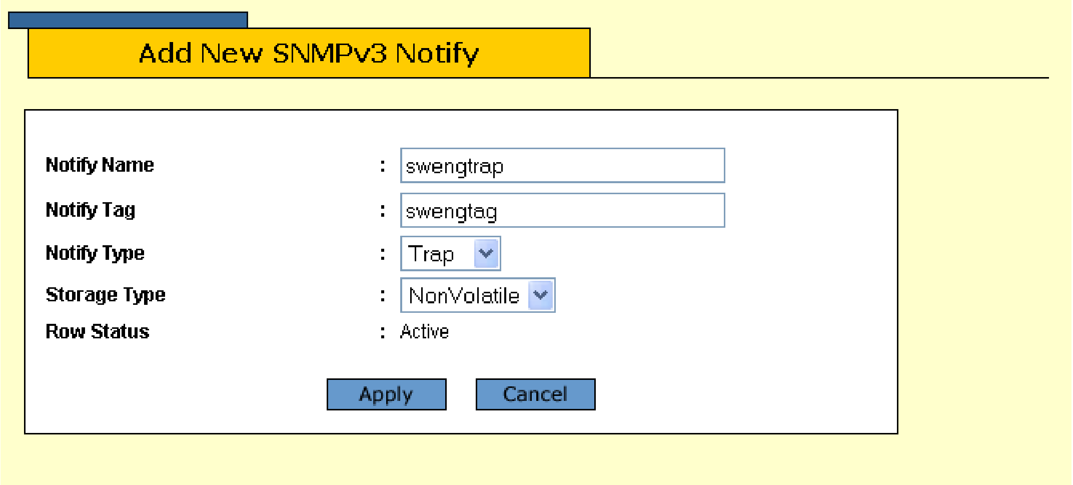
Total Entries: 16. Page 4 of 4

	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
●	swenginform	swenginformtag	Inform	NonVolatile	Active
○	swengtrap	swengtag	Trap	NonVolatile	Active
○	testenginform	testenginformtag	Inform	NonVolatile	Active
○	testengtrap	testengtag	Trap	NonVolatile	Active

Figure 71 SNMPv3 Notify Table Page

5. To create an SNMPv3 Notify Table entry, click **Add**.

   The Add New SNMPv3 Notify Page is shown in Figure 72.



Notify Name	:	swengtrap
Notify Tag	:	swengtag
Notify Type	:	Trap
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 72 Add New SNMPv3 Notify Page

6. In the Notify Name field, enter the name associated with this trap message.

   Enter a descriptive name of up to 32 alphanumeric characters. For example, you might want to define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.

7. In the Notify Tag field, enter a description name of the Notify Tag.

   Enter a name of up to 32 alphanumeric characters.

8. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table to the configuration file. After making changes to a Notify Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

NonVolatile
Select this storage type if you want the ability to save an entry in the Notify Table to the configuration file. After making changes to a Notify Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

> **Note**
> The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Notify Table.
11. To save your changes, select the **Save Config** menu selection.

Deleting a Notify Table Entry

To delete an entry in the SNMPv3 Notify Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Notify Table Page is shown in Figure 71 on page 213.
5. Click the circle next to the Notify Table entry that you want to delete. Then click **Remove**.

   A warning message is displayed. Click OK to remove the SNMPv3 Notify Table entry.
6. To save your changes, select the **Save Config** menu selection.

Modifying a Notify Table Entry

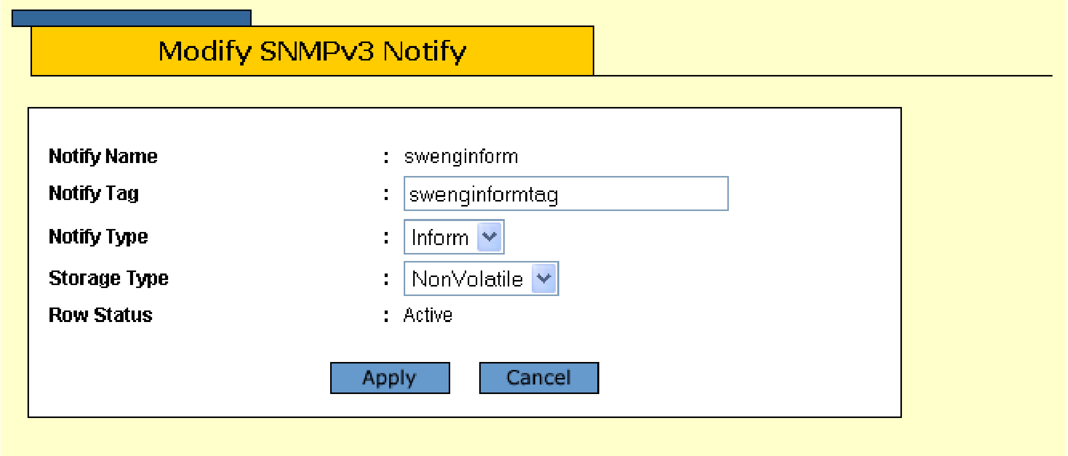
To modify an entry in the SNMPv3 Notify Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Notify Table Page is shown in Figure 71 on page 213.
5. Click the circle next to the table entry that you want to change. Then click **Modify**.

   The Modify SNMPv3 Notify Page is shown in Figure 73



Modify SNMPv3 Notify

Notify Name	:	swenginform
Notify Tag	:	swenginformtag
Notify Type	:	Inform
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 73 Modify SNMPv3 Notify Page

6. In the Notify Tag field, enter a description name of the Notify Tag.

   Enter a name of up to 32 alphanumeric characters.
7. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table to the configuration file. After making changes to an Notify Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Notify Table to the configuration file. After making changes to an Notify Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

   Note
   The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.

10. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 Target Address Table

You can create, delete, and modify an SNMPv3 Target Address Table entry. See the following procedures:

- ❑ Creating a Target Address Table Entry on page 218
- ❑ Deleting a Target Address Table Entry on page 221
- ❑ Modifying Target Address Table Entry on page 222

For reference information about the SNMPv3 Target Address Table, see Configuring the SNMPv3 Target Address Table on page 218.

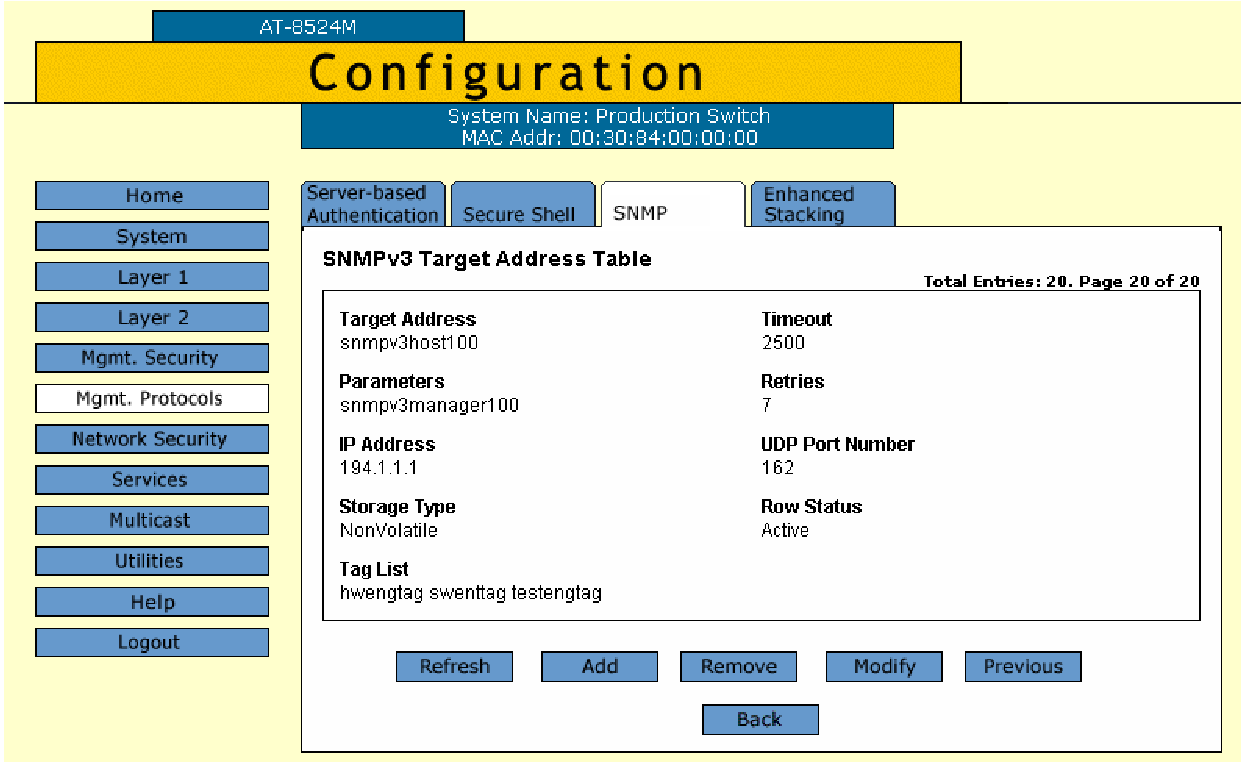
Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.

The SNMPv3 Target Address Table Page is shown in Figure 74.



SNMPv3 Target Address Table

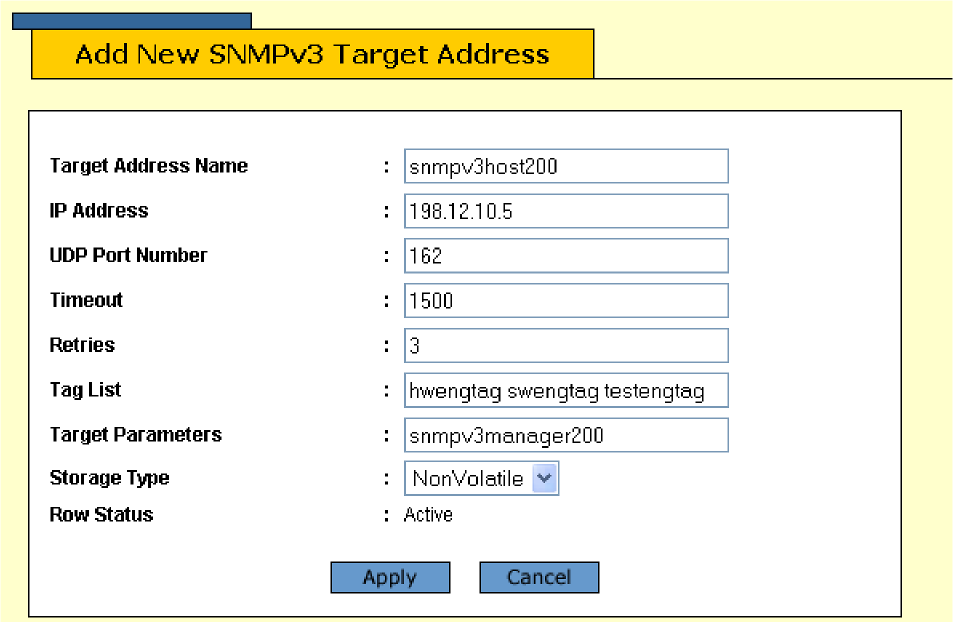
Total Entries: 20. Page 20 of 20

Target Address snmpv3host100	**Timeout** 2500
Parameters snmpv3manager100	**Retries** 7
IP Address 194.1.1.1	**UDP Port Number** 162
Storage Type NonVolatile	**Row Status** Active
Tag List hwengtag swenttag testengtag	

Figure 74 SNMPv3 Target Address Table Page

5. To create an SNMPv3 Target Address Table entry, click **Add**.

   The Add New SNMPv3 Target Address Table Page is shown in Figure 75.



Target Address Name	:	snmpv3host200
IP Address	:	198.12.10.5
UDP Port Number	:	162
Timeout	:	1500
Retries	:	3
Tag List	:	hwengtag swengtag testengtag
Target Parameters	:	snmpv3manager200
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 75 Add New SNMPv3 Target Address Table Page

6. In the Target Address Name field, enter the name of the SNMP manager, or host, that manages the SNMP activity on your switch.

   You can enter a name of up to 32 alphanumeric characters.

7. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address:
   XXX.XXX.XXX.XXX

8. In the UDP Port Number field, enter a UDP port number.

   You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

9. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

10. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

    When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

11. In the Tag List field, enter a list of tags that you configured in a SNMPv3 Notify Table with the Notify Tag parameter.

    See Creating a Notify Table Entry on page 213. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

12. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the SNMPv3 Target Parameters Table.

13. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table to the configuration file. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

NonVolatile
Select this storage type if you want the ability to save an entry in the Target Address Table to the configuration file. After making changes to a Target Address Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

> **Note**
> The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Target Address Table entry takes effect immediately.

14. Click **Apply** to update the SNMPv3 Target Address Table.
15. To save your changes, select the **Save Config** menu selection.

Deleting a Target Address Table Entry

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Target Address Table Page is shown in Figure 74 on page 219.
5. Display the SNMPv3 Target Address Table entry that you want to delete.

   Click **Next** or **Previous** to display an entry.
6. Click **Remove**.

   A warning message is displayed. Click OK to remove the Target Address Table entry.
7. To save your changes, select the **Save Config** menu selection.

Modifying Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table, perform the following procedure.

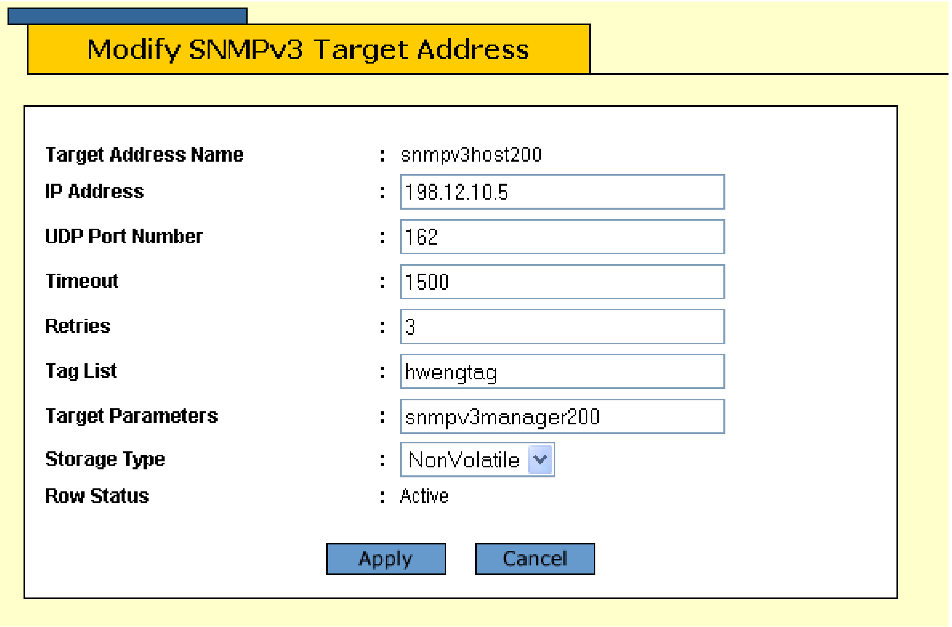
1. FFrom the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Target Address Table Page is shown in Figure 74 on page 219.
5. Display the Target Address Table entry that you want to change.

   Click **Next** or **Previous** to display an entry.
6. Click **Modify**.

   The Modify SNMPv3 Target Address Table Page is shown Figure 76.



Modify SNMPv3 Target Address

Target Address Name	:	snmpv3host200
IP Address	:	198.12.10.5
UDP Port Number	:	162
Timeout	:	1500
Retries	:	3
Tag List	:	hwengtag
Target Parameters	:	snmpv3manager200
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 76 Modify SNMPv3 Target Address Table Page

7. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address: XXX.XXX.XXX.XXX
8. In the UDP Port Number field, enter a UDP port number.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

9. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

10. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

    When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

11. In the Tag List field, enter a list of tags that you configured with the Notify Tag parameter in a Notify Table entry.

    See Creating a Notify Table Entry on page 213. Enter a Tag List of up to 256-alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

12. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the Target Parameters Table.

13. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table to the configuration file. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Address Table to the configuration file. After making changes to an Target Address Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

14. Click **Apply** to update the SNMPv3 Target Address Table.

15. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 Target Parameters Table

You can create, delete, and modify an SNMPv3 Target Parameters Table entry. See the following procedures:

- ❑ Creating a Target Address Table Entry on page 218
- ❑ Deleting a Target Address Table Entry on page 221
- ❑ Modifying Target Address Table Entry on page 222

For reference information about the SNMPv3 Target Parameters Table, see Configuring the SNMPv3 Target Parameters Table on page 224.

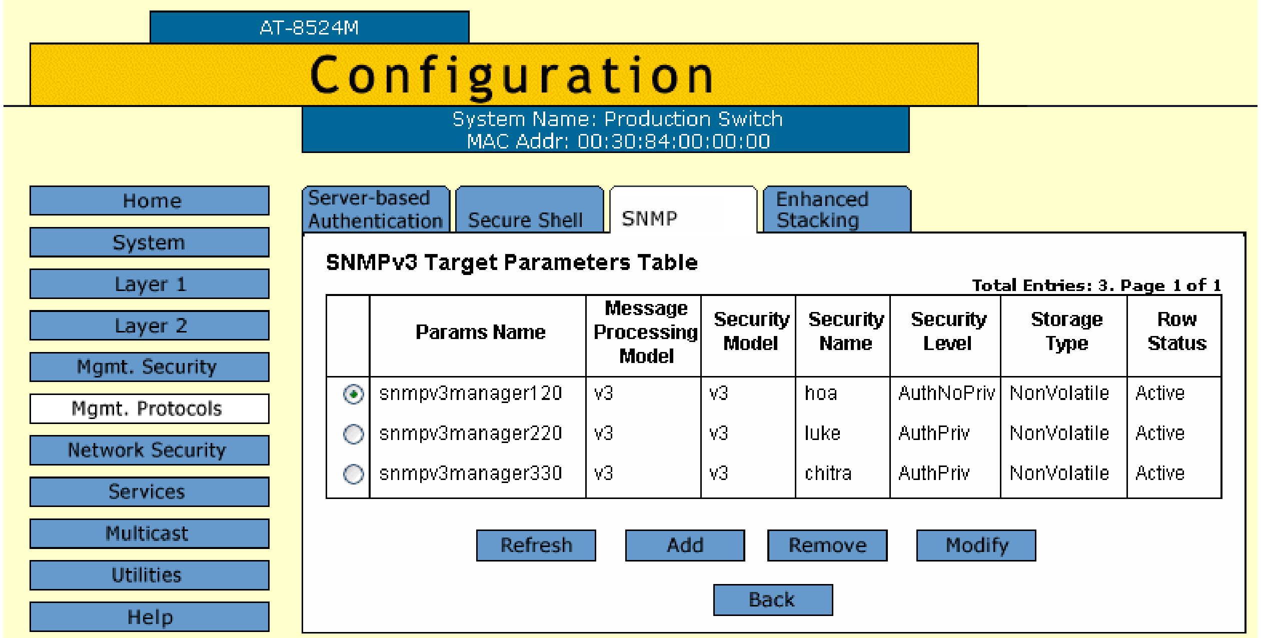
Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Target Parameters Table Page is shown in Figure 77.



SNMPv3 Target Parameters Table

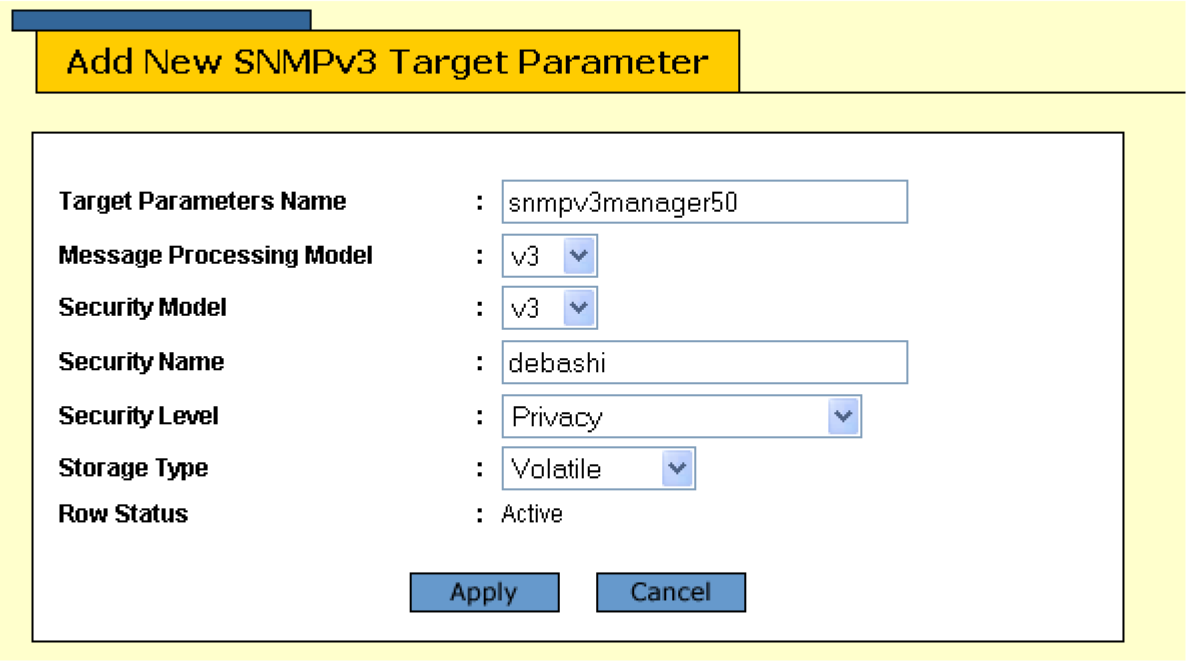
Total Entries: 3. Page 1 of 1

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
●	snmpv3manager120	v3	v3	hoa	AuthNoPriv	NonVolatile	Active
○	snmpv3manager220	v3	v3	luke	AuthPriv	NonVolatile	Active
○	snmpv3manager330	v3	v3	chitra	AuthPriv	NonVolatile	Active

Figure 77 SNMPv3 Target Parameters Table Page

5. To create an SNMPv3 Target Parameters Table entry, click **Add**.

   The Add New SNMPv3 Target Parameter Table Page is shown in Figure 78.



Add New SNMPv3 Target Parameter

Target Parameters Name	: snmpv3manager50
Message Processing Model	: v3
Security Model	: v3
Security Name	: debashi
Security Level	: Privacy
Storage Type	: Volatile
Row Status	: Active

Figure 78 Add New SNMPv3 Target Parameters Table Page

6. In the Target Parameters Name field, enter a name of the SNMP manager or host.

   Enter a value of up to 32 alphanumeric characters.

