Management Software

AT-S63

Web Browser User’s Guide

For AT-9400Ts Stacks

AT-S63 Version 4.0.0 for AT-9400 Basic Layer 3 Switches

PN 613-001028 Rev B

Allied Telesis™

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

Contents

Figures

Tables

Preface

This guide contains instructions on how to use the web browser windows in the AT-S63 Management Software to manage the AT-9424Ts, AT-9424Ts/XP, and AT-9448Ts/XP Switches in an AT-9400Ts Stack.

This preface contains the following sections:

❒ "How This Guide is Organized" on page 12

❒ "Product Documentation" on page 13

❒ "Where to Go First" on page 14

❒ "Starting a Management Session" on page 14

❒ "Document Conventions" on page 15

❒ "Contacting Allied Telesis" on page 16

Note
There are some management tasks on AT-9400Ts Stacks that cannot be performed from the web browser windows and that must be accomplished with the command line commands. For the complete list of the management functions supported by the management interfaces, refer to Chapter 1, "Overview," in the *AT-S63 Management Software Features Guide*.

⚠ **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 Telesis sales representative for current information on this product's export status.

How This Guide is Organized

This guide has the following sections and chapters:

Product Documentation

For overview information on the features of the AT-9400 Switch and the AT-S63 Management Software, refer to:

❐ AT-S63 Management Software Features Guide
(PN 613-001022)

For instructions on how to start a local or remote management session on a stand-alone AT-9400 Switch or a stack, refer to:

❐ Starting an AT-S63 Management Session Guide
(PN 613-001023)

For instructions on how to install or manage a stand-alone AT-9400 Switch, refer to:

❐ AT-9400 Gigabit Ethernet Switch Installation Guide
(PN 613-000987)

❐ AT-S63 Management Software Menus User's Guide
(PN 613-001025)

❐ AT-S63 Management Software Command Line User's Guide
(PN 613-001024)

❐ AT-S63 Management Software Web Browser User's Guide
(PN 613-001026)

For instructions on how to install or manage an AT-9400Ts Stack, refer to:

❐ AT-9400Ts Stack Installation Guide
(PN 613-000796)

❐ AT-S63 Management Software Command Line User's Guide
(PN 613-001024)

❐ AT-S63 Management Software Web Browser User's Guide for AT-9400Ts Stacks
(PN 613-001028)

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

Where to Go First

Allied Telesis recommends that you read Chapter 1, “Overview,” in the *AT-S63 Management Software Features Guide* before you begin to manage the switch for the first time. There you will find a variety of basic information about the unit and the management software, like the two levels of manager access levels and the different types of management sessions. The *AT-S63 Management Software Features Guide* is also your resource for background information on the features of the switch. You can refer there for the relevant concepts and guidelines when configuring a feature for the first time.

Starting a Management Session

For instructions on how to start a local or remote management session on a stack, refer to the *Starting an AT-S63 Management Session Guide*.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

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

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

Contacting Allied Telesis

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

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. 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 Allied Telesis web site at **www.alliedtelesis.com**. Select your country from the list on the web site and then select the appropriate tab.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender’s expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Management Software Updates

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

❒ Allied Telesis web site: **www.alliedtelesis.com**

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

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

Section I

Basic Operations

This section has the following chapters:

Chapter 1

Basic Switch Parameters

This chapter contains the following sections:

Configuring the Stack’s Name, Location, and Contact

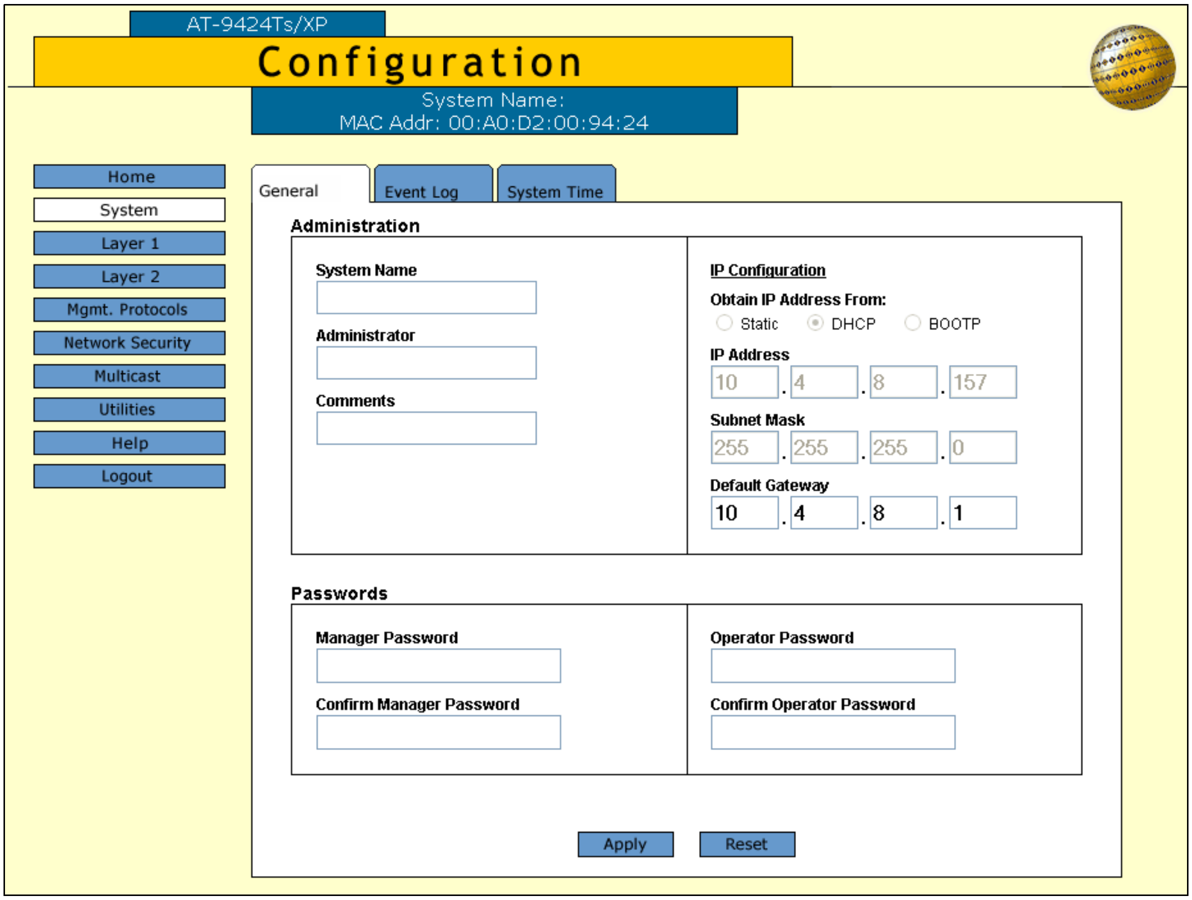
This procedure assigns a name to the switch. The name appears at the top of the web browser windows. Names can help you identify your switches when you manage them and avoid performing a configuration procedure on the wrong switch. This procedure also assigns the name of the administrator responsible for maintaining the unit and the location of the switch.

To assign a name, location, and contact to a switch:

1. From the Home page, click the **Configuration** button.

2. Click the **System** button in the Configuration menu.

3. Click the **General** tab shown in Figure 1.



System Name:
MAC Addr: 00:A0:D2:00:94:24

Administration

System Name

Administrator

Comments

IP Configuration

Obtain IP Address From:
○ Static ● DHCP ○ BOOTP

IP Address
10 . 4 . 8 . 157

Subnet Mask
255 . 255 . 255 . 0

Default Gateway
10 . 4 . 8 . 1

Passwords

Manager Password

Confirm Manager Password

Operator Password

Confirm Operator Password

Figure 1. General Tab

Note
This procedure describes the System Name, Administrator, and Comments parameters in the Administration section of the tab. The parameters in the IP Configuration section are described in “Displaying the IP Address of the Local Interface” on page 30. The Passwords section is described in “Changing the Manager or Operator Password” on page 22. The Reset button at the bottom of the tab resets the switch and is explained in “Resetting a Stack” on page 26.

4. Configure the parameters as needed. The parameters are described in Table 1.

Table 1. System Name, Administrator, and Comments Parameters

Parameter	Definition
System Name	This parameter specifies a name for the stack (for example, Sales Ethernet stack). The name is displayed at the top of the pages and tabs in the management software. The name can be from 1 to 39 characters. Spaces and special characters, such as exclamation points and asterisks, are permitted.
Administrator	This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 20 characters. Spaces and special characters are permitted.
Comments	This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. Spaces and special characters are permitted.

5. Click the **Apply** button.

6. To save your changes in the configuration file, click the **Save Config** button in the Configuration menu.

Changing the Manager or Operator Password

To change the manager or operator password:

1. From the Home page, click the **Configuration** button.
2. Click the **System** button in the Configuration menu.
3. Click the **General** tab shown in Figure 1.
4. In the Passwords section, enter the new values. The parameters are described in Table 2.

Note
Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in a password.

Table 2. Manager and Operator Passwords

Parameter	Definition
Manager Password Confirm Manager Password	You use these parameters 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.
Operator Password Confirm Operator Password	Use these parameters 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.

5. Click the **Apply** button to activate your change on the stack.

Note
The stack immediately activates your change. You must use the new password the next time you start a management session on the stack.

6. To save your changes in the configuration file, click the **Save Config** button in the Configuration menu.

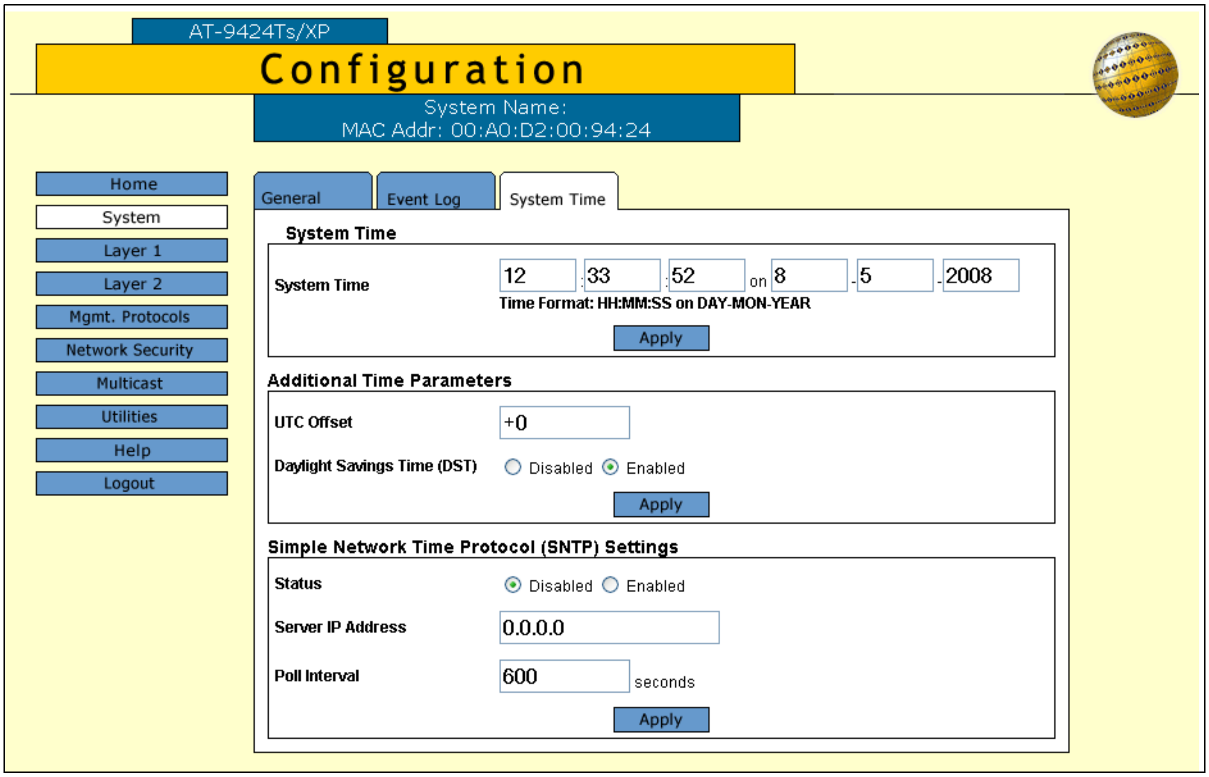
Setting the System Date and Time

The master switch adds the date and time to the event messages that it stores in the event logs and sends to a syslog server. It also adds the date and time to SNMP traps. To set the date and time:

1. From the Home page, click the **Configuration** button.

2. Click the **System** button in the Configuration menu.

3. Select the **System Time** tab, shown in Figure 2.



System Name:
MAC Addr: 00:A0:D2:00:94:24

System Time

System Time 12 : 33 : 52 on 8 - 5 - 2008
Time Format: HH:MM:SS on DAY-MON-YEAR

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 2. System Time Tab

Note
Because a stack does not support SNTP, do not adjust the values in the Additional Time Parameters section or the Simple Network Time Protocol (SNTP) Settings section of the tab.

4. In the System Time section of the tab, enter the time and date in the following formats.

   hh:mm:ss   dd-mm-yyyy

5. Click the **Apply** button.
6. To save your changes in the configuration file, click the **Save Config** button.

Resetting a Stack

This procedure resets a stack. The switches run their internal diagnostics, load the AT-S63 Management Software, and perform the discovery process. The reset can take several minutes to complete.

Note
The switches of a stack do not forward traffic during the reset process. Some network traffic may be lost.

Note
All unsaved parameter changes are discarded when a stack is reset. To save your changes, click the **Save Config** button in the Configuration menu.

Your web browser management session with the stack ends when it resets. You must reestablish the session to continue managing it.

To reset the stack:

1. From the Home page, click the **Configuration** button.

2. Click the **System** button in the Configuration menu.

3. Click the **General** tab shown in Figure 1.

4. Click the **Reset** button at the bottom of the tab.

5. At the confirmation prompt, click the **OK** button to reset the stack or the **Cancel** button to cancel the procedure.

   Resetting the stack ends your web browser management session. To continue managing the stack, wait for the units to complete the discovery process and then start a new management session.

Pinging a Remote System

This procedure instructs the stack to ping a node on your network. This can be useful in determining whether an active path exists between the stack and another network device.

Note
To ping a remote device, the stack must have a routing interface on the local subnet from where it will access the device. The stack uses the IP address of the interface as its source address in the ping packets. For background information on routing interfaces, refer to the *AT-S63 Management Software Features Guide*.

To instruct the stack to ping a network device:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Utilities** button.

3. Select the **Ping Client** tab, shown in Figure 3.

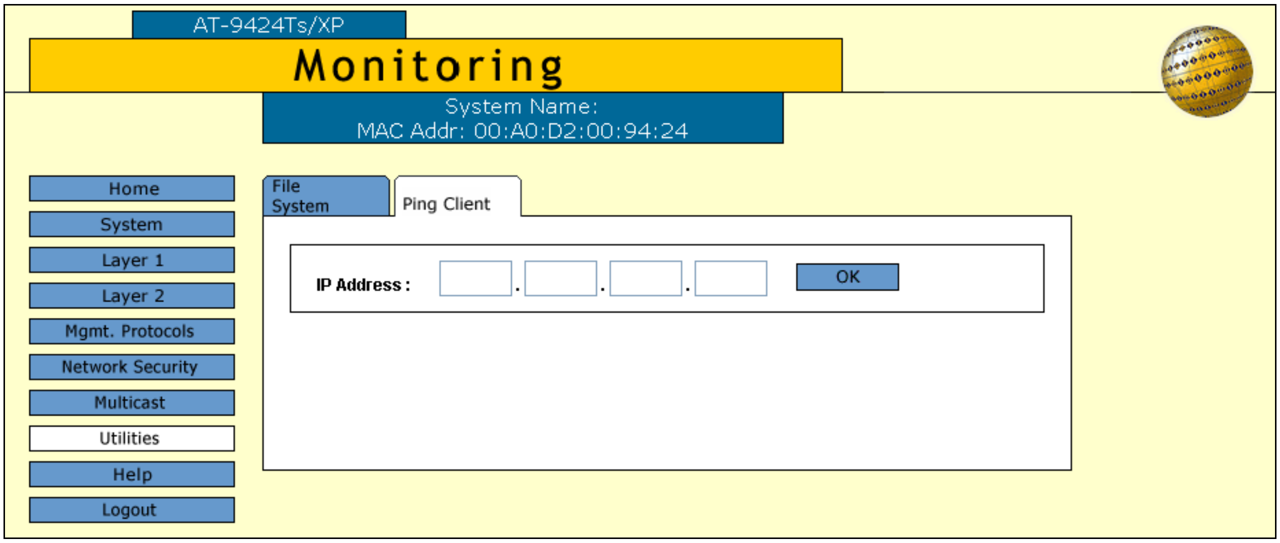


Figure 3. Ping Client Tab

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

5. Click the **OK** button. The results of the ping are displayed in a popup window.

6. To stop the ping, click the **OK** button in the pop window.

Restoring the Factory Default Values

The procedure in this section restores the factory default settings to all of the parameters on the switches in the stack. Review the following before performing this procedure:

- ❒ This procedure deletes all of the routing interfaces and port-based and tagged VLANs in the stack.
- ❒ This procedure does not delete any of the files in the master switch's file system. For instructions on how to delete files, refer to the *AT-S63 Command Line User's Guide for AT-9400 Stacks*.
- ❒ The speed of the Terminal Port on the master switch remains at its current setting.
- ❒ Returning a stack to the default parameter values does not alter the contents of the active boot configuration file. To reset the file to the default settings, you must establish a local management session with the switch after it reboots and select Save Config from the menu. Otherwise, the stack reverts back to the previous configuration the next time you reset or power cycle the unit.
- ❒ Because this procedure deletes the local interface on the stack, it will not be possible to reestablish a web browser management session. To resume managing the stack, begin a local management session.

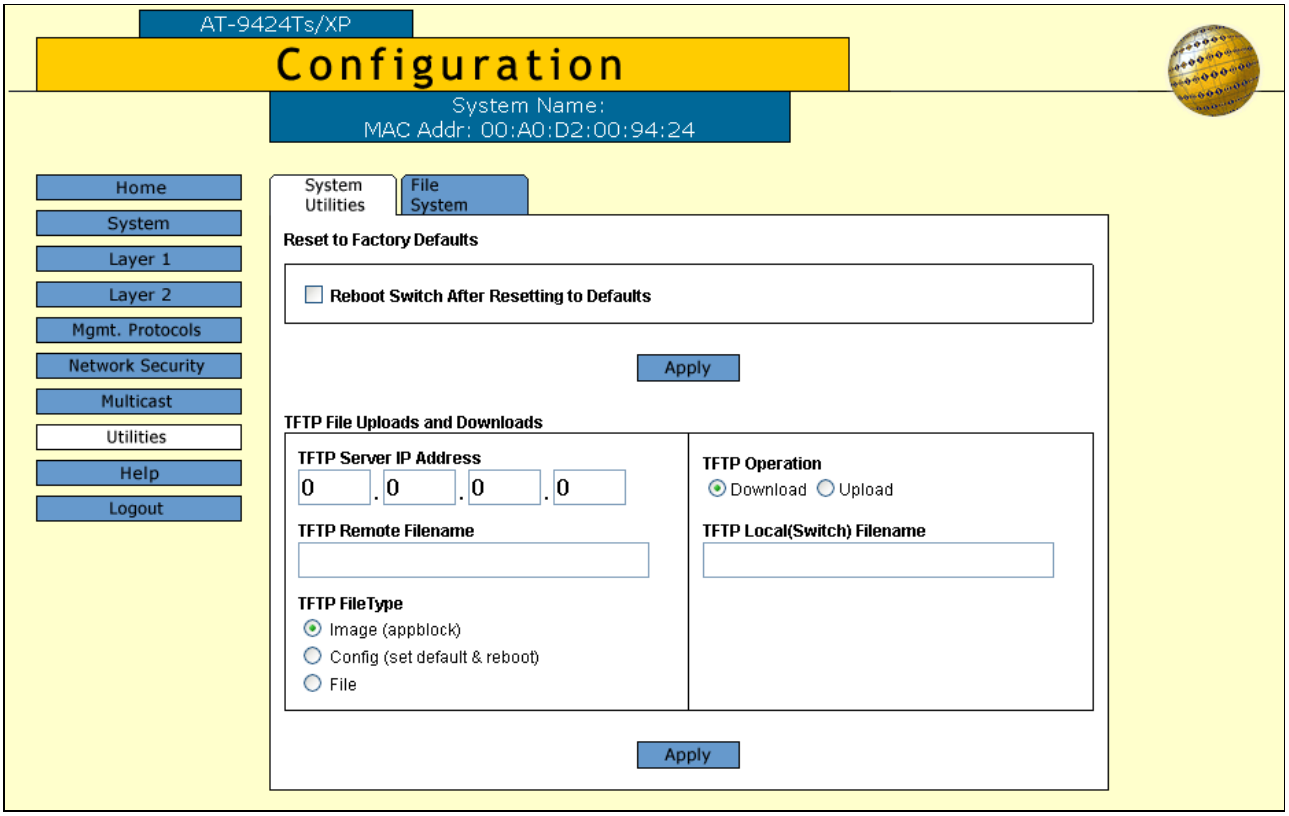
⚠ **Caution**
This procedure resets the stack. Some network traffic may be lost while the switches initialize their management software and perform the discovery process.

Note
The AT-S63 Management Software default values are listed in Appendix A, "AT-S63 Default Settings" in the *AT-S63 Management Software Features Guide*.

To restore the default settings to the AT-S63 Management Software on the stack:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Utilities** button to display the System Utilities tab, shown in Figure 4 on page 29.



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(Switch) Filename:

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

Figure 4. System Utilities Tab

3. Click the **Reboot Switch After Resetting to Defaults** check box.

4. Click the **Apply** button.

5. At the confirmation prompt, click the **OK** button to continue or the **Cancel** button to cancel the procedure.

   If you select OK, the stack resets and all of the parameters are returned to the default settings. After the reset is complete, you must establish a local management session if you want to continue managing the unit.

   As mentioned at the start of this procedure, returning a stack to its default settings does not alter the contents of the active boot configuration file. To return the file to the default settings, you must save the current switch settings after establishing a local management session with the stack. Otherwise, the stack will return to its previous parameter settings the next time you reset or power cycle the stack.

Displaying the IP Address of the Local Interface

This procedure is used to display the IP address and subnet mask of the local interface, which is used for remote Telnet and web browser management. To configure the local interface, you have to use the command line commands.

To view the IP address and subnet mask of the local interface of the stack:

1. From the Home page, click the **Configuration** button.
2. Click the **System** button in the Configuration menu.
3. Click the **General** tab, shown in Figure 1 on page 20. The parameters in the IP Configuration section of the web page are described in Table 3.

Table 3. IP Configuration Section of the General Tab

Parameter	Definition
Obtain IP Address from:	The options in this section indicate the source of the IP address of the local interface. If DHCP or BOOTP is checked, the interface obtained its IP address from a DHCP or BOOTP server on the network. If Static is checked, the IP address was set manually.
IP Address	This parameter displays the IP address of the local management interface. This address is either manually assigned to the interface or obtained from a DHCP or BOOTP server.
Subnet Mask	This parameter specifies the subnet mask for the interface. The IP address and subnet mask fields will be empty if no interface has been designated as the local interface on the stack.

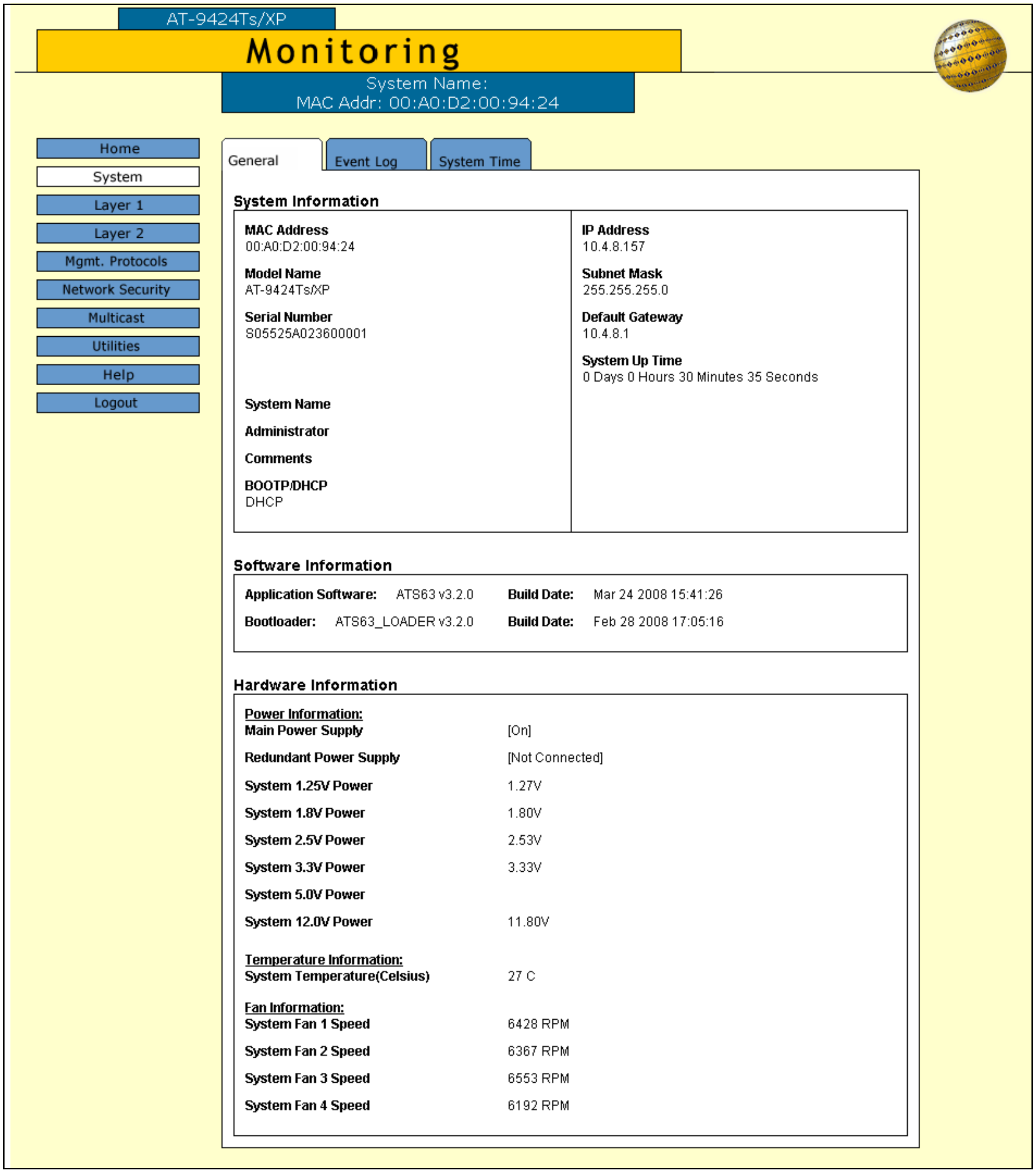
Table 3. IP Configuration Section of the General Tab

Parameter	Definition
Default Gateway	If the stack has more than one routing interface, this field displays the IP address of the next hop of the stack's default route. The stack uses the default route when it receives a network packet for routing, but cannot find a route for it in the routing table. This field will contain 0.0.0.0 if no default route is defined on the stack. If the only routing interface on the stack is the local interface, this field displays the default gateway address. This is the IP address of a router interface on your network. The stack uses this address as the next hop to reaching a remote network device when the stack's local interface and the remote device are on different subnets. The default value is 0.0.0.0.

Displaying System Information

To view basic information about the master switch:

1. From the Home page, click the **Monitoring** button.
2. Click the **System** button.
3. Select the **General** tab, shown in Figure 5.



System Name:
MAC Addr: 00:A0:D2:00:94:24

System Information

MAC Address
00:A0:D2:00:94:24

Model Name
AT-9424Ts/XP

Serial Number
S05525A023600001

System Name

Administrator

Comments

BOOTP/DHCP
DHCP

IP Address
10.4.8.157

Subnet Mask
255.255.255.0

Default Gateway
10.4.8.1

System Up Time
0 Days 0 Hours 30 Minutes 35 Seconds

Software Information

Application Software: ATS63 v3.2.0 **Build Date:** Mar 24 2008 15:41:26

Bootloader: ATS63_LOADER v3.2.0 **Build Date:** Feb 28 2008 17:05:16

Hardware Information

Power Information:

Main Power Supply	[On]
Redundant Power Supply	[Not Connected]
System 1.25V Power	1.27V
System 1.8V Power	1.80V
System 2.5V Power	2.53V
System 3.3V Power	3.33V
System 5.0V Power	
System 12.0V Power	11.80V

Temperature Information:

System Temperature(Celsius)	27 C

Fan Information:

System Fan 1 Speed	6428 RPM
System Fan 2 Speed	6367 RPM
System Fan 3 Speed	6553 RPM
System Fan 4 Speed	6192 RPM

Figure 5. General Tab (Monitoring)

The information in the tab is described in Table 4.

Table 4. General Tab

Parameter	Definition
System Information Section	
MAC Address	The MAC address of the master switch.
Model Name	The model name of the master switch.
Serial Number	The serial number of the master switch.
System Name	The name of the stack. To set the name, refer to “Configuring the Stack’s Name, Location, and Contact” on page 20.
Administrator	The name of the network administrator responsible for managing the stack. To set the name of the administrator, refer to “Configuring the Stack’s Name, Location, and Contact” on page 20.
Comments	The location of the stack, (for example, 4th Floor - rm 402B). To set the location, refer to “Configuring the Stack’s Name, Location, and Contact” on page 20.
BOOTP/DHCP	The source of the IP address of the local interface. This field will be “DHCP” or “BOOTP” if the local interface obtained its IP configuration from a DHCP or BOOTP server. Alternatively, if the IP address was set manually, this field will be “Static.” This field will be blank if the stack does not have a local interface.
IP Address	The IP address of the local interface.
Subnet Mask	The subnet mask of the local interface.

Table 4. General Tab

Parameter	Definition
Default Gateway	If the stack has more than one routing interface, this field displays the IP address of the next hop of the stack's default route. The stack uses the default route when it receives a network packet for routing, but cannot find a route for it in the routing table. This field will contain 0.0.0.0 if no default route is defined on the stack. If the only routing interface on the stack is the local interface, this field displays the default gateway address. This is the IP address of a router interface on your network. The stack uses this address as the next hop to reaching a remote network device when the stack's local interface and the remote device are on different subnets. The default value is 0.0.0.0.
System Up Time	The length of time since the stack was last reset or power cycled.
Software Information Section	
Application Software	The version number and build date of the AT-S63 Management Software.
Bootloader	The version number and build date of the AT-S63 bootloader.
Hardware Information Section	
Power Information	The status of the main power supply, the redundant power supply (if present), and internal power consumption of the master switch.
Temperature (Deg.C)	The ambient temperature as measured where the air enters the cooling vents on the side of the unit.
Fan Information	The speed or operating status of the system fans on the master switch.

Chapter 2

Port Parameters

This chapter explains how to view and change the port parameters, such as port speed, duplex mode, and packet filtering, of the switches in the stack. This chapter contains the following procedures:

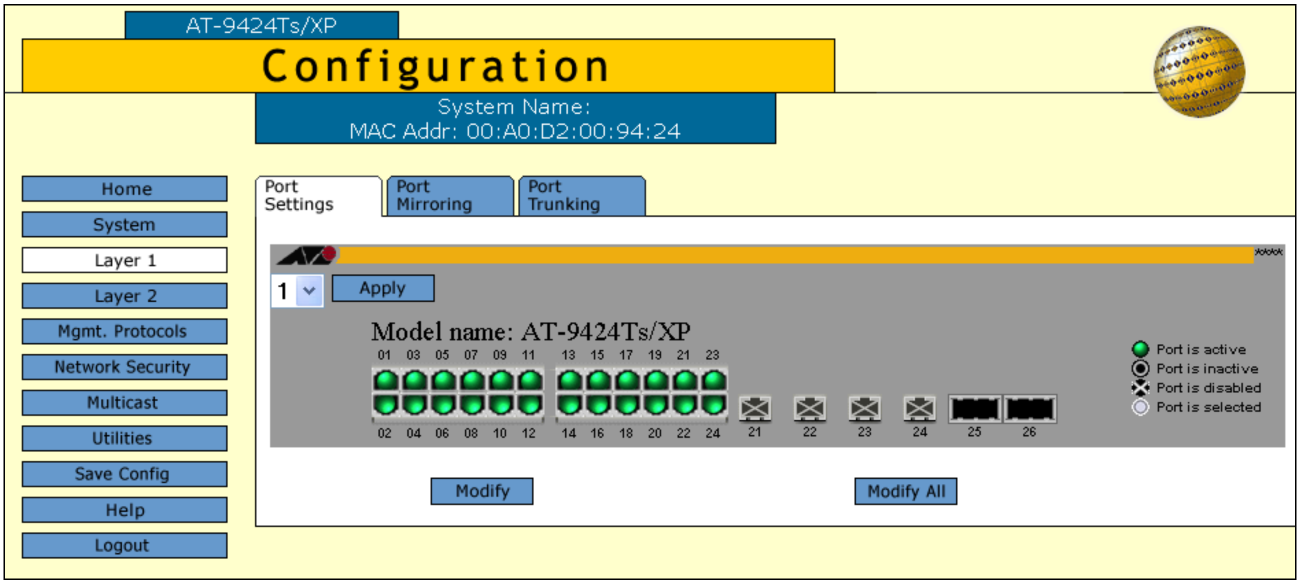
Configuring the Port Parameters

To configure the parameter settings of the ports in the stack:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 1** button.

3. Select the **Port Settings** tab to display the tab in Figure 6.



AT-9424Ts/XP

Configuration

System Name:
MAC Addr: 00:A0:D2:00:94:24

Model name: AT-9424Ts/XP

Figure 6. Port Settings Tab

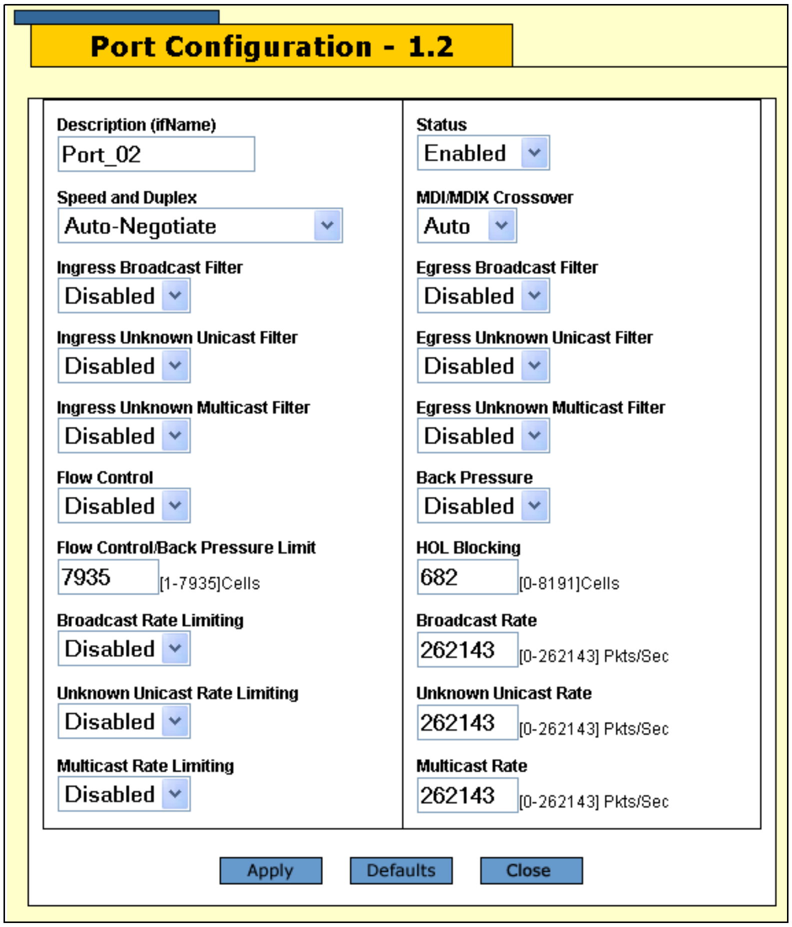
The Port Settings tab consists of an image of the front of one of the switches in the stack. The Stack ID pull-down menu in the upper left corner of the image identifies the switch. Ports that have links to end nodes are shown as green.

4. Using the stack ID pull-down menu in the upper left corner of the switch image, select the ID number of the switch you want to configure in the stack and click the **Apply** button. You can configure only one switch at a time. If the switch is already displayed, you can skip this step.

5. In the switch image, click the port you want to configure. The selected port turns white. You can configure more than one port at a time, but they must all be the same type (i.e., all twisted pair ports or all fiber optic ports). To deselect a port, click it again.

6. Click the **Modify** button to display the Port Configuration window in Figure 7. To configure all of the ports on the switch, click **Modify All**.

.



Port Configuration - 1.2

Description (ifName): Port_02

Status: Enabled

Speed and Duplex: Auto-Negotiate

MDI/MDIX Crossover: Auto

Ingress Broadcast Filter: Disabled

Egress Broadcast Filter: Disabled

Ingress Unknown Unicast Filter: Disabled

Egress Unknown Unicast Filter: Disabled

Ingress Unknown Multicast Filter: Disabled

Egress Unknown Multicast Filter: Disabled

Flow Control: Disabled

Back Pressure: Disabled

Flow Control/Back Pressure Limit: 7935 [1-7935]Cells

HOL Blocking: 682 [0-8191]Cells

Broadcast Rate Limiting: Disabled

Broadcast Rate: 262143 [0-262143] Pkts/Sec

Unknown Unicast Rate Limiting: Disabled

Unknown Unicast Rate: 262143 [0-262143] Pkts/Sec

Multicast Rate Limiting: Disabled

Multicast Rate: 262143 [0-262143] Pkts/Sec

Figure 7. Port Configuration Window

Note
The Port Configuration window in the figure above is from a 10/100/1000 Mbps twisted pair port. The window 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 page displays the settings of the lowest numbered port you selected. After you have configured the settings of the port, all of its settings, including those that were not changed, are copied to the other selected ports.

The **Defaults** button at the bottom of the page returns the port settings to the default values, which are found in Appendix A in the *AT-S63 Management Software Features Guide*.

7. Configure the parameters as needed. The parameters are described in in Table 5.

Table 5. Port Configuration Window

Parameter	Definition
Description (Name)	Assigns a name to a port. A name can have up to 15 alphanumeric characters. Spaces are allowed, but not special characters, such as asterisks or exclamation points. (You cannot assign a name when configuring more than one port.)
Status	Enable or disables a port. A disabled port does not accept or forward frames. You might disable a port if a problem occurs with the end node or cable. After the problem is fixed, you can enable the port again to resume normal operation. You might also disable an unused port to secure it from unauthorized connections. The possible settings are: Enabled - The port forwards ingress and egress packets. This is the default setting. Disabled - The port does not forward any ingress or egress packets.
Speed and Duplex	Sets the speed and duplex mode of a port. You can set a port to automatically adjust its speed and duplex mode with Auto-Negotiation or you can set these parameters manually. The default setting is Auto-Negotiation. The possible settings are: Auto-Negotiate 10Mbps - Half Duplex 10Mbps - Full Duplex 100Mbps - Half Duplex 100Mbps - Full Duplex 1Gb - Full Duplex

Table 5. Port Configuration Window

Parameter	Definition
Speed and Duplex (Continued)	The 1Gb - Full Duplex setting applies only to 1000Base SFP and GBIC modules and should not be used because an SFP or GBIC module should use Auto-Negotiation to set its speed and duplex mode.) A 10/100/1000Base-T twisted pair port operates at 1000 Mbps only when set to Auto-Negotiation. You cannot manually configure a 10/100/1000Base-T twisted pair port to 1000 Mbps. Note the following about the operation of Auto-Negotiation on a switch port. In order for a switch port to successfully autonegotiate 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 defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This results 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 its speed and duplex mode manually. If you disable Auto-Negotiation on a twisted pair port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. 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.

Table 5. Port Configuration Window

Parameter	Definition
MDI/MDIX Crossover	Sets the wiring configuration of a twisted pair port. The possible settings are: Auto - Sets the MDI or MDIX setting automatically. This is the default value. This setting is only available when a port is set to Auto-Negotiation. MDI - Sets a port to MDI. This setting is only available when a port's speed and duplex mode are set manually. MDIX - Sets a port to MDIX. This setting is only available when a port's speed and duplex mode are set manually. This parameter does not apply to fiber optic ports.
Ingress Broadcast Filter	Enables or disables the ingress broadcast filter on a port. Possible settings are: Enabled - The port discards ingress broadcast packets. Disabled - The port forwards ingress broadcast packets. This is the default setting.
Egress Broadcast Filter	Enables or disables the egress broadcast filter on a port. Possible settings are: Enabled - The port discards egress broadcast packets. Disabled - The port forwards egress broadcast packets. This is the default setting.
Ingress Unknown Unicast Filter	Use this parameter to configure a port to forward or discard unknown ingress unicast packets. The possible settings are: Enabled - The port discards unknown ingress unicast packets. Disabled - The port forwards unknown ingress unicast packets. This is the default setting.

Table 5. Port Configuration Window

Parameter	Definition
Egress Unknown Unicast Filter	Use this parameter to configure a port to forward or discard unknown egress unicast packets. The possible settings are: Enabled - The port discards unknown egress unicast packets. Disabled - The port forwards unknown egress unicast packets. This is the default setting.
Ingress Unknown Multicast Filter	Use this parameter to configure a port to forward or discard unknown ingress multicast packets. Possible settings are: Enabled - The port discards unknown ingress multicast packets. Disabled - The port forwards unknown ingress multicast packets. This is the default setting.
Egress Unknown Multicast Filter	Use this parameter to configure a port to forward or discard unknown egress multicast packets. Possible settings are: Enabled - The port discards unknown egress multicast packets. Disabled - The port forwards unknown egress multicast packets. This is the default setting.
Flow Control	Sets flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses flow control to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time. Possible settings are: Disabled - No flow control on the port. This is the default. Enabled - Flow control is activated.

Table 5. Port Configuration Window

Parameter	Definition
Back Pressure	Use this parameter to set backpressure on a port. This option only appears for ports operating in half-duplex mode. A port uses backpressure to control the flow of ingress packets. Possible settings are: Enabled - Backpressure is enabled. Disabled - Backpressure is disabled. This is the default.
Flow Control/Back Pressure Limit	Use this parameter to specify the threshold for flow control or backpressure. The threshold is specified in cells. A cell equals 128 bytes. The range is 1 to 7935. The default is 7935 cells.
HOL Blocking	HOL blocking 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 threshold is specified in number of cells. A cell is 128 bytes. The range is 1 to 8191. The default is 682.
Broadcast Rate Limiting	Use this parameter to enable or disable ingress broadcast packet limits. Possible settings are: Enabled - Broadcast packet ingress rate limiting is enabled. To set the rate limit, use the Broadcast Rate parameter. Disabled - Broadcast packet ingress rate limiting is disabled. This is the default.
Broadcast Rate	Use this parameter to set the broadcast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Table 5. Port Configuration Window

Parameter	Definition
Unknown Unicast Rate Limiting	Use this parameter to enable or disable unknown ingress unicast packet limits. Possible settings are: Enabled - Unknown unicast packet ingress rate limiting is enabled. To set the rate limit, use the Unknown Unicast Rate parameter. Disabled - Unknown unicast packet ingress rate limiting is disabled. This is the default.
Unknown Unicast Rate	Use this parameter to set the unknown unicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.
Multicast Rate Limiting	Use this parameter to enable or disable ingress multicast packet limits. Possible settings are: Enabled - Multicast packet ingress rate limiting is enabled. To set the rate limit, use the Multicast Rate parameter. Disabled - Multicast packet ingress rate limiting is disabled. This is the default.
Multicast Rate	Use this parameter to set the multicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

8. After entering the desired changes, click the **Apply** button.

9. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

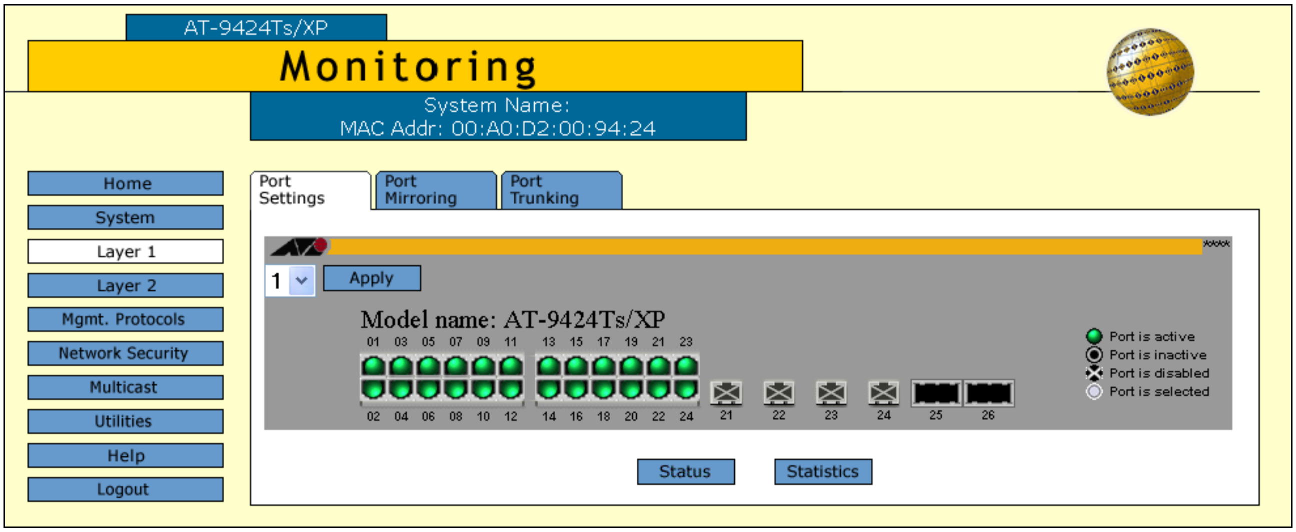
Displaying the Port Parameters and Statistics

To view the parameter settings or the statistics of the ports:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Layer 1** button.

3. Click the **Port Settings** tab, shown in Figure 8.



System Name:
MAC Addr: 00:A0:D2:00:94:24

Model name: AT-9424Ts/XP

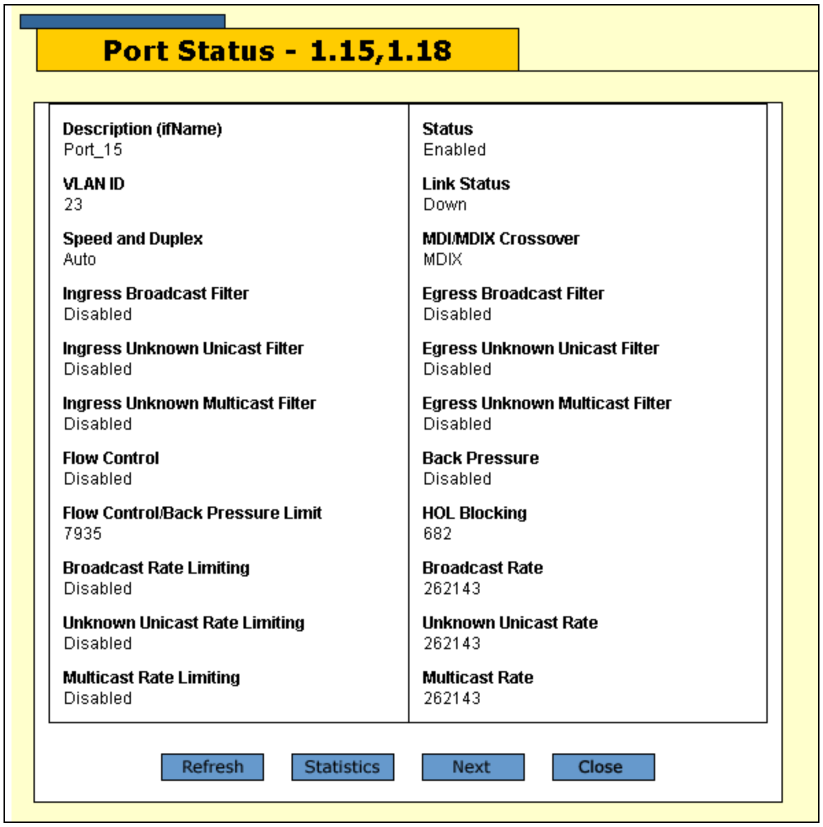
Figure 8. Port Settings Tab (Monitoring)

The Port Settings tab consists of an image of the front of one of the switches in the stack. The Stack ID pull-down menu in the upper left corner of the image identifies the switch. Ports that have links to end nodes are shown as green.

4. Using the stack ID pull-down menu, select the ID number of a switch whose ports you want to view in the stack and click the **Apply** button. You can view the ports of only one switch at a time. If the switch is already displayed, you can skip this step.

5. In the switch image, click the port you want to view. The selected port turns white. You can view more than one port at a time, but they must be of the same type (i.e., all twisted pair ports or all fiber optic ports). To deselect a port, click it again.

6. To view the port settings, click the **Status** button to display the window in Figure 9.



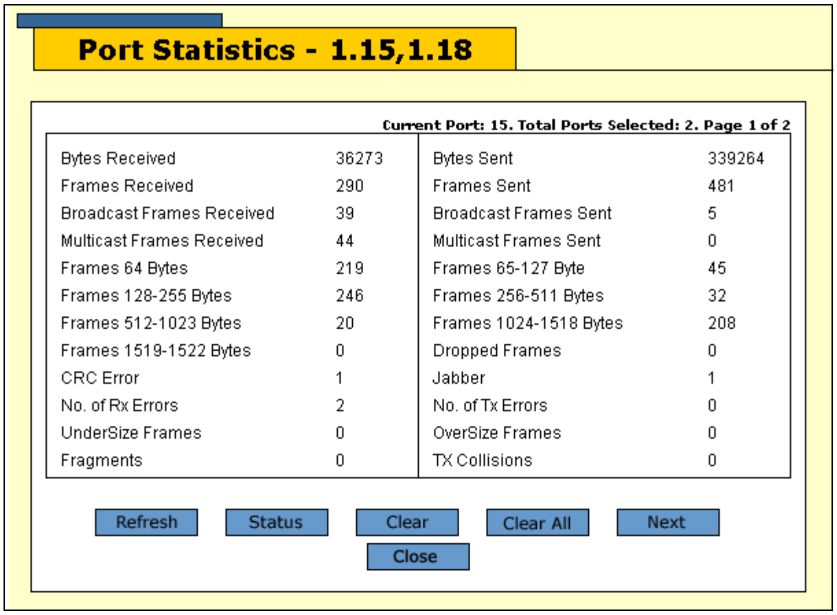
Port Status - 1.15,1.18

Description (ifName) Port_15	**Status** Enabled
VLAN ID 23	**Link Status** Down
Speed and Duplex Auto	**MDI/MDIX Crossover** MDIX
Ingress Broadcast Filter Disabled	**Egress Broadcast Filter** Disabled
Ingress Unknown Unicast Filter Disabled	**Egress Unknown Unicast Filter** Disabled
Ingress Unknown Multicast Filter Disabled	**Egress Unknown Multicast Filter** Disabled
Flow Control Disabled	**Back Pressure** Disabled
Flow Control/Back Pressure Limit 7935	**HOL Blocking** 682
Broadcast Rate Limiting Disabled	**Broadcast Rate** 262143
Unknown Unicast Rate Limiting Disabled	**Unknown Unicast Rate** 262143
Multicast Rate Limiting Disabled	**Multicast Rate** 262143

Figure 9. Port Status Page

If you selected more than one port, use the Next and Previous buttons to toggle through the ports. The parameters are described in Table 5 on page 38.

7. To display the port statistics, click the **Statistics** button to display the window in Figure 10.



Port Statistics - 1.15,1.18

Current Port: 15. Total Ports Selected: 2. Page 1 of 2

Bytes Received	36273	Bytes Sent	339264
Frames Received	290	Frames Sent	481
Broadcast Frames Received	39	Broadcast Frames Sent	5
Multicast Frames Received	44	Multicast Frames Sent	0
Frames 64 Bytes	219	Frames 65-127 Byte	45
Frames 128-255 Bytes	246	Frames 256-511 Bytes	32
Frames 512-1023 Bytes	20	Frames 1024-1518 Bytes	208
Frames 1519-1522 Bytes	0	Dropped Frames	0
CRC Error	1	Jabber	1
No. of Rx Errors	2	No. of Tx Errors	0
UnderSize Frames	0	OverSize Frames	0
Fragments	0	TX Collisions	0

Figure 10. Port Statistics Page

If you selected more than one port, use the Next and Previous buttons to toggle through the ports. The statistics are described in Table 6.

Table 6. Port Statistics

Statistic	Definition
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.

Table 6. Port Statistics

Statistic	Definition
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	Number of frames transmitted from the port, grouped by size.
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.
TX Collisions	Number of transmit collisions.

8. To clear all of the counters for a port, click the **Clear** button. To clear the counters for all of the ports on a switch in the stack, click the **Clear All** button. (The Clear and Clear All buttons are only available from a manager session. They are not available from an operator session.)

Restoring the Default Settings on the Ports

To restore the default parameter settings to the ports on a switch:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 1** button.

3. Click the **Port Settings** tab, shown in Figure 6 on page 36.

4. Use the stack ID pull-down menu to select the ID number of a switch with ports that you want to return to their default values and click the **Apply** button. You can configure only one switch at a time. If the switch is already displayed, you can skip this step.

5. In the switch image, click a port you want to return to the default values. The selected port turns white. You can configure more than one port at a time, but they must be the same type (i.e., all twisted pair ports or all fiber optic ports). To deselect a port, click it again.

6. Click the **Modify** button. To configure all of the ports on the switch, click the **Modify All** button.

7. In the The Port Configuration window, click the **Defaults** button. The parameter settings of the selected port(s) are returned to the default settings.

Chapter 3

SNMPv1 and SNMPv2c

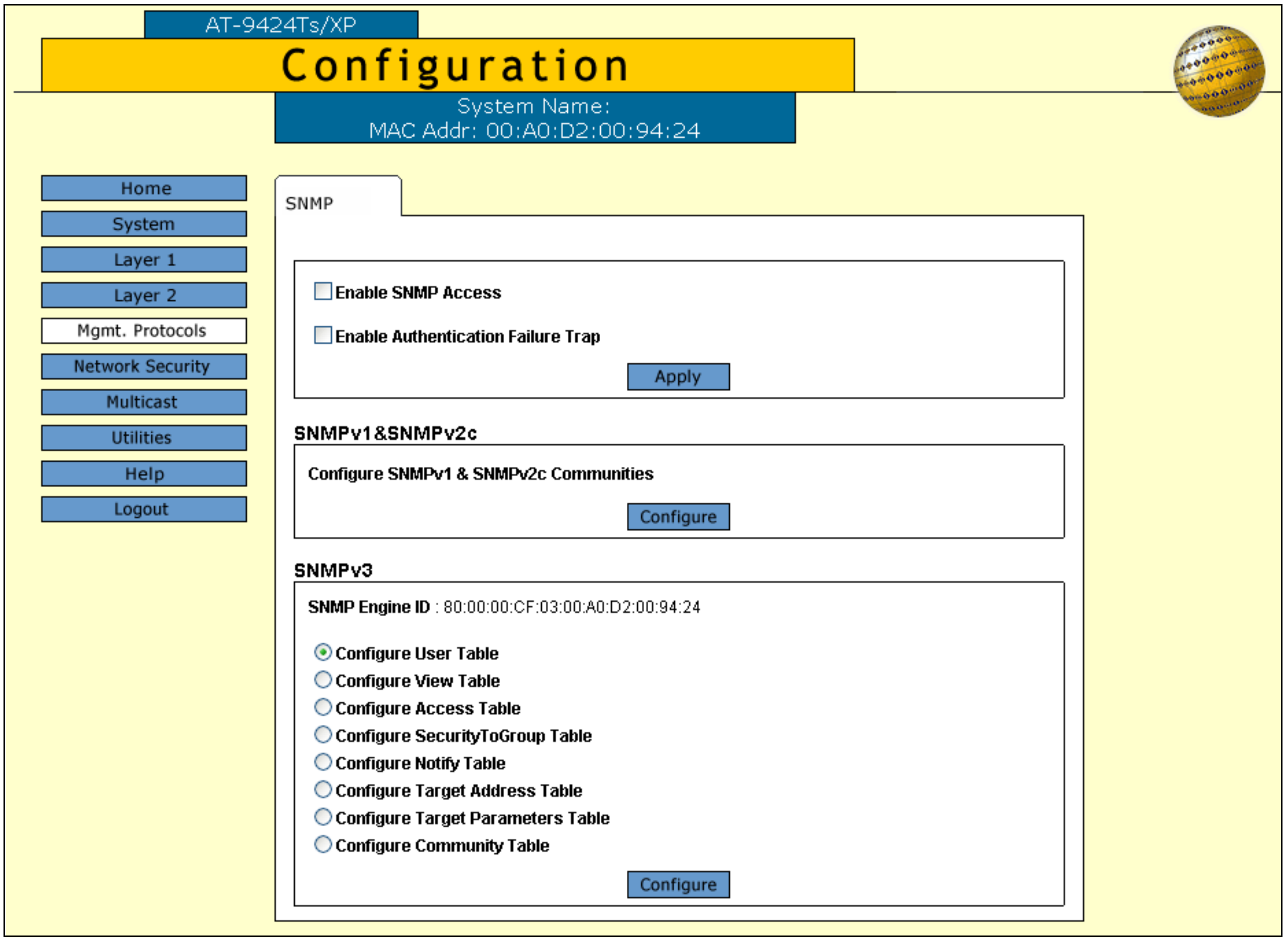
This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab shown in Figure 11.



□ Enable SNMP Access

□ Enable Authentication Failure Trap

Configure SNMPv1 & SNMPv2c Communities

SNMP Engine ID : 80:00:00:CF:03:00:A0:D2:00:94:24

● 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

3. Click the **Enable SNMP Access** check box to enable or disable SNMP management. When the box has a check, the feature is enabled so that you can manage the stack with an SNMP management program. No check indicates the feature is disabled. The default is disabled.

4. If you want the stack to send authentication failure traps, click the **Enable Authentication Failure Traps** check box. When there is a check in the box, this feature is enabled.

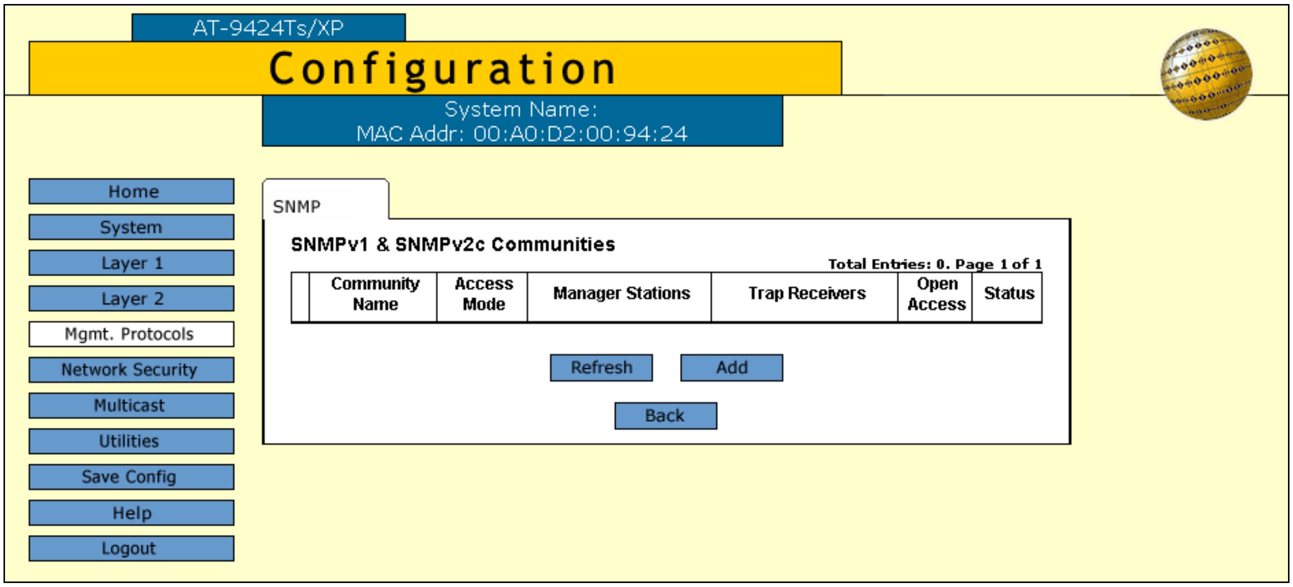
5. Click the **Apply** button.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Creating New SNMPv1 and SNMPv2c Community Strings

To create an SNMPv1 and SNMPv2c community string:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv1 & SNMPv2c section, click the **Configure** button to display the SNMPv1 & SNMPv2c Communities tab, shown in Figure 12.