> **Note**
> Enter a value for the Message Processing Model parameter only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the Message Processing Model is automatically assigned to SNMPv3.

7. In the Message Processing Model field, enter an SNMP Protocol that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

8. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

   v1
   Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

   v2c
   Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

   v3
   Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

9. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See Creating a User Table Entry on page 188.

10. In the Security Level field, select one of the following Security Levels:

    Note
    The value you configure for the Security Level must match the value configured for the User Name in the User Table Menu. See Creating a User Table Entry on page 188.

    No Authentication/Privacy
    This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate users and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

    Note
    If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

    Authentication
    This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

    Privacy
    This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption.

This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

11. In the Storage Type parameter, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to a Target Parameters Table entry with a Volatile storage type, then the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to a Target Parameters Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

    Note
    The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 Target Parameters Table.
13. To save your changes, select the **Save Config** menu selection.

Deleting a Target Parameters Table Entry

To delete an SNMPv3 Target Parameters Table entry, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Target Parameters Table Page is shown in Figure 77 on page 224.
5. Click the circle next to the Target Parameters Table entry that you want to delete. Then click **Remove**.

A warning message is displayed. Click OK to remove the Target Parameters Table entry.

6. To save your changes, select the **Save Config** menu selection.

Modifying a Target Parameters Table Entry

To modify an SNMPv3 Target Parameters Table entry, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

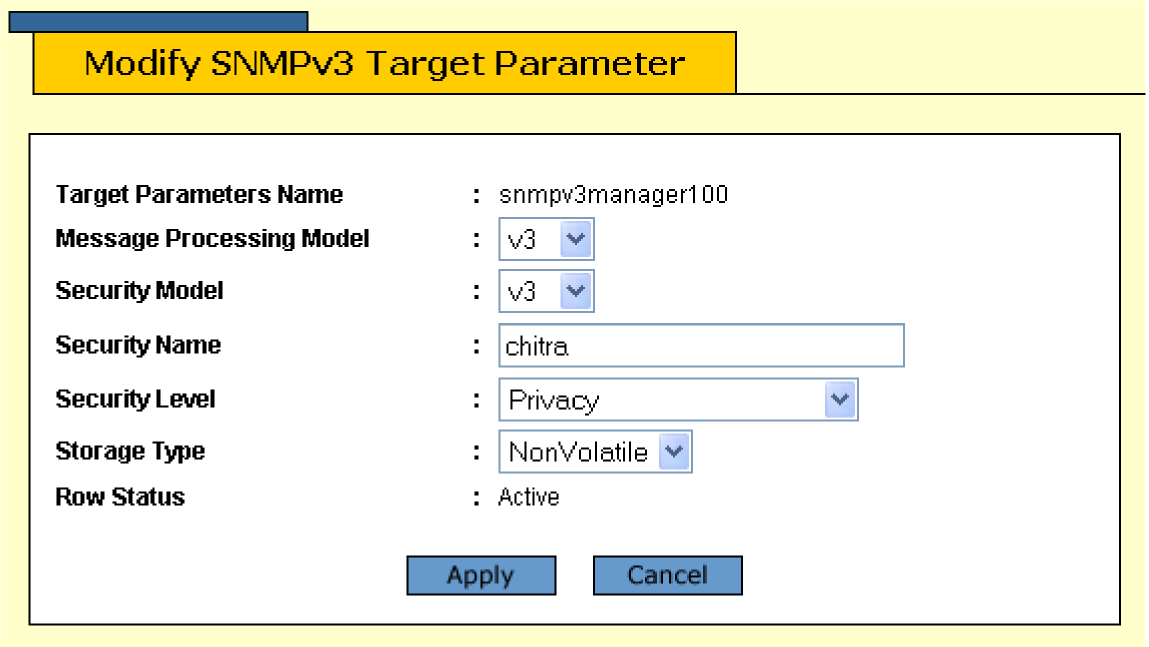
   The SNMP Tab is shown in Figure 58 on page 186.

4. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Target Parameters Table Page is shown in Figure 77 on page 224.

5. Click the circle next to the Target Parameters Table entry that you want to change. Then click **Modify**.

   The Modify SNMPv3 Target Parameter Table Page is shown in Figure 79 on page 228.



Modify SNMPv3 Target Parameter

Target Parameters Name	:	snmpv3manager100
Message Processing Model	:	v3
Security Model	:	v3
Security Name	:	chitra
Security Level	:	Privacy
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 79 Modify SNMPv3 Target Parameters Table Page

Note
Enter a value for the Message Processing Model field only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the switch automatically assigns the Message Processing Model to SNMPv3.

6. In the Message Processing Model field, enter a Security Model that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

7. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

   v1
   Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

   v2c
   Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

   v3
   Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

8. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See Creating a User Table Entry on page 188.

9. In the Security Level field, select one of the following Security Levels:

Note
The value you configure for the Security Level must match the value configured for the User Name in the SNMPv3 User Table Menu. See Creating a User Table Entry on page 188.

No Authentication/Privacy
This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate users and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note
If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication
This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

10. In the Storage Type parameter, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to an Target Parameters Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

11. Click **Apply** to update the SNMPv3 Target Parameters Table.
12. To save your changes, select the **Save Config** menu selection.

Configuring the SNMPv3 Community Table

You can create, delete, and modify an SNMPv3 Community Table entry. See the following procedures:

❑ Creating an SNMPv3 Community Table Entry on page 231

❑ Deleting an SNMPv3 Community Table Entry on page 234

❑ Modifying an SNMPv3 Community Table Entry on page 235

For reference information about the SNMPv3 Community Table, see Configuring the SNMPv3 Community Table on page 231.

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

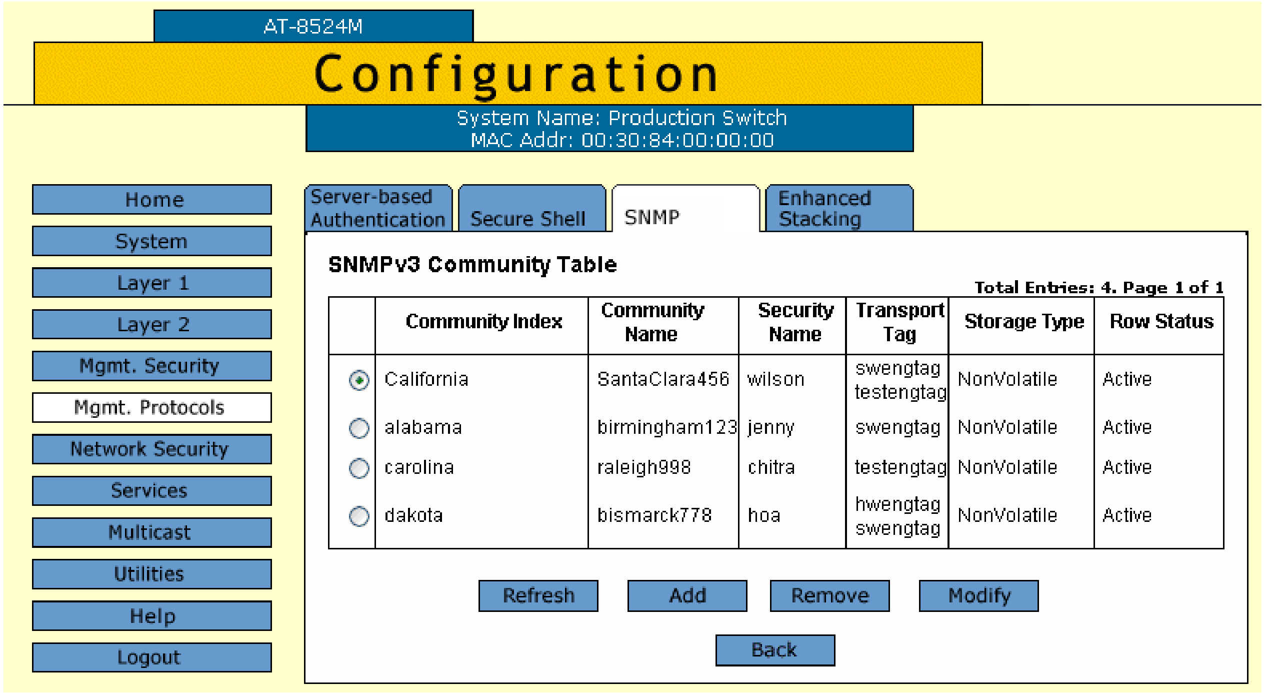
Creating an SNMPv3 Community Table Entry

To create an SNMPv3 Community Table entry, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Community Table Page is shown in Figure 80.



SNMPv3 Community Table

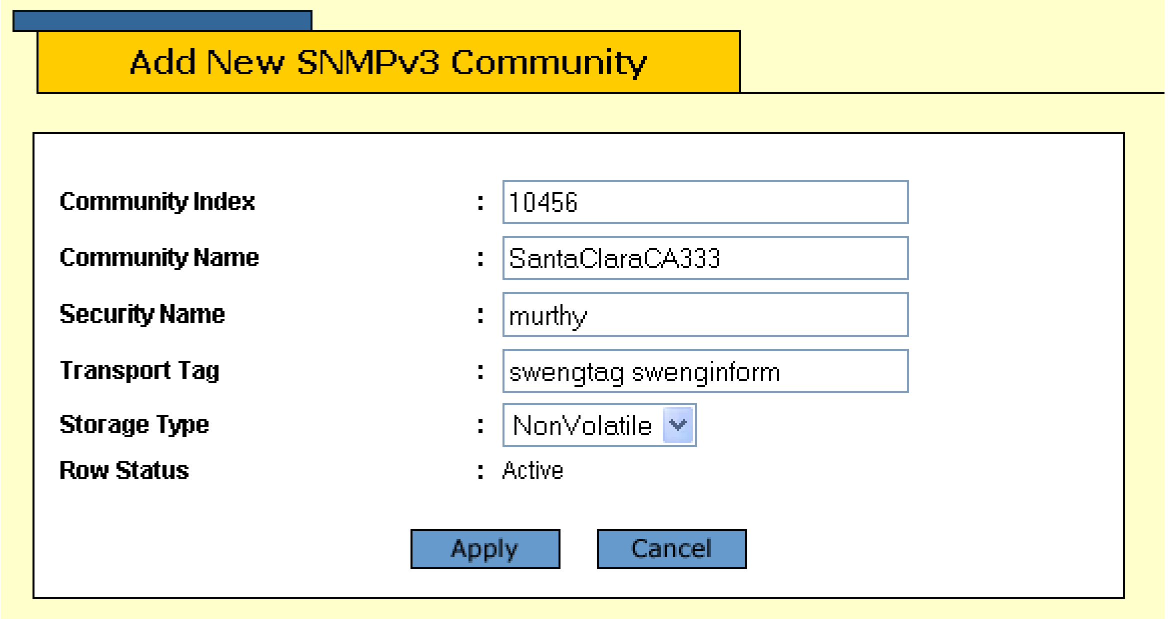
Total Entries: 4. Page 1 of 1

	Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
●	California	SantaClara456	wilson	swengtag testengtag	NonVolatile	Active
○	alabama	birmingham123	jenny	swengtag	NonVolatile	Active
○	carolina	raleigh998	chitra	testengtag	NonVolatile	Active
○	dakota	bismarck778	hoa	hwengtag swengtag	NonVolatile	Active

Figure 80 SNMPv3 Community Table Page

5. To create an SNMPv3 Community Table entry, click **Add**.

   The Add New SNMPv3 Community Table Page is shown in Figure 81.



Community Index	:	10456
Community Name	:	SantaClaraCA333
Security Name	:	murthy
Transport Tag	:	swengtag swenginform
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 81 Add New SNMPv3 Community Table Page

6. In the Community Index field, enter a numerical value for this Community.

   This parameter is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32-alphanumeric characters.

7. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

   The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

   Note
   Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

8. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

   This name must be unique. Enter a value of up to 32 alphanumeric characters.

   Note
   Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

9. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See Creating a Target Address Table Entry on page 218.

10. In the Storage Type field, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** menu selection does not appear.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After

making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** menu selection appears.

> **Note**
> The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Community Table.
12. To save your changes, select the **Save Config** menu selection.

Deleting an SNMPv3 Community Table Entry

To delete an entry in the SNMPv3 Community Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

   The SNMP Tab is shown in Figure 58 on page 186.
4. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Community Table Page is shown in Figure 80 on page 232.
5. Click the circle next to the SNMPv3 Community Table entry that you want to delete. Then click **Remove**.

   A warning message is displayed. Click OK to remove the SNMPv3 Community Table entry.
6. To save your changes, select the **Save Config** menu selection.

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table, perform the following procedure.

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.

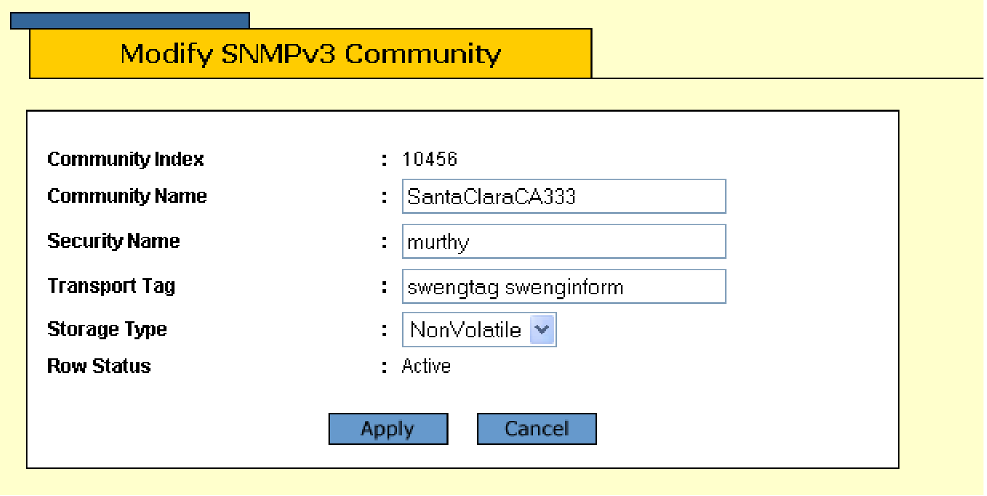
   The SNMP Tab is shown in Figure 58 on page 186.

4. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.

   The SNMPv3 Community Table Page is shown in Figure 80 on page 232.

5. Click the circle next to the SNMPv3 Community Table entry that you want to change. Then click **Modify**.

   The Modify SNMPv3 Community Table Page is shown in Figure 82.



Modify SNMPv3 Community

Community Index	:	10456
Community Name	:	SantaClaraCA333
Security Name	:	murthy
Transport Tag	:	swengtag swenginform
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 82 Modify SNMPv3 Community Table Page

6. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

   The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

   Note
   Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

7. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note
Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

8. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See Creating a Target Address Table Entry on page 218.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** menu selection does appear.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, **Save Config** menu selection appears, allowing you to save your changes.

Note
The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Community Table.

11. To save your changes, select the **Save Config** menu selection.

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

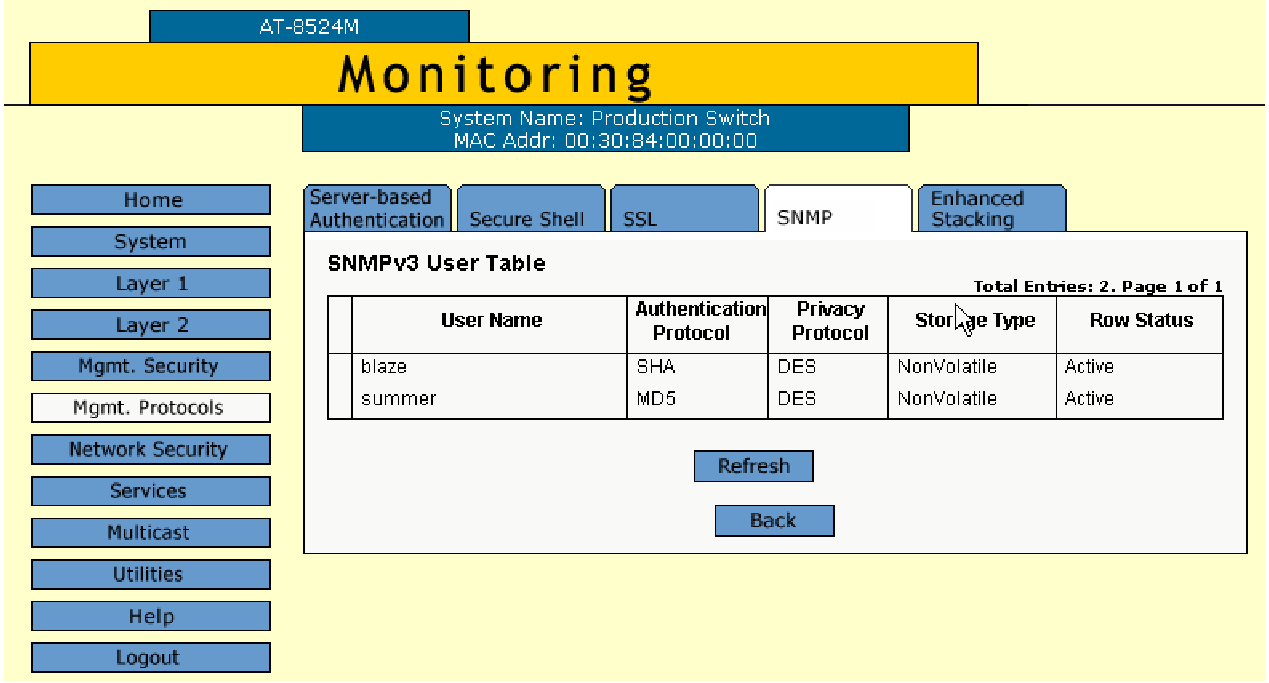
- ❑ Displaying User Table Entries on page 238
- ❑ Displaying View Table Entries on page 239
- ❑ Displaying Access Table Entries on page 240
- ❑ Displaying SecurityToGroup Table Entries on page 241
- ❑ Displaying Notify Table Entries on page 242
- ❑ Displaying Target Address Table Entries on page 243
- ❑ Displaying Target Parameters Table Entries on page 244
- ❑ Displaying SNMPv3 Community Table Entries on page 245

Displaying User Table Entries

To display entries in the SNMPv3 User Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to View User Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 User Table Page is shown in Figure 83.



SNMPv3 User Table

Total Entries: 2. Page 1 of 1

	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status
	blaze	SHA	DES	NonVolatile	Active
	summer	MD5	DES	NonVolatile	Active

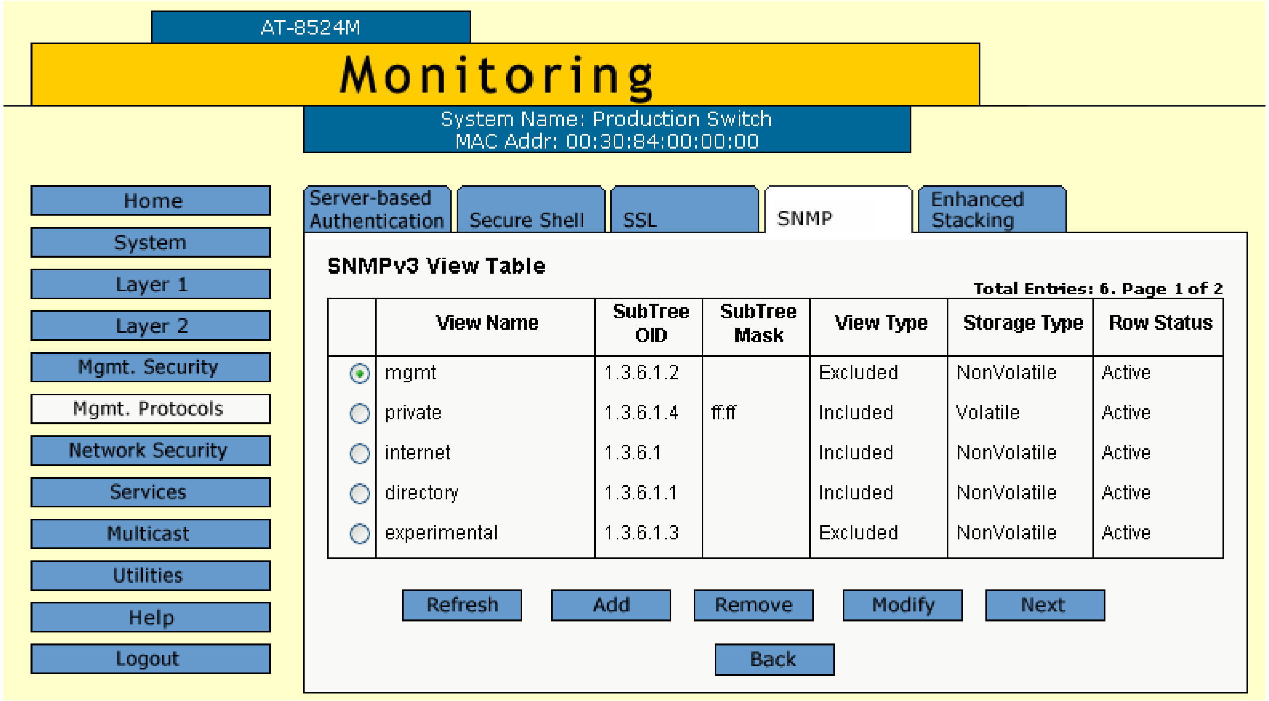
Figure 83 Monitoring, SNMPv3 User Table Page

Displaying View Table Entries

To display entries in the SNMPv3 View Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to View View Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 View Table Page is shown in Figure 84.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

SNMPv3 View Table

Total Entries: 6. Page 1 of 2

	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
●	mgmt	1.3.6.1.2		Excluded	NonVolatile	Active
○	private	1.3.6.1.4	ff:ff	Included	Volatile	Active
○	internet	1.3.6.1		Included	NonVolatile	Active
○	directory	1.3.6.1.1		Included	NonVolatile	Active
○	experimental	1.3.6.1.3		Excluded	NonVolatile	Active

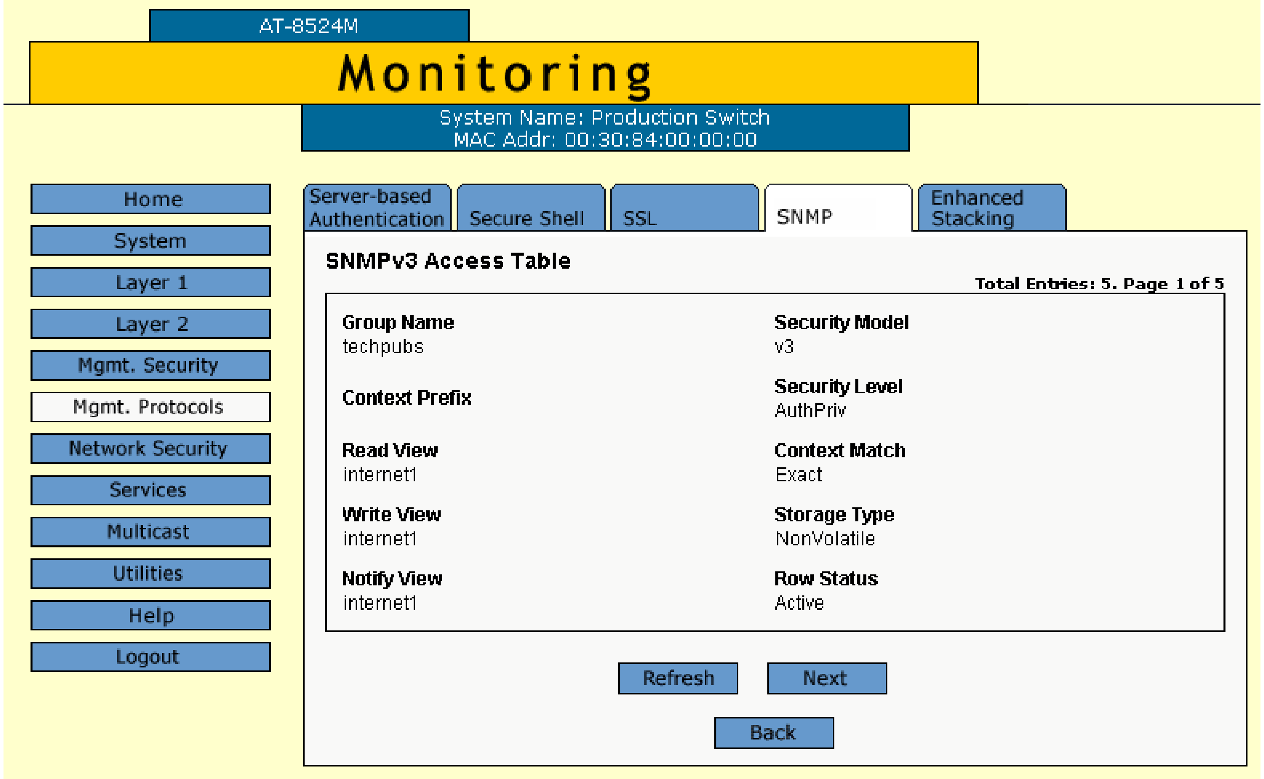
Figure 84 Monitoring, SNMPv3 View Table Page

Displaying Access Table Entries

To display entries in the SNMPv3 Access Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to View Access Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 Access Table Page is shown in Figure 85.



SNMPv3 Access Table

Total Entries: 5. Page 1 of 5

Group Name
techpubs

Security Model
v3

Context Prefix

Security Level
AuthPriv

Read View
internet1

Context Match
Exact

Write View
internet1

Storage Type
NonVolatile

Notify View
internet1

Row Status
Active

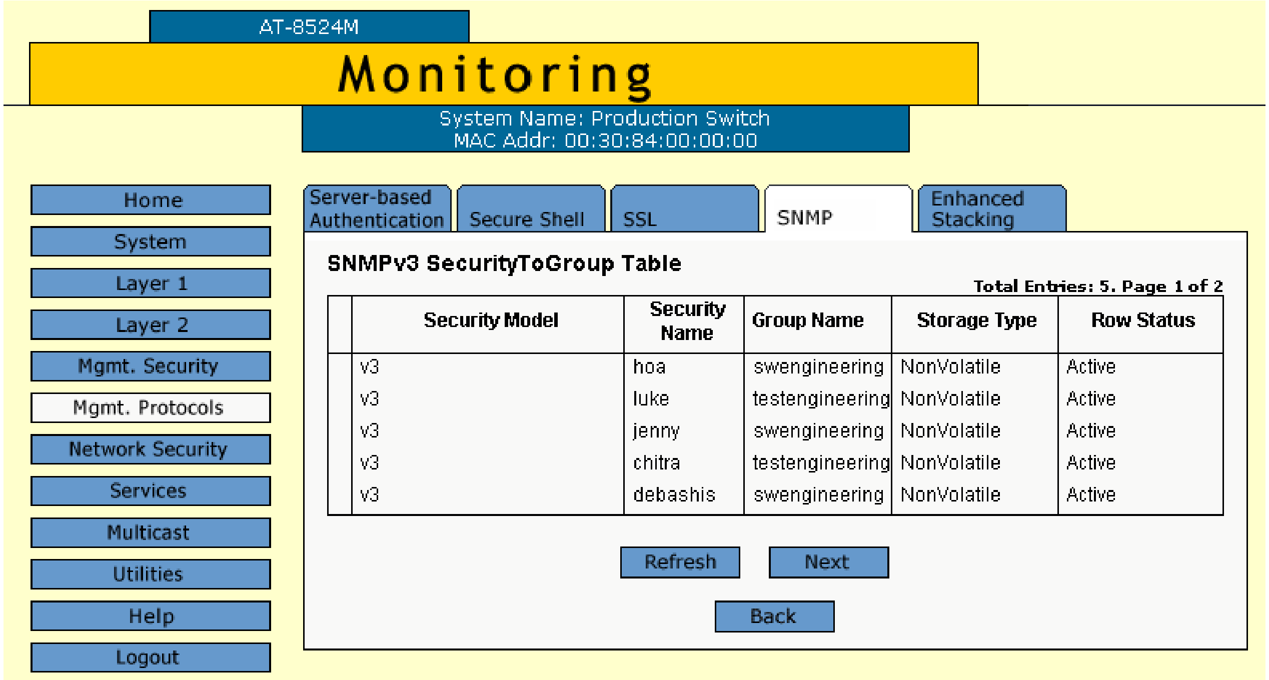
Figure 85 Monitoring, SNMPv3 Access Table Page

Displaying SecurityToGroup Table Entries

To display entries in the SNMPv3 SecurityToGroup Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to the View SecurityToGroup Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 SecurityToGroup Table Page is shown in Figure 86.



SNMPv3 SecurityToGroup Table

Total Entries: 5. Page 1 of 2

	Security Model	Security Name	Group Name	Storage Type	Row Status
	v3	hoa	swengineering	NonVolatile	Active
	v3	luke	testengineering	NonVolatile	Active
	v3	jenny	swengineering	NonVolatile	Active
	v3	chitra	testengineering	NonVolatile	Active
	v3	debashis	swengineering	NonVolatile	Active

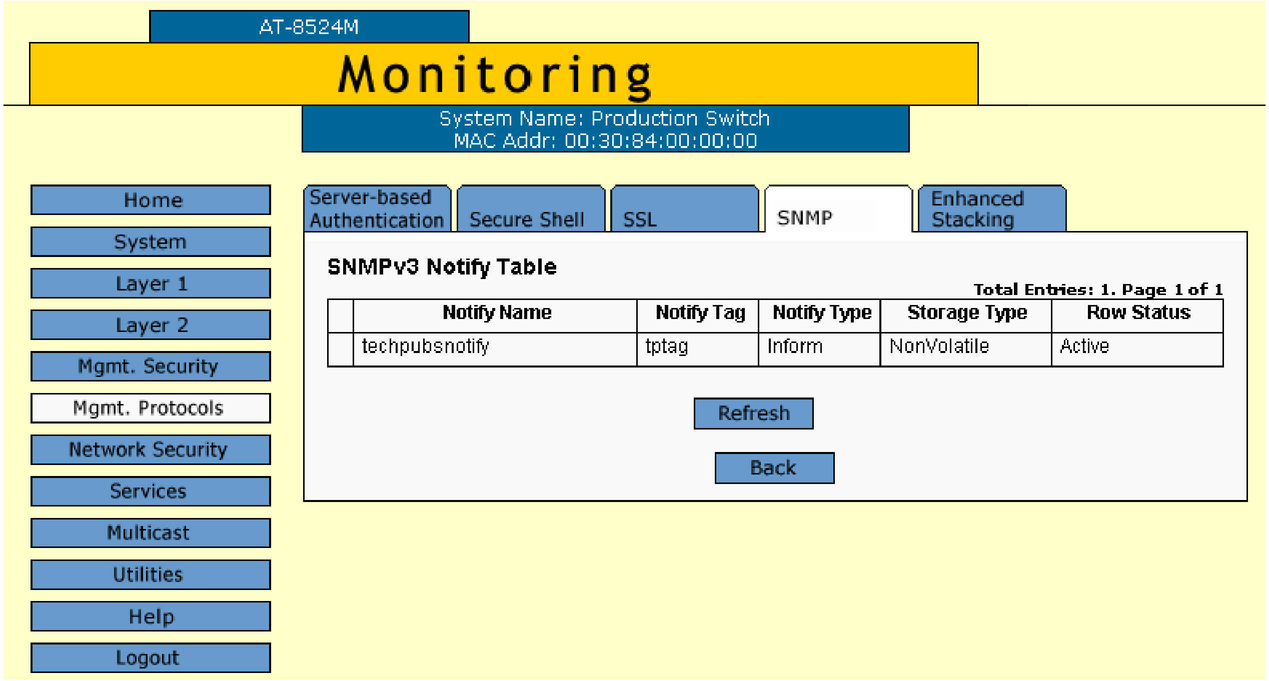
Figure 86 Monitoring, SNMPv3 SecurityToGroup Table Page

Displaying Notify Table Entries

To display entries in the SNMPv3 Notify Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to View Notify Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 Notify Table Page is shown in Figure 87.



SNMPv3 Notify Table

Total Entries: 1. Page 1 of 1

	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
	techpubsnotify	tptag	Inform	NonVolatile	Active

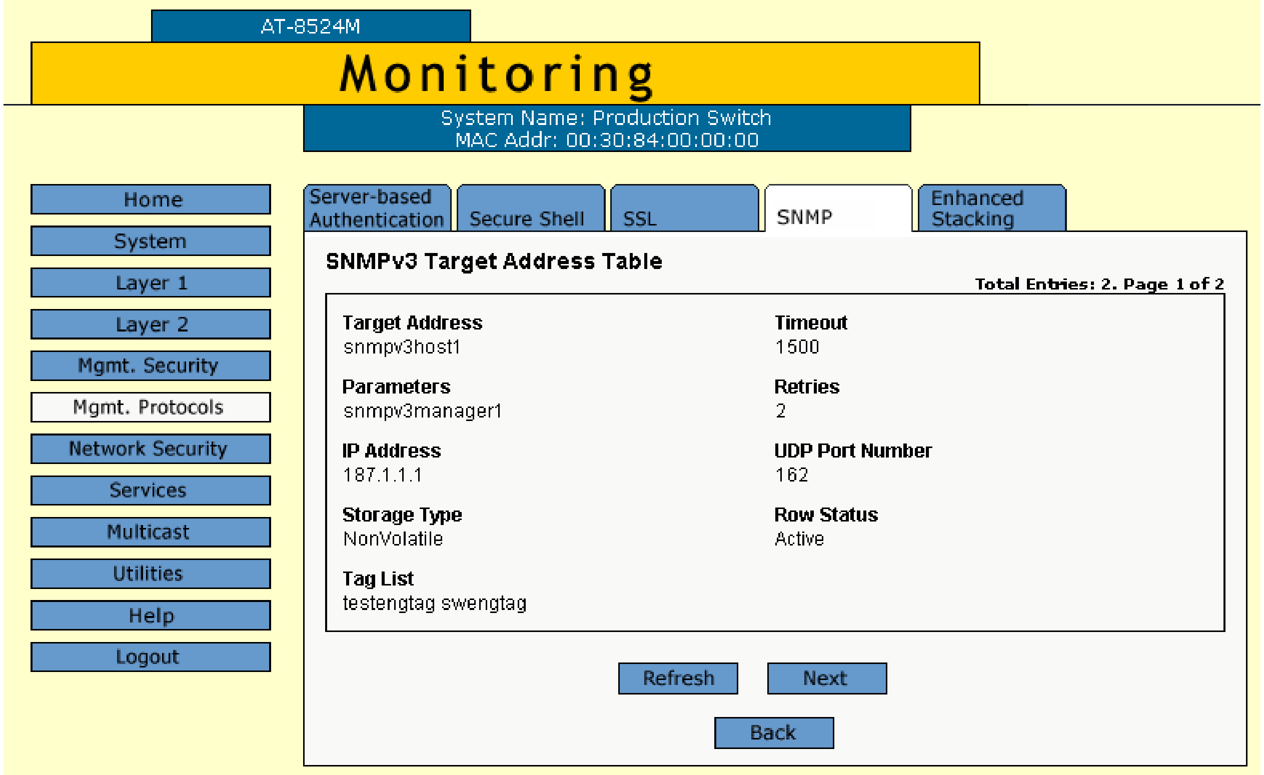
Figure 87 Monitoring, SNMPv3 Notify Table Page

Displaying Target Address Table Entries

To display entries in the SNMPv3 Target Address Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to View Target Address Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 Target Address Table Page is shown in Figure 88.



SNMPv3 Target Address Table

Total Entries: 2. Page 1 of 2

Target Address snmpv3host1	**Timeout** 1500
Parameters snmpv3manager1	**Retries** 2
IP Address 187.1.1.1	**UDP Port Number** 162
Storage Type NonVolatile	**Row Status** Active
Tag List testengtag swengtag	

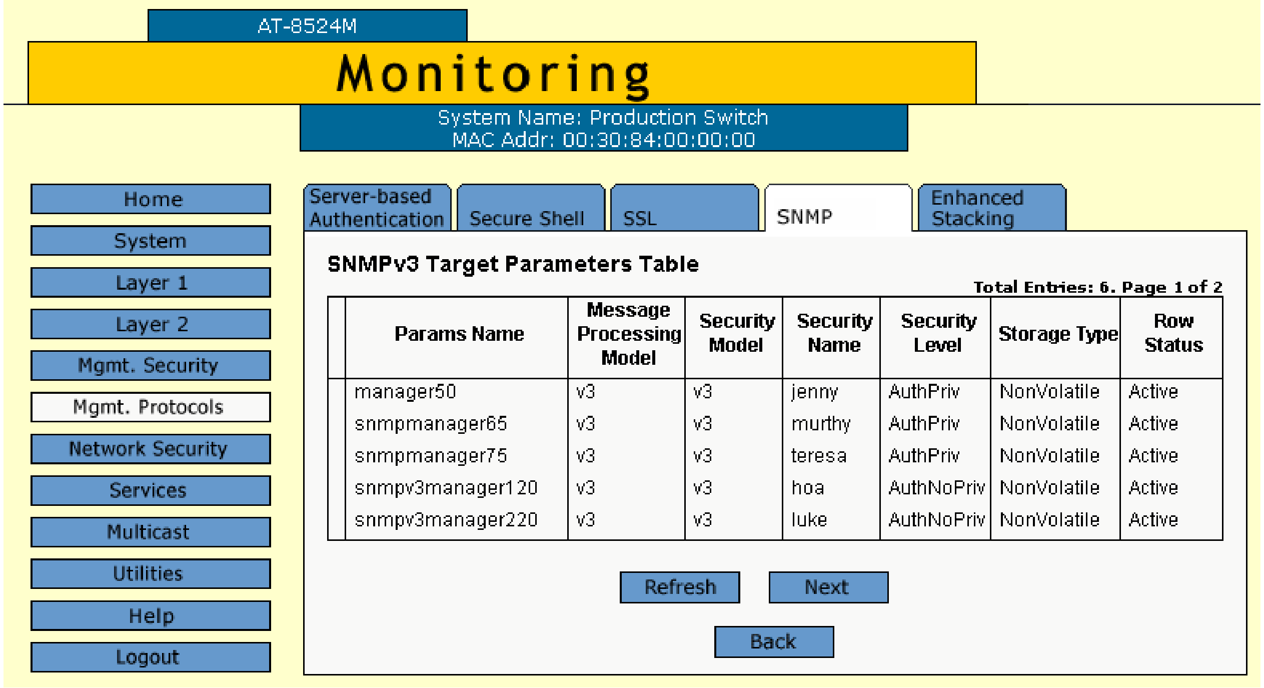
Figure 88 Monitoring, SNMPv3 Target Address Table Page

Displaying Target Parameters Table Entries

To display entries in the SNMPv3 Target Parameters Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to the View Target Parameters Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 Target Parameters Table Page is shown in Figure 88.



SNMPv3 Target Parameters Table

Total Entries: 6. Page 1 of 2

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
	manager50	v3	v3	jenny	AuthPriv	NonVolatile	Active
	snmpmanager65	v3	v3	murthy	AuthPriv	NonVolatile	Active
	snmpmanager75	v3	v3	teresa	AuthPriv	NonVolatile	Active
	snmpv3manager120	v3	v3	hoa	AuthNoPriv	NonVolatile	Active
	snmpv3manager220	v3	v3	luke	AuthNoPriv	NonVolatile	Active

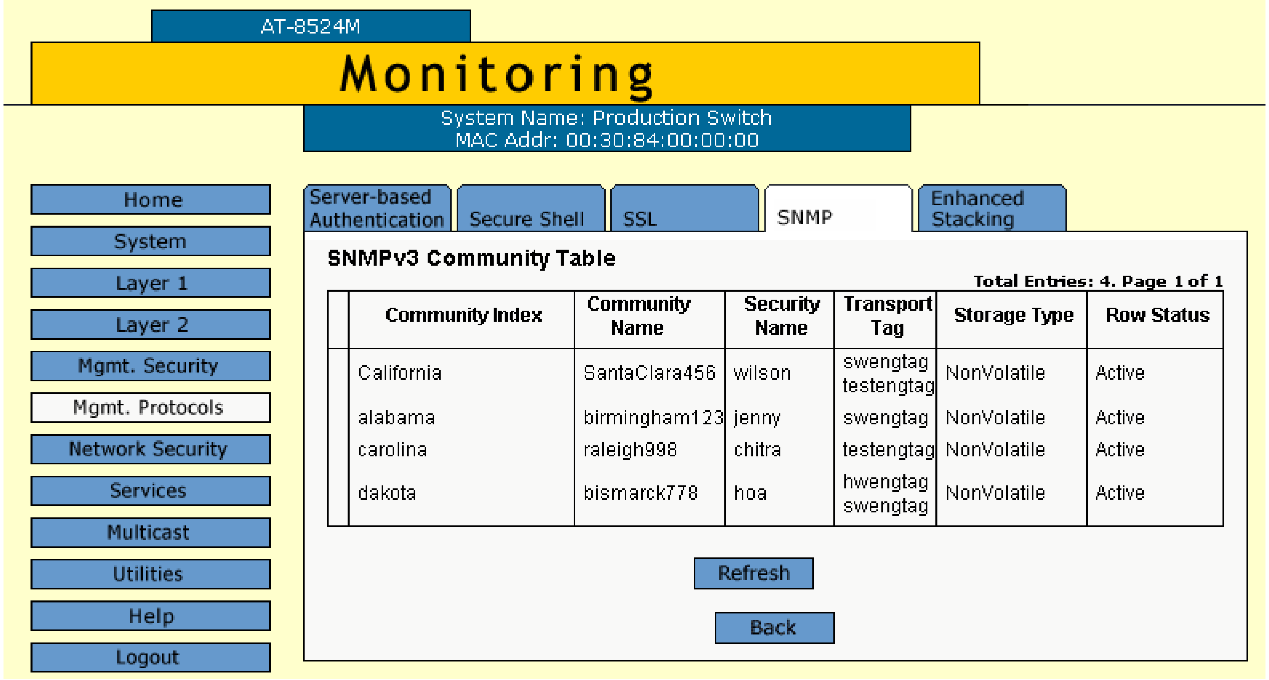
Figure 89 Monitoring, SNMPv3 Target Parameters Table Page

Displaying SNMPv3 Community Table Entries

To display entries in the SNMPv3 Community Table, perform the following procedure.

1. From the Home Page, select **Monitoring**.
2. Select the **Mgmt Protocols** menu selection.
3. Select the **SNMP** Tab.
4. From the SNMP Monitoring Tab, click the circle next to the View Community Table.
5. Click **View** at the bottom of the page.

   The Monitoring, SNMPv3 Community Table Page is shown in Figure 90.



SNMPv3 Community Table

Total Entries: 4. Page 1 of 1

	Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
	California	SantaClara456	wilson	swengtag testengtag	NonVolatile	Active
	alabama	birmingham123	jenny	swengtag	NonVolatile	Active
	carolina	raleigh998	chitra	testengtag	NonVolatile	Active
	dakota	bismarck778	hoa	hwengtag swengtag	NonVolatile	Active

Figure 90 Monitoring, SNMPv3 Community Table Page

Section IV

Spanning Tree Protocols

The chapter in this section explain the spanning tree protocols:

Chapter 20
STP, RSTP, and MSTP

This chapter explains how to configure the STP, RSTP and MSTP parameters on an AT-8500 Series switch from a web browser management session.

Sections in the chapter include:

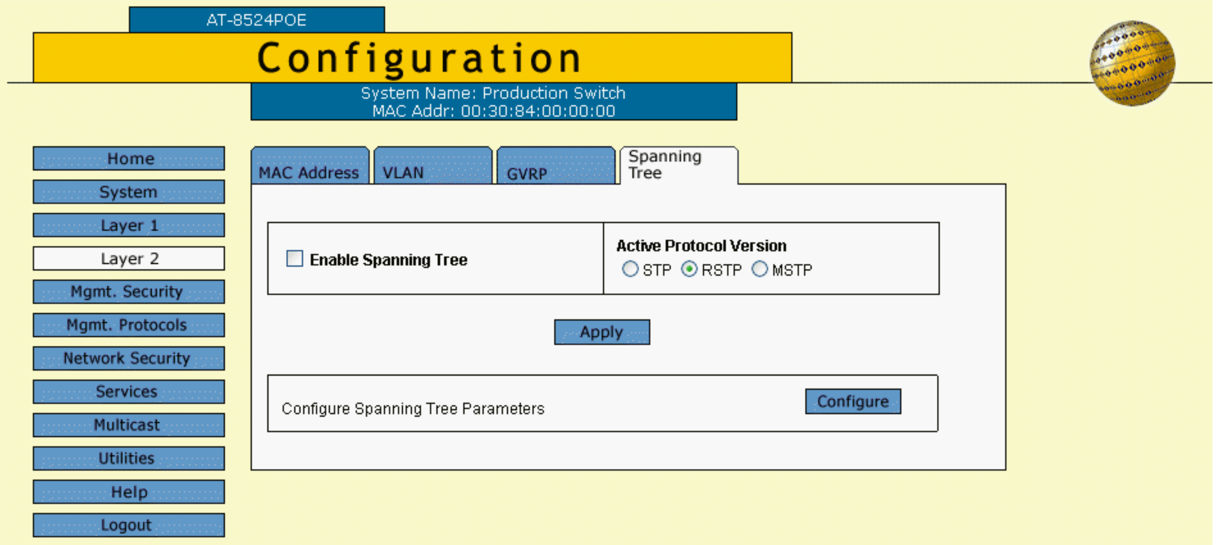
Note
For background information on STP, RSTP, and MSTP, refer to the *AT-S62 Menus Interface User’s Guide*.