System Name:
MAC Addr: 00:A0:D2:00:94:24

SNMPv1 & SNMPv2c Communities

Total Entries: 0. Page 1 of 1

	Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status

Figure 12. SNMPv1 & SNMPv2c Communities Tab

The tab displays the following information.

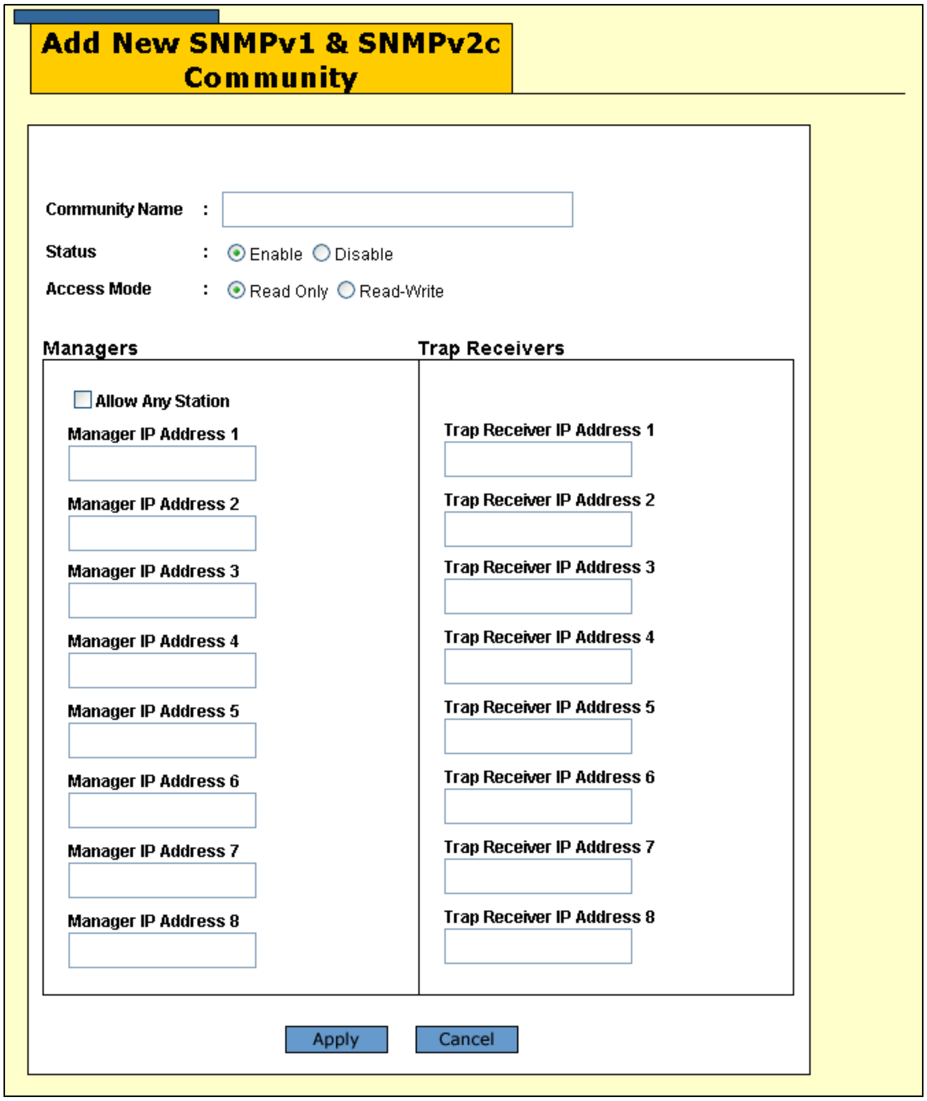
Table 7. SNMPv1 & SNMPv2c Communities Tab

Column	Definition
Community Name	The name of a community string.
Access Mode	The access mode of a community string. A string with a Read Only access mode can be used to view the MIB objects on the stack, but not change their values. A string with a Read/Write access mode can be used to view and change the SNMP MIB objects.

Table 7. SNMPv1 & SNMPv2c Communities Tab

Column	Definition
Manager Stations	The IP addresses of the management workstations that are permitted to use a string with a closed access status.
Trap Receivers	The IP addresses of trap receivers to receive traps from the stack.
Open Status	The access status of a community string. A string that has an open status of Yes can be used by any management workstation. In contrast, a string that has a status of No can only be used by a workstation if the workstation's IP address is assigned to it.
Status	The operating status of a community string. Enabled means the string is available for use and Disabled means it is unavailable.

4. To create a new community string, click the **Add** button to display the Add New SNMPv1 & SNMPv2c Community window in Figure 13 on page 54.



Add New SNMPv1 & SNMPv2c 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 & SNMPv2c Community Page

5. Configure the parameters, described in Table 8, as needed.

Table 8. SNMPv1 and SNMPv2c Community Parameters

Parameter	Definition
Community Name	Specifies the community string. The name can be up to 32 alphanumeric characters. Spaces and special characters (such as /, #, or &) are not permitted.
Status	Enables or disables the community string. A disabled community string cannot be used to manage a stack. The default is enabled.

Table 8. SNMPv1 and SNMPv2c Community Parameters

Parameter	Definition
Access Mode	Specifies the access mode for a SNMP community string. A string with a Read Only access mode can only be used to view the MIB objects on the switch. A string with a Read/Write access mode can be used to both view and change the SNMP MIB objects.
Allow Any Station	Sets the community string as opened or closed. If there is no check in the box next to the option, the community string is closed and 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 stack.
Manager IP Address 1 to 8	Specifies the IP addresses of management workstations. If you assign a community string a closed status, use these fields to specify the IP addresses of up to eight management workstations permitted to use the community string. Entering manager IP addresses for a community string with an open status has no affect on the string.
Trap Receiver IP Address 1 to 8	Specifies the IP addresses of up to eight trap receivers. These are nodes on your network, such as your management workstation, to act as trap receivers for the stack.

6. Click the **Apply** button to create the new community string.

7. Repeat this procedure starting with step 4 to add more community strings.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying SNMPv1 and SNMPv2c Communities

To modify an SNMPv1 and SNMPv2c community string:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button.
3. Select the **SNMP** tab, shown in Figure 11 on page 50.
4. In the SNMPv1 & SNMPv2c section, click the **Configure** button to display the SNMPv1 & SNMPv2c Communities tab, shown in Figure 12 on page 52.
5. Click the radio button of the community name you want to modify and click the **Modify** button. You can modify only one community string at a time.

   The settings of the selected SNMP community string are displayed in the Modify SNMPv1 & SNMPv2c Community page.
6. Modify the parameters as needed. The parameters are described in Table 8 on page 54. The community name of a string cannot be changed.
7. Click the **Apply** button to activate your changes.
8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting SNMPv1 and SNMPv2c Community Strings

To delete an SNMPv1 and SNMPv2c community string:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button.

3. Select the **SNMP** tab, shown in Figure 11 on page 50.

4. In the SNMPv1 & SNMPv2c section, click the **Configure** button to display the SNMPv1 & SNMPv2c Communities tab, shown in Figure 12 on page 52.

5. Click the radio button of the community name you want to delete and click the **Remove** button. You can delete only one community string at a time.

   A warning message is displayed.

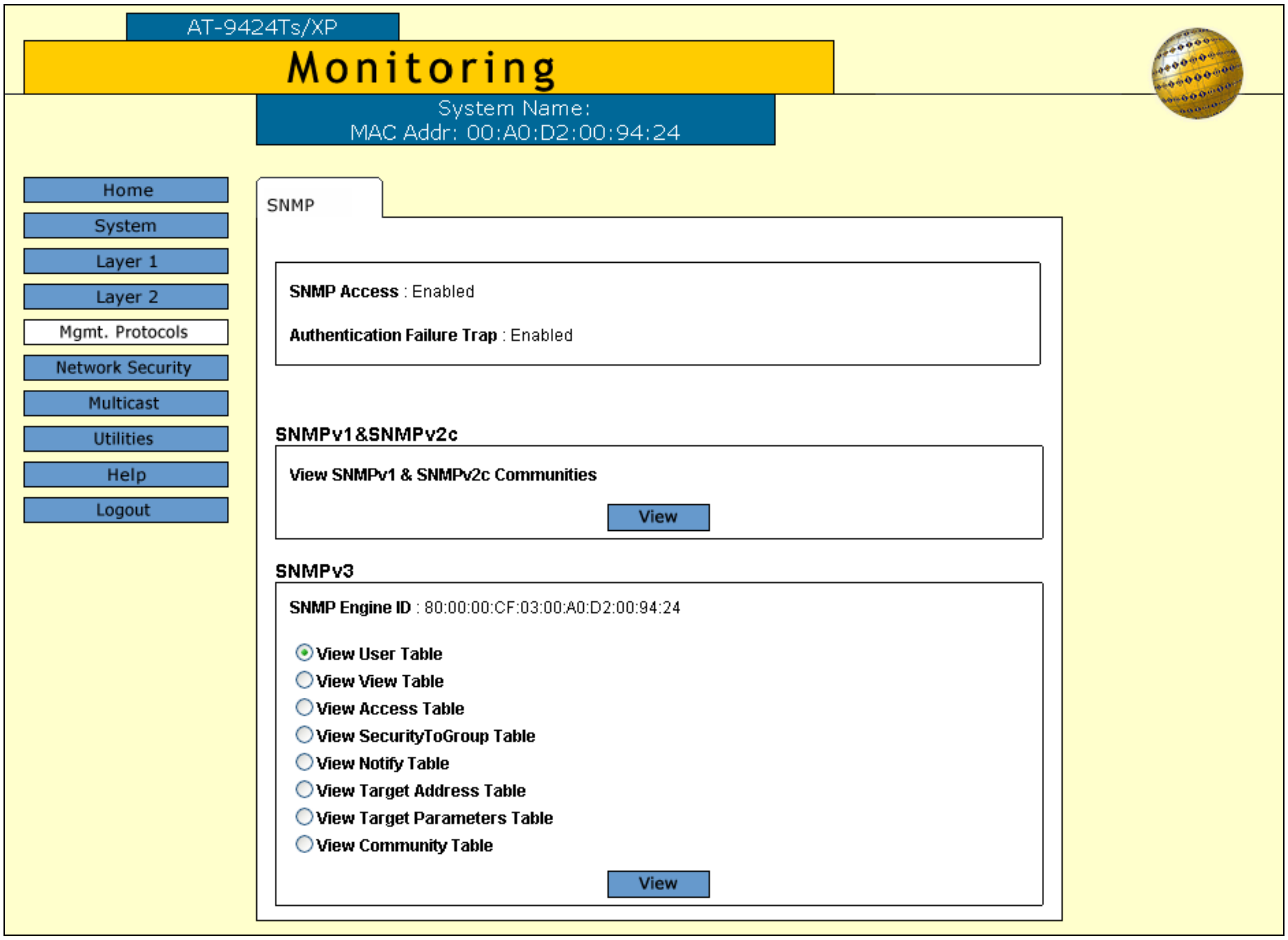
6. Click the **OK** button to delete the community string from the switch.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying the SNMPv1 and SNMPv2c Community Strings

To display the SNMPv1 and SNMPv2c community strings from an operator management session:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Mgmt. Protocols** button.
3. Select the **SNMP** tab to display the SNMP tab shown in Figure 14.



SNMP Access : Enabled

Authentication Failure Trap : Enabled

SNMPv1&SNMPv2c

View SNMPv1 & SNMPv2c Communities

View

SNMPv3

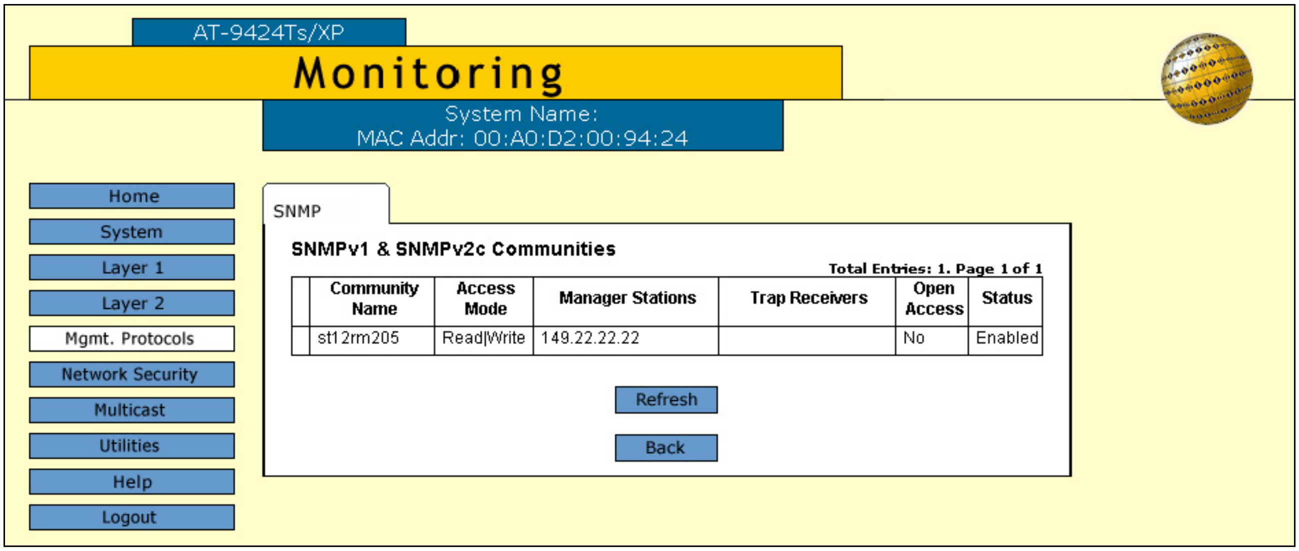
SNMP Engine ID : 80:00:00:CF:03:00:A0:D2:00:94:24

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

View

Figure 14. SNMP Tab (Monitoring)

4. In the SNMPv1 & SNMPv2c section, click the **View** button to display the SNMPv1 & SNMPv2c Communities tab, shown in Figure 15.



SNMPv1 & SNMPv2c Communities

Total Entries: 1. Page 1 of 1

	Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
	st12rm205	Read|Write	149.22.22.22		No	Enabled

Figure 15. SNMPv1 & SNMPv2c Communities Tab (Monitoring)

The columns in the table are described in Table 7 on page 52.

Chapter 4

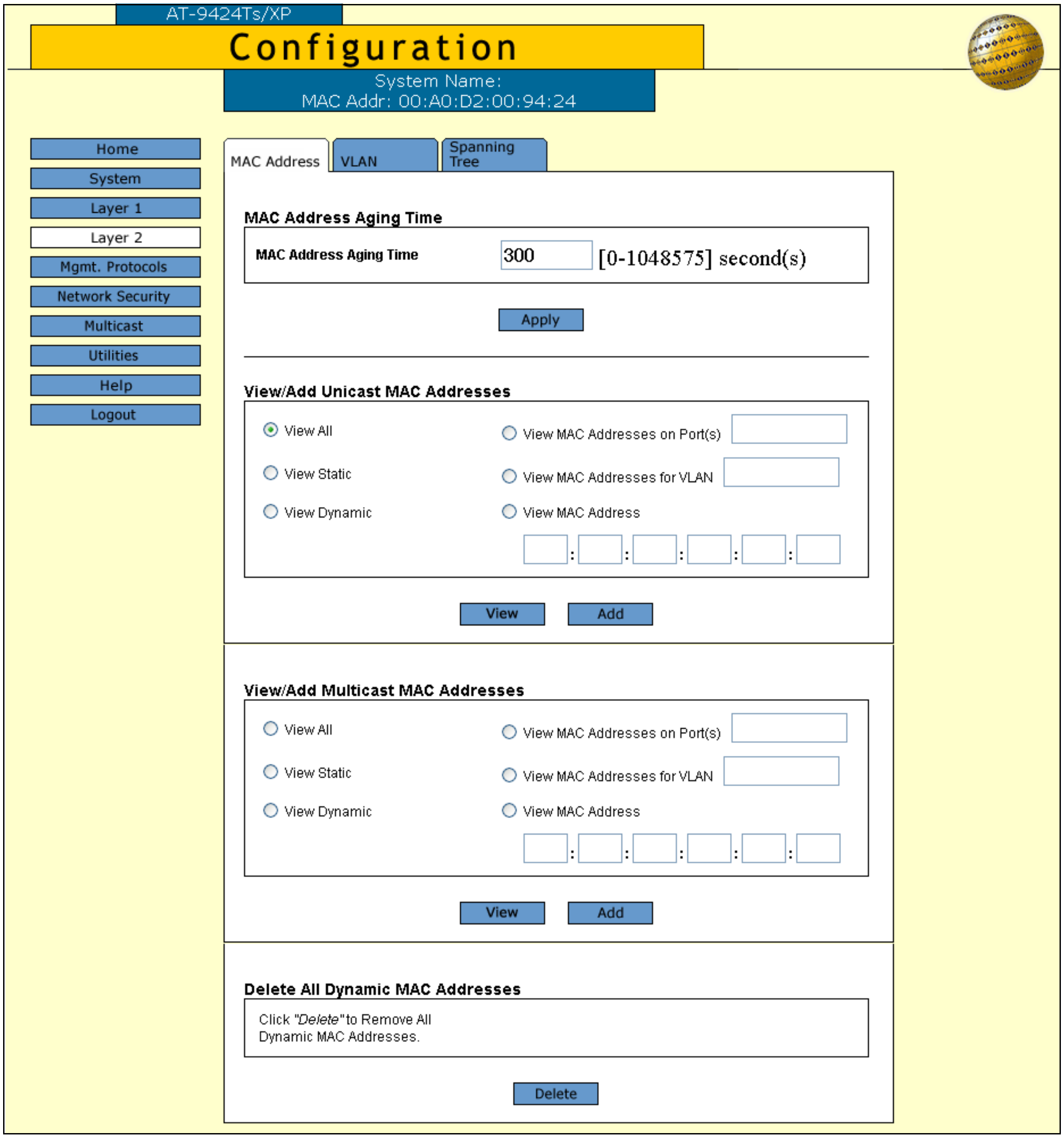
MAC Address Table

This chapter contains instructions on how to view the MAC addresses in the MAC address table. It also explained how to add static addresses to the table. This chapter contains the following procedures:

Displaying the MAC Address Table

To view the MAC address table on the master switch:

1. From the Home page, select **Monitoring** or **Configuration**.
2. From the Monitoring or Configuration menu, select the **Layer 2** option.
3. Select the **MAC Address** tab, shown in Figure 16.



System Name:
MAC Addr: 00:A0:D2:00:94:24

MAC Address Aging Time

MAC Address Aging Time 300 [0-1048575] second(s)

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.

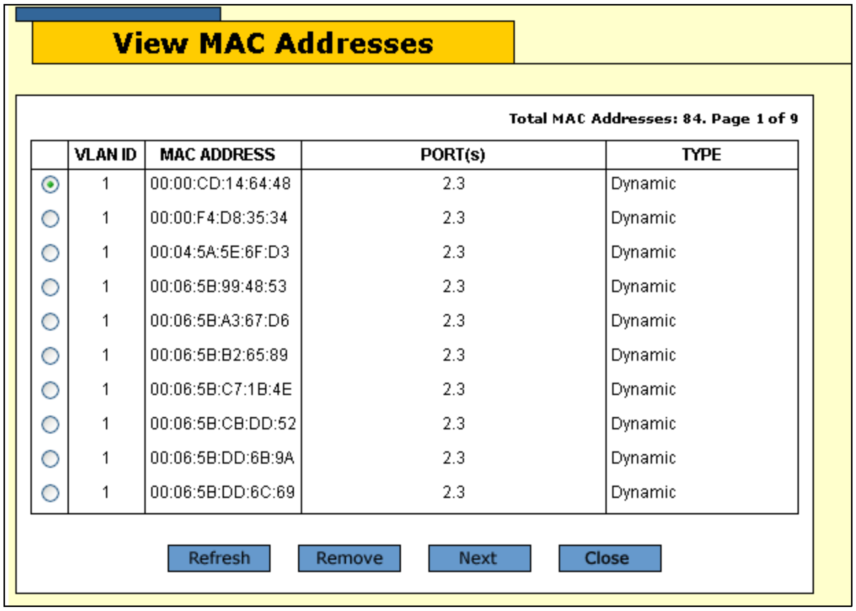
Figure 16. MAC Address Tab

The View Unicast MAC Addresses section and the View Multicast MAC Addresses section display unicast and multicast addresses, respectively. The options function the same in both sections. You can select only one option at a time.

Table 9. View MAC Addresses Window

Selection	Definition
View All	Displays all dynamic and static unicast or multicast addresses in the MAC address table.
View Static	Displays the static unicast or multicast addresses assigned to the ports.
View Dynamic	Displays the dynamic addresses learned on the ports.
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 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 where a MAC address was assigned or learned. In some situations, you might want to know which port learned a particular MAC address. 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. This option allows you to specify the MAC address and let the AT-S63 Management Software automatically locate the port where the address was learned.

4. After selecting an option, click the **View** button. Figure 17 shows an example of unicast MAC addresses.



View MAC Addresses

Total MAC Addresses: 84. Page 1 of 9

	VLAN ID	MAC ADDRESS	PORT(s)	TYPE
●	1	00:00:CD:14:64:48	2.3	Dynamic
○	1	00:00:F4:D8:35:34	2.3	Dynamic
○	1	00:04:5A:5E:6F:D3	2.3	Dynamic
○	1	00:06:5B:99:48:53	2.3	Dynamic
○	1	00:06:5B:A3:67:D6	2.3	Dynamic
○	1	00:06:5B:B2:65:89	2.3	Dynamic
○	1	00:06:5B:C7:1B:4E	2.3	Dynamic
○	1	00:06:5B:CB:DD:52	2.3	Dynamic
○	1	00:06:5B:DD:6B:9A	2.3	Dynamic
○	1	00:06:5B:DD:6C:69	2.3	Dynamic

Figure 17. View MAC Addresses Window

The columns in the table are described in Table 10.

Table 10. View MAC Addresses Window

Column	Definition
VLAN ID	Displays the ID numbers of the VLANs of the ports.
MAC Address	Displays the static and dynamic MAC addresses.
Port(s)	Displays the ports where the addresses were learned or assigned. The MAC address with port “CPU” is the address of the master switch.
Type	Displays the address type as either static or dynamic.

Adding Static Unicast or Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to a port. A switch port can have up to 255 static MAC addresses.

To add a static address to the MAC address table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. If the MAC Address tab is not selected, click it. The tab is shown in Figure 16 on page 62.

4. To add a static unicast address, click the **Add** button in the View/Add Unicast MAC Addresses section. To add a static multicast address, click the **Add** button in the View/Add Multicast MAC Addresses section. The Add MAC Address page is shown in Figure 18.

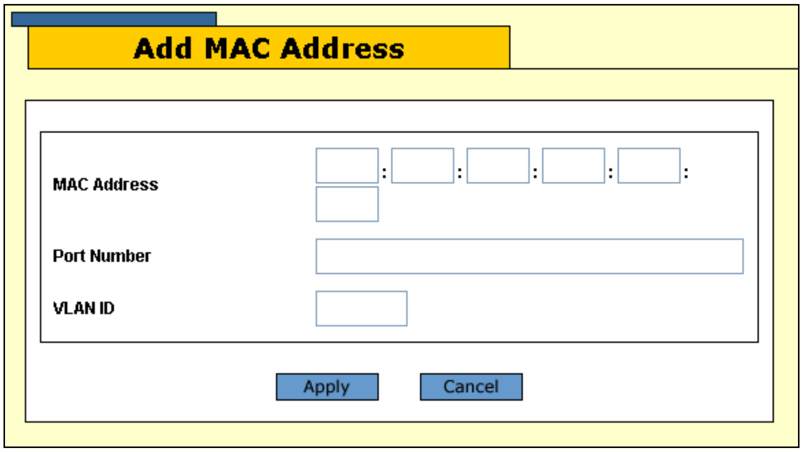


Figure 18. Add MAC Address Page

5. Click the **MAC Address** field and enter the new static unicast or multicast MAC address.

6. Click the **Port Number** field and enter the number of the stack port where you want to assign the static address. You can assign a static unicast address to just one port. Port numbers are entered in this format:

   stack ID:port number

   For a static multicast address, specify both the port when the multicast application is located and the ports where the host nodes are connected. The host nodes will not receive the multicast packets if you only specify the multicast application port.

7. Click the **VLAN ID** field and enter the ID number of the VLAN where the port is a member.

8. Click the **Apply** button.

9. Repeat this procedure to add other static addresses to the switch.

10. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting Unicast or Multicast MAC Addresses

To delete a static or dynamic unicast or multicast MAC address from the stack:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. If the MAC Address tab is not selected, click it. The tab is shown in Figure 16 on page 62.

4. Display the MAC addresses on the master switch, as explained in "Displaying the MAC Address Table" on page 62.

5. Click the button next to the MAC address you want to delete from the master switch. You can delete only one address at a time.

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

6. Click the **Remove** button to remove the MAC address from the table.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting All Dynamic MAC Addresses

To delete all dynamic unicast and multicast MAC addresses from the MAC address table:

1. From the Home page, select the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. If the MAC Address tab is not selected, click it. The tab is shown in Figure 16 on page 62.

4. In the Delete All Dynamic MAC Addresses section, click the **Delete** button to delete all of the dynamic unicast and multicast MAC address from the master switch. The switch immediately begins to learn new dynamic addresses.

Changing the Aging Time

This procedure changes the aging time of the MAC address table. The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. The switch deletes an address from the table if no packets are sent to or received from the address for the period of time specified in the timer. This prevents the table from becoming full of addresses of inactive nodes. The default setting for the aging time is 300 seconds (5 minutes).

To configure the aging time:

5. From the Home page, click the **Configuration** button.
6. From the Configuration menu, click the **Layer 2** button.
7. If the MAC Address tab is not selected, click it. The tab is shown in Figure 16 on page 62.
8. In the MAC Address Aging Time field, enter a new value in seconds. The range is 0 to 1048575 seconds. The default is 300 seconds (5 minutes). The value 0 disables the aging timer. If the aging timer is disabled, inactive dynamic addresses are not deleted from the table and the switch stops learning new addresses after the table reaches maximum capacity.
9. Click the **Apply** button. The new MAC address aging time is immediately activated on the switch.
10. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Chapter 5

Static Port Trunks

This chapter contains the procedures for managing static port trunks. The sections in this chapter are:

Note
The web browser windows do not support LACP trunks. LACP trunks have to be managed with the command line commands.

Creating Static Port Trunks

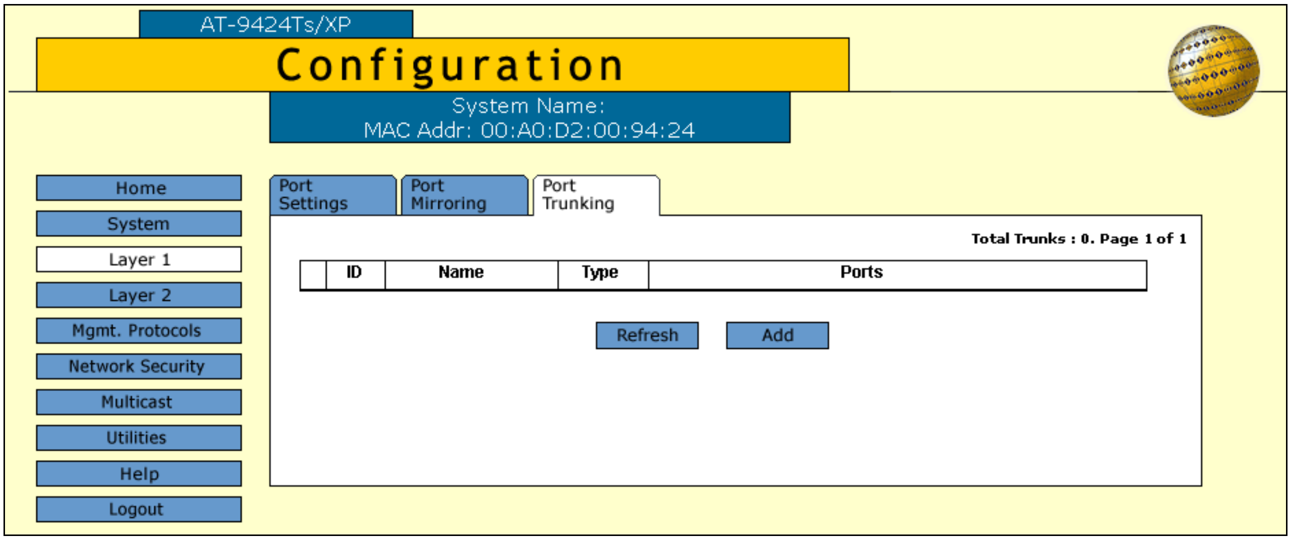
Caution
To prevent the formation of loops in your network and the occurrence of broadcast storms, do not connect the cables to the ports of a static trunk until after you have configured the ports on both the stack and the remote device.