Enabling or Disabling Spanning Tree

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

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 91.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

☐ Enable Spanning Tree

Active Protocol Version
○ STP ● RSTP ○ MSTP

Configure Spanning Tree Parameters

Figure 91 Spanning Tree Tab (Configuration)

4. To select an active spanning tree for the switch, click either **STP**, **RSTP**, or **MSTP** for the Active Protocol Version parameter. Only one protocol can be active on the switch at a time. The default is RSTP.
5. Click **Apply**.
6. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.

> **Note**
> Do not enable spanning tree on the switch until after you have selected an activate spanning tree protocol and configured the settings.

7. Click **Apply**.
8. If you activated STP, go to Configuring STP on page 249. If you activated RSTP go to Configuring RSTP on page 254. If you selected MSTP, go to Configuring MSTP on page 258.

Configuring STP

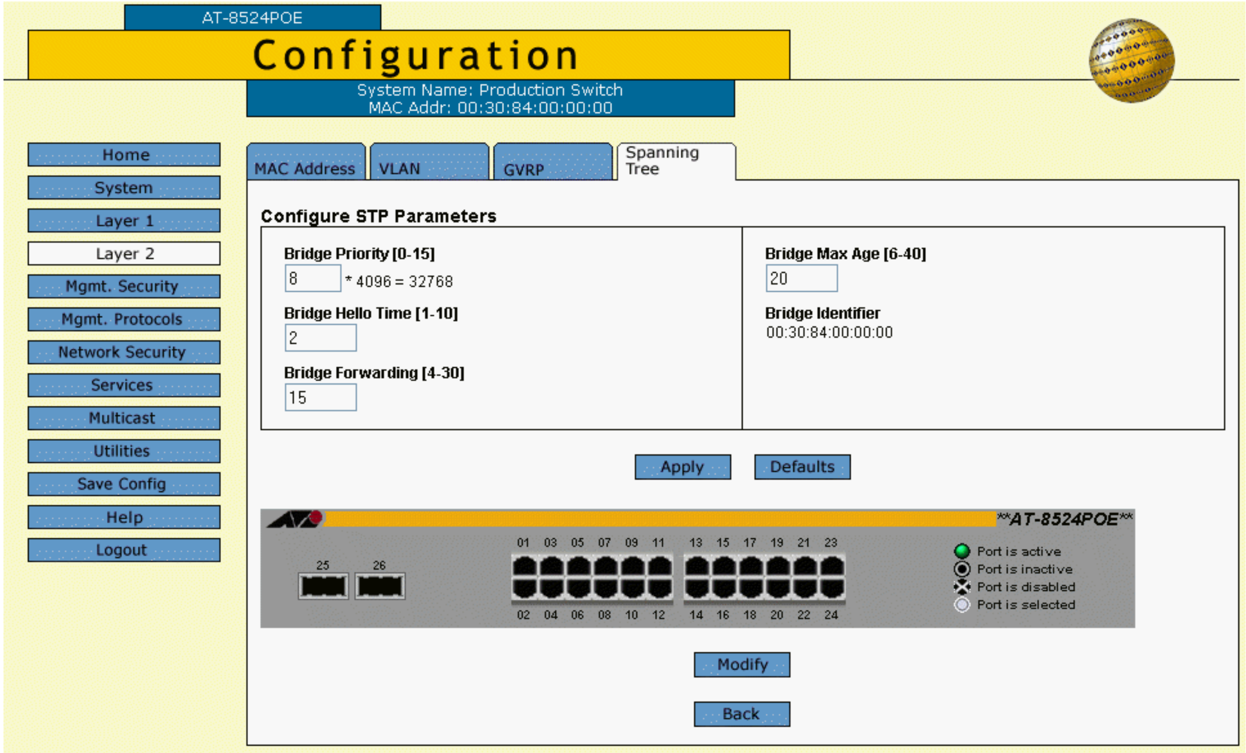
Caution
The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

This procedure assumes that you have already designated STP as the active spanning tree on the switch. For instructions, refer to Enabling or Disabling Spanning Tree on page 248.

To configure STP, perform the following procedure:

1. In the Spanning Tree tab, the Configure Spanning Tree Parameters section, click **Configure**.

   The STP Spanning Tree tab is shown in Figure 92.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Configure STP Parameters

Bridge Priority [0-15]
8 * 4096 = 32768

Bridge Hello Time [1-10]
2

Bridge Forwarding [4-30]
15

Bridge Max Age [6-40]
20

Bridge Identifier
00:30:84:00:00:00

Figure 92 STP Spanning Tree Tab

Note
The Defaults button returns all STP settings to the default settings.

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

   Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge.

   This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. There are sixteen increments. You specify the increment representing the desired bridge priority value. The increments are shown in Table 6.

Table 6 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

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

   Bridge Forwarding Delay
   The waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

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

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

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

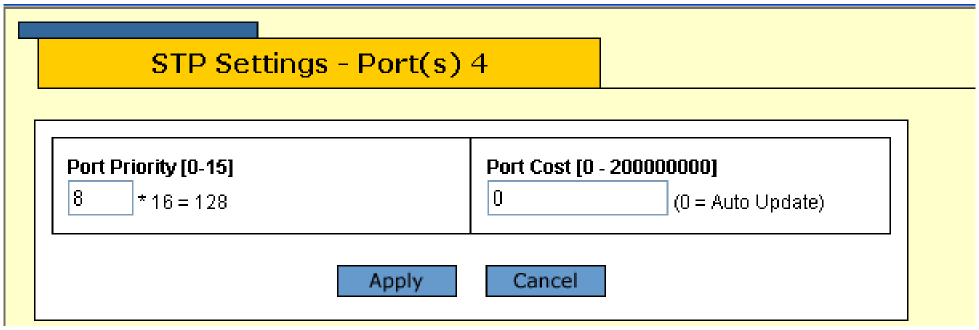
Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

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

3. After you have made the desired changes, click **Apply**.

4. To adjust a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The STP Port Settings window is shown in Figure 93.


STP Settings - Port(s) 4

Port Priority [0-15]
8 * 16 = 128

Port Cost [0 - 200000000]
0 (0 = Auto Update)

Figure 93 STP Port Settings Window

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

1 - Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range for

port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the increment of the desired value. Table 7 lists the values and increments. The default value is 128, which is increment 8.

Table 7 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

2 - Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 65,535. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Table 8 lists the STP port costs with Auto-Detect.

Table 8 STP Auto-Detect Port Costs

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

Table 9 lists the STP port costs with Auto-Detect when a port is part of a port trunk.

Table 9 STP Auto-Detect Port Trunk Costs

Port Speed	**Port Cost**
10 Mbps	4
100 Mbps	4
1000 Mbps	2

6. After configuring the parameters, click **Apply**.
7. To permanently save the change, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

Configuring RSTP

Caution

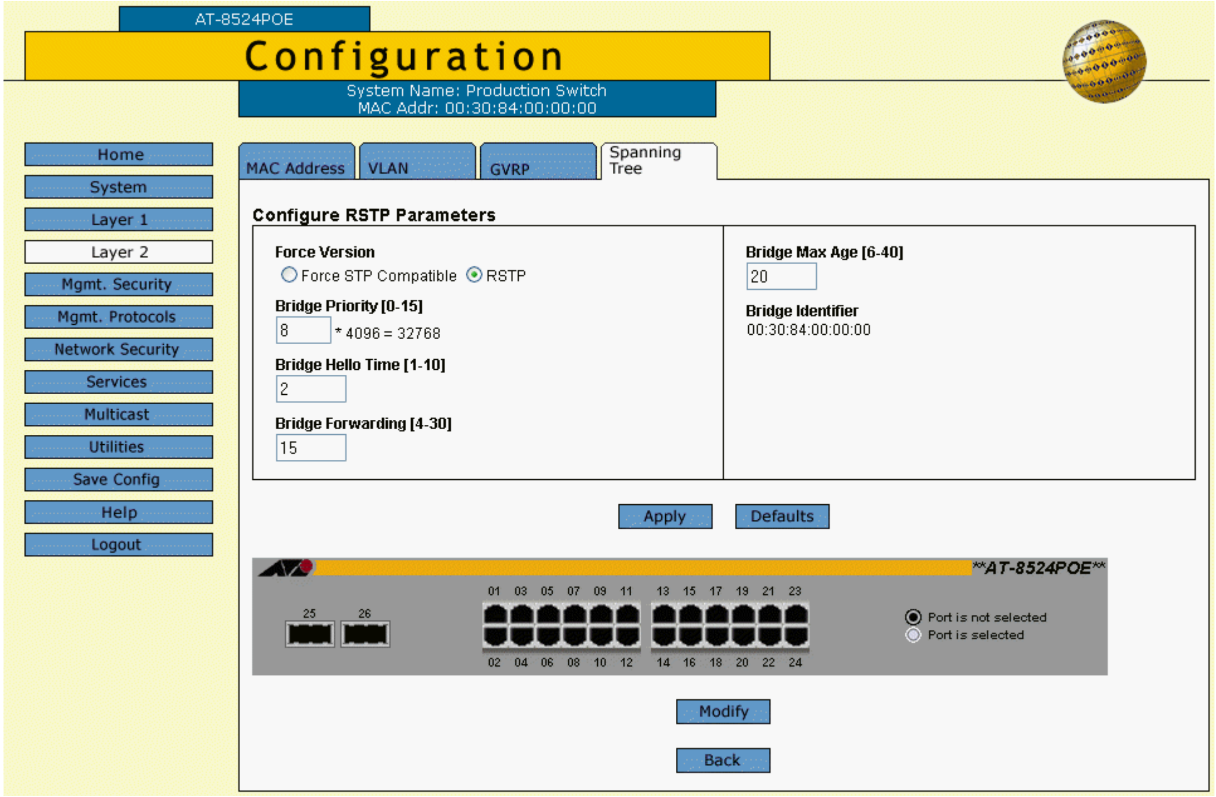
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

This procedure assumes that you have already designated RSTP as the active spanning tree on the switch. For instructions, refer to Enabling or Disabling Spanning Tree on page 248.

To configure RSTP, perform the following procedure:

1. In the Spanning Tree tab, Configure Spanning Tree Parameters section, click **Configure**.

   The RSTP Spanning Tree tab is shown in Figure 94.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Configure RSTP Parameters

Force Version
○ Force STP Compatible ● RSTP

Bridge Priority [0-15]
8 * 4096 = 32768

Bridge Hello Time [1-10]
2

Bridge Forwarding [4-30]
15

Bridge Max Age [6-40]
20

Bridge Identifier
00:30:84:00:00:00

Figure 94 RSTP Spanning Tree Tab

Note

The Defaults button returns all RSTP settings to the default settings.

2. Adjust the parameters are desired. The parameters are defined below.

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

   2 - Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 6, Bridge Priority Value Increments on page 250.

   3 - Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   4 - Bridge Forwarding
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

   5 - Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

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

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

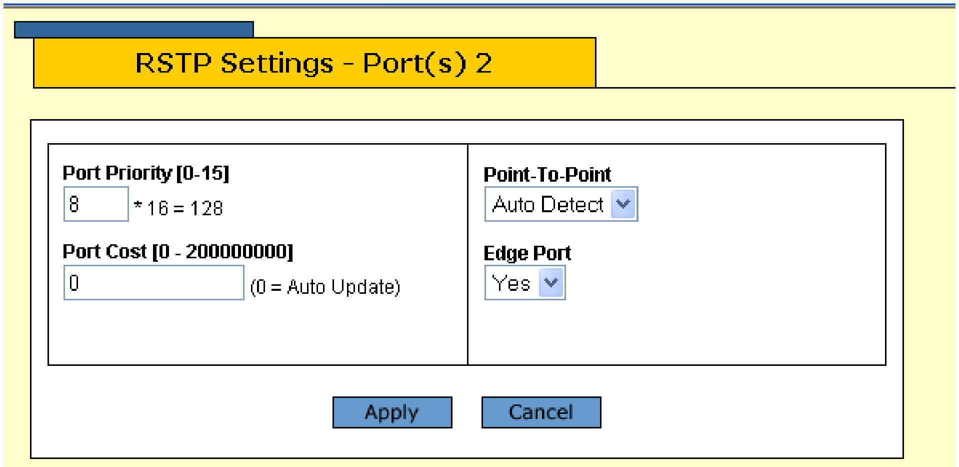
   MaxAge must be less than (2 x (ForwardingDelay - 1))

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

3. After you have made your changes, click **Apply**.

4. To adjust RSTP port settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The RSTP Port Settings window is shown in Figure 95.



RSTP Settings - Port(s) 2

Port Priority [0-15]
8 * 16 = 128

Port Cost [0 - 200000000]
0 (0 = Auto Update)

Point-To-Point
Auto Detect

Edge Port
Yes

Figure 95 RSTP Port Settings Window

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

1 - Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 7, Port Priority Value Increments on page 252.

2 - Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Table 10 lists the RSTP port costs with Auto-Detect when the port is not part of a port trunk.

Table 10 RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000

Table 10 RSTP Auto-Detect Port Costs

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

Table 11 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 11 RSTP Auto-Detect Port Trunk Costs

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

3 - Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to the *AT-S62 Menus Interface User's Guide*.

4 - Edge Port
This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to *AT-S62 Menus Interface User's Guide*.

6. After configuring the parameters, click **Apply**.
7. To permanently save the change, select the **Save Config** menu selection.

Configuring MSTP

This section is divided into the following procedures:

- ❑ Configuring MSTP and CIST Parameters on page 258
- ❑ Associating VLANs to MSTIs on page 261
- ❑ Configuring MSTP Port Parameters on page 264

This procedure assumes that you have already designated MSTP as the active spanning tree on the switch. For instructions, refer to Enabling or Disabling Spanning Tree on page 248.

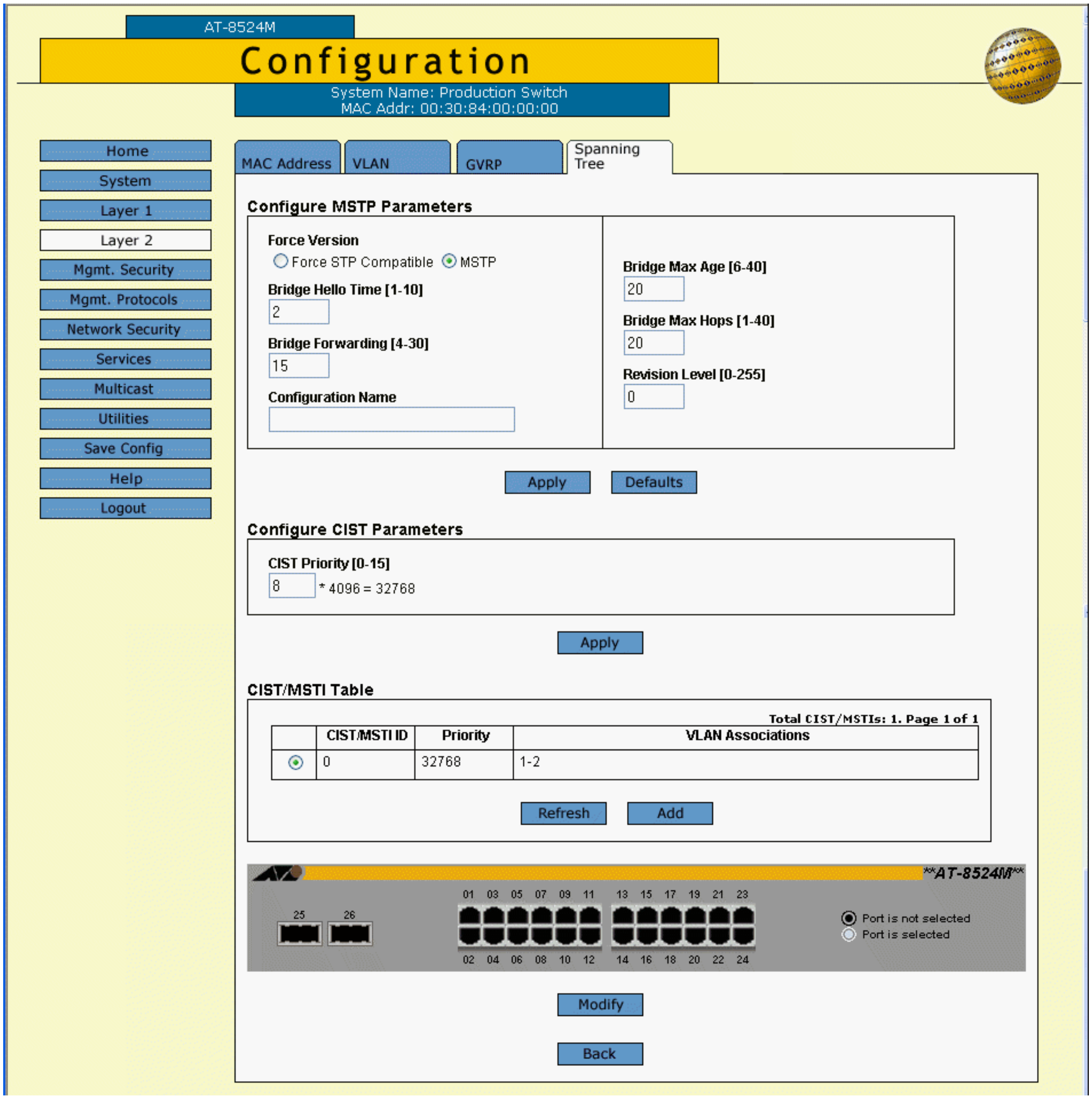
Configuring MSTP and CIST Parameters

To configure MSTP parameters, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

   The Spanning Tree Web Page appears as shown in Figure 91 on page 248.
4. Click **Configure**.

The MSTP Spanning Tree tab is shown in Figure 96.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:00

Configure MSTP Parameters

Force Version
○ Force STP Compatible ● MSTP

Bridge Hello Time [1-10]: 2

Bridge Forwarding [4-30]: 15

Configuration Name:

Bridge Max Age [6-40]: 20

Bridge Max Hops [1-40]: 20

Revision Level [0-255]: 0

Configure CIST Parameters

CIST Priority [0-15]: 8 * 4096 = 32768

CIST/MSTI Table

Total CIST/MSTIs: 1. Page 1 of 1

	CIST/MSTI ID	Priority	VLAN Associations
●	0	32768	1-2

● Port is not selected
○ Port is selected

Figure 96 MSTP Spanning Tree Tab

Note

This procedure explains the Configure MSTP Parameters and Configure CIST Parameters sections of the web page. The CIST/MSTI Table is explained in Associating VLANs to MSTIs on page 261. The graphic image of the switch is described in Configuring MSTP Port Parameters on page 264.

5. Adjust the bridge MSTP settings as needed. The parameters are described below.

   Force Version
   This selection determines whether the bridge will operate with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

   Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

   Bridge Forwarding
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

   Configuration Name
   The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case-sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

   Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

   All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

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

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

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

Bridge Max Hops
MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. Once the counter reaches zero, the BPDU is deleted.

Revision Level
The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

CIST Priority
The priority number for the bridge. This number is used in determining the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Once you have adjusted the parameters, click the **Apply** button.
7. To permanently save the changes, select the **Save Config** menu selection.

Associating VLANs to MSTIs

This section explains how to create and delete MSTI IDs and how to associate VLANs to MSTI IDs.

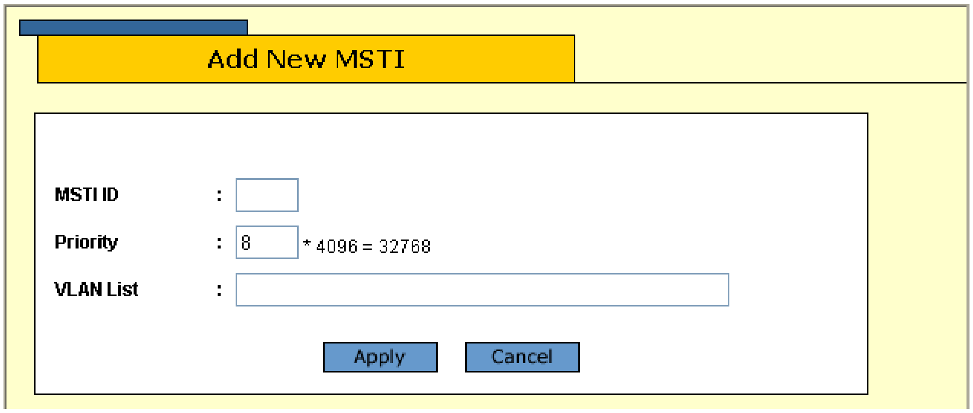
To manage the MSTI ID and VLAN associations, perform the following procedure:

1. Display the Spanning Tree Expanded Web Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP and CIST Parameters on page 258.

2. To create or delete an MSTI ID and to associate VLANs to MSTIs, do the following:

   a. In the CIST/MSTI Table section of the menu, click **Add**.

      The Add New MSTI window is shown in Figure 97.



Add New MSTI

MSTI ID :

Priority : 8 * 4096 = 32768

VLAN List :

Figure 97 Add New MSTI Window

   b. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.

   c. In the Priority field, enter a MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. The default is 0. There are sixteen increments. You specify the increment representing the desired bridge priority value. The increments are shown in Table 6 on page 250.

   d. In the VLAN List field, enter the VIDs of the VLANs to be associated with this MSTI. You can specify more than one VID at a time (e.g., 2,4,7).

   e. Click **Apply**.

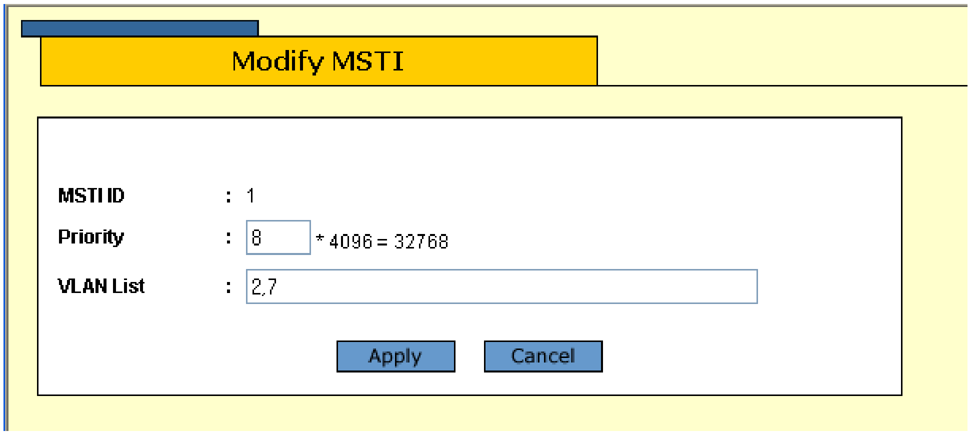
   f. Repeat this procedure to create more MSTI IDs.

3. To add or remove VLANs or to change the MSTI Priority value of an existing MSTI ID, do the following:

   a. In the CIST/MSTI Table section of the menu, click the circle next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.

   b. Click **Modify**.

The Modify MSTI window is shown in Figure 98.



Modify MSTI

MSTI ID : 1

Priority : 8 * 4096 = 32768

VLAN List : 2,7

Figure 98 Modify MSTI Window

c. In the Priority field, enter a new MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. The default is 0.There are sixteen increments. You specify the increment representing the desired bridge priority value. The increments are shown in Table 6 on page 250.

d. In the VLAN List field, modify the list of VIDs of the VLANs to be associated with this MSTI. You can add more VLANs or remove VLANs. You can specify more than one VID at a time (e.g., 2,4,7). If you remove a VLAN, the VLAN will be associated with CIST.

e. Click **Apply**.

f. Repeat this procedure to modify more MSTI IDs.

4. To delete an MSTI ID, do the following:

   a. In the CIST/MSTI Table section of the menu, click the circle next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.

   b. Click **Remove**.

      A confirmation prompt is displayed.

   c. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure.

      If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.

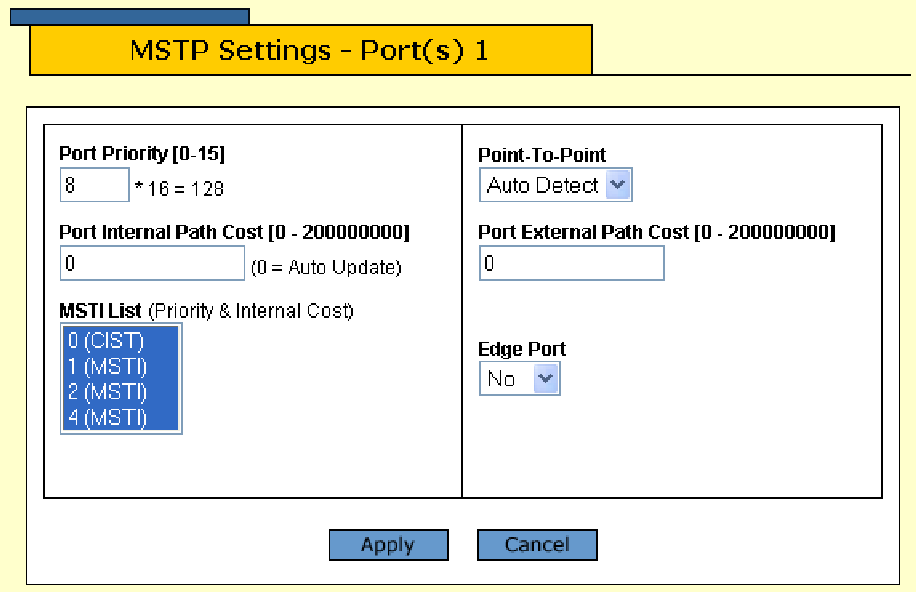
5. To permanently save the changes, select the **Save Config** menu selection.

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. Perform Steps 1 through 4 in the procedure Configuring MSTP and CIST Parameters on page 258 to display the Spanning Tree Expanded Web Page for MSTP.
2. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded Web Page, click the port you want to configure. You can select more than one port at a time. A selected port turns white.
3. Click **Configure**.

   The MSTP Port Settings window is shown in Figure 99.



MSTP Settings - Port(s) 1

Port Priority [0-15]
8 * 16 = 128

Port Internal Path Cost [0 - 200000000]
0 (0 = Auto Update)

MSTI List (Priority & Internal Cost)
0 (CIST)
1 (MSTI)
2 (MSTI)
4 (MSTI)

Point-To-Point
Auto Detect

Port External Path Cost [0 - 200000000]
0

Edge Port
No

Figure 99 MSTP Port Settings Window

4. Adjust the parameters as needed. The parameters are described below.

   The port parameters can be divided into two groups: generic parameters and MSTI-specific parameters. A generic port parameter is set just once on a port and applies to all MSTIs where a port, through its VLAN assignments, is a member. Generic parameters are:

   - ❑ External path cost
   - ❑ Point-to-point port
   - ❑ Edge port

An MSTI-specific parameter can be set on a per MSTI basis. This means that you can assign different values to a port's MSTI-specific parameters for each spanning tree instance where the port is a member. These parameters are:

❑ Internal path cost

❑ Port priority

When setting an MSTI-specific parameter, use the MSTI List in the window to select the intended MSTI. It should be noted that the MSTI List shows all of the spanning tree instances on the switch, and not just those where the selected port is currently a member. If you select an MSTI where the port is not a member, you can pre-configure the parameter in the event you later add the port as a member of the MSTI through a VLAN assignment.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. To select a port priority for a port, you enter the increment of the desired value. Table 7 on page 252 lists the values and increments. The default value is 128, which is increment 8.

This is an MSTI-specific parameter. If the port you are configuring is a member of more than one MSTI, you can assign the port a different priority value for each of its MSTI memberships. This is accomplished by entering a new priority value and then using the MSTI List option to select the MSTIs where you want the new parameter setting for the port to be applied.

Port Internal Path Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Table 10 lists the MSTP port cost with Auto Update when a port is not part of a port trunk.

Table 12 MSTP Auto Update Port Internal Path Costs

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

Table 11 lists the MSTP port costs with Auto Update when the port is part of a port trunk.

Table 13 MSTP Auto Update Port Trunk Internal Path Costs

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

This is also an MSTI-specific parameter. Like the priority parameter, you can, using the MSTI List, assign a different internal path cost for each MSTI where the port is a member.

Edge Port
This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to the *AT-S62 Menus Interface User's Guide*.

Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to the *AT-S62 Menus Interface User's Guide*.

Port External Path Cost
The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. The default setting is Auto, which sets port cost depending on the speed of the port. Table 14 lists the MSTP port costs with the Auto setting when the port is not a member of a trunk.

Table 14 MSTP Auto External Path Costs

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

Table 15 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 15 MSTP Auto External Path Trunk Costs

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

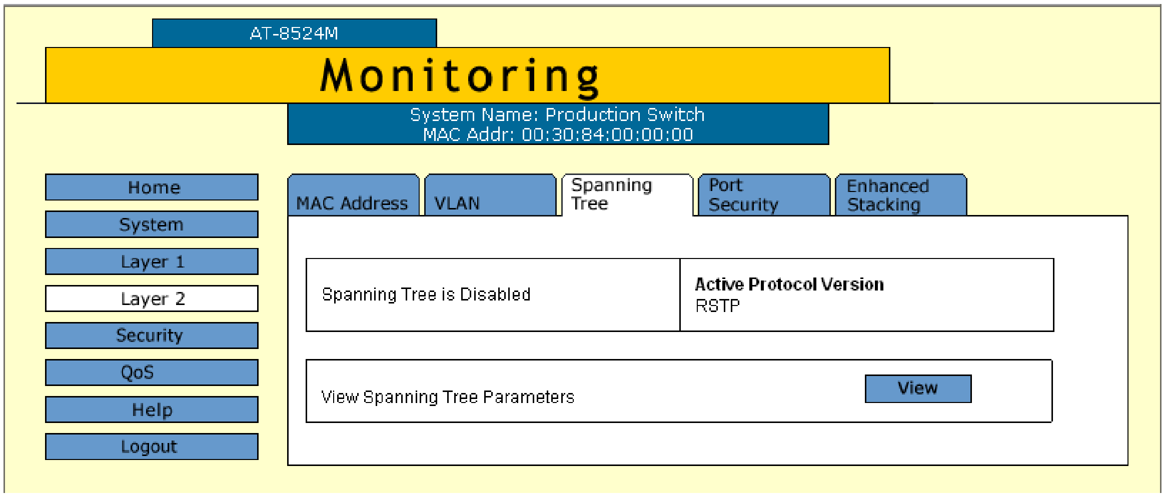
5. After adjusting the parameters, click **Apply**.
6. To permanently save the changes, select the **Save Config** menu selection.
7. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying Spanning Tree Settings

To display the parameter settings for the active spanning tree, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Layer 2**.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 100.



Spanning Tree is Disabled

Active Protocol Version
RSTP

View Spanning Tree Parameters

Figure 100 Spanning Tree Tab (Monitoring)

   This tab displays information on whether spanning tree is enable or disabled and which protocol version is active.

4. Click **View**.
5. To view port settings, click a port in the graphical image of the switch and click **Status** or **Settings**.

   For explanations of the spanning tree parameters, refer to earlier sections in this chapter.

Section V

Virtual LANs

The chapters in this section explain virtual LANs (VLANs). The chapters include:

Chapter 21

Virtual LANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs from a web browser management session. This chapter also explains how to select a multiple VLAN mode.

This chapter contains the following sections:

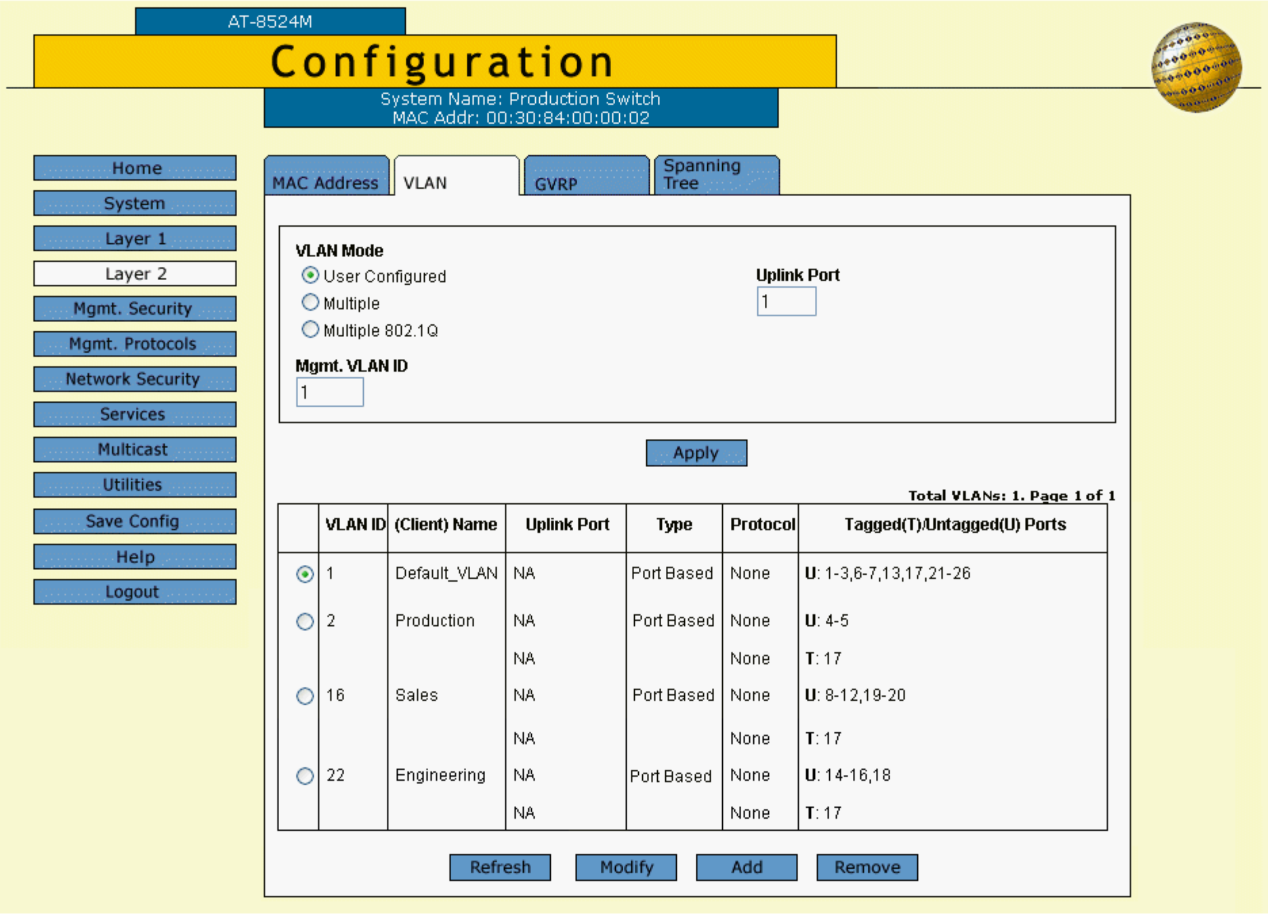
Note
For background information on port-based and tagged VLANs and the multiple VLAN modes, refer to the *AT-S62 Menus Interface User's Guide*.

Creating a New Port-based or Tagged VLAN

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

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 101.



VLAN Mode

● User Configured
○ Multiple
○ Multiple 802.1Q

Uplink Port: 1

Mgmt. VLAN ID: 1

Total VLANs: 1. Page 1 of 1

	VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Tagged(T)/Untagged(U) Ports
●	1	Default_VLAN	NA	Port Based	None	**U**: 1-3,6-7,13,17,21-26
○	2	Production	NA	Port Based	None	**U**: 4-5
			NA		None	**T**: 17
○	16	Sales	NA	Port Based	None	**U**: 8-12,19-20
			NA		None	**T**: 17
○	22	Engineering	NA	Port Based	None	**U**: 14-16,18
			NA		None	**T**: 17

Figure 101 VLAN Tab (Configuration)

Note

The tab will not include the Modify and Remove buttons if the only VLAN on the switch is the Default_VLAN.

The VLAN Mode and Uplink Port options are explained in Selecting a VLAN Mode on page 279. The Mgmt. VLAN ID option is explained in Specifying a Management VLAN on page 280.

This tab displays the VLANs on the switch. The columns in the tab are defined below:

VLAN ID
The VID number assigned to the VLAN.

(Client) Name
The name of the VLAN.

Uplink Port
This column contains “NA,” meaning Not Applicable, for tagged and port-based VLANs. For a protected ports VLAN, this column contains the uplink port(s) for the port groups. A tagged uplink port is designated with a “T” and an untagged uplink port has a “U.” If the switch is operating in one of the two multiple VLAN modes this column displays the port that is functioning as the uplink port for the other ports on the switch.

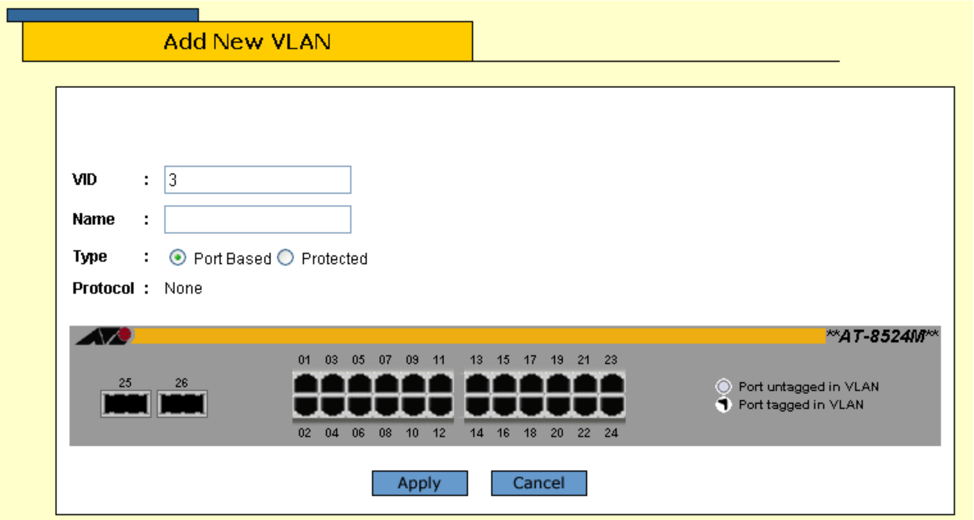
Type - Either Port Based, for both port-based and tagged VLANs, or GVRP Dynamic, for VLANs created by GVRP.

Protocol - If this column contains None, the VLAN is a port-based, tagged, or protected ports VLAN. If it contains GARP, the VLAN or the port is a dynamic GVRP VLAN or a dynamic GVRP port of a static VLAN.

Tagged(T)/Untagged(U) Port
Lists the ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

4. To create a new VLAN, click **Add**.

   The Add New VLAN page is shown in Figure 102.



Add New VLAN

VID : 3

Name :

Type : ● Port Based ○ Protected

Protocol : None

Figure 102 Add New VLAN Page

5. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

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

   Note
   A VLAN must have a VID.

   The switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-8500 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S62 software will still use VID 2 as the default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

6. Select the **Name** field and enter a name for the new VLAN.

   The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

   If the VLAN will be unique in your network, then the name should be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

   Note
   A VLAN must be assigned a name.

7. Select **Port Based** as the Type. This is the default setting. This is the correct setting when creating a port-based or tagged VLAN.

   Note
   The Type selection of Protected is used to create a protected ports VLAN, as explained in Chapter 21, Protected Ports VLANs on page 287.

8. To select the ports for the VLAN, click the ports in the switch image.

   Clicking repeatedly on a port toggles it through the following possible settings:

   □ Untagged port

   ⚑ Tagged port

   ■ Port not a member of the VLAN

9. Click **Apply**.

   Note
   Any untagged ports you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

   The new user-configured VLAN is now ready for network operations.

10. To permanently save the changes, select the **Save Config** menu selection.

Modifying a Port-based or Tagged VLAN

This procedure explains how to add or remove ports from a port-based or tagged VLAN. When modifying a VLAN, note the following:

❑ You cannot change the VID of a VLAN.

❑ You cannot change the name of a VLAN from a web browser management session; you can from a local, Telnet, or SSH session.

❑ You cannot modify VLANs when the switch is operating in one of the multiple VLAN modes.

To modify a VLAN, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 101 on page 271.
4. Click the button next to the name of the VLAN you want to modify.
5. Click **Modify**.

   The Modify VLAN window for the VLAN is displayed.
6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

   Clicking on a port toggles it through the following possible settings:

   □ Untagged port

   ◪ Tagged port

   ■ Port not a member of the VLAN
7. After making the necessary changes, click **Apply**.

Note
Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN will leave the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

8. To permanently save the change, select the **Save Config** menu selection.

Deleting a Port-based or Tagged VLAN

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 101 on page 271.
4. Click the button next to the name of the VLAN you want to delete. You cannot delete the Default_VLAN.
5. Click **Remove**.

   A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.
7. To permanently save the change, select the **Save Config** menu selection.

Displaying VLANs

To display the current VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The columns in the tab are defined below.

   VLAN ID
   The VID number assigned to the VLAN.

   (Client) Name
   The name of the VLAN. If the switch is operating in one of the multiple VLAN modes, the names of the VLANs start with “Client,” with the exception of the VLAN containing the uplink port, which starts with “Uplink.”

   Uplink Port
   This column contains “NA,” meaning Not Applicable, for tagged and port-based VLANs. For a protected ports VLAN, this column contains the uplink port(s) for the port groups. A tagged uplink port is designated with a “T” and an untagged uplink port has a “U.” If the switch is operating in one of the two multiple VLAN modes this column displays the port that is functioning as the uplink port for the other ports on the switch.

   Type - If this column contains Port Based, the VLAN is a port-based or tagged VLAN. If it contains GARP, the VLAN was created automatically by GVRP.

   Protocol - If this column contains None, the VLAN is a port-based, tagged, or protected ports VLAN. If it contains GARP, the VLAN or the port is a dynamic GVRP VLAN or a dynamic GVRP port of a static VLAN.

   Tagged(T)/Untagged(U) Port
   The ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

Selecting a VLAN Mode

The AT-S62 management software features three VLAN modes:

- ❑ Port-based and tagged VLAN Mode (default mode)
- ❑ IEEE 802.1Q-compliant Multiple VLAN Mode
- ❑ Non-IEEE 802.1Q compliant Multiple VLAN Mode

For background information on port-based and tagged VLANs and the multiple VLAN modes, refer to the *AT-S62 Menus Interface User's Guide*.

> **Note**
> Any existing port-based or tagged VLANs are deleted when you change the VLAN mode from the user configured mode to a multiple VLAN mode and, at some point, reset the switch. The user configured VLAN information will be lost and will need to be recreated if you later return the switch to the user configured VLAN mode.

To select a VLAN mode for the switch, perform the procedure below:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 101 on page 271.
4. In the VLAN Mode section, select a VLAN mode. Only one mode can be active on the switch at a time. The modes are:
   - ❑ User Configured - Port-based and tagged VLAN Mode
   - ❑ Multiple - Non-IEEE 802.1Q-compliant Multiple VLAN Mode
   - ❑ Multiple 802.1Q - IEEE 802.1Q-compliant Multiple VLAN Mode
5. If you select one of the multiple VLAN modes, specify an uplink port in the Uplink Port field. This port will function as the uplink port for the VLANs. The default is port 1.
6. Click **Apply**.

   The new mode is automatically activated on the switch.
7. To permanently save the change, select the **Save Config** menu selection.

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-8500 Series switch expects to receive management packets. This VLAN is important if you will be managing a switch remotely or using the enhanced stacking feature of the switch.

Management packets are packets generated by a management workstation when you remotely manage a switch using Telnet, SSH, or a web browser. The switch will act upon the management packets only if they are received on a port that is a member of the management VLAN.

The default management VLAN on an AT-8500 Series switch is the Default_VLAN. If you do not create any additional VLANs and link the switches together using untagged ports, then there will be no need to specify a new management VLAN in order to remotely manage the devices.

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

Below are several rules to observe when using this feature:

- ❑ The management VLAN must exist on each AT-8500 Series switch that you want to manage.
- ❑ All of the switches in an enhanced stack must use the same management VLAN. Consequently, you must use the following procedure to specify the management VLAN in the AT-S62 software on each slave and master switch of an enhanced stack.
- ❑ The uplink and downlink ports on each switch that are functioning as the tagged or untagged data links between the switches must be either tagged or untagged members of the management VLAN.
- ❑ The port on the switch to which the management station is connected must be a member of the management VLAN. (This rule does not apply when managing the switch locally through the RS232 Terminal Port.)

Here is an example. Let’s assume that you have an enhanced stack of seven AT-8500 Series switches with one master switch. If the uplink and downlink ports between the various switches are members of the Default_VLAN and if the management station is connected to a port of the Default_VLAN, you will be able to manage all the switches without designating a new management VLAN because the Default_VLAN is the default management VLAN.

Now let's assume that you decide to create a VLAN called NMS with a VID of 24 for the sole purpose of remote Telnet, SSH, and web browser network management of your switches. For this, you would need to create the NMS VLAN on each AT-8500 Series switch that you want to manage remotely, being sure to assign each NMS VLAN the VID of 24. Then you would need to be sure that the uplink and downlink ports connecting the switches together are either tagged or untagged members of the NMS VLAN. You would also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you must be sure to connect your management station to a port on a switch that is a tagged or untagged member of the management VLAN.