Note
Before creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port to be in the trunk. Verify that its settings are appropriate for the remote device. When you create a trunk, the AT-S63 Management Software copies the settings of the trunk's lowest numbered port to the other ports so that they all have the same settings.

You should also check to be sure that all of the ports are untagged members of the same VLAN, a requirement of static trunks.

To create a static port trunk:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 1** button.
3. Click the **Port Trunking** tab, shown in Figure 19.



Total Trunks : 0. Page 1 of 1

	ID	Name	Type	Ports

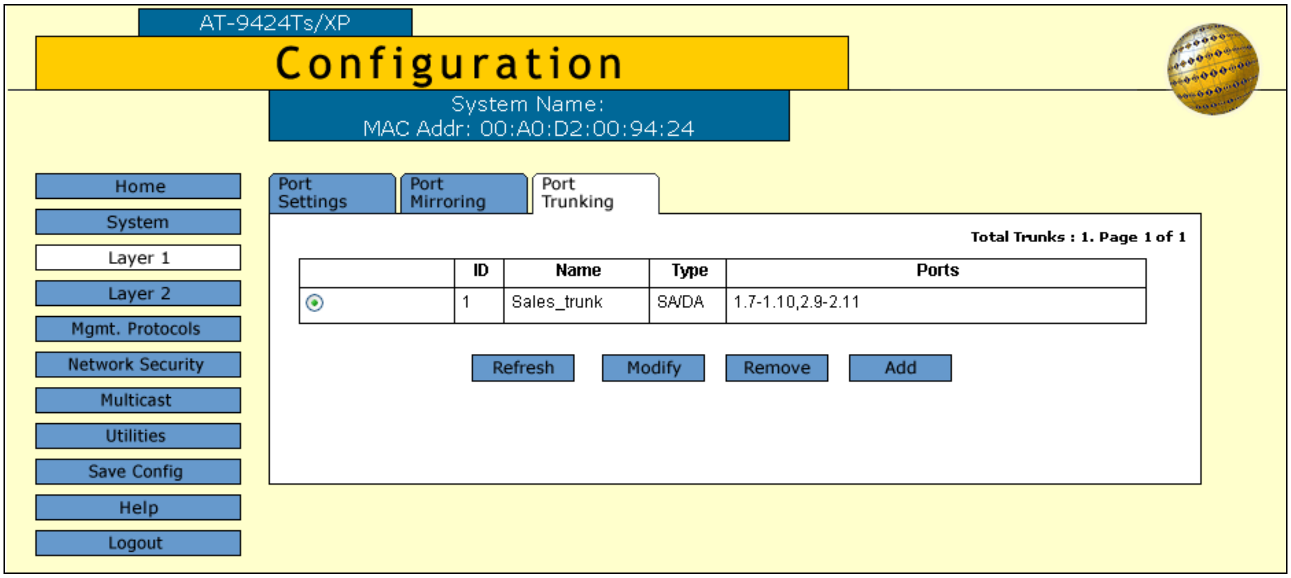
Figure 19. Port Trunking Tab

The table lists the current static ports trunks in the stack. Table 11 describes the columns in the table.

Table 11. Port Trunking Tab

Column	Definition
ID	Displays the ID numbers of the trunks.
Name	Displays the names of the trunks.
Type	Displays the load distribution methods. The possible settings 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)
Ports	Displays the ports of the trunks.

4. To create a new static trunk, click the **Add** button to display the Add New Trunk popup window in Figure 20.



Total Trunks : 1. Page 1 of 1

	ID	Name	Type	Ports
●	1	Sales_trunk	SA/DA	1.7-1.10,2.9-2.11

Figure 20. Add New Trunk Window

Note
Although a static port trunk can consist of ports from different switches in a stack, you can only choose ports from one switch during the initial configuration. Afterwards, you can add more ports to it from other switches in the stack.

5. Use the pull-down Stack ID menu in the upper left corner of the switch image to select one of the switches in the stack with ports that you want to be members of the port trunk and click the **Apply** button. If the switch is already displayed, you can skip this step.

6. In the switch image, click the ports of the trunk. A selected port turns white. To deselect a port, click it again.

7. Click the **Trunk Name** field and enter a name of up to 16 alphanumeric characters for the trunk. Spaces or special characters, such as asterisks and exclamation points, are not permitted. Each trunk must have a unique name.

8. From the Trunk Method pull-down menu, select the load distribution method for the trunk. The possible settings 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)

9. Click the **Apply** button to create the new trunk.

10. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

11. To add more ports to the trunk from other switches in the stack, refer to “Modifying Static Port Trunks” on page 75.

12. Configure the ports on the remote device for port trunking.

13. Connect the cables to the ports of the trunk on the switch and on the remote device.

    The port trunk is ready for network operations.

Modifying Static Port Trunks

This section contains the procedure for modifying static port trunks. Here are the guidelines:

- ❐ All of the ports of a static port trunk have to be untagged members of the same VLAN.
- ❐ If you add a new port that becomes the lowest numbered port in the trunk, its parameter settings overwrite the settings of the existing ports in the trunk. Consequently, if you plan to add a new port that will be the lowest numbered port in the truck, you should verify its settings beforehand to be sure that they are correct.
- ❐ If you add any other port, its settings are automatically changed to match the settings of the existing ports in the trunk.

⚠ **Caution**
To prevent the formation of loops and broadcast storms in your network, disconnect the cables from the ports of a trunk before modifying it.

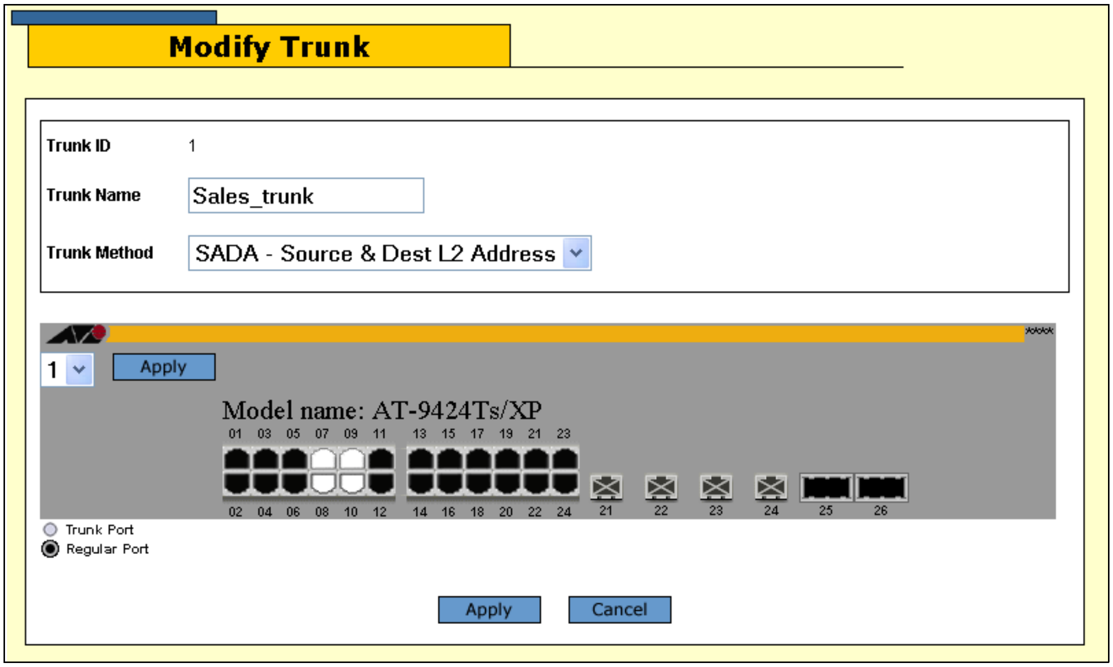
To modify a port trunk:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 1** button.

3. Click the **Port Trunking** tab, shown in Figure 19 on page 72.

4. Click the radio button of the port trunk you want to modify and click the **Modify** button. An example of the Modify Trunk window is shown in Figure 21.



Modify Trunk

Trunk ID 1

Trunk Name Sales_trunk

Trunk Method SADA - Source & Dest L2 Address

1 Apply

Model name: AT-9424Ts/XP

○ Trunk Port
● Regular Port

Apply Cancel

Figure 21. Modify Trunk Window

5. To add or remove ports from the trunk, use the Stack ID pull-down menu in the switch image to select the ID number of one of the switches in the stack and click the **Apply** button. You can add or remove ports from a trunk from just one switch at a time.

6. In the switch image click the ports that you want to add or remove from the trunk. A trunk member is white.

7. To change the name of the trunk, click the **Trunk Name** field and enter a new name of up to 16 alphanumeric characters. Spaces and special characters, such as asterisks and exclamation points, are not permitted. Each trunk must have a unique name.

8. To change the load distribution method of the trunk, select the new setting from the **Trunk Method** pull-down menu.

9. Click the **Apply** button. Your changes are immediately activated on the trunk.

10. To add or remove more ports from the trunk from other switches in the stack, repeat this procedure starting with step 4.

11. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

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

Deleting Static Port Trunks

⚠ **Caution**

To prevent the formation of loops and broadcast storms in your network, disconnect the cables from the ports of a trunk before deleting it.

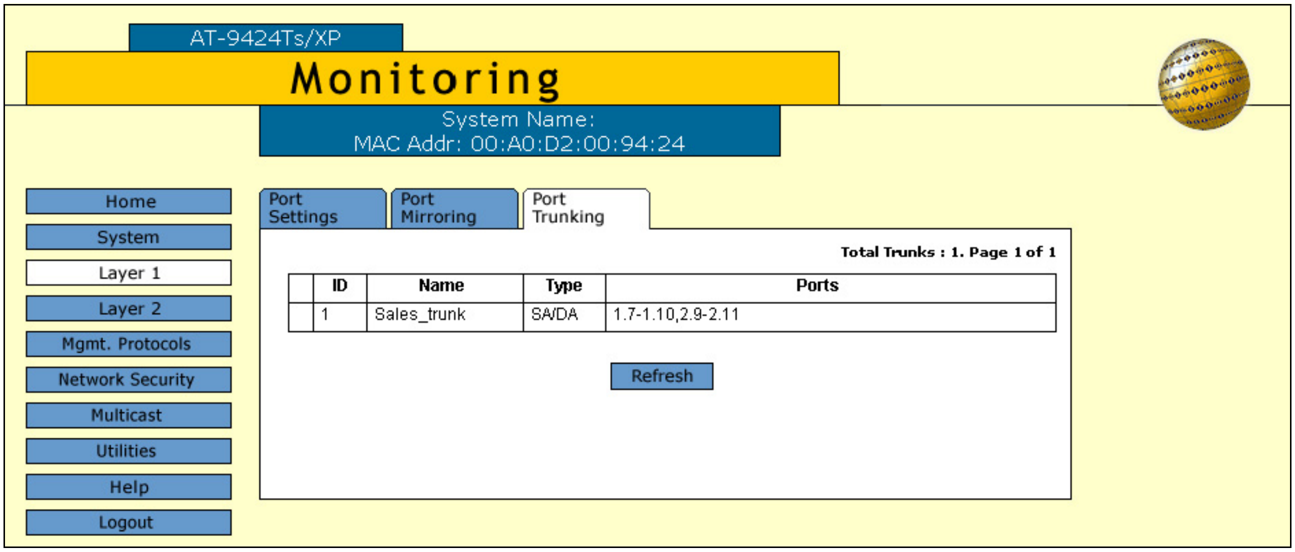
To delete a port trunk from the stack:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 1** button.
3. Click the **Port Trunking** tab, shown in Figure 19 on page 72.
4. Click the radio button of the port trunk you want to delete and click the **Remove** button. The port trunk is deleted from the switch. You can delete only one trunk at a time.
5. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying Static Port Trunks

To display the port trunks in the stack:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Layer 1** button.
3. Click the **Port Trunking** tab, shown in Figure 22.



Total Trunks : 1. Page 1 of 1

	ID	Name	Type	Ports
	1	Sales_trunk	SA/DA	1.7-1.10,2.9-2.11

Figure 22. Port Trunking Tab (Monitoring)

The table is described in Table 11 on page 73.

Chapter 6
Port Mirroring

This chapter contains the procedures for managing the port mirroring feature. The sections in the chapter include:

Overview

The port mirror feature allows you to unobtrusively monitor the ingress or egress traffic on one or more ports on a stack by copying the traffic to another stack port. By connecting a network analyzer to the port where the traffic is being copied to, you can monitor the traffic on the other ports without impacting network performance or speed.

The port(s) whose traffic you want to mirror is called the *source port(s)*. The port where the traffic will be copied to is called the *destination port*.

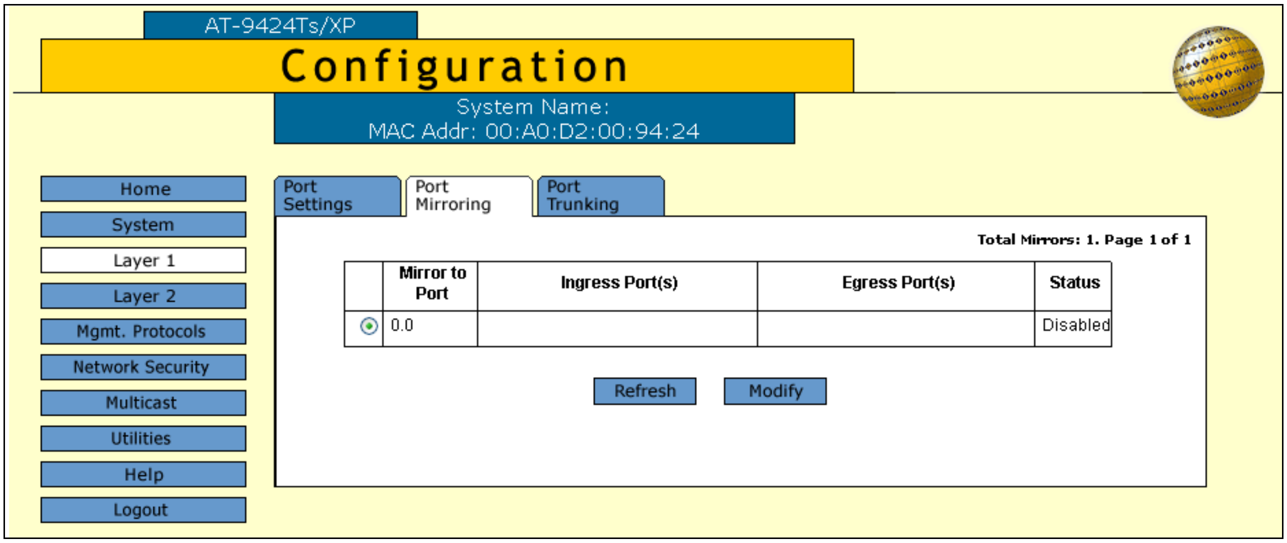
Observe the following guidelines when creating a port mirror:

- A stack can have only one destination port.
- You can mirror more than one source port at a time. However, the destination port may have to discard packets if the source ports are very active.
- The destination and source ports can be located on different switches in the stack.
- You can mirror the ingress or egress traffic of the source ports, or both.

Creating the Port Mirror

To configure the port mirror:

1. From the home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 1** button.
3. Click the **Port Mirroring** tab, shown in Figure 23.



System Name:
MAC Addr: 00:A0:D2:00:94:24

Total Mirrors: 1. Page 1 of 1

	Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
◉	0.0			Disabled

Figure 23. Port Mirroring Tab

Table 12 describes the columns in the Port Mirroring table.

Table 12. Port Mirroring Tab

Column	Definition
Mirror to Port	Displays the destination port of the mirrored traffic. A stack can have only one destination port. A value of 0.0 (zero) means there is no port mirror.
Ingress Ports	Displays the source ports of mirrored ingress traffic.
Egress Ports	Displays the sources ports of mirrored egress traffic.

Table 12. Port Mirroring Tab

Column	Definition
Status	Displays the status of port mirroring on the stack. The possible states are: Enabled - The port mirror is active. Disabled - The port mirror is disabled. When the port mirror is disabled, no traffic is copied to the destination port.

4. This step explains how to specify the source ports of the port mirror. The source ports should be designated before the destination port. If you want to mirror the traffic of source ports that are located on different switches in the stack, you have to select the ports a switch at a time.

   To select the source ports:

   a. Click the **Modify** button to display the popup window in Figure 24.

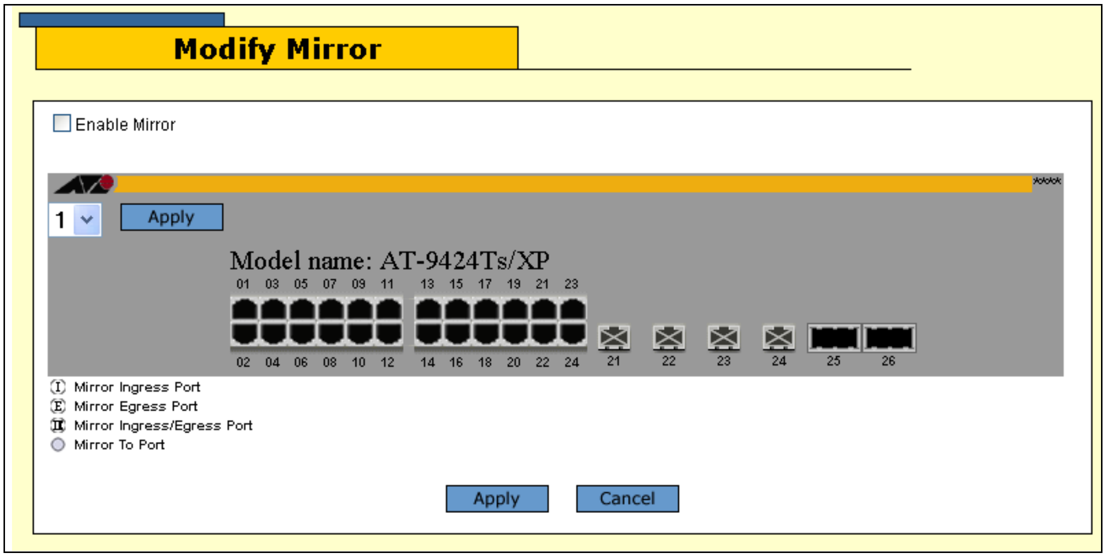


Figure 24. Modify Mirror Window

   b. Use the stack ID pull-down menu in the upper left corner of the switch image to select the ID number of a switch that has one or more ports whose traffic you want to mirror, and click the **Apply** button. If the switch is already displayed, you can skip this step.

c. In the switch image, click the source ports for the port mirror. Clicking a port toggles it through the settings in Table 13.

Table 13. Port Mirror Settings

Icon	Definition
I	The port’s ingress traffic is copied to the destination port.
E	The port’s egress traffic is mirrored to the destination port.
IE	The port’s ingress and egress traffic is copied to the destination port.
□	This is the destination (mirror) port. A stack can have only one destination port.
■	This port is not part of the port mirror.

d. Click the **Apply** button to close the popup window.

e. To add more source ports to the port mirror from other switches in the stack, repeat this step for each switch.

5. To specify the destination port and to activate the port mirror:

a. From the Port Mirroring tab click the **Modify** button to display the popup window in Figure 24 on page 82.

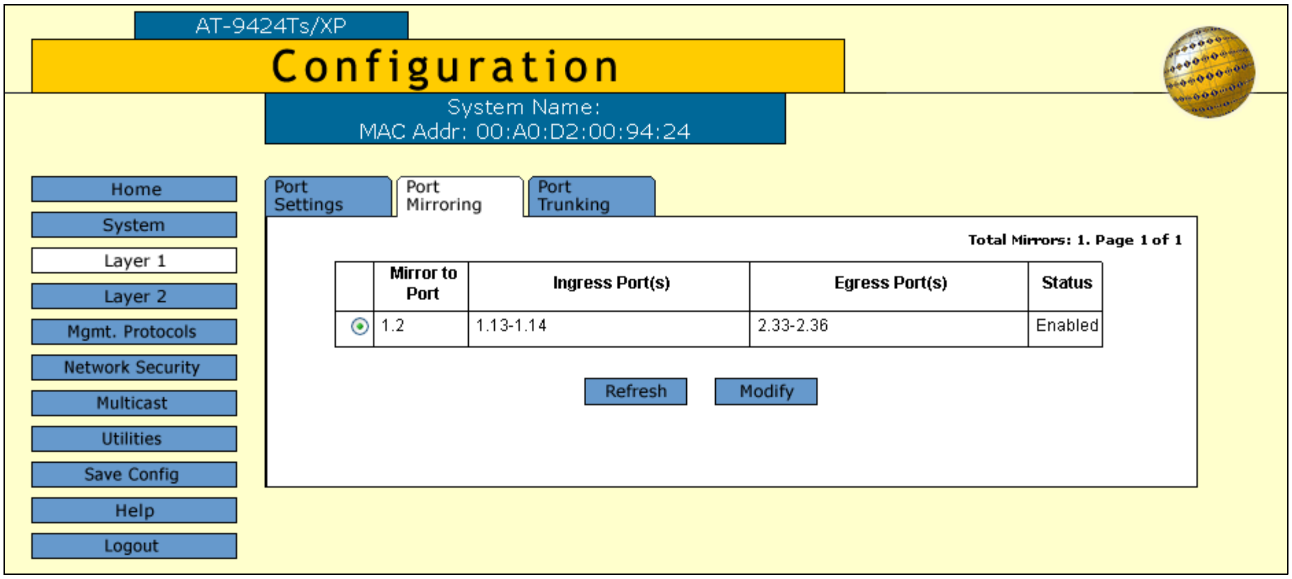
b. Using the stack ID pull-down menu in the upper left corner of the switch image, select the ID number of the switch that has the port you want to be the destination port, and click the **Apply** button. If the switch is already displayed, you can skip this step.

c. Click the port to be the destination port until it turns solid white, as shown in Table 13.

d. Click the **Enable Mirror** checkbox. A check should appear in the box.

e. Click the **Apply** button. The port mirror is now activated. The ingress or egress traffic on the source ports is now copied to the destination port.

An example of how the Port Mirroring tab looks when it is configured for port mirroring is shown in Figure 25. In the example the ingress traffic on the source ports 1.13 and 1.14 and the egress traffic on the source ports 2.33 to 2.36 are copied to the destination port 1.2.



Total Mirrors: 1. Page 1 of 1

	Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
●	1.2	1.13-1.14	2.33-2.36	Enabled

Figure 25. Example of the Port Mirroring Tab

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying the Port Mirror

To modify the port mirror:

1. From the home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 1** button.
3. Click the **Port Mirroring** tab, shown in Figure 23 on page 81.
4. Click the **Modify** button to display the Modify Mirror popup window in Figure 24 on page 82.
5. Click the **Enable Mirror** checkbox to remove the check and click the **Apply** button.

Note
You should disable the port mirror before modifying it.

6. To add or remove source ports:
    a. Click the **Modify** button.
    b. Using the stack ID pull-down menu in the switch image, select the ID number of a switch that has a port you want to remove as a source port or add as a source port. If the switch is already displayed, you can skip this step.
    c. Click the port until it displays the desired setting, listed in Table 13 on page 83.
    d. Click **Apply** to close the Modify Mirror popup window.
    e. Repeat this step to add or remove other source ports.
7. To change the destination port, you must first deselect the current destination port before designating the new port. To change the destination port:
    a. Click the **Modify** button.
    b. Using the stack ID pull-down menu in the upper left corner of the switch image, select the ID number of the switch that has the current destination port. If the switch is already displayed, you can skip this step.
    c. Click the destination port to change it to one of the other settings in Table 13 on page 83.

d. Using the stack ID pull-down menu in the upper left corner of the switch image, select the ID number of the switch that has the port that you want to make the new destination port. If the switch is already displayed, you can skip this step.

e. Click the port until it turns solid white, as shown in Table 13 on page 83.

f. Click **Apply** to close the Modify Mirror popup window.

8. To activate the port mirror again:

a. Click the **Modify** button.

b. Click the **Enable Mirror** checkbox to add the check and click the **Apply** button.

9. To save your changes in the configuration file on the master switch, click the **Save Config** button in the Configuration menu.

Disabling the Port Mirror

This procedure is used to disable port mirroring so that the stack stops copying traffic from the source ports to the destination port. The destination port, however, is still reserved for port mirroring. To resume normal network operations on the destination port, refer to “Deleting the Port Mirror” on page 88.

To disable the port mirror:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 1** button.

3. Click the **Port Mirroring** tab, shown in Figure 23 on page 81.

4. Click the **Modify** button to display the pop-up.window in Figure 24 on page 82.

5. Click the **Enable Mirror** checkbox to remove the check and click the **Apply** button. The stack stops copying the traffic on the source ports to the destination port.

6. To save your changes in the configuration file on the master switch, click the **Save Config** button in the Configuration menu.

Deleting the Port Mirror

To return the destination port to normal network operations:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 1** button.

3. Select the **Port Mirroring** tab, shown in Figure 23 on page 81.

4. Click the **Modify** button to display the popup window in Figure 24 on page 82.

5. If the port mirror is not already disabled, click the **Enable Mirror** checkbox to remove the check and click the **Apply** button.

6. Click the **Modify** button again.

7. Using the stack ID pull-down list in the switch image, select the stack ID of the switch that has the destination port and click the **Apply** button. (You can skip this step if the switch is displayed by default when you clicked the Modify button.)

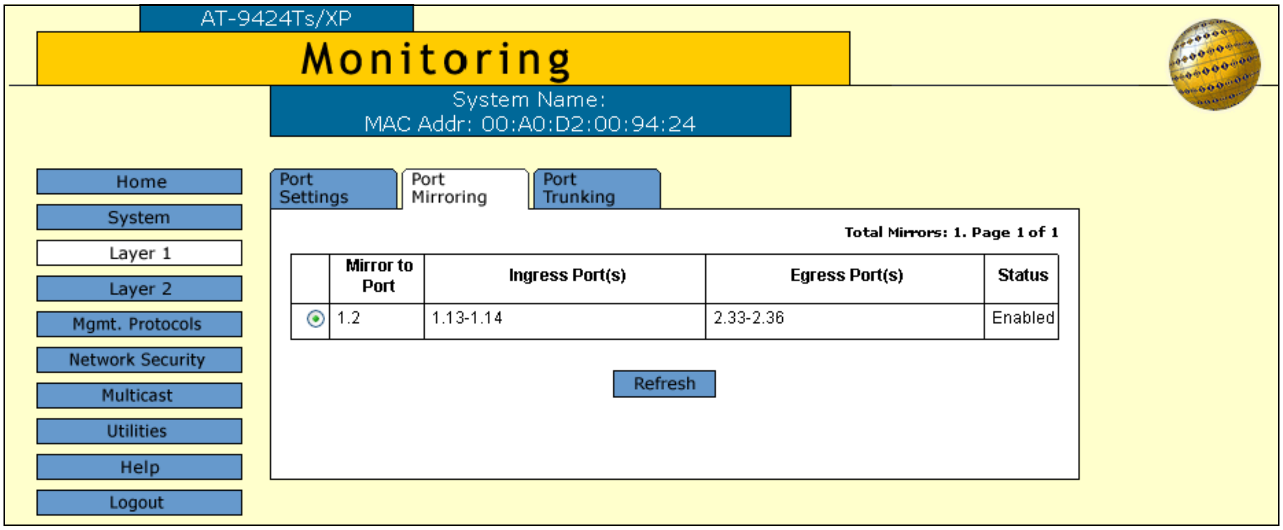
8. Click the destination port until it changes from white to black and click the **Apply** button

9. To save your changes in the master configuration file on the master switch, click the **Save Config** button in the Configuration menu.

Displaying the Port Mirror

To display the port mirror settings from the operator account:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Layer 1** button.
3. Select the **Port Mirroring** tab, shown in Figure 26.



Total Mirrors: 1. Page 1 of 1

	Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
◉	1.2	1.13-1.14	2.33-2.36	Enabled

Figure 26. Port Mirroring Tab (Monitoring)

The columns in the Port Mirroring are described in Table 12 on page 81.

Section II

Advanced Operations

This section has the following chapters:

Chapter 7

File System

This chapter contains the procedures for working with the switch’s file system. The sections include:

- ❒ “Listing the Files in Flash Memory or on a Compact Flash Card” on page 94
- ❒ “Selecting the Active Boot Configuration File” on page 97

Note
You cannot copy, rename, or delete files from a web browser management session. To perform those functions, use the command line commands.

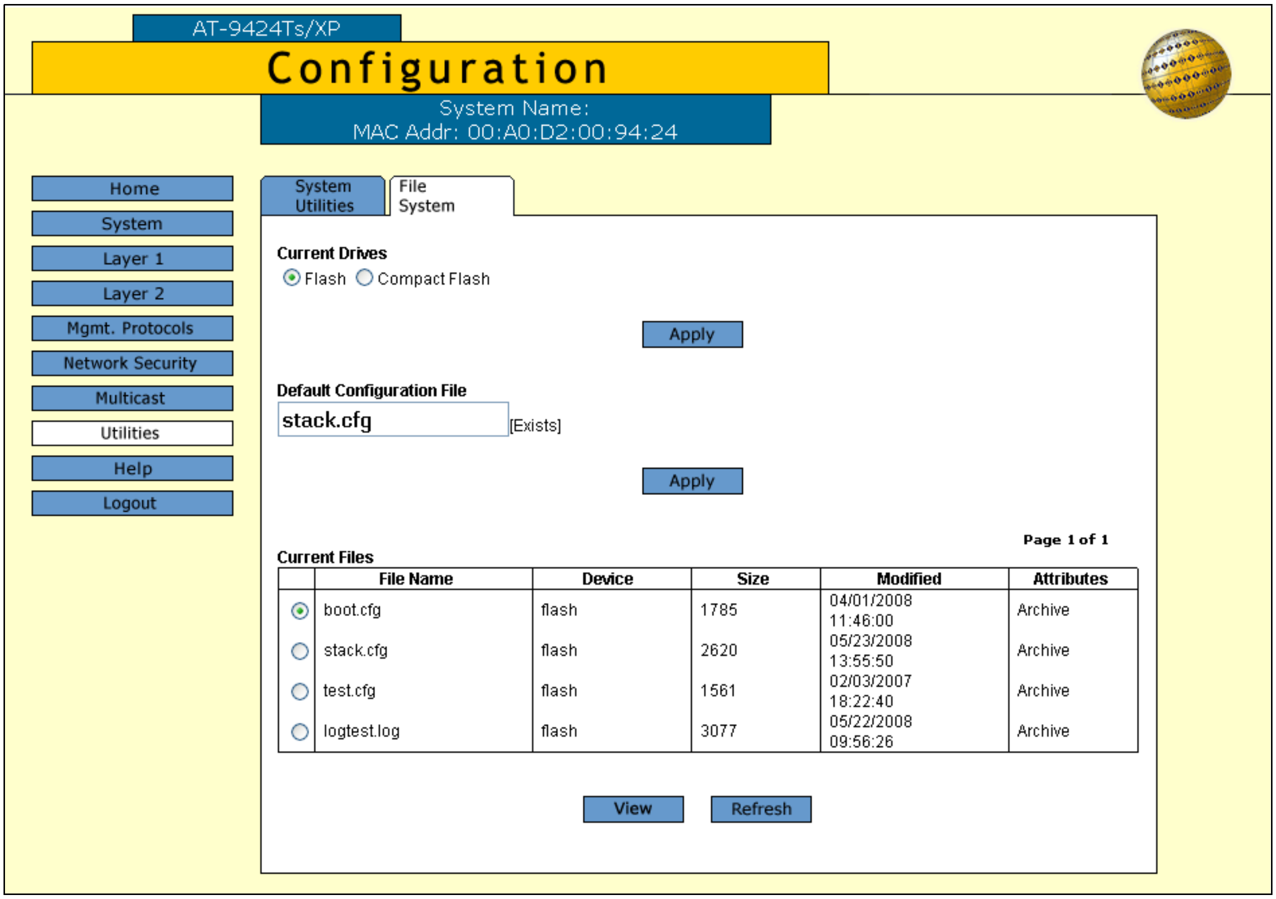
Listing the Files in Flash Memory or on a Compact Flash Card

To display a list of the system files that are stored in the master switch's flash memory or on a compact flash card:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Utilities** button.

3. Select the **File System** tab. to display the FIle System tab in Figure 27.



System Name:
MAC Addr: 00:A0:D2:00:94:24

Current Drives
● Flash ○ Compact Flash

Default Configuration File
stack.cfg [Exists]

Page 1 of 1

Current Files

	File Name	Device	Size	Modified	Attributes
●	boot.cfg	flash	1785	04/01/2008 11:46:00	Archive
○	stack.cfg	flash	2620	05/23/2008 13:55:50	Archive
○	test.cfg	flash	1561	02/03/2007 18:22:40	Archive
○	logtest.log	flash	3077	05/22/2008 09:56:26	Archive

Figure 27. File System Tab

The Current Drives field specifies the location of the files that are displayed in the Current Files section of the tab. The two options are Flash, which is the switch's flash memory and is the default setting, and Compact Flash, which is the compact flash slot.

The Default Configuration File field specifies the filename of the active configuration file that the stack uses to store its parameter settings and to configure its operating parameters when reset or power cycled.

The Current Files table lists the files in the flash memory or the compact flash card in the master switch. The information in the tab is defined in this table.

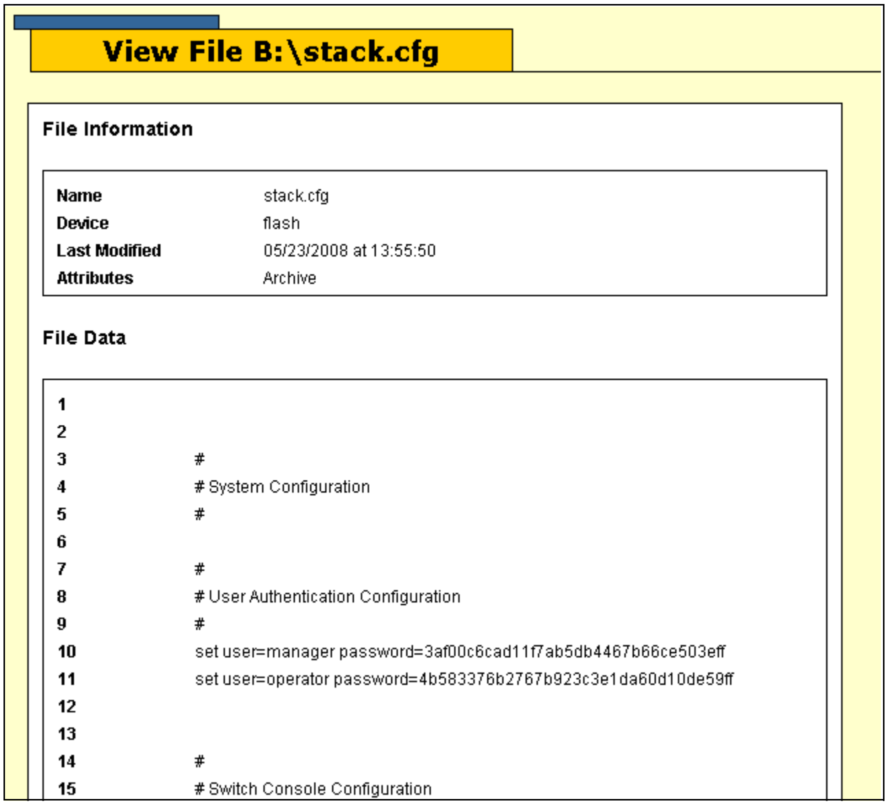
Table 14. File System Tab

Field or Column	Definition
File Name	Name of the system file.
Device	The location of the file. This can be either "flash" for flash memory or "cflash" for a compact flash card.
Size	Size of the file, in bytes.
Modified	The time the file was created or last modified, in the following date and time format: month/day/year hours:minutes:seconds.
Attributes	The file type, one of the following: ❒ Normal ❒ Read Only ❒ Hidden ❒ System ❒ Volume ❒ Directory ❒ Archive ❒ Invalid

4. To view the files on a compact flash card, insert the card into the slot on the master switch, select **Compact Flash** under Current Drivers, and click the **Apply** button.

5. To view the contents of a configuration file, click the file in the Current Files section of the tab and click the **View** button. You can view one file at a time.

   The contents of the configuration file are displayed in the Viewing File popup window. An example is shown in Figure 28.



View File B:\stack.cfg

File Information

Name	stack.cfg
Device	flash
Last Modified	05/23/2008 at 13:55:50
Attributes	Archive

File Data

```


#
# System Configuration
#

#
# User Authentication Configuration
#
set user=manager password=3af00c6cad11f7ab5db4467b66ce503eff
set user=operator password=4b583376b2767b923c3e1da60d10de59ff


#
# Switch Console Configuration
```

Figure 28. Viewing File Window

Selecting the Active Boot Configuration File

This procedure changes the active boot configuration file on the master switch. The master switch uses the active boot configuration file to store the configuration settings of the stack and to configure the operating parameters of the stack whenever it is reset or power cycled. Review the following before performing this procedure:

- ❐ You cannot create a new configuration file from a web browser management session. That task must be performed with the command line commands.
- ❐ The new active configuration file must already exist in the master switch's file system or on a flash memory card. To view the master switch's configuration files, see "Listing the Files in Flash Memory or on a Compact Flash Card" on page 94. Configuration files have a ".cfg" extension.
- ❐ Specifying a new active boot configuration file does not change the current operating configuration of the stack. To reconfigure the stack using the settings in a new active configuration file, you have to reset or power cycle the stack at the end of this procedure.
- ❐ Selecting Save Config after changing the active configuration file overwrites the settings in the file with the current settings of the stack.
- ❐ The active configuration file can be on a flash memory card. However, the master switch does not copy the configuration file to its file system. Instead, it uses and updates the file directly on the card. If you remove the card, the master switch will not able to save any further configuration changes until you reinsert the flash card or specify another active boot configuration file. Furthermore, removing a flash card and resetting the stack causes the stack to return to its default settings.

To change the master switch's active configuration file:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Utilities** button.
3. Select the **File System** tab to display the File System tab in Figure 27 on page 94.
4. In the Default Configuration File field, enter the name of the file to be the new active configuration file. When entering the file name, note the following:
    - ❐ Be sure to include the ".cfg" extension.
    - ❐ Precede the name with "cflash:" if the file is stored on a flash card in the switch.

5. Click the **Apply** button.

   The master switch searches the file system or flash memory card for the file. If it finds the file, it displays the file name in the Default Configuration File field along with the word “Exists.” The file is now the active boot configuration file on the switch.

   If the switch can not locate the file, it displays the name of the previous boot configuration file. Repeat steps 4 and 5, being sure to enter the name correctly.

6. Do one of the following:

   ❒ To configure the stack using the parameter settings in the new active configuration file, do **not** select Save Config. Instead, reset or power cycle the stack.

   ❒ Or, to overwrite the settings in the new active configuration file with the stack’s current settings, click the **Save Config** button.

Chapter 8

File Downloads and Uploads

This chapter explains how to upload and download files, such as configuration files, to the master switch of a stack. This chapter contains the following sections:

- ❒ "General Guidelines" on page 100
- ❒ "Downloading a Master Configuration File" on page 101
- ❒ "Uploading a Configuration File or an Event Log File" on page 104

Note
For instructions on how to upgrade the AT-S63 Management Software on the switches of a stack, refer to the *AT-S63 Software Release Notes*.

General Guidelines

Here are the general guidelines to uploading or downloading files to the master switch of a stack for the web browser windows:

❐ You have to use TFTP.

❐ There has to be a node on your network with the TFTP server software.

❐ You should start the TFTP server before you begin the upload or download procedure.

❐ The stack must have a routing interface on the local subnet from where it reaches the TFTP server. The master switch uses the IP address of the interface as its source address to communicate with the server. If the stack does not have a routing interface, you can upload or download files from a local management session on the switch using Xmodem.

❐ You cannot use the web browser windows to upload or download files to the compact flash memory card in a switch.

Downloading a Master Configuration File

This procedure explains how to download a new master configuration file from a TFTP server to the master switch of a stack. You might perform this procedure to return the switches of a stack to an earlier configuration or to assign a stack the same settings as another stack.

⚠ **Caution**

This procedure is disruptive to the network operations of a stack. A stack resets after receiving a new configuration file. The switches do not forward network traffic while they initialize their management software and perform the discovery process.

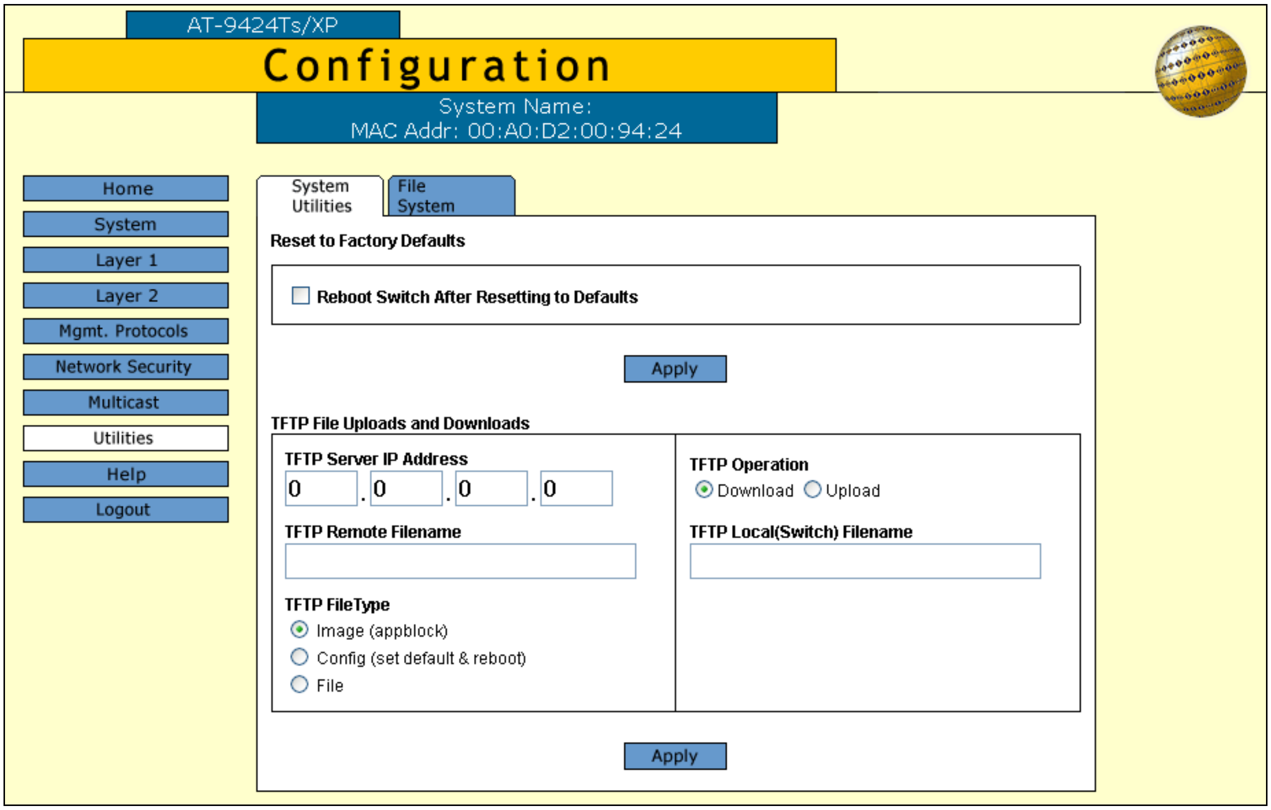
Review the information in “General Guidelines” on page 100 before performing this procedure.

If the configuration file that you are downloading is from a different stack, review these guidelines:

- ❐ A configuration file should only be downloaded onto the stack from where it was taken or from a stack that has the same number and models of AT-9400 Switches. Otherwise, the behavior of the stack may be unpredictable.
- ❐ If the file contains commands for creating routing interfaces with static IP addresses, downloading the same configuration file onto more than one stack may result in IP address conflicts in your network, where routing interfaces on different stacks have the same IP addresses.

To download a configuration file to the master switch:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Utilities** button to display the System Utilities tab in Figure 29.



System Name:
MAC Addr: 00:A0:D2:00:94:24

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(Switch) Filename:

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

Figure 29. System Utilities Tab

3. In the TFTP Server IP Address field, enter the IP address of the network node that has the TFTP server software.

4. For the TFTP Operation parameter, click the **Download** button.

5. Select the **TFTP Remote Filename** field and enter the name of the configuration file that is stored on the TFTP server. The filename extension has to be “.cfg”.

6. Select the **TFTP Local Filename** field and enter a name for the file. This is the name the switch uses to store the file in its file system.

7. For the TFTP File Type parameter, select one of the following:

   - Config - Select this option if you want the master switch to immediately begin to use the new file as its active configuration file after storing the file in its file system.
   - File - Select this option to store the configuration file in the file system in the master switch. You would use this option if you did not want the stack to immediately begin to use the new configuration file and planned to designate it as the active configuration file at a later time.

8. Click the **Apply** button.

   If you selected the Config option in step 6, the master switch, after receiving the new file from the TFTP server, stores it in its file system and marks it as its new active configuration file. It then displays a message on your screen when it is ready to reset the stack. When you see the prompt, click **OK** to initiate the reset and the discovery process.

   If you selected the File option, the master switch simply stores the file in its file system, without marking it as its new active configuration file. For instructions on how to manually designate the file as the active file on the stack, refer to "Selecting the Active Boot Configuration File" on page 97.

Uploading a Configuration File or an Event Log File

This procedure explains how to upload a boot configuration file or an event log file from the file system of the master switch to a TFTP server. You might upload a configuration file in order to transfer it to another stack on your network or to maintain a history of the settings of a stack. Similarly, you might upload an event log to maintain a history of the operational events of a stack or to troubleshoot a network problem.

Uploading a file from the master switch does not interfere with the network operations of a stack.

Review the information in “General Guidelines” on page 100 before performing this procedure.

To upload a configuration file or an event log file:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Utilities** button to display the System Utilities tab, shown in Figure 29 on page 102.

3. Select the **TFTP Server IP Address** field and enter the IP address of the network node with the TFTP server software.

4. For the TFTP Operation parameter, click the **Upload** radio button.

5. Select the **TFTP Remote Filename** field and enter a name for the file when it is stored on the TFTP server.

6. Select the **TFTP Local Filename** field and enter the name of the file that you want to upload from the file system in the master switch. Configuration files have the filename extension “.cfg”. Event log files have the extension “.log”.

7. For the TFTP File Type, click the **File** radio button.

Note
If you select Image as the TFTP File Type, the switch uploads its active AT-S63 image file to the FTP server and stores it under the name specified in step 5. Allied Telesis does not recommend uploading a switch’s image file. If you need an AT-S63 image file to download onto another switch, go to the Allied Telesis web site for the latest version.

8. Click the **Apply** button to begin the upload. The management software notifies you when the upload is complete.

Chapter 9

Event Logs and the Syslog Client

This chapter describes how to view switch activity by displaying and saving the contents of the event logs. It also explains how to send events to syslog servers on your network by creating syslog output definitions. Sections in the chapter include:

Note
The event logs, even when disabled, log all of the AT-S63 initialization events that occur when a stack is reset or power cycled. Any switch events that occur after AT-S63 initialization are entered into the logs only if the event log feature is enabled, which is the default setting for this feature.

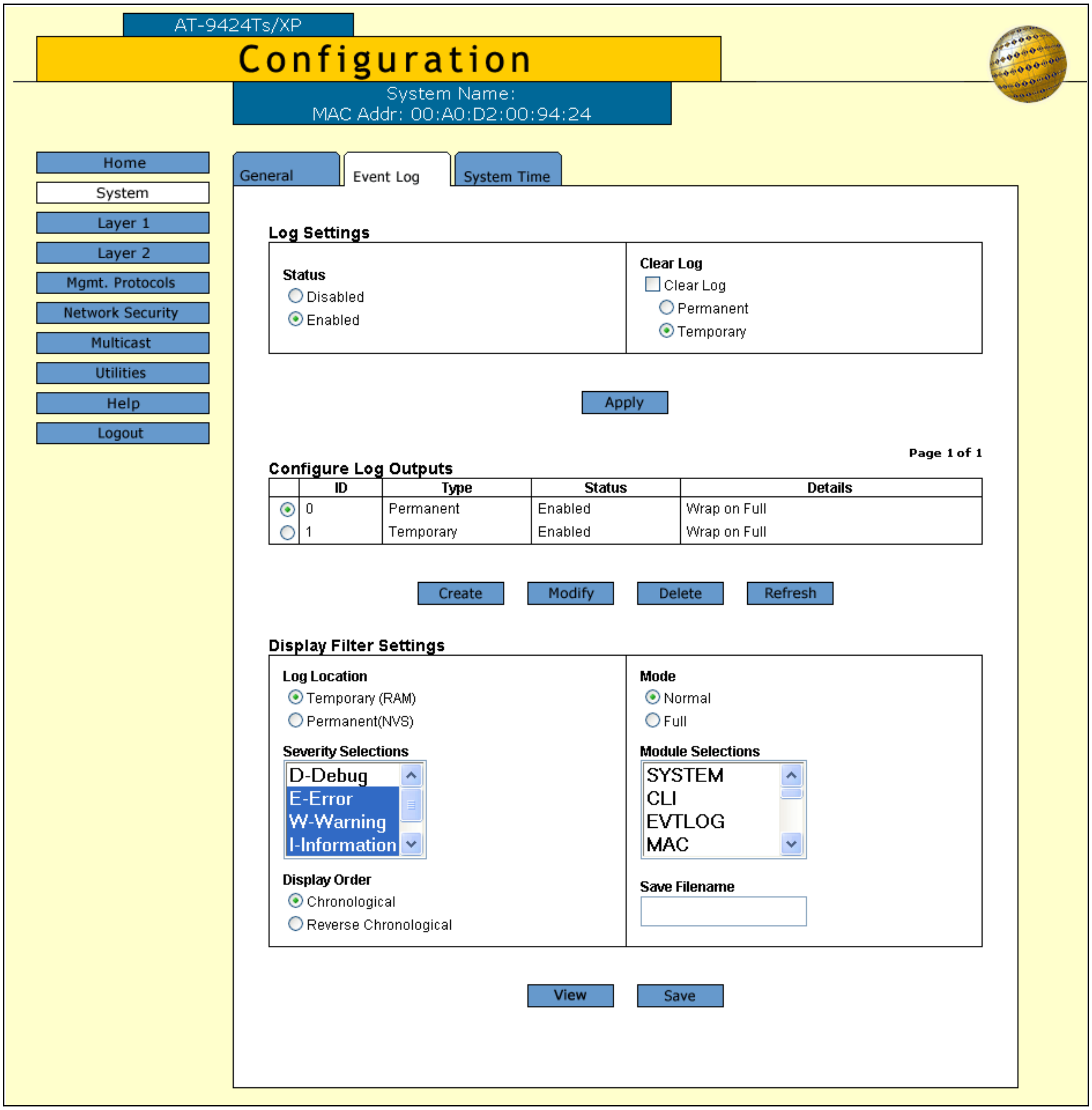
Enabling or Disabling the Event Logs

To enable or disable the event logs:

1. From the Home page, click either the **Configuration** button.

1. From the Configuration menu, click the **System** button.

2. Click the **Event Log** tab, shown in Figure 30.



System Name:
MAC Addr: 00:A0:D2:00:94:24

Log Settings

Status
○ Disabled
● Enabled

Clear Log
☐ Clear Log
○ Permanent
● Temporary

Page 1 of 1

Configure Log Outputs

	ID	Type	Status	Details
●	0	Permanent	Enabled	Wrap on Full
○	1	Temporary	Enabled	Wrap on Full

Display Filter Settings

Log Location
● Temporary (RAM)
○ Permanent(NVS)

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 30. Event Log Tab

3. In the Log Settings section, click **Enabled** for the Status to enable the event logs, or **Disabled** to disable the event logs and to stop the master switch from storing events in the event log. The default setting is enabled.

4. Click **Apply** to activate the settings on the switch.

   If you enabled the logs, the switch immediately begins to add events to the logs.

5. To save your changes in the master configuration file on the master switch, click the **Save Config** button in the Configuration menu.

Displaying the Event Messages

To view the events messages in the event logs:

1. From the Home page, click either the **Monitoring** or the **Configuration** button.

2. Click the **System** button.

3. Select the **Event Log** tab, shown in Figure 30 on page 106.

4. Configure the parameters in the Display Filter Settings section to define the types of events you want to view. The parameters are described in Table 15.

5. After configuring the parameters, click the **View** button. For examples of the event log window, refer to Figure 31 on page 111 and Figure 32 on page 112.

Table 15. Display Filter Settings Parameters

Parameter	Definition
Log Location	Specifies the event log you want to view: The options are: Temporary (Memory) - Displays the event log stored in temporary memory. This log stores approximately 4,000 events. Select this option if the switch has been running for some time without a reset or power cycle. This is the default. Permanent (NVS) - Displays the event log stored in nonvolatile memory, which stores up to 2,000 events. Select this option to view the events that occurred prior to a recent reset or power cycle.
Severity Selections	Defines the severity of the events to be displayed. You can select more than one severity by using the Ctrl key when making your selections. The default is error, warning, and information events. The options are: D - Debug - Debug messages provide detailed high-volume information only intended for technical support personnel.

Table 15. Display Filter Settings Parameters

Parameter	Definition
Severity Selections (continued)	E - Error - Only error messages are displayed. Error messages indicate that the switch operation is severely impaired. W - Warning - Only warning messages are displayed. These messages indicate that an issue may require manager attention. I - Information - Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation. ALL - Messages of all severity levels are displayed.
Display Order	Controls the chronological order of the events in the display. The options are: Chronological - Lists the events starting with the oldest events. This is the default. Reverse Chronological - Lists the events starting with the most recent events.
Mode	Controls the format of the events in the display. The options are: Normal - Displays an event's time of occurrence, module originator, severity, and description for each event. This is the default. An example of Normal mode is shown in Figure 31 on page 111. Full - Displays the same information as Normal, plus the file name, line number, and event ID. An example of Full mode is shown in Figure 32 on page 112.
Module Selections	Specifies the AT-S63 software modules whose events will be displayed. The modules are listed in Table 16. You can select more than one module by using the Ctrl key as you make your selections. The default is All.

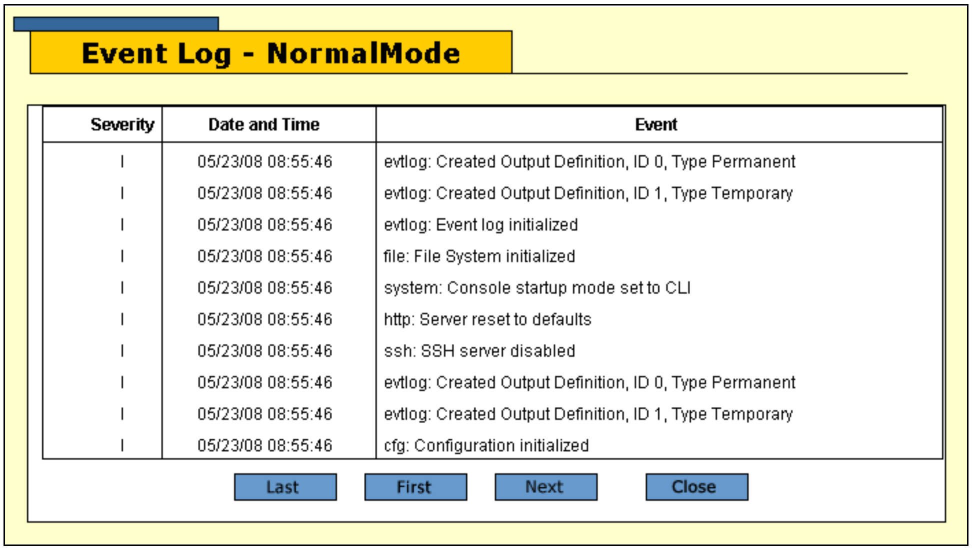
Table 16. AT-S63 Software Modules

Name	Description
ALL	All modules
ACL	Port access control lists
CFG	Switch configuration file
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
DOS	Denial of Service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP VLAN Registration Protocol
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
MLDSNOOP	MLD snooping
PACCESS	802.1X Port-based Access Control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RPS	Redundant power supply
RRP	RRP Snooping

Table 16. AT-S63 Software Modules

Name	Description
RTC	Real time clock
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	TELNET
TFTP	Trivial File Transfer Protocol
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

Figure 31 shows an example of an event log in Normal mode.

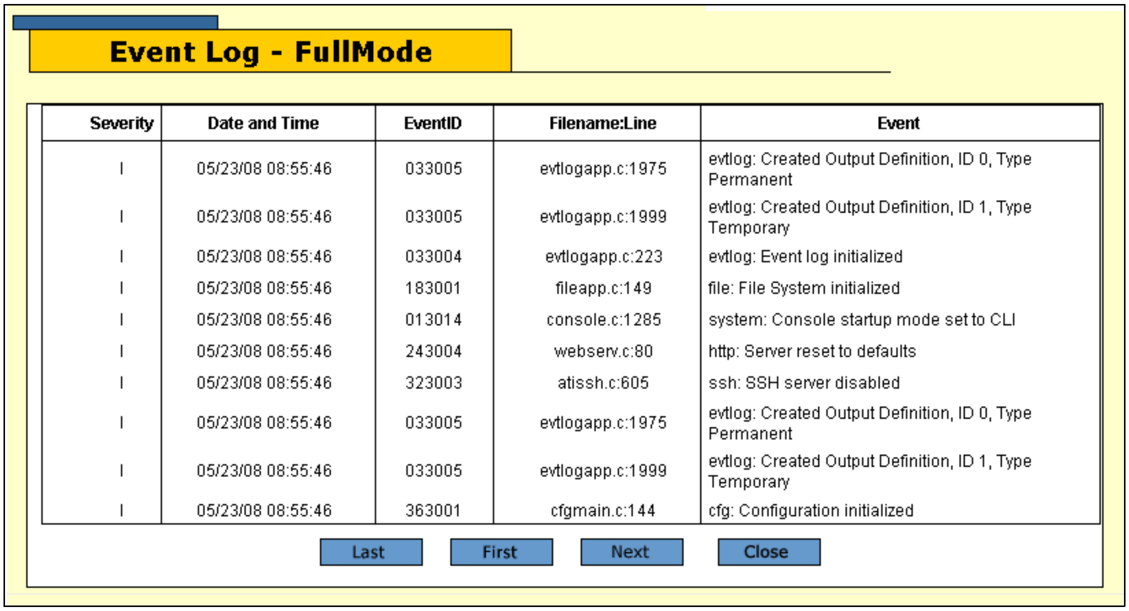


Event Log - NormalMode

Severity	Date and Time	Event
I	05/23/08 08:55:46	evtlog: Created Output Definition, ID 0, Type Permanent
I	05/23/08 08:55:46	evtlog: Created Output Definition, ID 1, Type Temporary
I	05/23/08 08:55:46	evtlog: Event log initialized
I	05/23/08 08:55:46	file: File System initialized
I	05/23/08 08:55:46	system: Console startup mode set to CLI
I	05/23/08 08:55:46	http: Server reset to defaults
I	05/23/08 08:55:46	ssh: SSH server disabled
I	05/23/08 08:55:46	evtlog: Created Output Definition, ID 0, Type Permanent
I	05/23/08 08:55:46	evtlog: Created Output Definition, ID 1, Type Temporary
I	05/23/08 08:55:46	cfg: Configuration initialized

Figure 31. Event Log Example Displayed in Normal Mode

An example of the Full mode is shown in Figure 32.