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

To set the management VLAN, do the following:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 101 on page 271.
4. For the Mgmt. VLAN ID parameter, enter the VID of the VLAN on the switch that is to function as the management VLAN. The VLAN must already exist on the switch. The default is 1, which is the VID of the Default_VLAN.
5. Click **Apply**.

   The change in the designated management VLAN is immediately activated on the switch.
6. To permanently save the change, select the **Save Config** menu selection.

Chapter 22

GARP VLAN Registration Protocol

This chapter explains how to configure GVRP on the switch. The procedures include:

- ❑ Configuring GVRP on page 283
- ❑ Enabling or Disabling GVRP on a Port on page 285
- ❑ Displaying the GVRP Settings on page 286

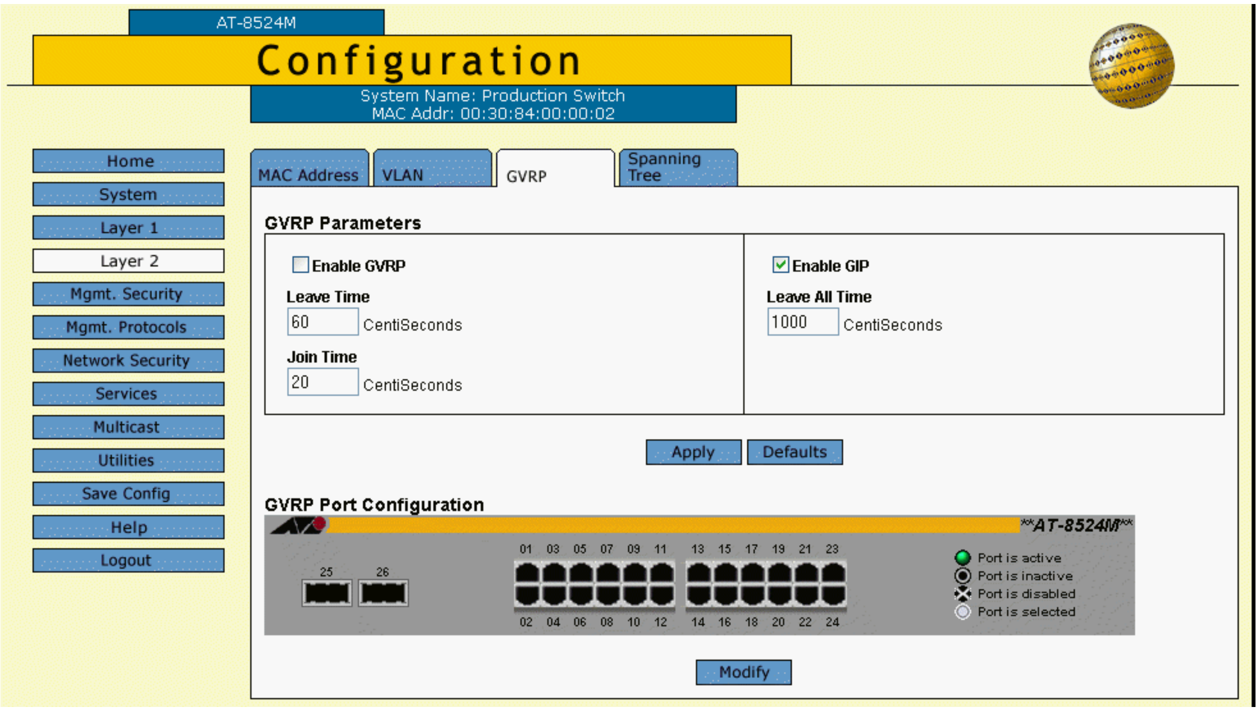
Note
For background information and guidelines on GVRP, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring GVRP

To configure the GVRP parameters, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 103.



GVRP Parameters

☐ Enable GVRP

Leave Time: 60 CentiSeconds

Join Time: 20 CentiSeconds

☑ Enable GIP

Leave All Time: 1000 CentiSeconds

Figure 103 GVRP Tab (Configuring)

The GVRP tab is not shown if MSTP is enabled on the switch.

The Default button returns all GVRP parameter settings to their default values.

4. Configure the following parameters:

   Enable GVRP
   Click this box to enable or disable GVRP. A check in the box enables GVRP. No check disables GVRP. The default setting is disabled.

   Leave Time
   Sets the duration of the Leave Period timer. The range is from 30 to180 centiseconds and the default is 60.

Join Time
Sets the duration of the Join Period timer. The range is from 10 to 60 centiseconds and the default is 20.

If you change this timer, it must in relation to the GVRP Leave Timer according to the following equation:

Join Timer <= 2 x (GVRP Leave Timer)

Enable GIP
Enables the operation of GIP. If enabled, attribute registrations and de-registrations processed on a port are propagated to other ports in the GIP-connected ring. GIP must be enabled in order to use GVRP.

Note
Do not disable GIP if you intend to use GVRP. GIP is required to propagate VLAN information among the ports of the switch.

Leave All Time
Sets the duration of the LeaveAll Period timer. The range is from 500 to 3000 centiseconds and the default is 1000.

⚠ **Caution**
The settings for the three GVRP timers must be the same on all GVRP-active devices in your network.

5. Click **Apply**.

   The new GVRP settings are activated on the switch.

6. To permanently save the changes, select the **Save Config** menu selection.

Enabling or Disabling GVRP on a Port

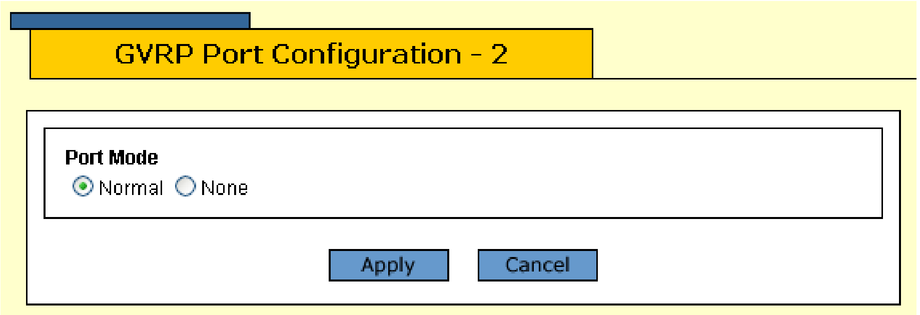
This procedure enables and disables GVRP on a switch port. The default setting for GVRP on a port is enabled. Only those ports where GVRP is enabled transmit PDUs.

> **Note**
> Allied Telesyn recommends disabling GVRP on unused ports and those ports that are connected to GVRP-inactive devices. This will protect against unauthorized access to restricted areas of your network.

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 103 on page 283.
4. Click the port you want to configure in the graphic image of the switch. A selected port turns white. To deselect a port, click it again. You can configure more than one port at a time.
5. Click **Modify**.

   The GVRP Port Configuration page is shown in Figure 104.



Port Mode
● Normal ○ None

Figure 104 GVRP Port Configuration Page

6. Change the port mode if desired.

   A setting of Normal means the port processes and propagates GVRP information. This is the default setting. A setting of None prevents the port from processing GVRP information and from transmitting PDUs.
7. Click **Apply**.

   The change to the GVRP port mode is activated on the port.
8. To permanently save the change, select the **Save Config** menu selection.

Displaying the GVRP Settings

To view the GVRP settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Layer 2** option.
3. Select the **GVRP** tab.

   For definitions of the GVRP parameters, refer to Configuring GVRP on page 283.

4. To view GVRP switch and port configuration information, select one of the following and click **View**:

   View Port Configuration
   Displays the status of GVRP on each port. Normal indicates that GVRP is active on a port while None means it is inactive.

   View GVRP Database
   Refer to the *AT-S62 Menus Interface User's Guide* for descriptions of the status information displayed by the selection.

   View GVRP State Machine for VLAN
   Refer to the *AT-S62 Menus Interface User's Guide* for descriptions of the status information displayed by the selection. You must enter a VID number.

   View GVRP Counters
   Refer to the *AT-S62 Menus Interface User's Guide* for descriptions of the status information displayed by the selection.

   View GIP Connected Ports Ring
   Refer to the *AT-S62 Menus Interface User's Guide* for descriptions of the status information displayed by the selection.

Chapter 23

Protected Ports VLANs

This chapter explains how to create, modify, and delete a protected ports VLAN using a web browser management session. This chapter contains the following sections:

- ❑ Deleting a Protected Ports VLAN on page 288
- ❑ Displaying a Protected Ports VLAN on page 289

Note
For background information on protected ports VLANs, refer to the *AT-S62 Menus Interface User's Guide*.

Note
You cannot create or modify protected ports VLANs from the web browser interface. These functions must be performed from the menus interface or the command line interface.

Deleting a Protected Ports VLAN

To delete a protected ports VLAN from the switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.
4. Click the button next to the name of the protected ports VLAN you want to delete. You cannot delete the Default_VLAN.
5. Click **Remove**.

   A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. All ports in the VLAN are returned to the Default_VLAN as untagged ports.
7. To permanently save the change, select the **Save Config** menu selection.

Displaying a Protected Ports VLAN

To display the details of a protected port VLAN, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Layer 2** menu selection.
3. Select the **VLAN** tab.
4. Click the circle next to the protected ports VLAN you want to view and click **View**.

   The specifications of the selected VLAN are displayed.

Section VI

Port Security

The chapters in this section explain the port security features of the AT-8524M switch The chapters include:

Chapter 24

MAC Address Security

This chapter explains how to display and configure MAC address security on the ports on a switch. It contains the following section:

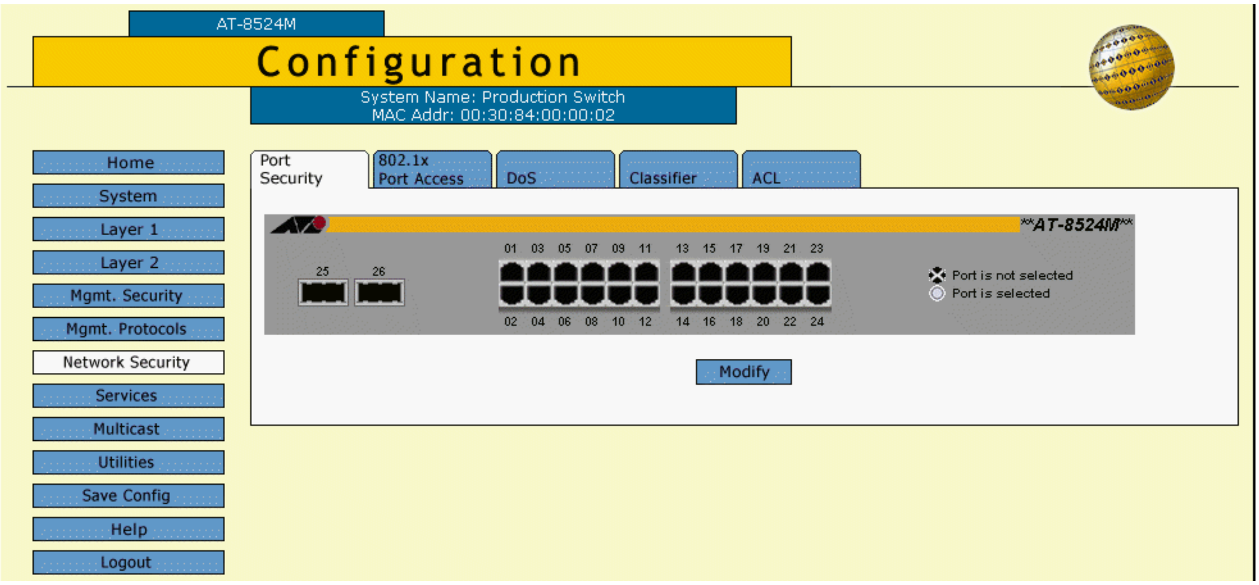
Note
For background information and guidelines on MAC address security, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring MAC Address Security

MAC address security allows you to control access to a port on the switch using the MAC addresses of the end nodes. To configure MAC address security, perform the following procedure:

1. From the Home page, select **Configuration**.
2. Select the **Network Security** menu selection.
3. Select the **Port Security** tab.

   The Port Security tab is shown in Figure 105.

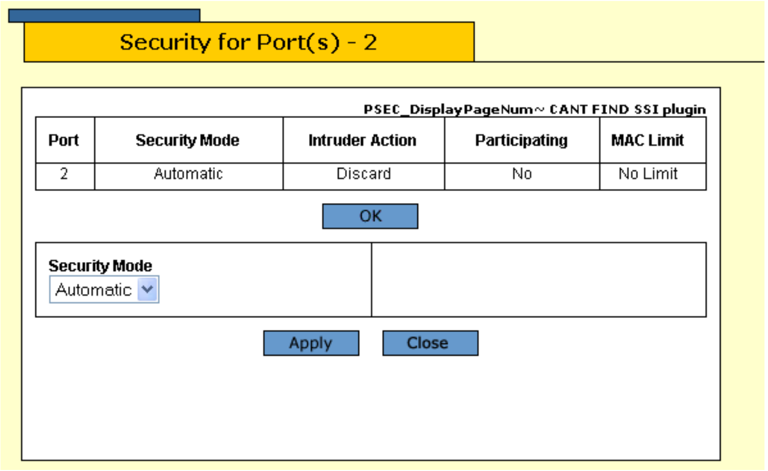


System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Figure 105 Port Security Tab

4. Click the port you want to configure. A selected port turns white. To deselect a port, click it again. You can configure more than one port at a time.
5. Click **Modify**.

The Security for Port(s) window is shown in Figure 106.



Port	Security Mode	Intruder Action	Participating	MAC Limit
2	Automatic	Discard	No	No Limit

Security Mode: Automatic

Figure 106 Security for Port(s) Window

The top portion of the window displays the current security settings of the selected ports.

6. From the Security Mode pull-down menu, select the desired port security level for the port. Options are:

Automatic
Disables port security on a port. This is the default setting.

Limited
Allows you to specify a maximum number of dynamic source MAC addresses a port can learn. Once a port has learned its maximum number, it will not learn any new addresses and will only accept frames from the source nodes of the learned addresses.

A dynamic MAC address learned on a port operating in the Limited security mode never times out from the MAC address table, even when the corresponding end node is inactive.

You can add static addresses to a port running this security level. Static addresses are not included in the count of the maximum number of dynamic addresses.

Secured
Instructs a port to forward frames using only static MAC address. The port will not learn any dynamic MAC addresses and will delete any dynamic addressees that it has already learned. Only those end nodes whose MAC addresses are entered as static addresses can forward frames through the port.

Locked
Instructs a port to immediately stop learning new dynamic MAC addresses. Frames are forwarded using the dynamic MAC addresses that the port has already learned and any static MAC addresses assigned to the port.

Dynamic MAC addresses learned by the port prior to the activation of this security level never time out from the MAC address table, even when the corresponding end nodes are inactive. However, the port will not learn any new dynamic addresses.

You can continue to add new static MAC addresses to a port operating under this security level.

7. If you select the Limited security level, additional options are displayed in the window for you to configure. They are defined here:

   Intrusion Action
   Specifies what the switch should do if a port receives an invalid frame. Options are

   ❑ Discard - Discards the invalid frame.

   ❑ Trap - Discards the invalid frame and sends an SNMP trap.

   ❑ Discard - Discards the invalid frame, sends an SNMP trap, and disables the port.

   Threshold
   Specifies the maximum number of dynamic MAC addresses you want the port to be able to learn. The range is 1 to 256. The default is 100.

   Port Participating
   Applies only when the intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard. If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send the SNMP trap or disable the port. If you want the switch to send a trap and/or disable the port, you must sent this option to Yes.

8. After configuring the parameters, click **Apply**.

   Note
   A change to a port’s MAC security is immediately activated on the port.

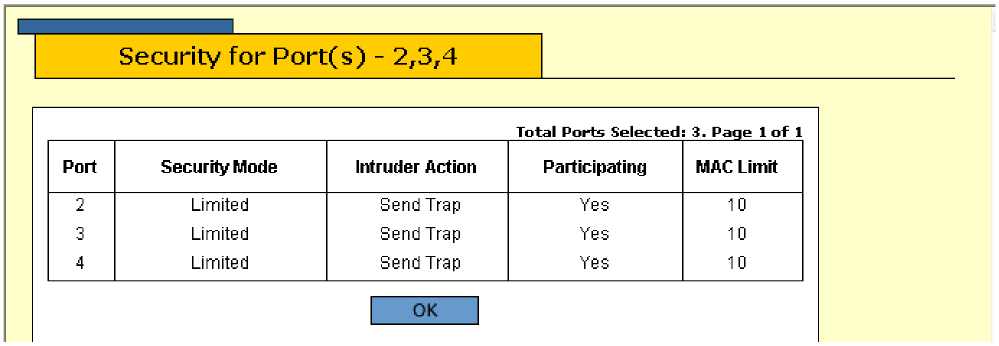
9. To permanently save the changes, select the **Save Config** menu selection.

Displaying MAC Address Security

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select **Network Security**.
3. Select the **Port Security** tab.
4. Click the port whose port security level you want to view. A selected port turns white. You can select more than one port at a time.
5. Click **View**.

   The security information for the selected ports is displayed in the Security for Port(s) page. An example is shown in Figure 107.



Security for Port(s) - 2,3,4

Total Ports Selected: 3. Page 1 of 1

Port	Security Mode	Intruder Action	Participating	MAC Limit
2	Limited	Send Trap	Yes	10
3	Limited	Send Trap	Yes	10
4	Limited	Send Trap	Yes	10

Figure 107 Security for Port(s) Tab

This page is for viewing purposes only. The columns in the page are defined below:

Port
The number of the port.

Security Mode
The active security mode on the port.

Intruder Action
The column specifies the action taken by a port when it receives an invalid frame.

- ❑ Discard: The port discards invalid frames. This is the default.
- ❑ Send Trap: The port discards invalid frames and sends a trap.
- ❑ Disable Port: The port discards invalid frames, sends a trap, and disables the port.

Participating

This column applies only when the intrusion action on a port is set to trap or disable. It does not apply when intrusion action is set to discard. If this column contains No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send the SNMP trap or disable the port. When this column contains Yes, the port sends a trap and/or is disabled after receiving an invalid frame.

MAC Limit

This column specifies the maximum number of dynamic MAC addresses the port will learn. It only applies when a port is operating in the Limited security mode.

Chapter 25

802.1x Port-based Access Control

This chapter contains instructions on how to configure the 802.1x port-based access control feature on the switch.

Note
For background information and guidelines on 802.1x port-based access control, refer to the *AT-S62 Menus Interface User's Guide*.

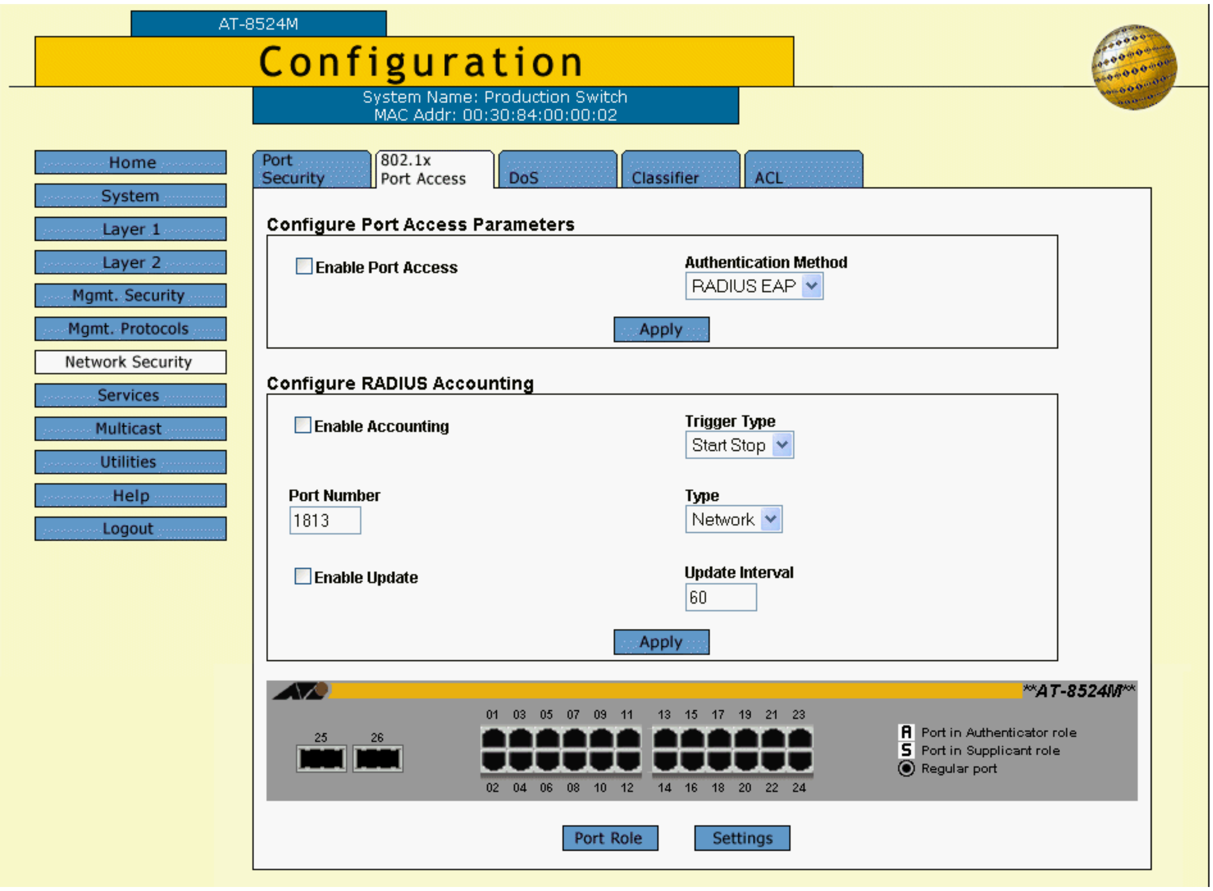
Enabling or Disabling Port-based Access Control

This procedure explains how to enable or disable port-based access control on the switch. If you have not assigned port roles and configured the parameter settings, you should skip this procedure and go first to Setting Port Roles on page 300. This procedure also explains how to configure RADIUS accounting.

To enable or disable port-based access control or configure RADIUS accounting, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Network Security** menu selection.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 108.



Configure Port Access Parameters

□ Enable Port Access

Authentication Method: RADIUS EAP

Configure RADIUS Accounting

□ Enable Accounting

Trigger Type: Start Stop

Port Number: 1813

Type: Network

□ Enable Update

Update Interval: 60

A Port in Authenticator role
S Port in Supplicant role
◉ Regular port

Figure 108 802.1x Port Access Tab (Configuration)

Note
The Authentication Method field cannot be changed.