Severity	Date and Time	EventID	Filename:Line	Event
I	05/23/08 08:55:46	033005	evtlogapp.c:1975	evtlog: Created Output Definition, ID 0, Type Permanent
I	05/23/08 08:55:46	033005	evtlogapp.c:1999	evtlog: Created Output Definition, ID 1, Type Temporary
I	05/23/08 08:55:46	033004	evtlogapp.c:223	evtlog: Event log initialized
I	05/23/08 08:55:46	183001	fileapp.c:149	file: File System initialized
I	05/23/08 08:55:46	013014	console.c:1285	system: Console startup mode set to CLI
I	05/23/08 08:55:46	243004	webserv.c:80	http: Server reset to defaults
I	05/23/08 08:55:46	323003	atissh.c:605	ssh: SSH server disabled
I	05/23/08 08:55:46	033005	evtlogapp.c:1975	evtlog: Created Output Definition, ID 0, Type Permanent
I	05/23/08 08:55:46	033005	evtlogapp.c:1999	evtlog: Created Output Definition, ID 1, Type Temporary
I	05/23/08 08:55:46	363001	cfgmain.c:144	cfg: Configuration initialized

Figure 32. Event Log Example Displayed in Full Mode

The columns in the tables are described in Table 17:

Table 17. Event Log

Column	Definition
Severity	Displays the event’s severity, which can be one of the following: E - Error - Switch operation is severely impaired. W - Warning - An issue that may require network manager attention. I - Informational - Information that can be ignored during normal operation. D - Debug - Messages intended for technical support and software development.
Date and Time	The date and time of the event.
Event	This item contains two parts. The first is the name of the AT-S63 module that generated the event. The second is a description of the event.
Event ID (full mode only)	A unique, random number assigned to each event.

Table 17. Event Log

Column	Definition
Filename:Line (full mode only)	The originator of the event displayed as the name of the AT-S63 software source file and the line number.

Clearing an Event Log

To delete all of the event messages in a log:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **System** button.
3. Select the **Event Log** tab, shown in Figure 30 on page 106.
4. In the Log Settings section, click the radio button of the event log you want to clear.
5. Click the **Clear Log** check box.
6. Click the **Apply** button to delete the events in the log. If the event logs are enabled, the switch begins to store new events in the log.

Modifying an Event Log’s Full Action

This procedure is used to control the behavior of an event log when it reaches its maximum capacity of messages. This is referred to as an event log’s full action. An event log can either delete the oldest entries as it adds new entries or stop adding new entries to preserve the log contents.

Note
Event messages are sent to syslog servers even when the logs are full.

To configure the full action of an event log:

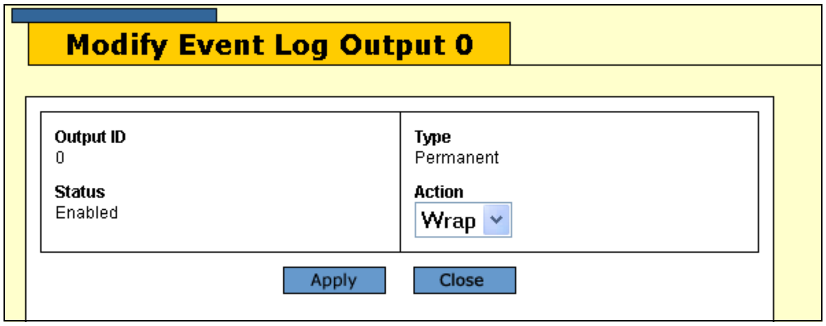
1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **System** button.

3. Select the **Event Log** tab, shown in Figure 30 on page 106.

4. Under Current Log Outputs, select Output 0, Permanent, to configure the log in permanent memory, or Output 1, Temporary, to configure the log in temporary memory.

5. Click the **Modify** button. An example of the Modify Event Log Output window is shown in Figure 33.



Output ID
0

Status
Enabled

Type
Permanent

Action
Wrap

Figure 33. Modify Event Log Output Window

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

   - Wrap - After reaching maximum capacity the log deletes the oldest entries to make room for new entries.
   - Halt - After reaching maximum capacity the log stops adding new entries to preserve the current messages.

7. Click the **Apply** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Saving an Event Log to a File

To save an event log as a file in the master switch’s file system:

1. From the Configuration menu, click the **System** button.

2. Click the **Event Log** tab, shown in Figure 30 on page 106.

3. Configure the parameters in the Display Filter Settings section of the tab to define the log events you want to save in the file. For instructions, refer to Table 15 on page 108.

4. Select the **Save Filename** field and enter a name for the file. The name can be up to 16 alphanumeric characters and must include the extension “.log”.

5. Click the **Save** button. The specified events are saved to the switch’s file system as an ASCII file.

6. To view the contents of the file, refer to “Listing the Files in Flash Memory or on a Compact Flash Card” on page 94. To upload the file to a TFTP server, refer to “Uploading a Configuration File or an Event Log File” on page 104. (To upload the file using Xmodem, you have to use a local management session.)

Configuring Syslog Output Definitions

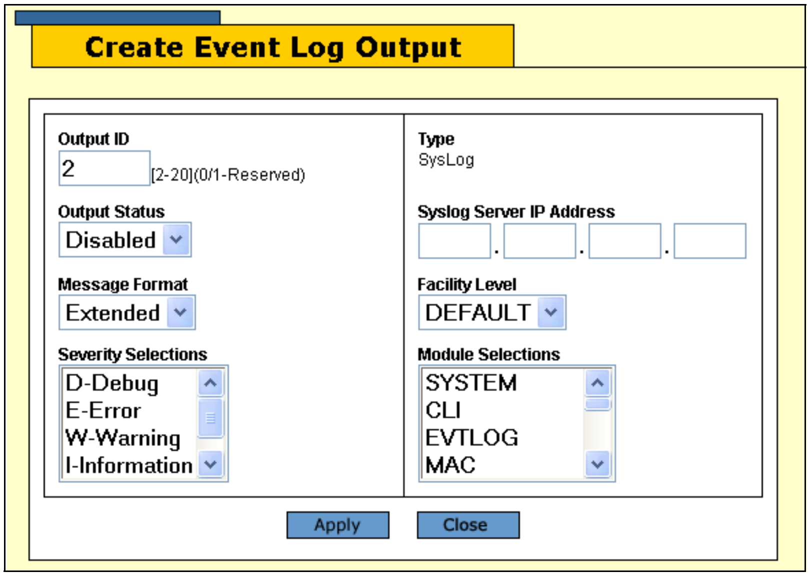
To create a syslog output definition for sending the event messages to a syslog server on your network:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **System** button.

3. Select the **Event Log** tab, shown in Figure 30 on page 106.

4. In the Configure Log Outputs section of the tab, click the **Create** button to display the Create Log Output page in Figure 34.



Create Event Log Output

Output ID

2 [2-20](0/1-Reserved)

Output Status

Disabled

Message Format

Extended

Severity Selections

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

Type

SysLog

Syslog Server IP Address

. . .

Facility Level

DEFAULT

Module Selections

SYSTEM
CLI
EVTLOG
MAC

Figure 34. Create Event Log Output Page

5. Configure the parameters in Table 18 as needed.

Table 18. Syslog Output Definition Parameters

Parameter	Definition
Output ID	Specifies a unique identification number for the syslog output definition. The range is 2 to 20. The default is the next available number.

Table 18. Syslog Output Definition Parameters

Parameter	Definition
Output Status	Sets the status of the syslog output definition. The options are: Enabled - The master switch uses the definition to send the event messages to the defined syslog server. Disabled - The master switch does not use the definition to send event messages.
Message Format	Controls the format of the event messages. The options are: Extended - The event messages contain the time, module, severity, description, file name, line number, and event ID. This is the default. Normal - The event messages contain just the time, module, severity, and description.
Severity Selections	Specifies the severity of the events to send to the syslog server. Use Ctrl key to select more than one severity. The options are: ALL - Sends all of the event messages. This is the default. Error - Sends just error event messages. Error messages indicate that the switch operation is severely impaired. Warning - Sends only warning event messages. These messages indicate that an issue may require manager attention. Information - Sends only informational event messages. Informational messages display useful information that you can ignore during normal operation. Debug - Sends debug event messages. These events provide detailed high-volume information intended only for technical support personnel.

Table 18. Syslog Output Definition Parameters

Parameter	Definition
Type	Sets the output definition's type. The only option is Syslog.
Syslog Server IP Address	Specifies the IP address of the syslog server.
Facility Level	Sets the numerical code the master switch adds to the entries when it sends them to the syslog server. The options are: Default - This setting uses the functional groupings defined in the RFC 3164 standard. local 1 through local 7 - These settings assign a specific identifier of 1 to 7 to the events.
Module Selections	Specifies the AT-S63 Management Software module(s) whose events are to be sent to the syslog server. To select more than one, use the Ctrl key when making your selections. The default is All. For a list of modules, refer to Table 16 on page 110.

6. Click the **Apply** button to create the new syslog output definition. If the status of the output definition is enabled, the switch immediately begins to send the event messages to the syslog server.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying Syslog Output Definitions

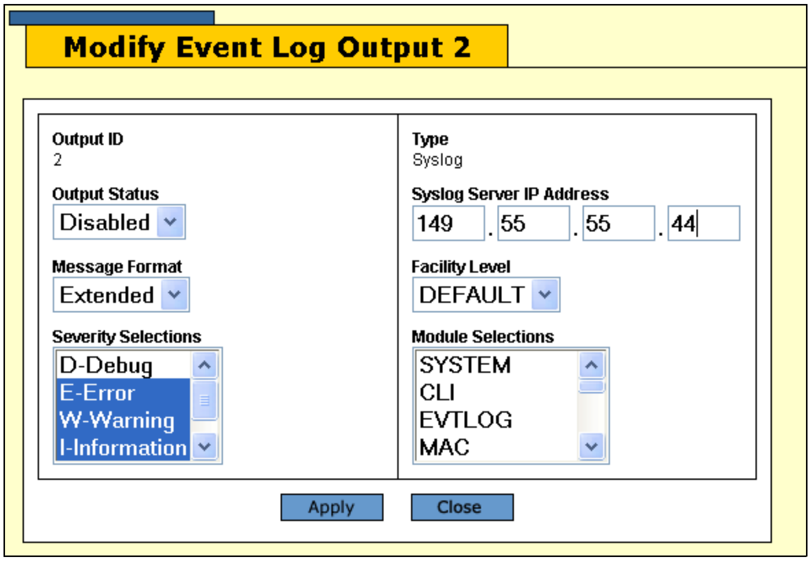
To modify a syslog output definition:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **System** button.

3. Select the **Event Log** tab, shown in Figure 30 on page 106.

4. In the Configure Log Outputs section of the tab, click the radio button of the log output file you want to modify and click the **Modify** button to display the Modify Event Log Output window. An example of the window is shown in Figure 35.



Modify Event Log Output 2

Output ID
2

Type
Syslog

Output Status
Disabled

Syslog Server IP Address
149 . 55 . 55 . 44

Message Format
Extended

Facility Level
DEFAULT

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

Module Selections
SYSTEM
CLI
EVTLOG
MAC

Figure 35. Modify Event Log Output Window

5. Modify the parameters as needed. The parameters are described in Table 18 on page 117.

6. Click the **Apply** button to apply your changes or the **Close** button to close the window without making changes.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting Syslog Output Definitions

To delete a syslog output definition:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **System** button.

3. Select the **Event Log** tab, shown in Figure 30 on page 106.

4. In the Configure Log Outputs section of the tab, click the radio button of the syslog output definition you want to delete and click the **Delete** button. You can delete only one definition at a time.

   The syslog output definition is deleted from the list and the switch stops sending log events to the syslog server.

5. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Chapter 10

IGMP Snooping

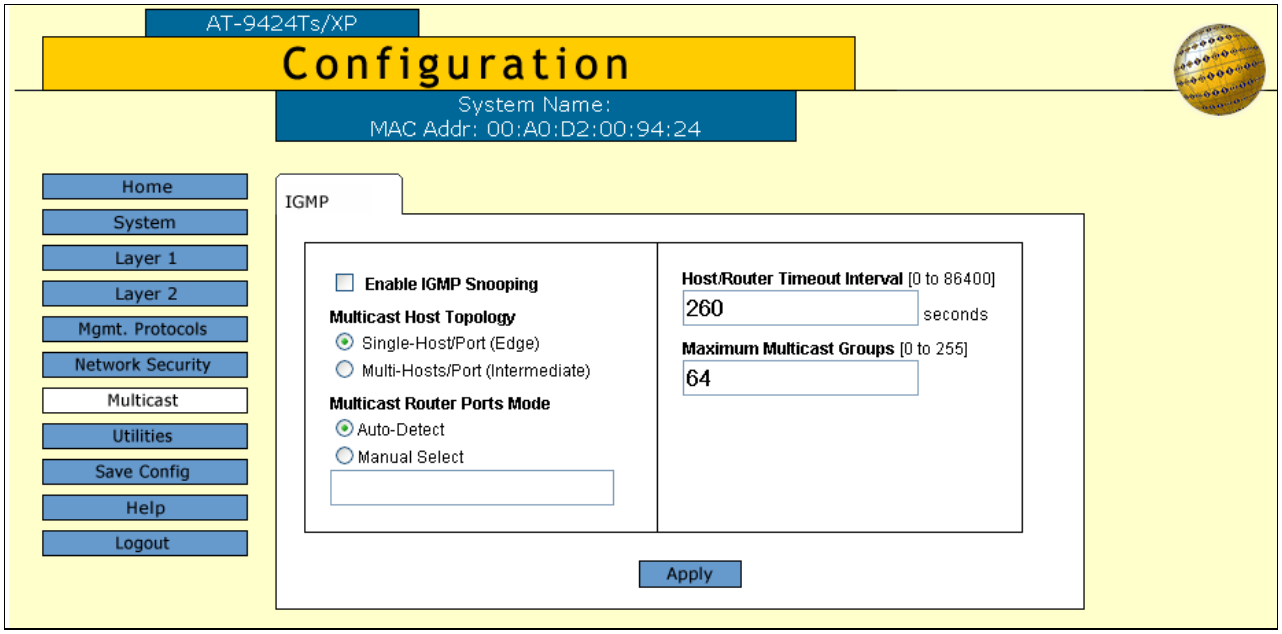
This chapter describes how to configure the IGMP snooping feature. The sections in the chapter include:

Configuring IGMP Snooping

To configure IGMP snooping:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Multicast** button to display the IGMP tab, shown in Figure 36.



AT-9424Ts/XP

System Name:
MAC Addr: 00:A0:D2:00:94:24

☐ **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 [0 to 255]
64

Figure 36. IGMP Tab

3. Configure the parameters, described in Table 19, as needed.

Table 19. IGMP Tab

Parameter	Definition
Enable IGMP Snooping Status	Enables and disables IGMP snooping on the stack. A check in the box indicates that IGMP snooping is enabled.
Multicast Host Topology	Defines whether there is only one host node per port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

Table 19. IGMP Tab

Parameter	Definition
Multicast Host Topology (continued)	The Single-Host/Port (Edge) setting is appropriate when there is only one host node connected to each port on the stack. At this setting the stack immediately stops sending multicast packets out a port when a host node sends a leave request to leave a multicast group or when the host node stops sending reports and times out. The stack 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 Multi-Host/Port (Intermediate) setting is appropriate if there is more than one host node connected to a port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. At this setting the stack 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 continue to receive the multicast packets. Only after all of the host nodes connected to a port have transmitted leave requests or have timed out does the stack stop sending multicast packets out the port. If a stack has a mixture of host nodes, that is, some connected directly to the stack and others through an Ethernet hub, you should select the Intermediate Multi-Host Port (Intermediate) selection.
Multicast Router Ports Mode	Specifies whether the router ports are determined automatically or if you enter them manually. If you want the stack 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. Port numbers are entered in this format: stack ID:port number

Table 19. IGMP Tab

Parameter	Definition
Host/Router Timeout Interval	Specifies the time period in seconds for determining inactive host nodes. 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. If you set the timeout to zero (0), the timeout interval is disabled and inactive host nodes are never timed out. This parameter also controls the time interval used to determine whether a multicast router is still active. The stack makes the determination by watching for queries from the router. If the stack does not detect any queries from a multicast router during the specified time interval, the router is considered inactive on the port. The actual timeout may be ten seconds less that the specified value. For example, a setting of 25 seconds can result in the stack classifying a host node or multicast router as inactive after just 15 seconds. A setting of 10 seconds or less can result in the immediate timeout of an inactive host node or router.
Maximum Multicast Groups	Specifies the maximum number of IGMP multicast groups the stack can learn. This parameter is useful with networks that contain a large number of multicast groups. The range is 0 to 255 groups. The default is 64 multicast groups. The combined number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

4. Click the **Apply** button.Your changes are immediately implemented on the stack.

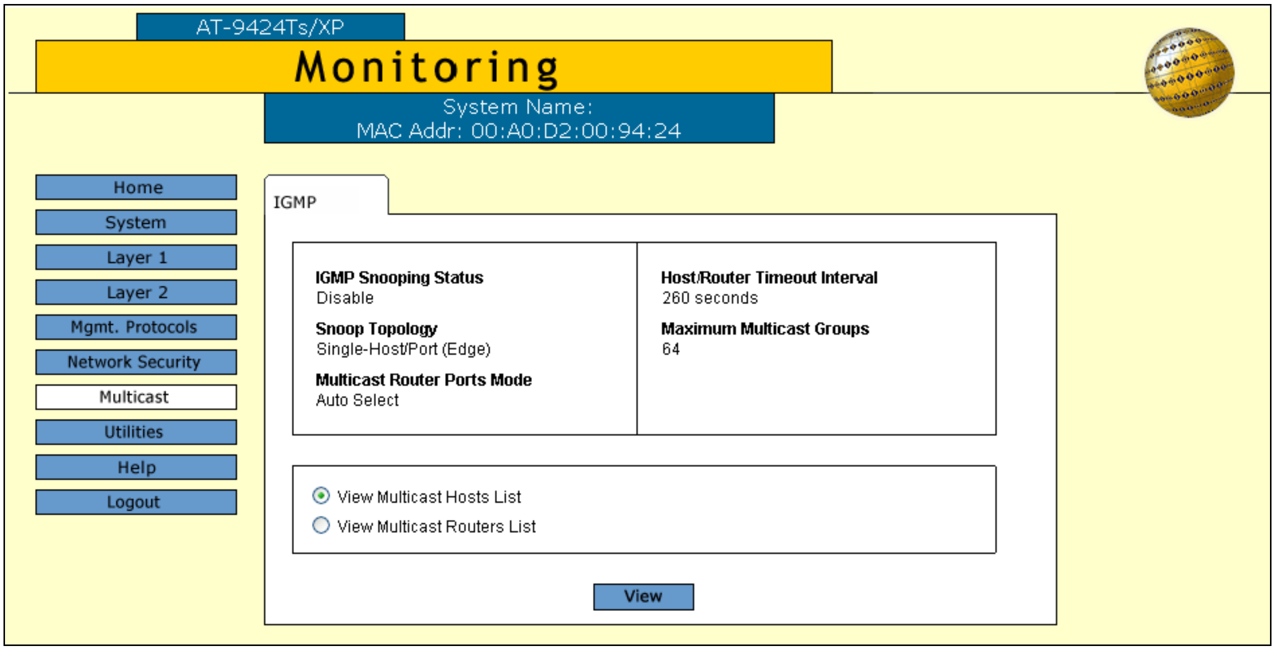
5. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying the Host Nodes and the Multicast Routers

To view the host nodes and the multicast routers connected to the ports on the stack:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Multicast** button to display the IGMP tab shown in Figure 37.



System Name:
MAC Addr: 00:A0:D2:00:94:24

IGMP Snooping Status
Disable

Snoop Topology
Single-Host/Port (Edge)

Multicast Router Ports Mode
Auto Select

Host/Router Timeout Interval
260 seconds

Maximum Multicast Groups
64

● View Multicast Hosts List
○ View Multicast Routers List

Figure 37. IGMP Tab (Monitoring)

The parameters in the tab are defined in Table 19 on page 124.

3. To view the multicast addresses and the host nodes, click the **View Multicast Hosts List** radio button and the **View** button. The contents of the window are described in this table.

Table 20. View Multicast Hosts List Window

Column	Definition
Multicast Group	The multicast address of the group.
VLAN ID	The VID of the VLAN where the port is an untagged member.

Table 20. View Multicast Hosts List Window

Column	Definition
Member Port/Trunk ID	Displays the port on the stack where the host node is connected. If the host node is connected to the stack through a trunk, the trunk ID number, not the port number, is displayed.
Host IP	Displays the IP address of the host node connected to the port.
Version	Displays the version of IGMP used by the host.
Exp. Time	Displays the number of seconds remaining before a host is timed out if no further IGMP reports are received from it.

4. To view the multicast routers, click the **View Multicast Router List** radio button and the **View** button. The contents of the window are described in this table.

Table 21. View Multicast Routers List Window

Column	Definition
Port	Displays the port on the stack where the multicast router is connected.
VLAN ID	Displays the VID of the VLAN in which the port is an untagged member.
Router IP	Displays the IP address of the port on the router.

Section III

SNMPv3

This section has the following chapter:

Chapter 11
SNMPv3

This chapter provides the following procedures for configuring SNMPv3 parameters using a web browser management session:

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to first enable SNMP access on the stack. Then you configure the SNMPv3 tables. See the following procedures:

- ❐ “Enabling or Disabling SNMP Management” on page 133
- ❐ “Configuring the SNMPv3 User Table” on page 134
- ❐ “Configuring the SNMPv3 View Table” on page 139
- ❐ “Configuring the SNMPv3 Access Table” on page 144
- ❐ “Configuring the SNMPv3 SecurityToGroup Table” on page 150
- ❐ “Configuring the SNMPv3 Notify Table” on page 154
- ❐ “Configuring the SNMPv3 Target Address Table” on page 158
- ❐ “Configuring the SNMPv3 Target Parameters Table” on page 163
- ❐ “Configuring the SNMPv3 Community Table” on page 168

Enabling or Disabling SNMP Management

Before you can manage a stack with SNMP, you have to enable SNMP access on the stack, as explained in this section. Furthermore, if you want the stack to send authentication failure traps when there is an unsuccessful login attempt, you also have to enable authentication failure traps.

To enable or disable SNMP access and authentication failure traps:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the **SNMP** tab, shown in Figure 11 on page 50.
3. Click the **Enable SNMP Access** check box to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the stack can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

   Note
   If the Enable SNMP Access check box is not checked, the stack cannot be managed through SNMP.

4. If you want the stack to send authentication failure traps, click the **Enable Authentication Failure Traps** check box. A check in the box indicates that the stack sends the trap.
5. Click the **Apply** button.
6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 User Table

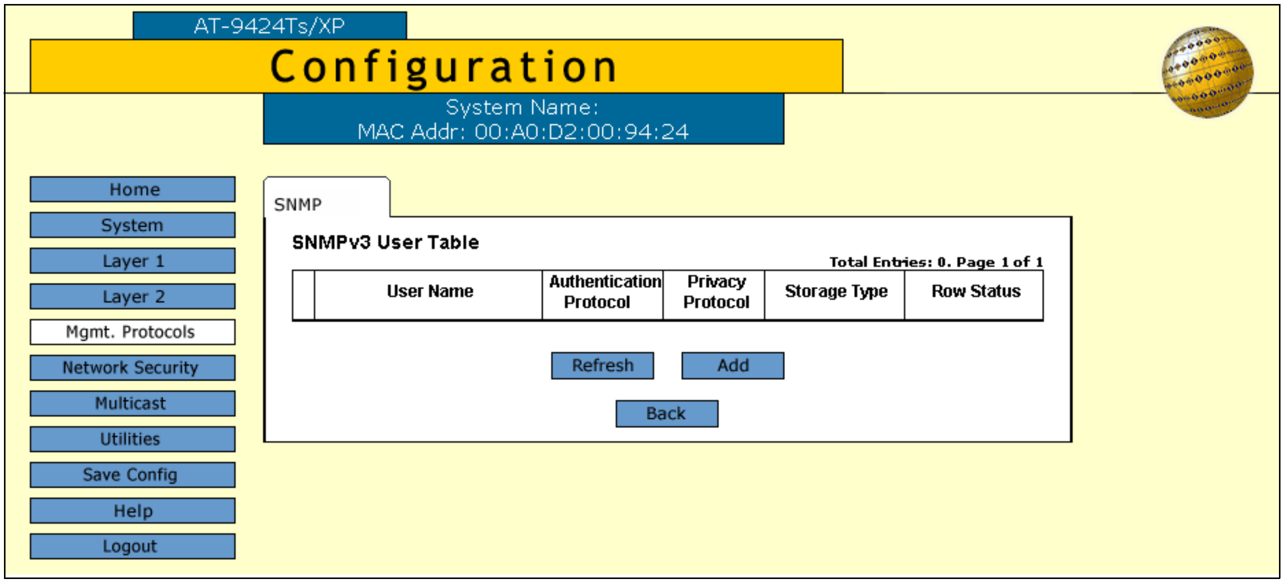
To create, delete, or modify SNMPv3 User Table entries, refer to the following procedures:

- “Creating a User Table Entry” on page 134
- “Deleting a User Table Entry” on page 137
- “Modifying a User Table Entry” on page 137

Creating a User Table Entry

To create an entry in the SNMPv3 User Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure User Table** and then the **Configure** button to display the SNMPv3 User Table tab in Figure 38.



System Name:
MAC Addr: 00:A0:D2:00:94:24

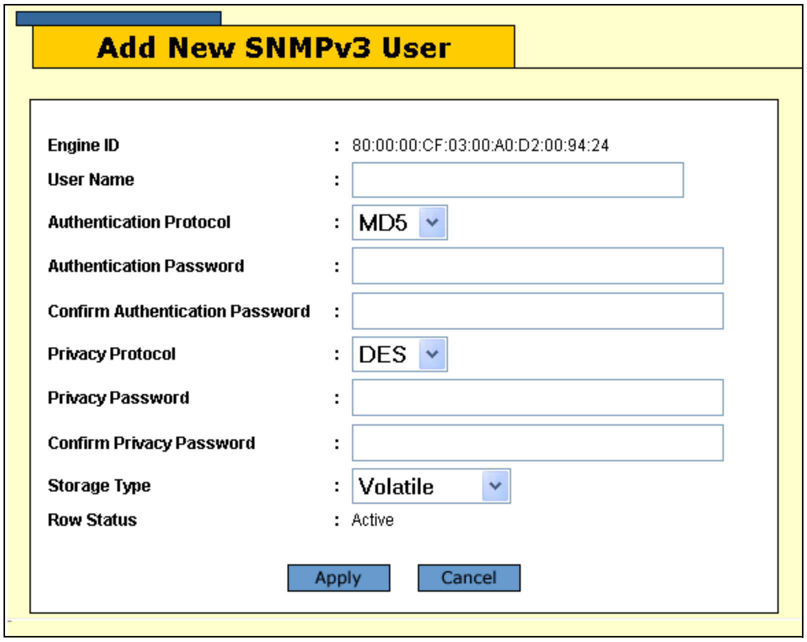
SNMPv3 User Table

Total Entries: 0. Page 1 of 1

	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status

Figure 38. SNMPv3 User Table Tab

4. Click the **Add** button to display the Add New SNMPv3 User window in Figure 39.



Add New SNMPv3 User

Engine ID	: 80:00:00:CF:03:00:A0:D2:00:94:24
User Name	:
Authentication Protocol	: MD5
Authentication Password	:
Confirm Authentication Password	:
Privacy Protocol	: DES
Privacy Password	:
Confirm Privacy Password	:
Storage Type	: Volatile
Row Status	: Active

Figure 39. Add New SNMPv3 User Page

5. Configure the parameters, described in Table 22, for the new entry and click the **Apply** button.

Table 22. SNMPv3 User Entry Parameters

Parameter	Description
User Name	A descriptive name of up to 32 alphanumeric characters for the user.
Authentication Protocol	The user’s authentication protocol. The possible values are: M-MD5 This value represents the MD5 authentication protocol. Users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol. S-SHA - This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

Table 22. SNMPv3 User Entry Parameters

Parameter	Description
Authentication Protocol (continued)	N-None - This value represents no authentication protocol. When messages are received, users are not authenticated. This selection does not support a Privacy Protocol. **Note** You may want to assign NONE to a super user.
Authentication Password Confirm Authentication Password	An authentication password of 8 to 32 alphanumeric characters. Applies only to MD5 and SHA authentication protocols. You must enter the same password in both fields.
Privacy Protocol	Applies only to MD5 and SHA authentication protocols. The possible values are: D-DES - This value makes the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the device are encrypted with the DES protocol. N-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 stack are not encrypted.
Privacy Password Confirm Privacy Password	A privacy password of 8 to 32 alphanumeric characters. Applies only to DES privacy protocol. You must enter the same password in both fields.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a User Table Entry

To delete an entry from the SNMPv3 User Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button next to **Configure User Table** and then click **Configure** to display the SNMPv3 User Table tab in Figure 38 on page 134.

4. Click the radio button of the User Table entry you want to delete and click the **Remove** button.

5. At the confirmation prompt, click the **OK** button.

6. To save your changes in the master configuration file, click the **Save Config** button.

Modifying a User Table Entry

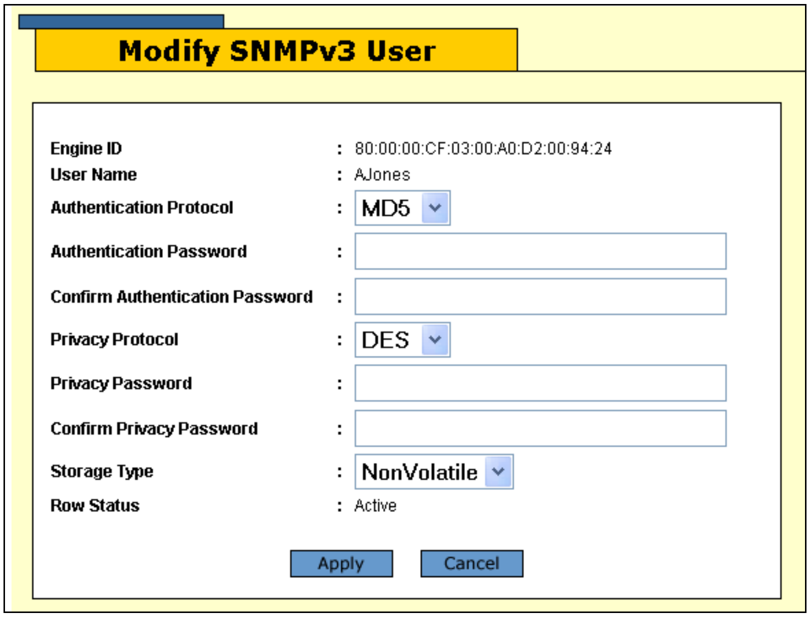
To modify an entry in the SNMPv3 User Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **Configure User Table** and then the **Configure** button to display the SNMPv3 User Table tab in Figure 38 on page 134.

4. Click the radio button of the SNMPv3 user entry you want to change and then click the **Modify** button. An example of the Modify SNMPv3 User window is shown in Figure 40.



Modify SNMPv3 User

Engine ID	:	80:00:00:CF:03:00:A0:D2:00:94:24
User Name	:	AJones
Authentication Protocol	:	MD5
Authentication Password	:	
Confirm Authentication Password	:	
Privacy Protocol	:	DES
Privacy Password	:	
Confirm Privacy Password	:	
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 40. Modify SNMPv3 User Page

5. Modify the parameters as needed. The parameters are described in Table 22 on page 135.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 View Table

To create, delete, or modify SNMPv3 View Table entries, refer to the following procedures:

- ❒ “Creating a View Table Entry” on page 139
- ❒ “Deleting a View Table Entry” on page 142
- ❒ “Modifying a View Table Entry” on page 142

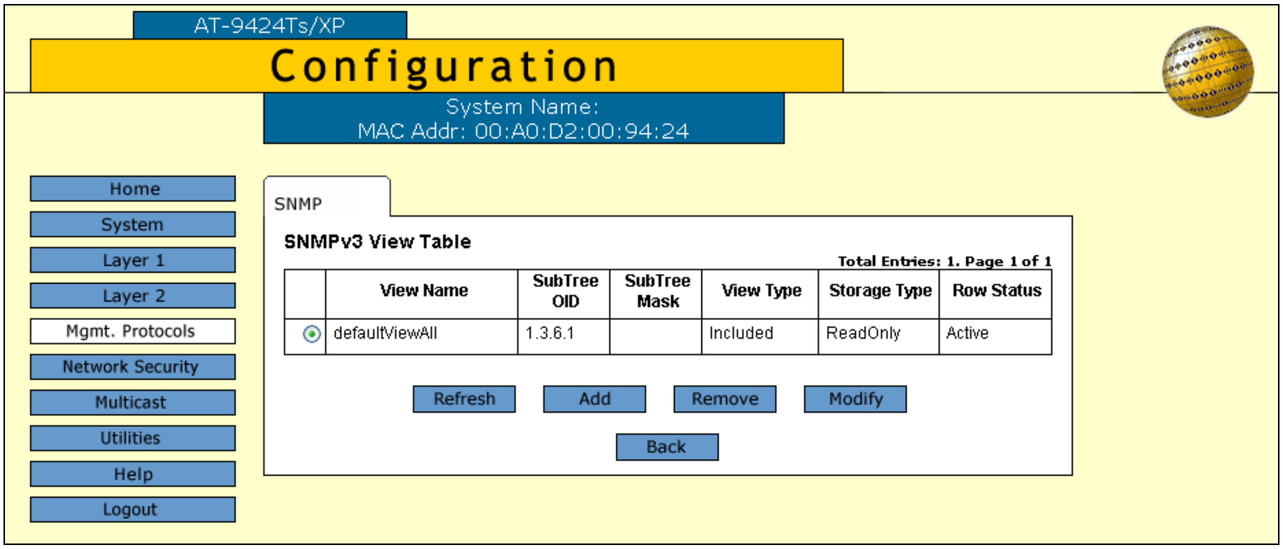
Creating a View Table Entry

To create an entry in the SNMPv3 View Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **Configure View Table** and then click the **Configure** to display the SNMPv3 View Table tab Figure 41.



System Name:
MAC Addr: 00:A0:D2:00:94:24

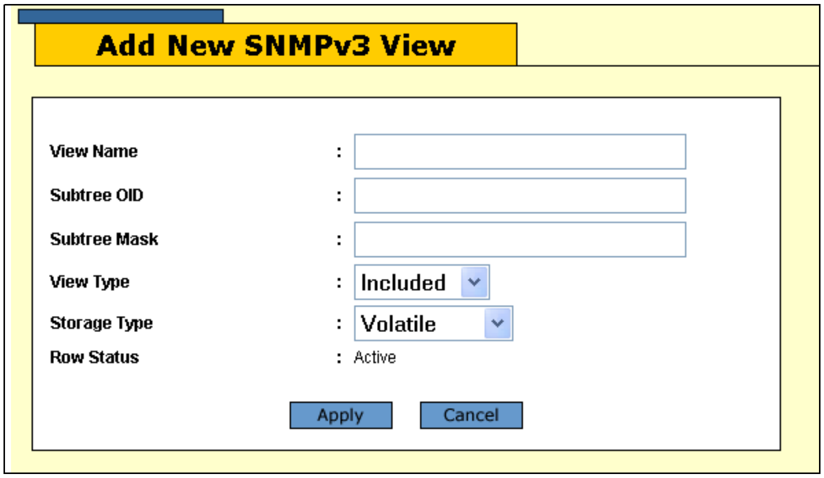
SNMPv3 View Table

Total Entries: 1. Page 1 of 1

	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
●	defaultViewAll	1.3.6.1		Included	ReadOnly	Active

Figure 41. SNMPv3 View Table Tab

4. Click the **Add** button to display the Add New SNMPv3 View page in Figure 42.



Add New SNMPv3 View

View Name	:	
Subtree OID	:	
Subtree Mask	:	
View Type	:	Included
Storage Type	:	Volatile
Row Status	:	Active

Figure 42. Add New SNMPv3 View Page

5. Configure the parameters, described in Table 23, for the new entry and click the **Apply** button.

Table 23. SNMPv3 View Table Parameters

Parameter	Description
View Name	A descriptive name for this view of up to 32 alphanumeric characters. **Note** The "defaultViewAll" value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use this default value for an SNMPv3 View Table entry.

Subtree OID	The 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 for TCP/IP is:
	`tcp`

Table 23. SNMPv3 View Table Parameters

Parameter	Description

Subtree Mask	A subtree mask in hexadecimal format. This is an optional parameter used to further refine the value in the View Subtree parameter. This parameter is in binary format.
	The relationship between a subtree mask and a subtree is similar to the relationship between an IP address and a subnet mask. The subnet mask further refines the IP address. In the same way, the OID table entry defines a MIB View and the subtree mask further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB, ifEntry.0.3 has the following value:
	`1.3.6.1.2.1.2.2.1.0.3`
	To restrict the user's view to the third row (all columns) of the ifEntry MIB, enter the following value for the Subtree Mask parameter
	`ff:bf`

View Type	The possible values are: I-Included - Enter this value to permit the View Name to see the subtree specified above. E-Excluded - Enter this value to not permit the View Name to see the subtree specified above.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a View Table Entry

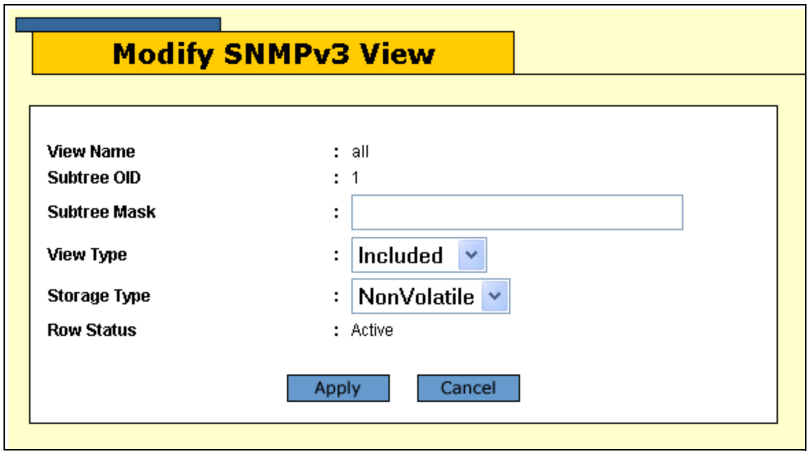
To delete an entry from the SNMPv3 View Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure View Table** and then the **Configure** button to display the SNMPv3 View Table tab in Figure 41 on page 139.
4. Click the radio button for the View Table entry you want to delete and then click the **Remove** button.
5. At the confirmation prompt, click the **OK** button.
6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying a View Table Entry

To modify an entry in the SNMPv3 View Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure View Table** and the **Configure** button to display the SNMPv3 View Table tab in Figure 41 on page 139.
4. Click the radio button of the SNMPv3 View Table entry you want to change and then click the **Modify** button. An example of the Modify SNMPv3 View page is shown in Figure 43.



Modify SNMPv3 View

View Name : all
Subtree OID : 1
Subtree Mask :
View Type : Included
Storage Type : NonVolatile
Row Status : Active

Figure 43. Modify SNMPv3 View Page

5. Modify the parameters as needed. The parameters are described in Table 23 on page 140.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 Access Table

To create, delete, or modify SNMPv3 Access Table entries, refer to the following procedures:

- "Creating an Access Table" on page 144
- "Deleting an Access Table Entry" on page 148
- "Modifying an Access Table Entry" on page 148

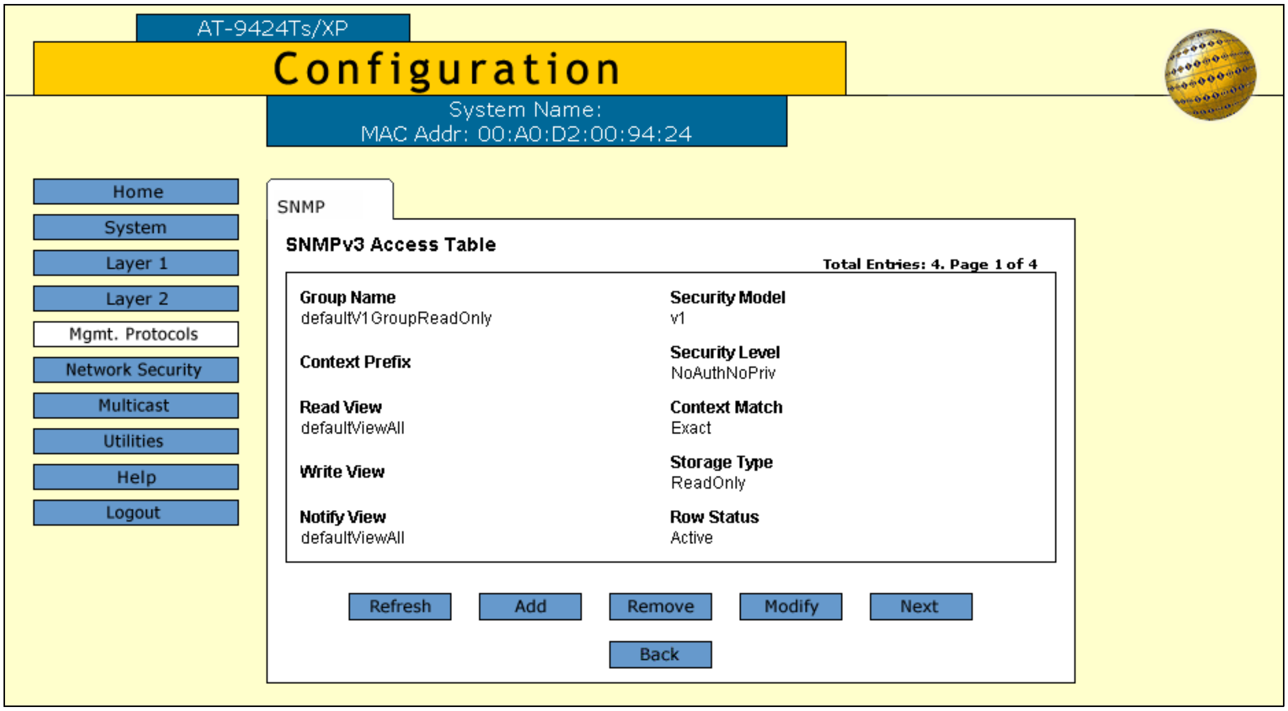
Creating an Access Table

To create an entry in the SNMPv3 Access Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for the **Configure Access Table** and the click the **Configure** button to display the SNMPv3 Access Table tab in Figure 44.



System Name:
MAC Addr: 00:A0:D2:00:94:24

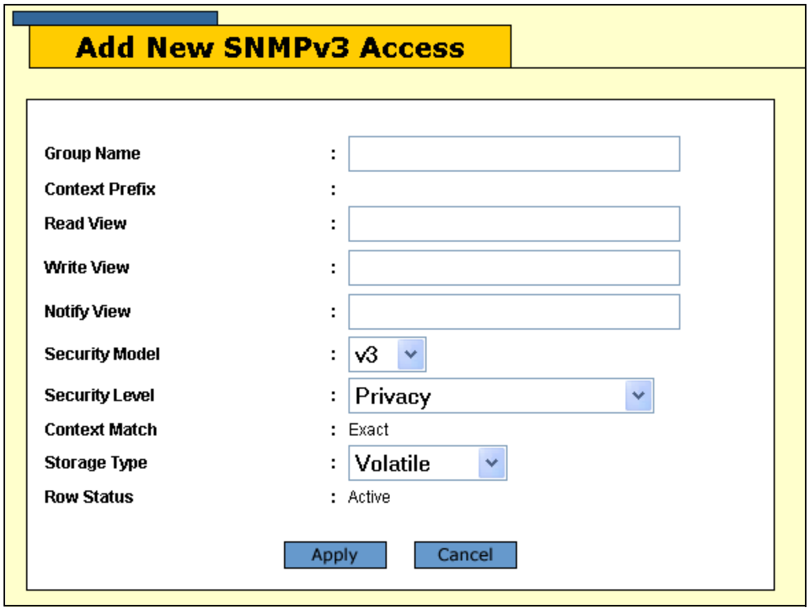
SNMPv3 Access Table

Total Entries: 4. Page 1 of 4

Group Name defaultV1GroupReadOnly	**Security Model** v1
Context Prefix	**Security Level** NoAuthNoPriv
Read View defaultViewAll	**Context Match** Exact
Write View	**Storage Type** ReadOnly
Notify View defaultViewAll	**Row Status** Active

Figure 44. SNMPv3 Access Table Tab

4. To create an SNMPv3 Access Table entry, click the **Add** button to display the Add New SNMPv3 Access window in Figure 45.



Add New SNMPv3 Access

Group Name :
Context Prefix :
Read View :
Write View :
Notify View :
Security Model : v3
Security Level : Privacy
Context Match : Exact
Storage Type : Volatile
Row Status : Active

Figure 45. Add New SNMPv3 Access Window

5. Configure the parameters, described in Table 24, for the new entry and click the **Apply** button.

Table 24. SNMPv3 Access Table Parameters

Parameter	Description
Group Name	A descriptive name for the group 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, unique group names allow you to more easily distinguish the difference groups. There are four default values for this field: ❒ defaultV1GroupReadOnly ❒ defaultV1GroupReadWrite ❒ defaultV2cGroupReadOnly ❒ defaultV2cGroupReadWrite These values are reserved for SNMPv1 and SNMPv2c implementations.
Context Prefix	This parameter is preset to null. It cannot be changed.

Table 24. SNMPv3 Access Table Parameters

Parameter	Description
Read View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table. A Read View Name 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.
Write View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table. A Write View Name 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.
Notify View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table. A Notify View Name allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.
Security Model	The possible values are: Select one of the following SNMP protocols as the Security Model for this Group Name. 1-v1 - Select this value to associate the Group Name with the SNMPv1 protocol. 2-v2c - Select this value to associate the Group Name with the SNMPv2c protocol. 3-v3 - Select this value to associate the Group Name with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 entities (users) and encrypt messages.
Security Level	The possible values are: No Authentication/Privacy - This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Table 24. SNMPv3 Access Table Parameters

Parameter	Description
Security Level (continued)	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 encrypt messages using a privacy protocol and authenticate SNMP entities. 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 only security level for SNMPv1 and SNMPv2c is No Authentication/Privacy.
Context Match	This parameter is preset to exact and cannot be changed.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting an Access Table Entry

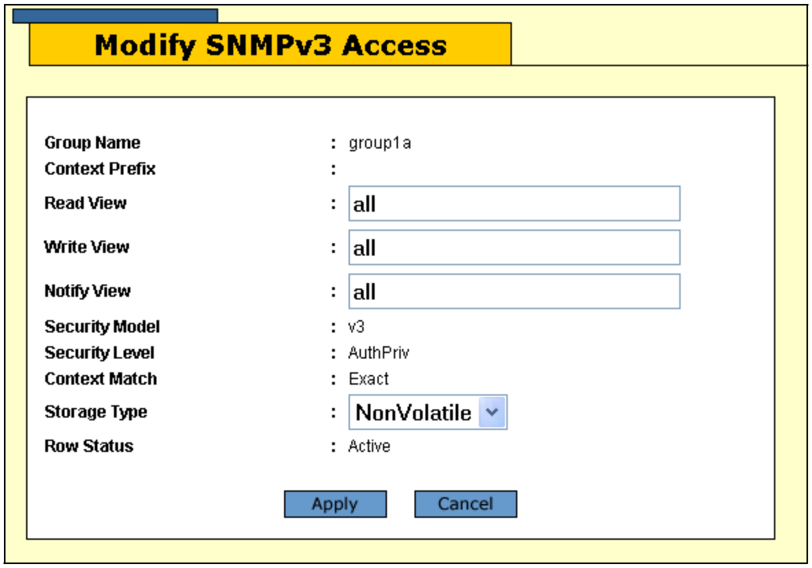
To delete an entry from the SNMPv3 Access Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure Access Table** and then the **Configure** button to display the SNMPv3 Access Table tab in Figure 44 on page 144.
4. Toggle through the access table entries using the **Next** and **Previous** buttons to display the entry you want to delete.
5. Click the **Remove** button.
6. At the confirmation prompt, click the **OK** button.
7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click the **Configure** button to display the SNMPv3 Access Table tab in Figure 44 on page 144.
4. Toggle through the access table entries using the **Next** and **Previous** buttons to display the entry you want to modify.
5. Click the **Modify** button to display the entry’s Modify SNMPv3 Access window. An example of the window is shown in Figure 46.



Modify SNMPv3 Access

Group Name	:	group1a
Context Prefix	:	
Read View	:	all
Write View	:	all
Notify View	:	all
Security Model	:	v3
Security Level	:	AuthPriv
Context Match	:	Exact
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 46. Modify SNMPv3 Access Window

6. Modify the parameters as needed. The parameters are described in Table 24 on page 145.

7. After modifying the entry, click the **Apply** button.

8. At the confirmation prompt, click the **OK** button.

9. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 SecurityToGroup Table

To create, delete, or modify SNMPv3 SecurityToGroup Table entries, refer to the following procedures:

- ❐ "Creating a SecurityToGroup Table Entry" on page 150
- ❐ "Deleting a SecurityToGroup Table Entry" on page 152
- ❐ "Modifying a SecurityToGroup Table Entry" on page 153

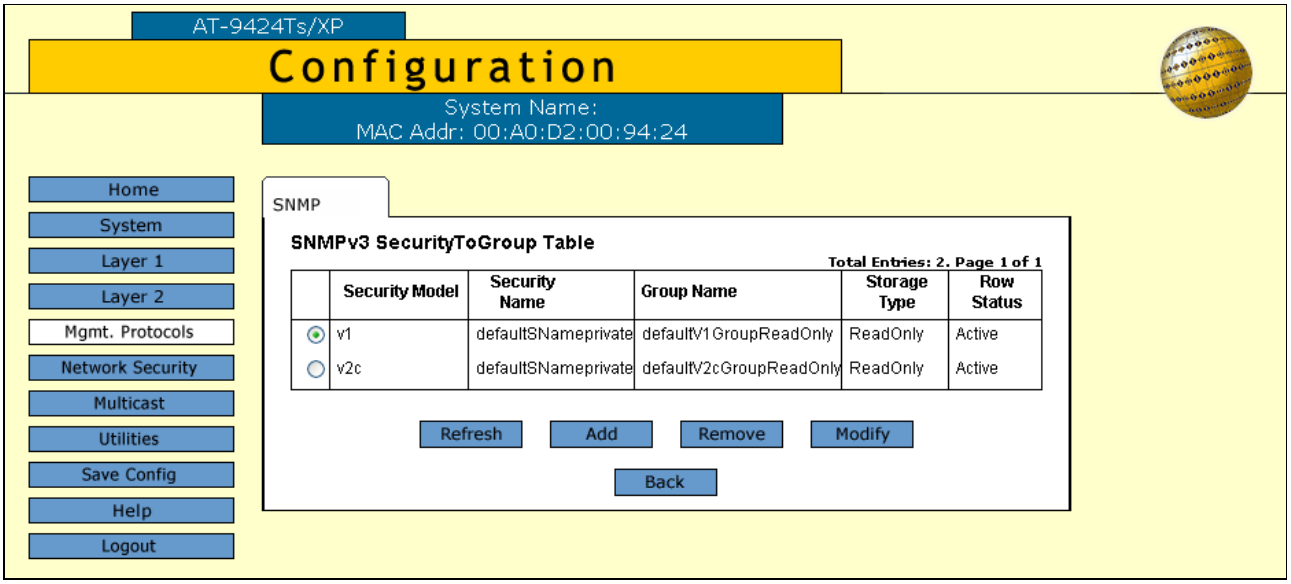
Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for the **Configure SecurityToGroup Table** and then the **Configure** button to display the SNMPv3 SecurityToGroup Table tab in Figure 47.



AT-9424Ts/XP

Configuration

System Name:
MAC Addr: 00:A0:D2:00:94:24

SNMP

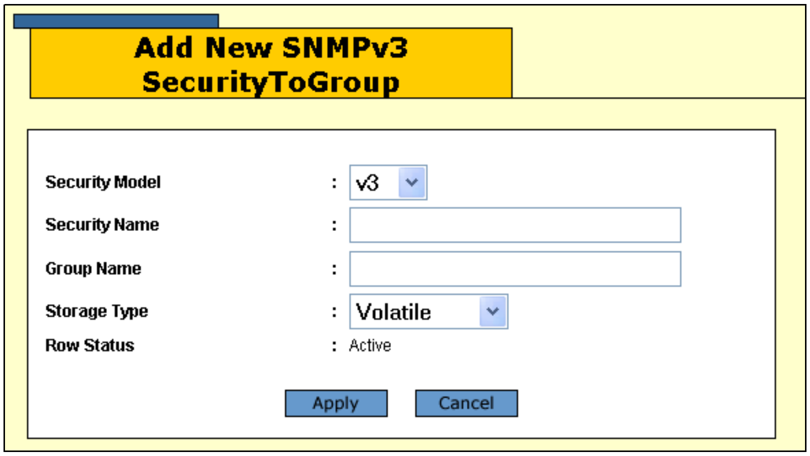
SNMPv3 SecurityToGroup Table

Total Entries: 2. Page 1 of 1

	Security Model	Security Name	Group Name	Storage Type	Row Status
●	v1	defaultSNameprivate	defaultV1GroupReadOnly	ReadOnly	Active
○	v2c	defaultSNameprivate	defaultV2cGroupReadOnly	ReadOnly	Active

Figure 47. SNMPv3 SecurityToGroup Table Tab

4. To create an SNMPv3 SecurityToGroup Table entry, click the **Add** button to display the Add New SNMPv3 SecurityToGroup page in Figure 48.



Add New SNMPv3 SecurityToGroup

Security Model : v3

Security Name :

Group Name :

Storage Type : Volatile

Row Status : Active

Figure 48. Add New SNMPv3 SecurityToGroup Page

5. Configure the parameters, described in Table 25, for the new entry and click the **Apply** button.

Table 25. SNMPv3 Security to Group Table Parameters

Parameter	Description
Security Model	The corresponding SNMP protocol of the User Name. The possible values are: 1-v1 - Select this value to associate the Group Name with the SNMPv1 protocol. 2-v2c - Select this value to associate the Group Name with the SNMPv2c protocol. 3-v3 - Select this value to associate the Group Name with the SNMPv3 protocol.
Security Name	The Security Name that you want to associate with a group. Enter a Security Name that you configured in “Configuring the SNMPv3 User Table” on page 134.

Table 25. SNMPv3 Security to Group Table Parameters

Parameter	Description
Group Name	A Group Name that you configured in the SNMPv3 Access Table. Refer to “Configuring the SNMPv3 Access Table” on page 144. There are four default values for this field: ❐ defaultV1GroupReadOnly ❐ defaultV1GroupReadWrite ❐ defaultV2cGroupReadOnly ❐ defaultV2cGroupReadWrite These values are reserved for SNMPv1 and SNMPv2c implementations.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a SecurityToGroup Table Entry

To delete an entry from the SNMPv3 SecurityToGroup Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure SecurityToGroup Table**, and then click the **Configure** button to display the SNMPv3 SecurityToGroup Table tab in Figure 47 on page 150.
4. Click the radio button of the SecurityToGroup Table entry you want to delete and then click the **Remove** button.
5. At the confirmation prompt, click the **OK** button.

6. To save your changes in the master configuration file, click the **Save Config** button.

Modifying a SecurityToGroup Table Entry

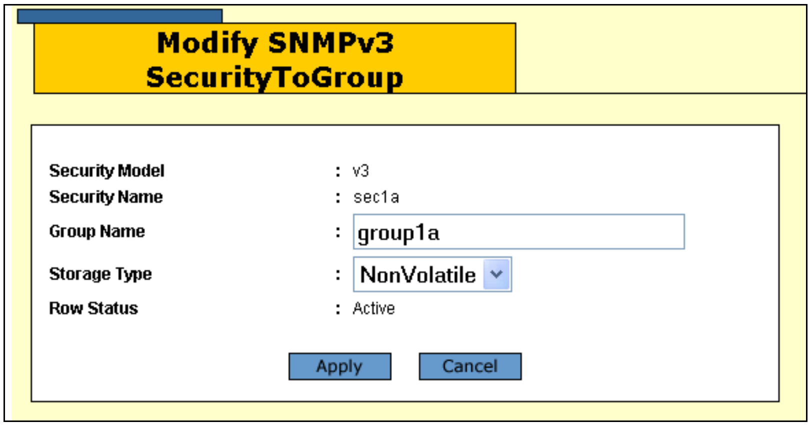
To modify an entry in the SNMPv3 SecurityToGroup Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for the **Configure SecurityToGroup Table** and then click the **Configure** button to display the SNMPv3 SecurityToGroup Table tab, shown in Figure 47 on page 150.

4. Click the radio button of the SecurityToGroup Table entry you want to change, and then click the **Modify** button to display the Modify SNMPv3 SecurityToGroup window for the entry. An example of the window is shown in Figure 49.



Security Model	: v3
Security Name	: sec1a
Group Name	: group1a
Storage Type	: NonVolatile
Row Status	: Active

Figure 49. Modify SNMPv3 SecurityToGroup Window

5. Modify the parameters as needed. The parameters are described in Table 25 on page 151.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 Notify Table

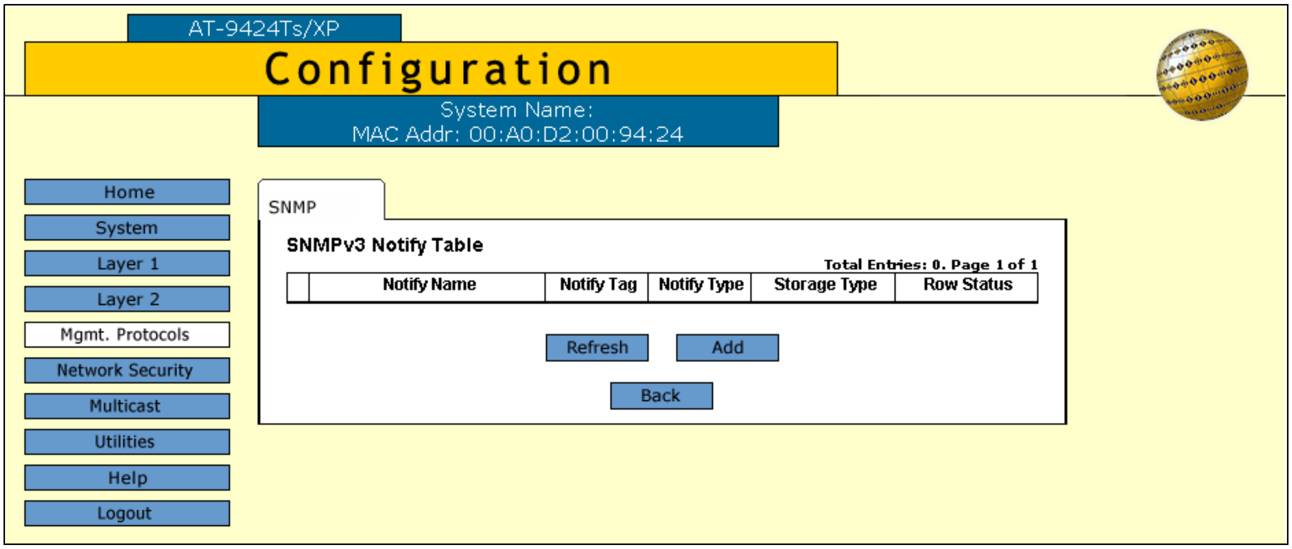
Here are the procedures for managing the SNMPv3 Notify Table:

- "Creating a Notify Table Entry" on page 154
- "Deleting a Notify Table Entry" on page 156
- "Modifying a Notify Table Entry" on page 156

Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure Notify Table**, and the **Configure** button to display the SNMPv3 Notify Table tab, shown in Figure 50.