---

4. To enable or disable the feature, do the following:

   a. Click the **Enable Port Access** check box. A check in the box means that the feature is activated on the switch. No check means that the feature is disabled. The default is disabled.

   b. Click **Apply**.

5. If you want to use the RADIUS accounting feature, configure the parameters in the RADIUS Accounting section of the tab. The parameter are described below:

   Enable Accounting
   Activates or deactivates RADIUS accounting on the switch. A check in the box indicates the feature is activated. No check means the feature is disabled. The default is Disabled.

   Trigger Type
   Specifies the action that causes the switch to send accounting information to the RADIUS server. The choices are:

   ❑ Start Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

   ❑ Stop - The switch sends accounting information only when a client logs off.

   Port Number
   Specifies the UDP port for RADIUS accounting. The default is port 1813.

   Type
   Specifies the type of RADIUS accounting. The default is Network. This value cannot be changed.

   Enable Update
   Controls whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled. If you enable this feature, use the next option to specify the intervals at which the switch is to send the accounting updates.

   Update Interval
   Specifies the intervals at which the switch is to send interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

6. Click **Apply**.

7. To permanently save the changes, select the **Save Config** menu selection.

Setting Port Roles

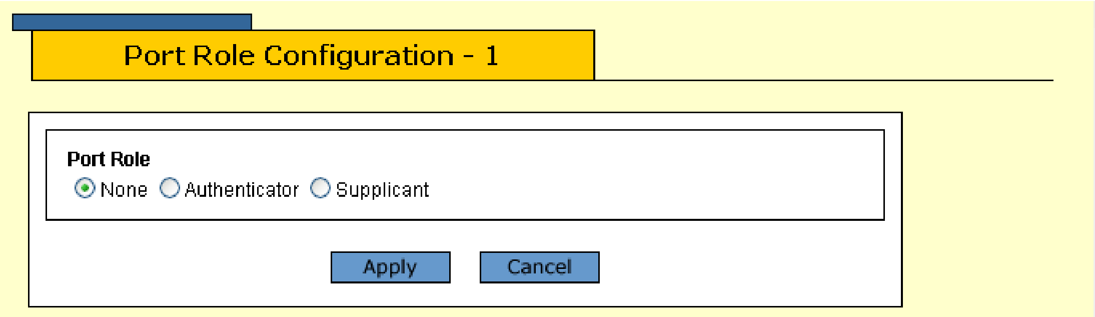
To set port roles for port-based access control, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select **Security**.
3. Select the **802.1x Port Access** tab.

   The Security page is as shown in Figure 108 on page 298.

   The graphic image of the switch shows which ports have been assigned port roles. Ports with an “A” are authenticators while ports with an “S” are supplicants. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.
4. To set a port’s role, click on the port. The selected port turns white. You can select more than one port at a time.
5. Click **Port Role**.

   The Port Role Configuration page is shown in Figure 109.


Port Role Configuration - 1

Port Role

● None ○ Authenticator ○ Supplicant

Figure 109 Port Role Configuration Page

6. Select the desired role for the port. Click **None** if the port is not to participate in port access control. This is the default setting. Clicking **Authenticator** configures the port to function as an authenticator. This is the appropriate setting if the port is connected to a supplicant. Clicking **Supplicant** sets the port to function as an supplicant. This is the appropriate setting if the port is connected to an authenticator. A port can have only one port role at a time.
7. Click **Apply**.

   The new role is immediately activated on the port.
8. To permanently save the change, select the **Save Config** menu selection.

9. To configure authenticator port settings, go to Configuring Authenticator Port Parameters on page 302. To configure supplicant port settings, go to Configuring Supplicant Port Parameters on page 306.

Configuring Authenticator Port Parameters

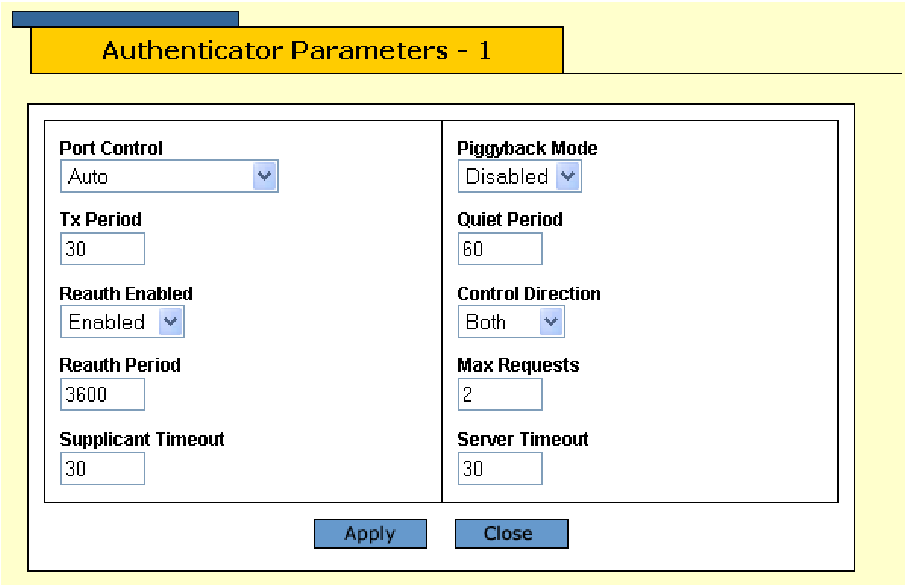
To configure authenticator port parameters, perform the following procedure:

1. From the 802.1x Port Access tab shown in Figure 108 on page 298, click the authenticator port that you want to configure. You can select more that one authenticator port at a time. The selected port turns white.

Note
A port must already be designated as an authenticator before you can configure its settings. For instructions on how to set the role of a port, refer to Setting Port Roles on page 300.

2. Click **Settings**.

The Authenticator Parameters page is shown in Figure 110.



Authenticator Parameters - 1

Port Control: Auto
Tx Period: 30
Reauth Enabled: Enabled
Reauth Period: 3600
Supplicant Timeout: 30
Piggyback Mode: Disabled
Quiet Period: 60
Control Direction: Both
Max Requests: 2
Server Timeout: 30

Figure 110 Authenticator Parameters Page

3. Adjust the parameters as needed. The parameters are described below:

Port Control
This parameter can take the following values:

□ **Auto**: Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch using the client's MAC address. This is the default setting.

- ❑ **Force-authorized**: Disables IEEE 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.

- ❑ **Force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

TX Period
Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds. The default value is 30 seconds.

Reauth Enabled
Controls whether the client must periodically reauthenticate. The default setting of enabled requires the client to periodically reauthenticate. The time period between reauthentications is set with the Reauth Period option. If this parameter is set to disabled, the client is not required to reauthenticate after the initial authentication, unless there is a change to the status of the link between the supplicant and the switch or the switch is reset or power cycled.

Reauth Period
Specifies the time period between reauthentications of the client. The default value is 3600 seconds. The range is 1 to 65,535 seconds. Option 3 - Reauth Enabled must be set to Enabled for this parameter to be operational.

Supplicant Timeout
Sets the switch-to-client retransmission time for the EAP-request frame. The range is 1 to 600 seconds. The default value is 30 seconds.

Piggyback Mode
Controls who can use the switch port in cases where there are multiple clients (e.g., the port is connected to an Ethernet hub). If set to enabled, the port allows all clients on the port to piggy-back onto the initial client's authentication and forwards all packets,

regardless of the client. If set to Disabled, then the switch port forwards only those packets from the client who was authenticated and discards packets from all other users.

Quiet Period
Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65,535 seconds. The default value is 60 seconds.

Control Direction
Specifies how the port is to handle ingress and egress broadcast and multicast packets when in the unauthorized state. When a port is set to the Authenticator role, it remains in the unauthorized state until the client logs on by providing a username and password combination. In the unauthorized state, the port will only accept EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, is discarded until the supplicant has logged on.

You can use this selection to control how an Authenticator port will handle egress broadcast and multicast traffic when in the unauthorized state. You can instruct the port to forward this traffic to the client, even though the client has not logged on, or you can have the port discard the traffic.

The two selections are:

- ❑ **Ingress** - An authenticator port, when in the unauthorized state, will discard all ingress broadcast and multicast packets from the client. while forwarding all egress broadcast and multicast traffic to the same client.
- ❑ **Both** - An authenticator port, when in the unauthorized state, will not forward ingress or egress broadcast and multicast packets from or to the client until the client has logged on. This is the default.

Max Requests
Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The range is 1 to 10 retransmissions. The default value is 2 retransmissions.

Server Timeout
Sets the timer used by the switch to determine authentication server timeout conditions. The range is 1 to 65,535 seconds. The default value is 30 seconds.

4. Click **Apply**.

5. To permanently save the changes, select the **Save Config** menu selection.

Configuring Supplicant Port Parameters

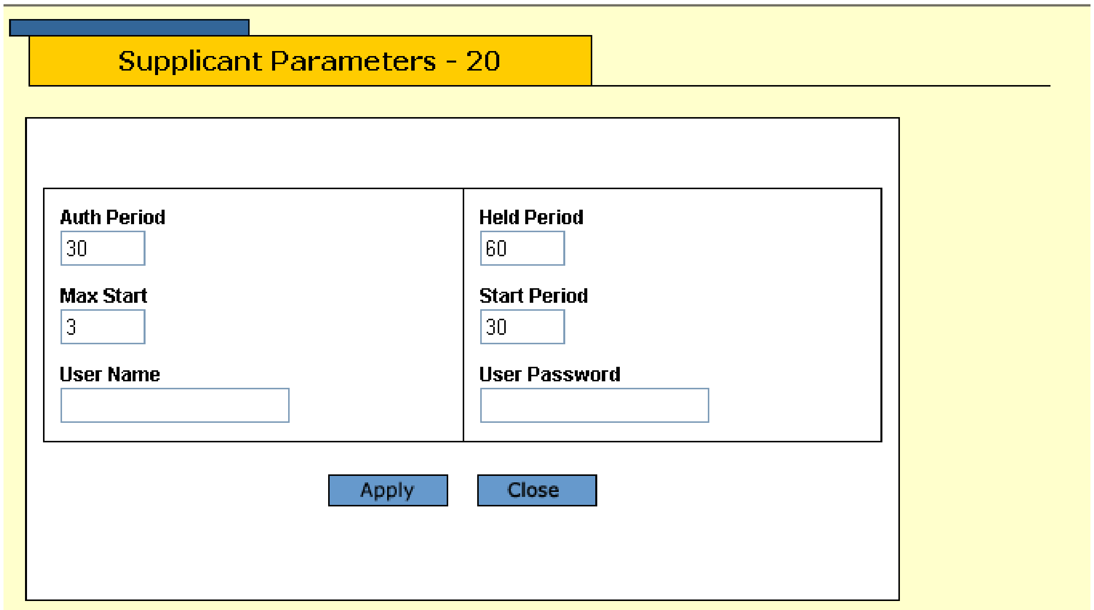
To configure supplicant port parameters, perform the following procedure:

1. From the 802.1x Port Access tab shown in Figure 108 on page 298, click the supplicant port that you want to configure. You can select more that one supplicant port at a time. The selected port turns white.

> **Note**
> A port must already be designated as a supplicant before you can configure its settings. For instructions on how to set the role of a port, refer to Setting Port Roles on page 300.

2. Click **Settings**.

   The Supplicant Parameters page is shown in Figure 110.



Supplicant Parameters - 20

Auth Period
30

Held Period
60

Max Start
3

Start Period
30

User Name

User Password

Figure 111 Supplicant Parameters Page

3. Adjust the parameters as needed. The parameters are described below:

   Auth Period
   Specifies the period of time in seconds that the supplicant will wait for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 60 seconds. The default is 30 seconds.

Held Period
Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. Once the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535 seconds. The default value is 60 seconds.

Max Start
Specifies the maximum number of times the supplicant will send EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

Start Period
Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

User Name
Specifies the username for the switch port. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be up to 30 alphanumeric characters (A to Z, a to z, 1 to 9). Spaces are allowed, but special characters, such as an asterisk or exclamation point, should be avoided. The username is case-sensitive.

User Password
Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be up to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Spaces are allowed, but special characters, such as an asterisk or exclamation point, should be avoided. The password is case-sensitive.

4. Click **Apply**.

5. To permanently save the changes, select the **Save Config** menu selection.

Displaying the Port-based Access Control Settings

To display port-based access control settings, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Network Security** menu selection.
3. Select the **802.1x Port Access** tab.

   For definitions of the parameters in the tab, refer to Enabling or Disabling Port-based Access Control on page 298.
4. To view the status of a port, click the port and click **Status**. You can select more than one port at a time.
5. To view authenticator or supplicant port access settings, click the port and click **Settings**. For definitions of the authenticator parameters, refer to Configuring Authenticator Port Parameters on page 302. For definitions of the supplicant port parameters, refer to Configuring Supplicant Port Parameters on page 306.

Note
To view the settings of multiple ports, the selected ports must have the same port role (authenticator or supplicant).

Section VII

Management Security

The chapters in this section explain the management security features of the AT-S62 software. The chapters include:

- Chapter 26: Encryption Keys, PKI, and SSL on page 310
- Chapter 27: Secure Shell Protocol on page 316
- Chapter 28: RADIUS and TACACS+ Authentication Protocols on page 320
- Chapter 29: Management Access Control List on page 326

Chapter 26
Encryption Keys, PKI, and SSL

This chapter explains how to view the encryption keys, PKI certificates, and SSL settings. It includes the following sections:

- ❑ Displaying Encryption Keys on page 311
- ❑ Displaying PKI Settings and Certificates on page 312
- ❑ Displaying the SSL Settings on page 315

Note
For background information on encryption keys and certificates, refer to the *AT-S62 Menus Interface User's Guide*.

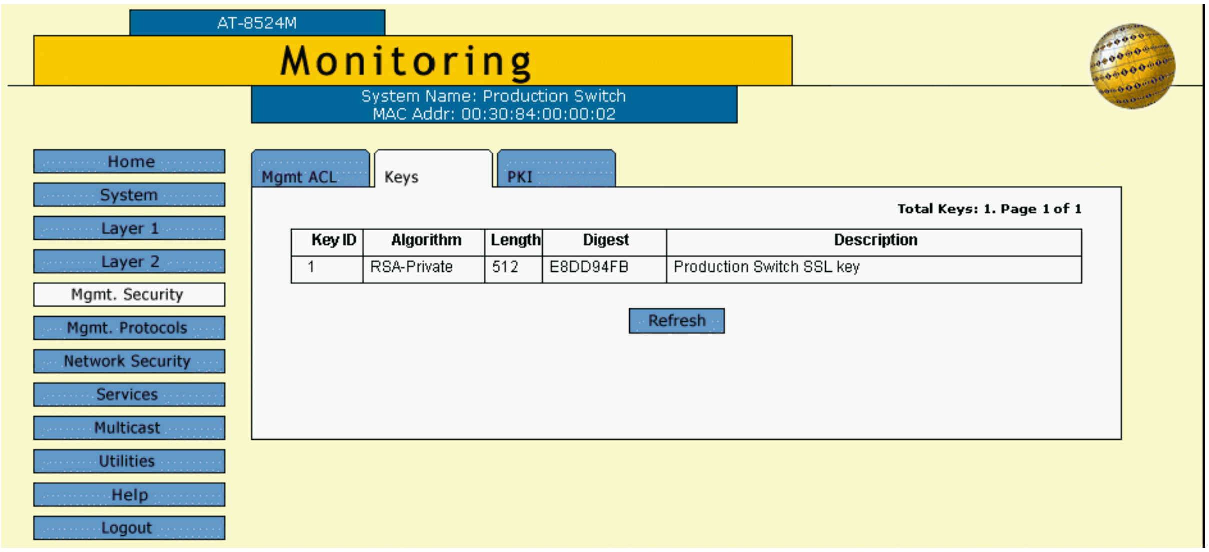
You cannot create encryption keys, self-signed certificates, or enrollment requests from a web browser management session. Nor can you adjust SSL or PKI parameter settings. These functions must be performed from a local or Telnet management session using the menu interface or the command line interface.

Displaying Encryption Keys

To display the SSL and SSH encryption key pairs, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Security** menu selection.
3. Select the **Keys** tab.

   The Keys tab is shown in Figure 112.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Total Keys: 1. Page 1 of 1

Key ID	Algorithm	Length	Digest	Description
1	RSA-Private	512	E8DD94FB	Production Switch SSL key

Figure 112 Keys Tab (Monitoring)

This tab lists the key pairs existing on the switch. The fields in the menu are described below:

ID
The identification number of the key.

Algorithm
The algorithm used in creating the encryption. This is always RSA - Private.

Length
The length of the key in bits.

Digest
The CRC32 value of the MD5 digest of the public key.

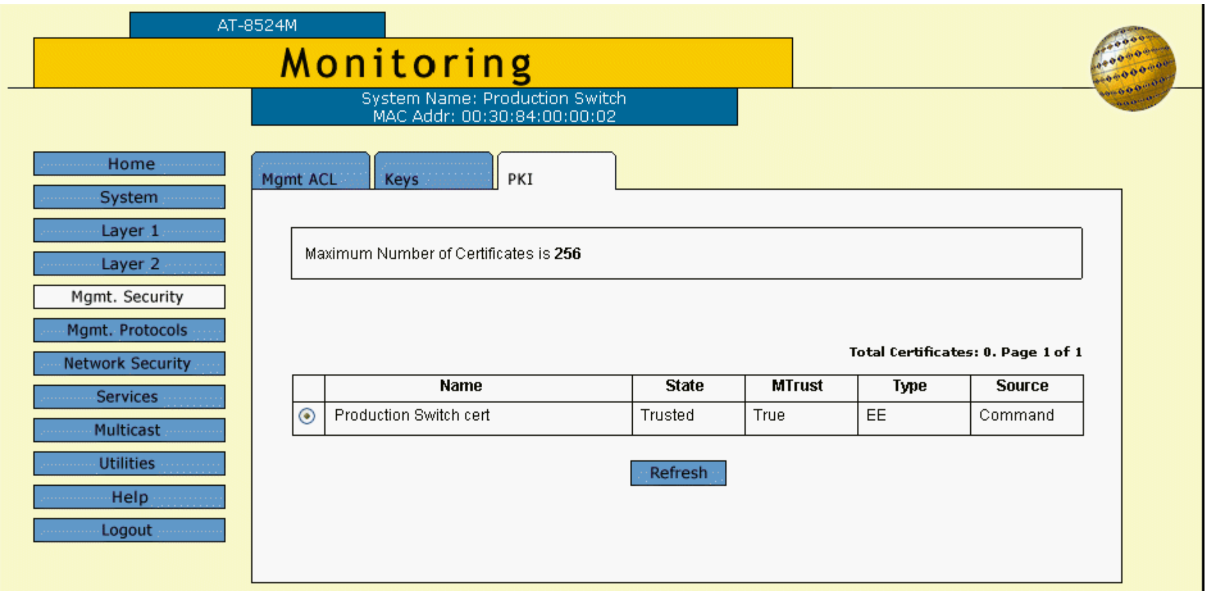
Description
The key's description.

Displaying PKI Settings and Certificates

To display the self-signed and CA certificates stored in the certificate database and the PKI settings, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Security** menu selection.
3. Select the **PKI** tab.

   The PKI tab is shown in Figure 112.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Maximum Number of Certificates is **256**

Total Certificates: 0. Page 1 of 1

	Name	State	MTrust	Type	Source
◉	Production Switch cert	Trusted	True	EE	Command

Figure 113. PKI Tab (Monitoring)

The upper section states the maximum number of certificates that can be configured on the switch.

The lower section displays a table that lists the currently configured certificates and contains the following columns of information:

Name
The certificate name.

State
The state of the certificate, one of the following:

❑ Trusted - The certificate is from a trusted CA.

❑ Untrusted - The certificate is from an untrusted CA.

MTrust (Manually Trusted)
The certificate has been manually verified that it is from a trusted or untrusted authority.

Type
The certificate type, one of the following:

- ❑ EE - The certificate was issued by a CA.
- ❑ CA - The certificate belongs to a CA.
- ❑ Self - A self-signed certificate.

Source
The certificate was created on the switch.

4. To view the details about a certificate, click the certificate and click **View**.

The X509 Certificate Details page provides the following information about the certificate:

Name
The name of the certificate.

State
Whether the certificate is Trusted or Untrusted.

Manually Trusted
You verified the certificate is from a trusted or untrusted authority.

Type
The type of the certificate. The options are EE, SELF, and CA.

Source
The certificate was created on the switch.

Version
The version number of the AT-S63 management software.

Serial Number
The certificate's serial number.

Signature Algorithm
The signature algorithm of the certificate.

Public Key Algorithm
The public key algorithm.

Not Valid Before
The date the certificate became active.

Not Valid After
The date the certificate expires. Self-signed certificates are valid for two years.

Subject
The Subject distinguished name.

Issuer
The certificate issuer’s distinguished name.

MD5 Fingerprint
The MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint
The Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

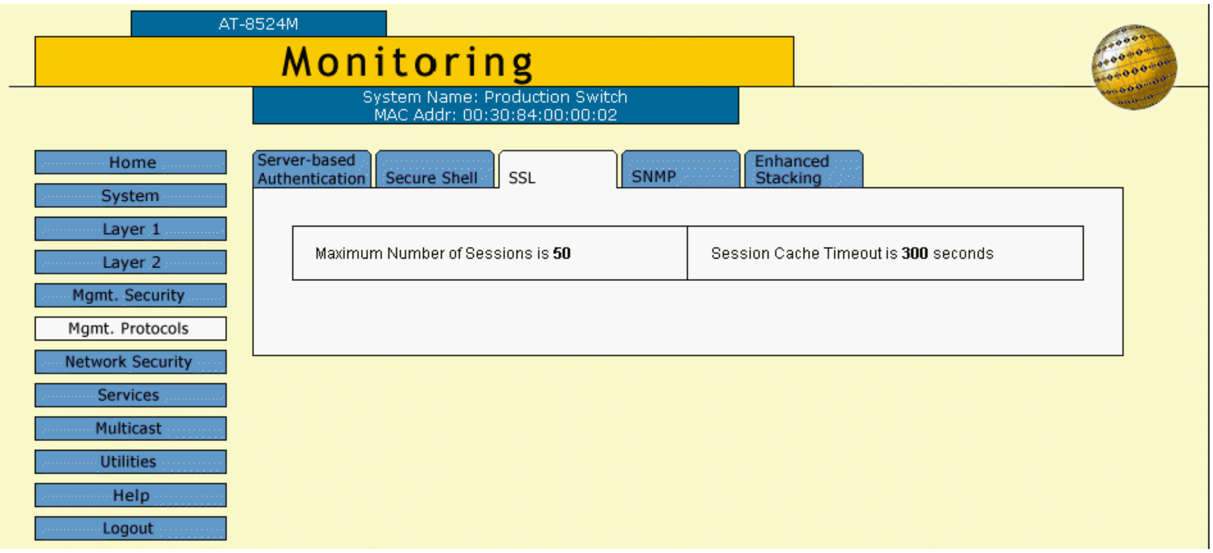
5. Click **Close** to close the page.

Displaying the SSL Settings

To display the SSL settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** menu selection.
3. Select the **SSL** tab.

   The SSL tab is shown in Figure 114.



Maximum Number of Sessions is **50**

Session Cache Timeout is **300** seconds

Figure 114 SSL Tab (Monitoring)

The SSL tab provides the following information:

Maximum Number of Sessions
The maximum number of SSL sessions allowed at one time.

Session Cache Timeout
The length of time before the session cache times out, in seconds.

Chapter 27

Secure Shell Protocol

This chapter contains the procedure for configuring the SSH protocol settings. Sections in this chapter include:

Note
For background information on SSH, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring the SSH Server

This section describes how to configure the SSH server software on the switch. For an overview of all the steps to configuring the SSH server, refer to the *AT-S62 Menus Interface User's Guide*.

This procedure assumes that you have already created the two key pairs. You cannot create encryption keys from a web browser management session.

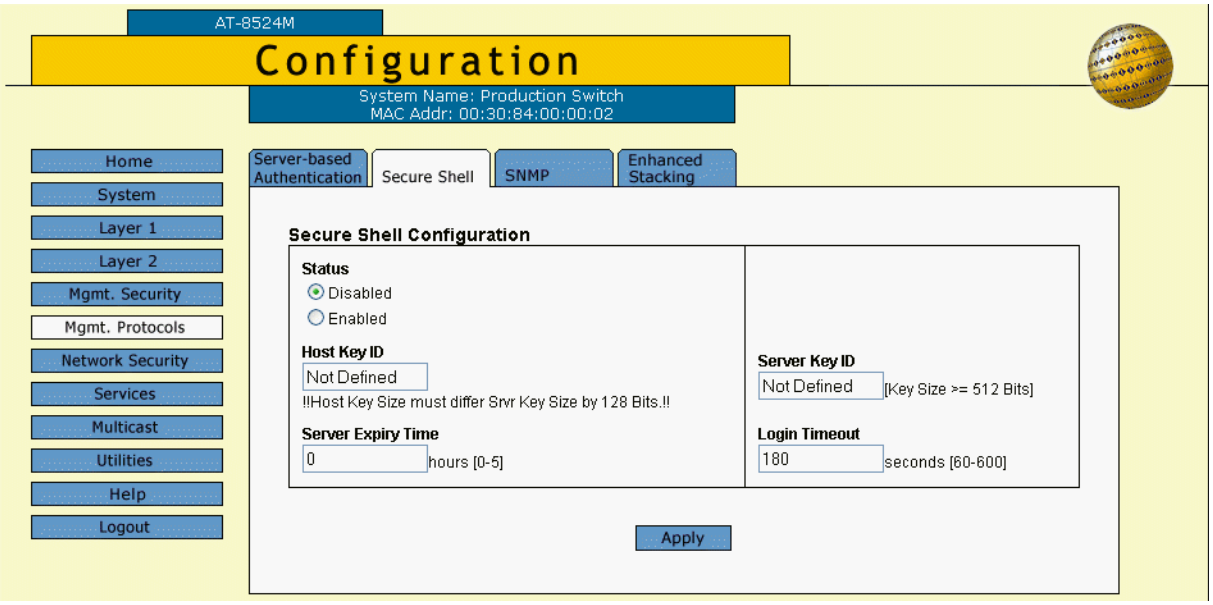
Prior to configuring the SSH feature, you must disable the SSH server. When you have completed your configuration changes, enable the SSH server to permit SSH client connections.

Note
Allied Telesyn recommends disabling the Telnet server before activating SSH. For instructions, refer to the *AT-S62 Menus Interface User's Guide*. (The Telnet server cannot be disabled from the web browser interface.)

To configure the SSH server software on the switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu selection.
3. Select the **Secure Shell** tab.

   The Secure Shell tab is shown in Figure 115.



Secure Shell Configuration

Status
● Disabled
○ Enabled

Host Key ID
Not Defined
!!Host Key Size must differ Srvr Key Size by 128 Bits.!!

Server Expiry Time
0 hours [0-5]

Server Key ID
Not Defined [Key Size >= 512 Bits]

Login Timeout
180 seconds [60-600]

Figure 115 Secure Shell Tab (Configuration)

4. Configure the parameters as needed. The parameters are described below:

   Status
   Enables or disables the feature. Choose from one of the following:

   Disabled - Disables the SSH server. You must set this field to Disabled when configuring SSH. This is the default.

   Enabled - Enables the SSH server. Select this value after you have finished configuring SSH and want to log on to the server.

   Note
   You cannot disable the SSH server when there is an active SSH connection.

   Host Key ID
   Specifies the key ID of the encryption key pair to act as the SSH host key. The key pair must already exist on the switch.

   Server Key ID
   Specifies the ID of the encryption key pair to act as the SSH server key. The key pair must already exist on the switch.

   Server Key Expiry Time
   Specifies the time, in hours, for the server key to expire. This timer determines how often the switch generates a new server key. A server key is regenerated for security purposes. A server key is only valid for the time period configured in the Server Key Expiry (Expiration) Time timer. Allied Telesyn recommends you set this field to 1. With this setting, a new key is generated every hour.

   The default is 0 hours which means the server key never expires. The range is 0 to 5 hours.

   Login Timeout
   Specifies the amount of time a switch waits before releasing the SSH server from an incomplete SSH client connection. Enter a time in seconds. The default is 180 seconds (3 minutes). The range is 60 to 600 seconds.

5. When you have finished setting the parameters, click **Apply**.

6. To permanently save the change, select the **Save Config** menu selection.

Displaying SSH Information

To display SSH information, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** menu selection.
3. Select the **Secure Shell** tab.

   The tab contains the following information:

   ❑ Versions Supported: Indicates the versions of SSH supported by the AT-S62 software.

   ❑ Status: Indicates whether or not the SSH server is enabled or disabled.

   ❑ Server Port: Indicates the well-known port for SSH. The default is port 22.

   ❑ Host Key ID: Indicates the host key ID defined for SSH.

   ❑ Server Key ID: Indicates the server key ID defined for SSH.

   ❑ Server Key Expiry: Indicates the length of time, in hours, until the server key is regenerated. The default is 0 hours which means the server key is not regenerated.

   ❑ Login Timeout: Indicates the time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.

   ❑ Authentication Available: Indicates the authentication method available. Currently, password authentication is the only supported method.

   ❑ Ciphers Available: Indicates the SSH ciphers that are available on the switch.

   ❑ MAC(s) Available: Indicates the Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.

   ❑ Data Compression: Indicates whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 28

RADIUS and TACACS+ Authentication Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedures:

- ❑ Configuring RADIUS and TACACS+ on page 321
- ❑ Displaying the RADIUS or TACSACS+ Settings on page 325

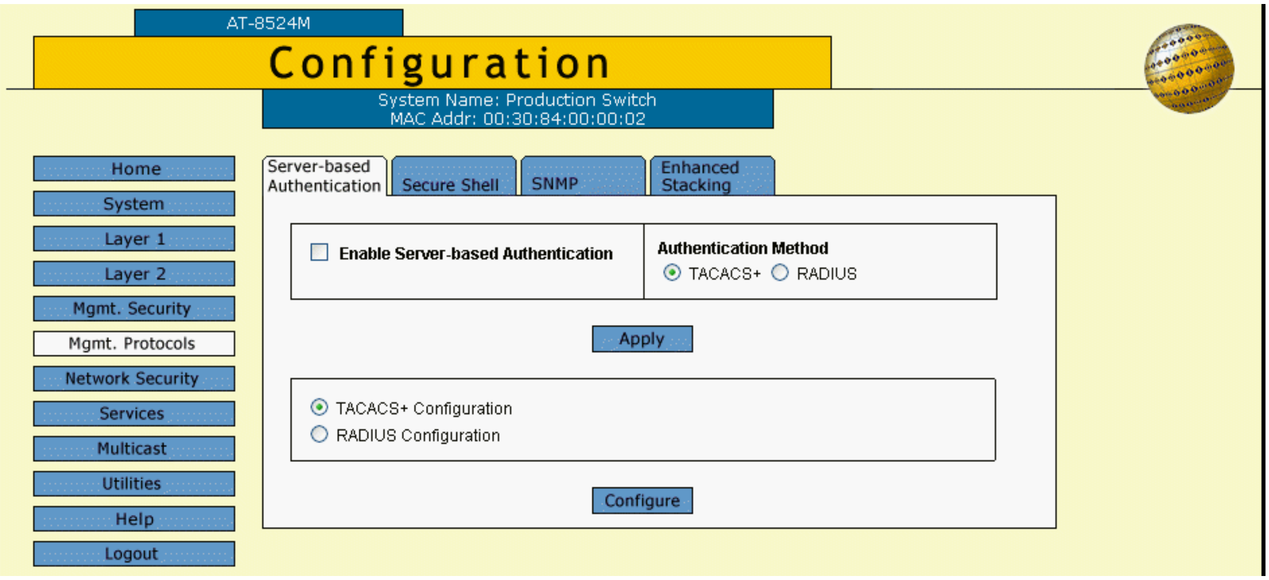
Note
For background information and guidelines on the authentication protocols, refer to the *AT-S62 Menus Interface User's Guide*.

Configuring RADIUS and TACACS+

To configure the authentication protocols, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **Mgmt. Protocols** menu selection.
3. Select the **Server-based Authentication** tab.

   The Server-based Authentication tab is shown in Figure 116.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

□ Enable Server-based Authentication

Authentication Method
● TACACS+ ○ RADIUS

● TACACS+ Configuration
○ RADIUS Configuration

Figure 116 Server-based Authentication Tab (Configuration)

Note
The Enable Server-based Authentication check box applies only to new manager accounts. It does not apply to 802.1x port-based access control.

4. To select an authentication protocol, click either RADIUS or TACACS+ in the Authentication Method section of the tab. The default is TACACS+.

Note
The switch can support only one authentication protocol at a time. Additionally, you cannot select a different authenticator protocol when this feature is enabled.

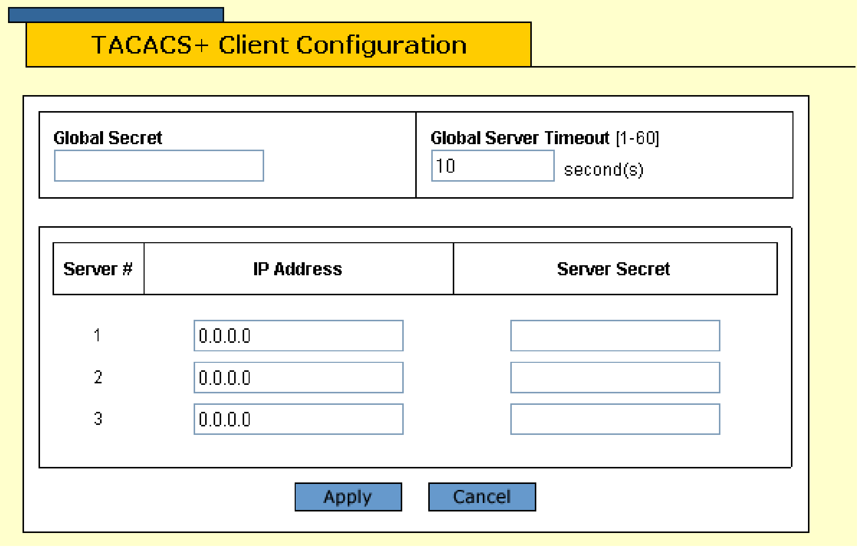
5. Click **Apply**.

> **Note**
> To configure TACACS+, go to Step 6. To configure RADIUS, go to Step 7.

6. To configure TACACS+, do the following:

   a. In lower section of the Server-based Authentication tab, click TACACS+ Configuration and click **Configure**.

   The TACACS+ Client Configuration page is shown in Figure 117.



TACACS+ Client Configuration

Global Secret

Global Server Timeout [1-60]
10 second(s)

Server #	IP Address	Server Secret
1	0.0.0.0	
2	0.0.0.0	
3	0.0.0.0	

Figure 117 TACACS+ Configuration Page

   b. Configure the parameters as needed. They are described below.

   Global Secret
   If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

   Global Server Timeout
   This parameter specifies the maximum amount of time the switch will wait for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and **Server Secret**
Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server’s secret in the Global Secret field.

c. When you are finished configuring the parameters, click **Apply**.

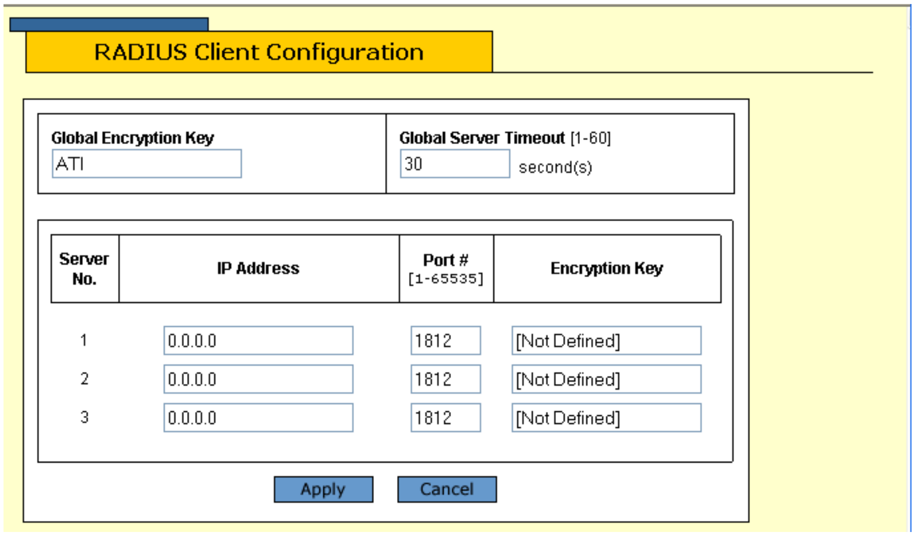
d. To enable the authentication feature on the switch, click the Enable Server-based Authentication check box. A check in the box indicates that this feature is enabled. No check indicates the feature is disabled. The default is disabled.

e. To permanently save the changes, use the Save Changes button in the General tab. For directions, refer to Saving Your Parameter Changes on page 23.

7. To configure RADIUS, do the following:

a. In the bottom part of the Server-based Authentication tab, click **RADIUS Configuration** and click **Configure**.

The RADIUS Client Configuration page is shown in Figure 117.



RADIUS Client Configuration

Global Encryption Key: ATI

Global Server Timeout [1-60]: 30 second(s)

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	0.0.0.0	1812	[Not Defined]
2	0.0.0.0	1812	[Not Defined]
3	0.0.0.0	1812	[Not Defined]

Figure 118 RADIUS Configuration Page

b. Configure the parameters as needed. They are described below.

Global Encryption Key
If all of the RADIUS servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server’s IP address.

Global Server Timeout
This parameter specifies the maximum amount of time the switch waits for a response from a RADIUS server before assuming the server will not respond. If the timeout expires and the server has not responded, the switch queries the next RADIUS server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and **Encryption Key**
Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

c. After you have finished configuring the parameters, click **Apply**.

d. To enable the authentication feature on the switch, click the Enable Server-based Authentication check box. A check in the box indicates that this feature is enabled. No check indicate the feature is disabled. The default is disabled.

Note
The Enable Server-based Authentication check box applies only when you are using the RADIUS client software to support new manager accounts. If you will be using RADIUS for 802.1x port-based access control but not for new manager accounts, you should leave the check box empty.

e. To permanently save the changes, select the **Save Config** menu selection.

Displaying the RADIUS or TACSACS+ Settings

To display the RADIUS or TACACS+ settings on a switch, do the following:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** menu selection,
3. Select the **Server-based Authentication** tab.

   The upper part of the page displays whether server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view the authentication protocol settings.
4. To view the TACACS+ or RADIUS settings, click **TACACS+** or **RADIUS**.
5. Click **View**.

   The TACACS+ or RADIUS client configuration page is displayed.

Chapter 29

Management Access Control List

This chapter explains how to create a Management Access Control List (ACL). You can use the ACL to restrict Telnet and web browser management access to the switch. Sections in this chapter include:

- ❑ Creating a Management ACL on page 327
- ❑ Adding or Deleting an ACE on page 329
- ❑ Displaying the Management ACL on page 330

Note
For background information on the Management ACL, refer to the *AT-S62 Menus Interface User's Guide*.

Creating a Management ACL

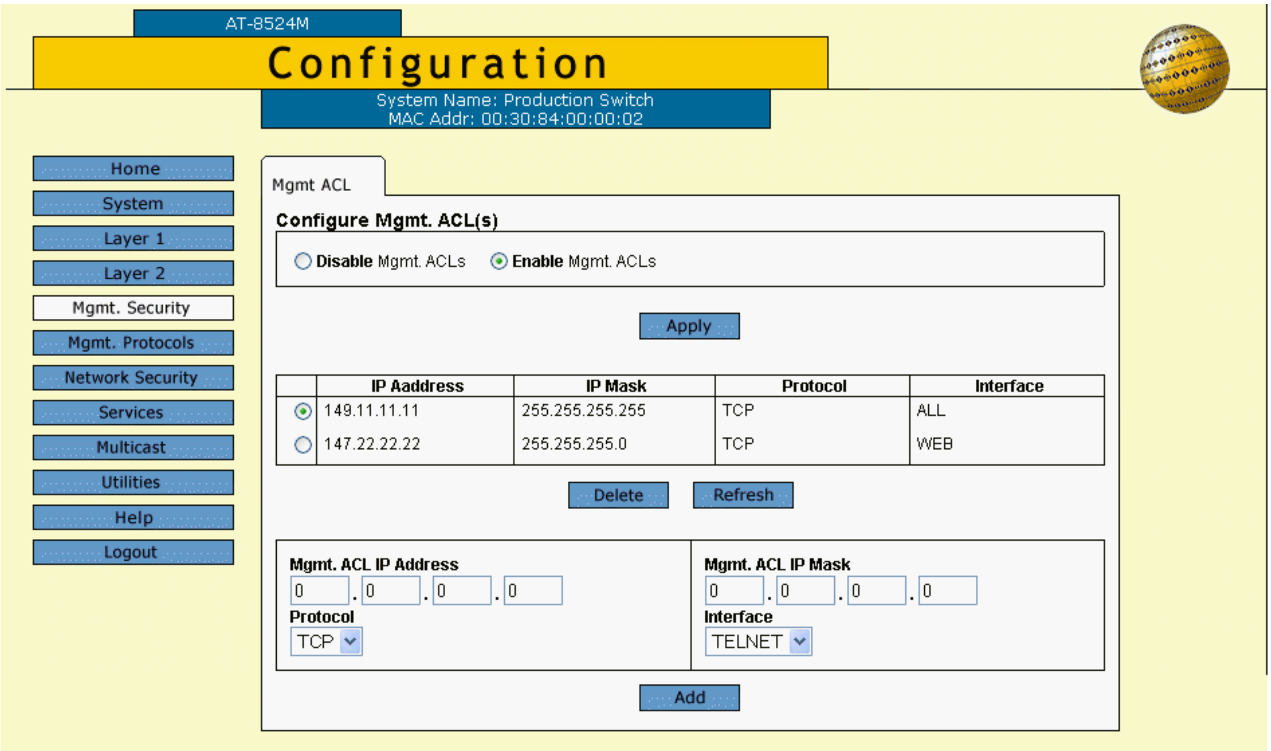
To create a Management ACL, perform the following procedure:

Note
Activating the Management ACL without specifying any ACEs will block you from managing the device remotely.

1. From the Home Page, select **Configuration**.

2. Select the **Mgmt Security** menu option.

   This menu option has only one tab, Mgmt ACL, shown in Figure 119.



System Name: Production Switch
MAC Addr: 00:30:84:00:00:02

Configure Mgmt. ACL(s)

○ **Disable** Mgmt. ACLs ● **Enable** Mgmt. ACLs

	IP Aaddress	IP Mask	Protocol	Interface
●	149.11.11.11	255.255.255.255	TCP	ALL
○	147.22.22.22	255.255.255.0	TCP	WEB

Mgmt. ACL IP Address 0 . 0 . 0 . 0
Protocol TCP

Mgmt. ACL IP Mask 0 . 0 . 0 . 0
Interface TELNET

Figure 119 Mgmt. ACL Tab (Configuration)

ACEs already existing in the Management ACL are listed in the middle section of the tab.

3. To add a new ACE, in the Mgmt. ACL IP Address field enter the IP address of a specific management workstation (for example, 149.11.11.11) or a subnet. You must enter an IP address. If you enter an IP address of a specific management node, then that node will be permitted remote management access to the switch. If you enter a subnet, any management node in the subnet will be permitted remote management access to the switch.

4. In the Mgmt. ACL IP Mask field enter a mask that indicates the parts of the IP address the switch should filter on. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not. If you are filtering on a specific IP address, use the mask 255.255.255.255. If you are filtering on a subnet, the mask will depend on the address. For example, to allow all management workstations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.
5. From the Protocol list, select **TCP** .
6. From the Interface list, select the interface that you want the management workstation to be able to use when managing the switch. Your choices are:

   ❑ Telnet - Permits Telnet management.

   ❑ Web - Permits web browser management.

   ❑ All - Permits both Telnet and web browser.

7. Click **Add**.
8. If desired, repeat this procedure starting with Step 4 to add more ACEs to the Management ACL.
9. Once you have added all of the ACEs, click the check box **Enable MGMT**. **ACL** and then click **Apply**.

   The Management ACL is now active on the switch.

10. To permanently save your changes, select the **Save Config** menu selection.

Adding or Deleting an ACE

You can add or delete ACEs from the management ACL at any time. To add a new ACE, simply repeat the procedure in the previous section. New ACEs are immediately activated on the switch once added to the ACL.

To remove an ACE, from the Mgmt ACL menu, click the button next to the ACE you want to delete and click **Delete**. You can delete only one ACE at a time.

Displaying the Management ACL

To display the ACEs in the Management ACL, do the following:

1. From the Home page, select **Monitoring**.
2. Click **Mgmt. Security**.
3. Select the **Mgmt ACL** tab.

   The information in the tab is described below:

   IP Address
   The IP address of a management workstation or subnet.

   IP Mask
   The mask used by the switch to filter the IP address.

   Protocol
   The protocol of the Telnet or web browser management packets. This will be either TCP or ALL.

   Interface
   The management interface allowed by the ACE. This will be TELNET, WEB, or ALL.

Index