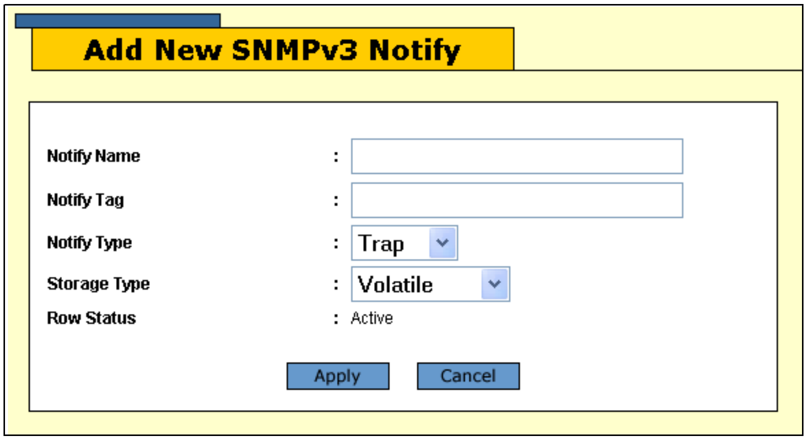
SNMPv3 Notify Table

Total Entries: 0. Page 1 of 1

	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status

Figure 50. SNMPv3 Notify Table Tab

4. Click the **Add** button to display the Add New SNMPv3 Notify page in Figure 51.



Add New SNMPv3 Notify

Notify Name :
Notify Tag :
Notify Type : Trap
Storage Type : Volatile
Row Status : Active

Figure 51. Add New SNMPv3 Notify Page

5. Configure the parameters, described in Table 26, for the new entry and click the **Apply** button.

Table 26. SNMPv3 Notify Table Parameters

Parameter	Description
Notify Name	The name to be associated with this trap message. The name can be up to 32 alphanumeric characters. For example, you might define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.
Notify Tag	The name of a Notify Tag. The name can be up to 32 alphanumeric characters. This parameter is added to the Tag List parameter in the SNMPv3 Target Address Table, which defines the IP addresses of the devices to receive the traps or inform messages.
Notify Type	The possible values are: T-Trap - This option sends traps. SNMPv3 does not expect hosts to respond to traps. I-Inform - This option sends inform messages. SNMPv3 expects hosts to respond to inform messages.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off.

Table 26. SNMPv3 Notify Table Parameters

Parameter	Description
Storage Type (continued)	N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a Notify Table Entry

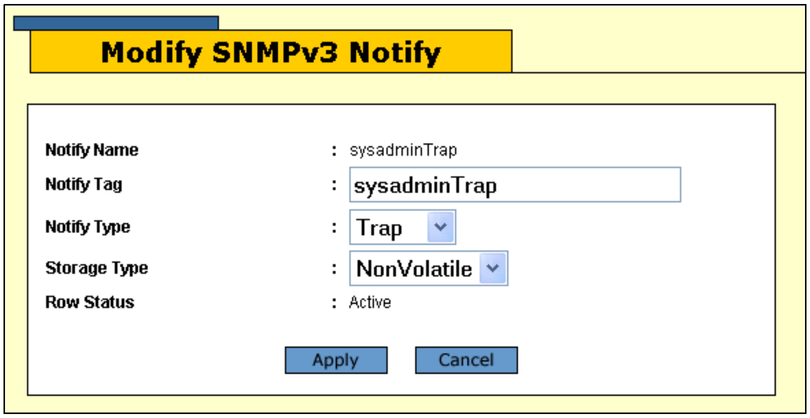
To delete an entry from the SNMPv3 Notify Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure Notify Table**, and the **Configure** button to display the SNMPv3 Notify Table tab in Figure 50 on page 154.
4. Click the radio button for the Notify Table entry you want to delete, and then click **Remove**.
5. At the confirmation prompt, click the **OK** button.
6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying a Notify Table Entry

To modify an entry in the SNMPv3 Notify Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure Notify Table**, and then click the **Configure** button to display the SNMPv3 Notify Table tab in Figure 50 on page 154.
4. Click the radio button of the table entry you want to change and then click the **Modify** button to display the Modify SNMPv3 Notify window. An example of the window is shown in Figure 52.



Notify Name	:	sysadminTrap
Notify Tag	:	sysadminTrap
Notify Type	:	Trap
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 52. Modify SNMPv3 Notify Page

5. Modify the parameters as needed. The parameters are described in Table 26 on page 155.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 Target Address Table

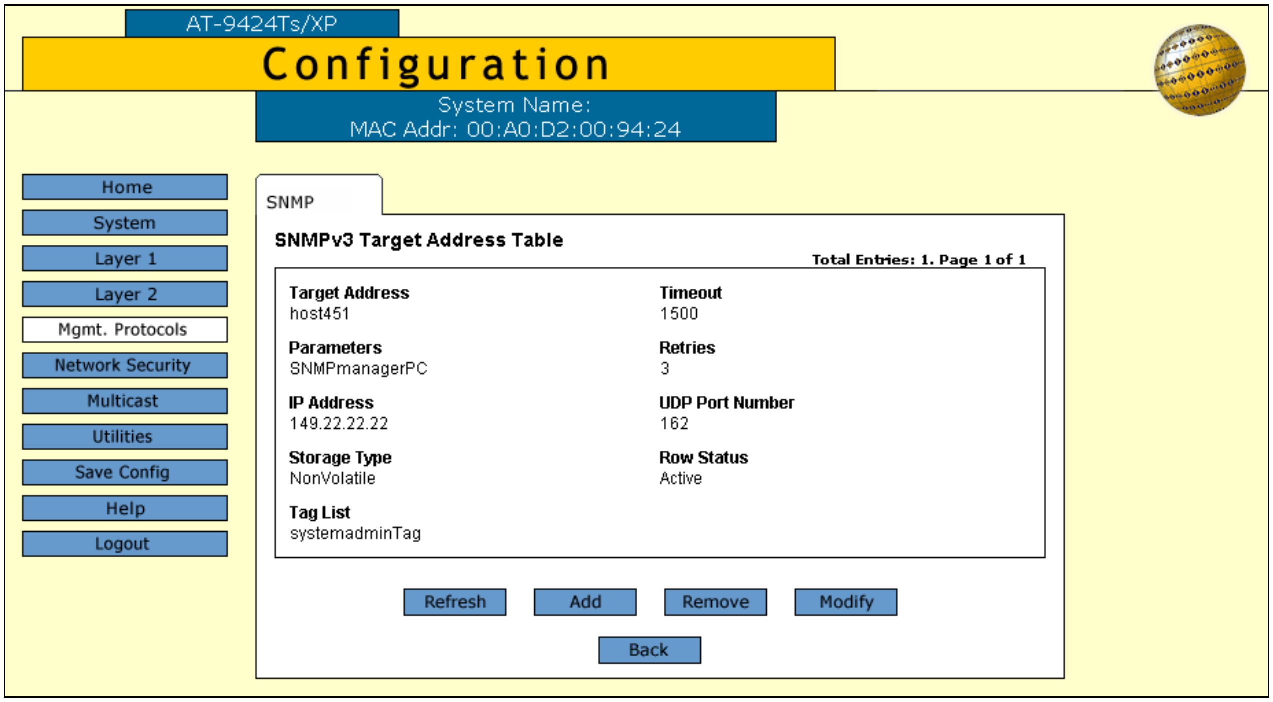
Here are the procedures for managing the SNMPv3 Target Address Table:

- "Creating a Target Address Table Entry" on page 158
- "Deleting a Target Address Table Entry" on page 160
- "Modifying a Target Address Table Entry" on page 161

Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the button next to the **Configure Target Address Table**, and then click the **Configure** button to display the SNMPv3 Target Address Table tab shown in Figure 53.



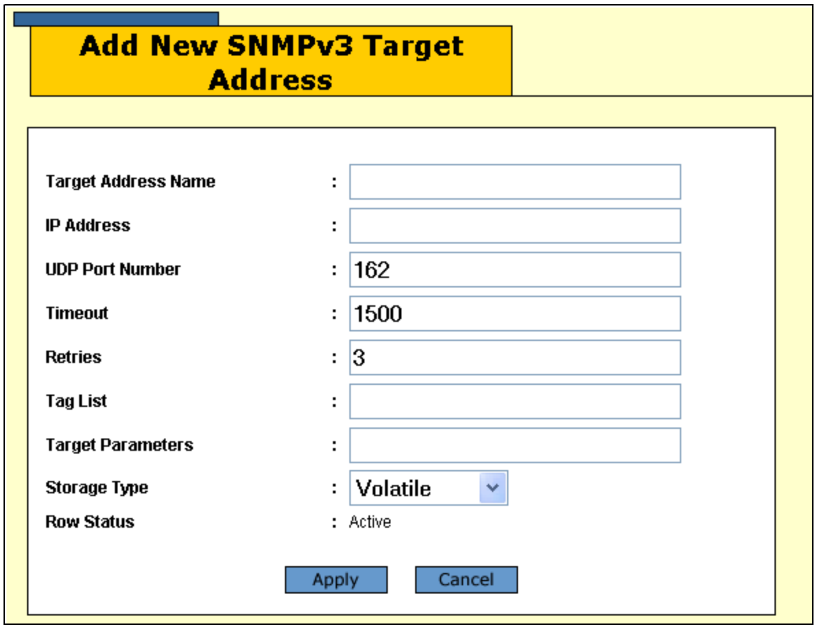
SNMPv3 Target Address Table

Total Entries: 1. Page 1 of 1

Target Address host451	**Timeout** 1500
Parameters SNMPmanagerPC	**Retries** 3
IP Address 149.22.22.22	**UDP Port Number** 162
Storage Type NonVolatile	**Row Status** Active
Tag List systemadminTag	

Figure 53. SNMPv3 Target Address Table Tab

4. Click the **Add** button to display the Add New SNMPv3 Target Address window in Figure 54.



Add New SNMPv3 Target Address

Target Address Name	:	
IP Address	:	
UDP Port Number	:	162
Timeout	:	1500
Retries	:	3
Tag List	:	
Target Parameters	:	
Storage Type	:	Volatile
Row Status	:	Active

Figure 54. Add New SNMPv3 Target Address Window

5. Configure the parameters, described in Table 27, for the new entry and click the **Apply** button.

Table 27. SNMPv3 Target Address Table Parameters

Parameter	Description
Target Address Name	The name of the SNMP manager, or host, that manages the SNMP activity on the stack. The name can be up to 32 alphanumeric characters.
IP Address	The IP address of the host. The IP address is entered in this format: XXX.XXX.XXX.XXX
UDP Port Number	The UDP port. The range is 0 to 65,535. The default port is 162.
Timeout	The timeout value in milliseconds. When an Inform message is generated, a response from the device is required. The timeout value determines how long SNMPv3 considers the Inform message as 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.

Table 27. SNMPv3 Target Address Table Parameters

Parameter	Description
Retries	The number of times the stack retrIes, or resends, an Inform message. When an Inform message is generated, a response from the stack is required. This parameter determines how many times the stack resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.
Tag List	The tag or list of tags defined by the Notify Tag parameter in the corresponding entry in the SNMPv3 Notify Table. The tag list can be up to 256 alphanumeric characters. Separate entries with spaces, for example: `hwengtag swengtag testengtag`
Target Parameters	The corresponding Target Parameters name. This value has to match the name of the corresponding entry in the SNMPv3 Target Parameters Table.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a Target Address Table Entry

To delete an entry from the SNMPv3 Target Address Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **Configure Target Address Table** and then click the **Configure** button to display the SNMPv3 Target Address Table tab, shown in Figure 53 on page 158.

4. Toggle through the entries with the **Next** and **Previous** buttons until the table displays the entry you want to delete.

5. Click the **Remove** button.

6. At the confirmation prompt, click the **OK** button.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying a Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table:

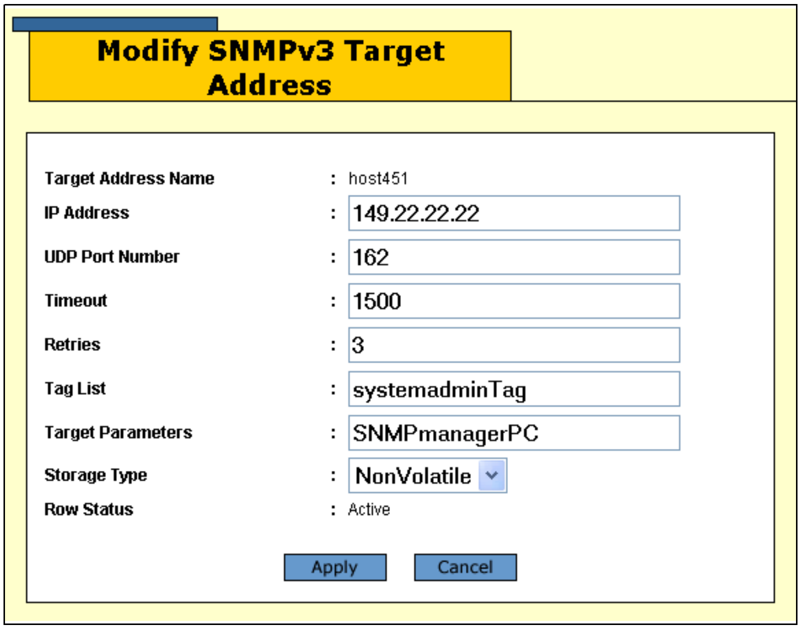
1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for the **Configure Target Address Table** and then click the **Configure** button to display the SNMPv3 Target Address Table tab in Figure 53 on page 158.

4. Toggle through the entries with the **Next** and **Previous** buttons until the table displays the entry you want to modify.

5. Click the **Modify** button to display the Modify SNMPv3 Target Address window. An example of the window is shown in Figure 55.



Target Address Name	:	host451
IP Address	:	149.22.22.22
UDP Port Number	:	162
Timeout	:	1500
Retries	:	3
Tag List	:	systemadminTag
Target Parameters	:	SNMPmanagerPC
Storage Type	:	NonVolatile
Row Status	:	Active

Figure 55. Modify SNMPv3 Target Address Page

6. Modify the parameters, described in Table 27 on page 159, as needed.

7. After modifying the entry, click the **Apply** button.

8. At the confirmation prompt, click the **OK** button.

9. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 Target Parameters Table

Here are the procedures for managing the SNMPv3 Target Parameters Table:

- “Creating a Target Address Table Entry” on page 158
- “Deleting a Target Address Table Entry” on page 160
- “Modifying a Target Address Table Entry” on page 161

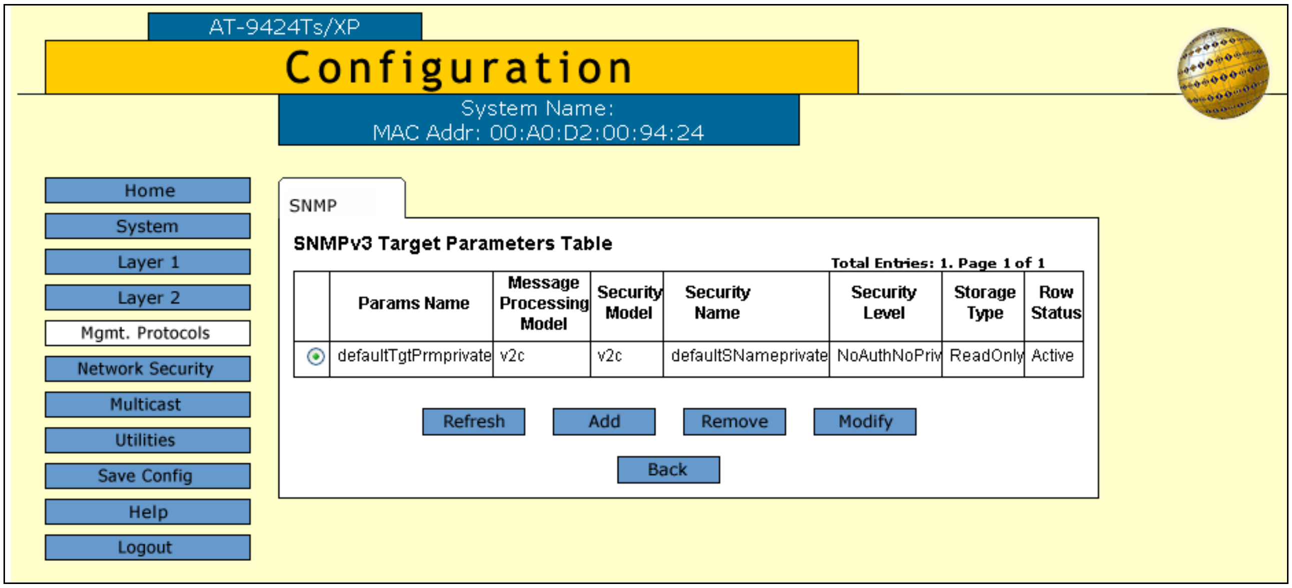
Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for the **Configure Target Parameters Table** and then click the **Configure** button to display the SNMPv3 Target Parameters Table tab in Figure 56.



System Name:
MAC Addr: 00:A0:D2:00:94:24

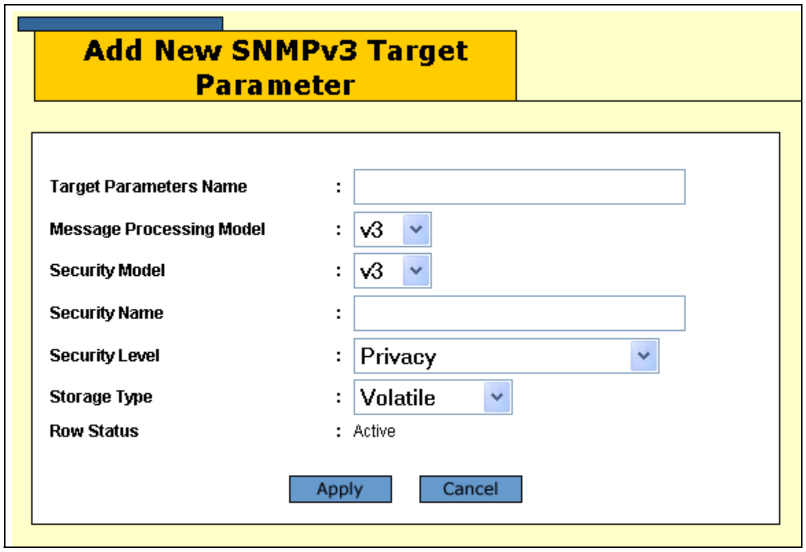
SNMPv3 Target Parameters Table

Total Entries: 1. Page 1 of 1

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
◉	defaultTgtPrmprivate	v2c	v2c	defaultSNameprivate	NoAuthNoPriv	ReadOnly	Active

Figure 56. SNMPv3 Target Parameters Table Tab

4. Click the **Add** button to display the Add New SNMPv3 Target Parameter page, shown in Figure 57.



Add New SNMPv3 Target Parameter

Target Parameters Name	:	
Message Processing Model	:	v3
Security Model	:	v3
Security Name	:	
Security Level	:	Privacy
Storage Type	:	Volatile
Row Status	:	Active

Figure 57. Add New SNMPv3 Target Parameters Page

5. Configure the parameters, described in Table 28, for the new entry and click the **Apply** button.

Table 28. SNMPv3 Target Parameters Table Parameters

Parameter	Description
Target Parameters Name	A name for the entry of up to 32 alphanumeric characters.
Message Processing Model	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 stack automatically assigns the Message Processing Model to SNMPv3.
Security Model	The Security Model for this Security Name or User Name. The possible values are 1-v1 - This value associates the Security Name or User Name with the SNMPv1 protocol. 2-v2c - This value associates the Security Name or User Name with the SNMPv2c protocol. 3-v3 - This value associates the Security Name or User Name with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 entities (users) and to encrypt messages.

Table 28. SNMPv3 Target Parameters Table Parameters

Parameter	Description
Security Name	The user name of the appropriate entry in the SNMPv3 User Table.
Security Level	The possible values are: **Note** This value must match the security level of the corresponding user name in the SNMPv3 User Table. No Authentication/Privacy - This option provides no authentication and no privacy protocol. This security level is appropriate if you do not want authentication of SNMP entities or encryption. This security level provides the least security. **Note** The only security level for SNMPv1 and SNMPv2c is No Authentication/Privacy. Authentication - This option provides authentication, but no privacy protocol. The SNMP user is authenticated, but without encryption. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol. Privacy - This option provides authentication and the privacy protocol. This security level encrypts messages using a privacy protocol and authenticate SNMP entities. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting a Target Parameters Table Entry

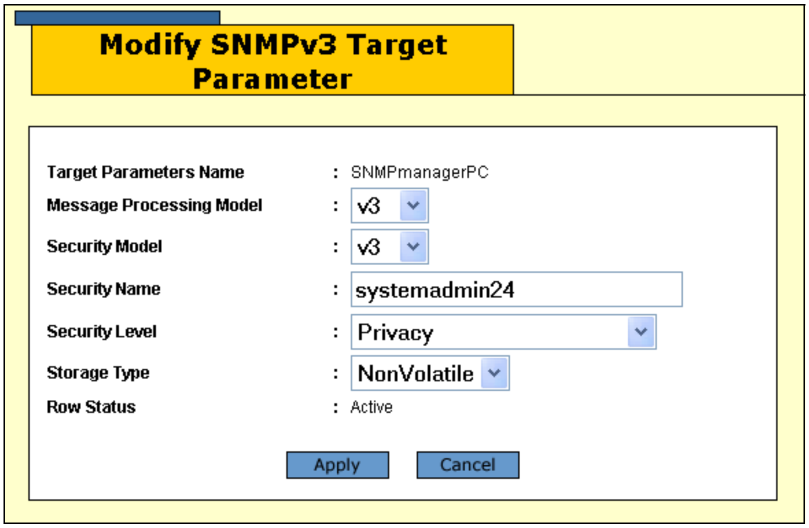
To delete an entry from the SNMPv3 Target Parameters Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure Target Parameters Table** and then the **Configure** button to display the SNMPv3 Target Parameters Table tab in Figure 56 on page 163.
4. Click the radio button of the Target Parameters Table entry you want to delete and then the **Remove** button.
5. At the confirmation prompt, click the **OK** button.
6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying a Target Parameters Table Entry

To modify an entry in the SNMPv3 Target Parameters Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure Target Parameters Table** and then click the **Configure** button to display the SNMPv3 Target Parameters Table tab in Figure 56 on page 163.
4. Click the radio button of the Target Parameters Table entry that you want to change, and then click the **Modify** button. An example of the Modify SNMPv3 Target Parameter window is shown in Figure 58.



Modify SNMPv3 Target Parameter

Target Parameters Name : SNMPmanagerPC

Message Processing Model : v3

Security Model : v3

Security Name : systemadmin24

Security Level : Privacy

Storage Type : NonVolatile

Row Status : Active

Figure 58. Modify SNMPv3 Target Parameter Window

5. Modify the parameters as needed. The parameters are described in Table 28 on page 164.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the SNMPv3 Community Table

To create, delete, or modify SNMPv3 Community Table entries, refer to the following procedures:

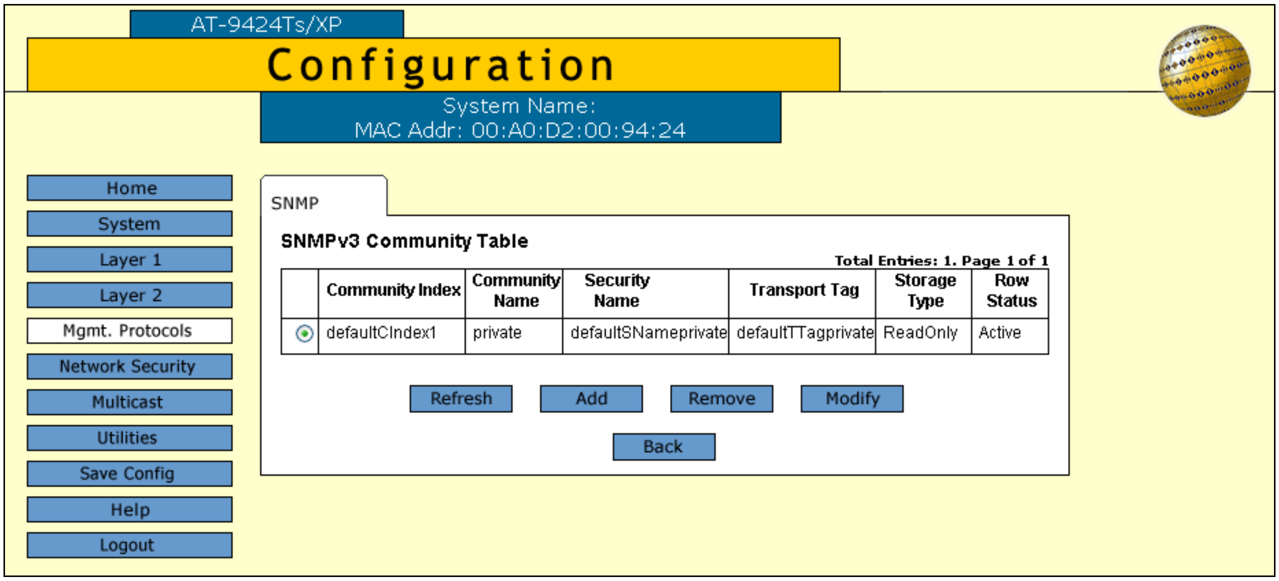
- "Creating an SNMPv3 Community Table Entry" on page 168
- "Deleting an SNMPv3 Community Table Entry" on page 170
- "Modifying an SNMPv3 Community Table Entry" on page 170

Note
The SNMPv3 Community Table is used to configure the protocol for use with SNMPv1 or SNMPv2c. Allied Telesis does not recommend this configuration.

Creating an SNMPv3 Community Table Entry

To create an entry in the SNMPv3 Community Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure Community Table** and then click the **Configure** button to display the SNMPv3 Community Table tab, shown in Figure 59.



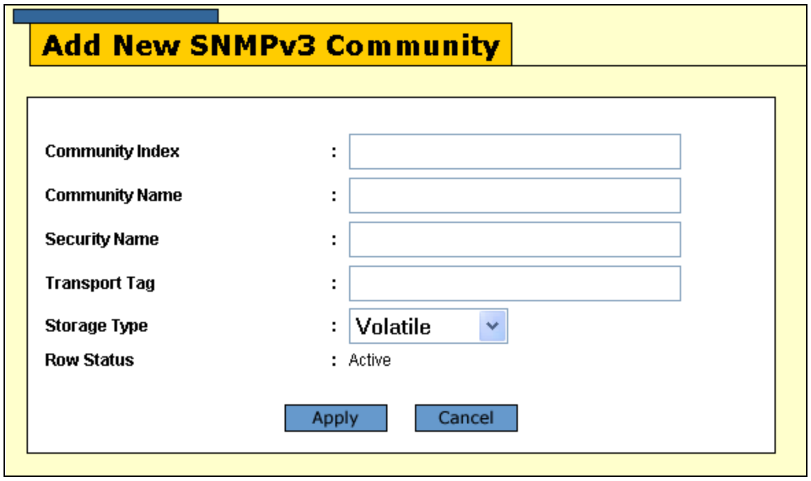
SNMPv3 Community Table

Total Entries: 1. Page 1 of 1

	Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
●	defaultCIndex1	private	defaultSNameprivate	defaultTTagprivate	ReadOnly	Active

Figure 59. SNMPv3 Community Table Tab

4. Click the **Add** button to display the Add New SNMPv3 Community page in Figure 60.



Add New SNMPv3 Community

Community Index	:	
Community Name	:	
Security Name	:	
Transport Tag	:	
Storage Type	:	Volatile
Row Status	:	Active

Figure 60. Add New SNMPv3 Community Page

5. Configure the parameters, described in Table 28, for the new entry and click the **Apply** button.

Table 29. SNMPv3 Community Table Parameters

Parameter	Description
Community Index	An index value of up to 32- alphanumeric characters.
Community Name	A community name of up to 64-alphanumeric characters. The community name acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.
Security Name	A name of up to 32 alphanumeric characters of an SNMPv1 and SNMPv2c user. The name must be unique.
Transport Tag	A name of up to 32 alphanumeric characters. The Transport Tag parameter links an SNMPv3 Community Table entry to an SNMPv3 Target Address Table entry. Add the value of the Transport Tag parameter to the Tag List parameter in the Target Address Table. See “Creating a Target Address Table Entry” on page 158.
Storage Type	The storage method of the entry. The possible values are: V-Volatile - This setting prevents the stack from saving the entry in the master configuration file. An entry with this storage type is discarded the next time the stack is reset or powered off. N-NonVolatile - This setting allows the stack to save the entry in the master configuration file when the save command is issued. Allied Telesis recommends this storage type.
Row Status	The status of the entry. All entries have a status of Active.

6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting an SNMPv3 Community Table Entry

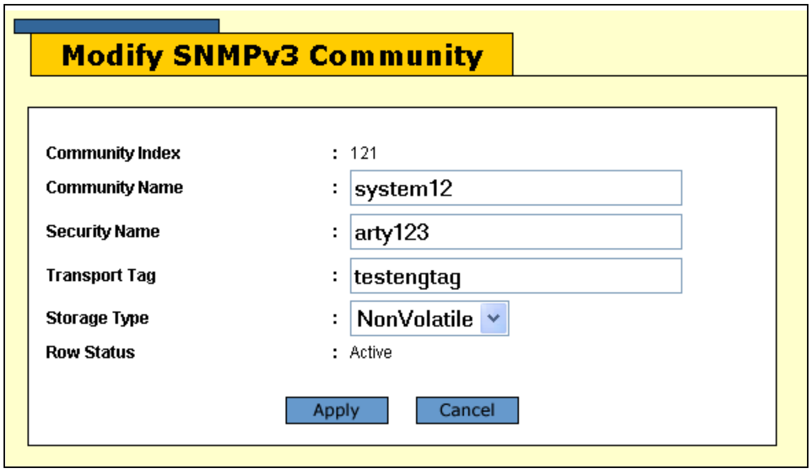
To delete an entry from the SNMPv3 Community Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **Configure Community Table** and the **Configure** button to display the SNMPv3 Community Table tab in Figure 59 on page 168.
4. Click the radio button of the SNMPv3 Community Table entry you want to delete and the **Remove** button.
5. At the confirmation prompt, click the **OK** button.
6. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for the **Configure Community Table**, and the **Configure** button to display the SNMPv3 Community Table tab in Figure 59 on page 168.
4. Click the radio button of the SNMPv3 Community Table entry you want to change and then click the **Modify** button to display the Modify SNMPv3 Community window. An example of the window is shown in Figure 61.



Community Index : 121
Community Name : system12
Security Name : arty123
Transport Tag : testengtag
Storage Type : NonVolatile
Row Status : Active

Figure 61. Modify SNMPv3 Community Page

5. Modify the parameters as needed. The parameters are described in Table 28 on page 164.

6. After modifying the entry, click the **Apply** button.

7. At the confirmation prompt, click the **OK** button.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying the SNMPv3 Tables

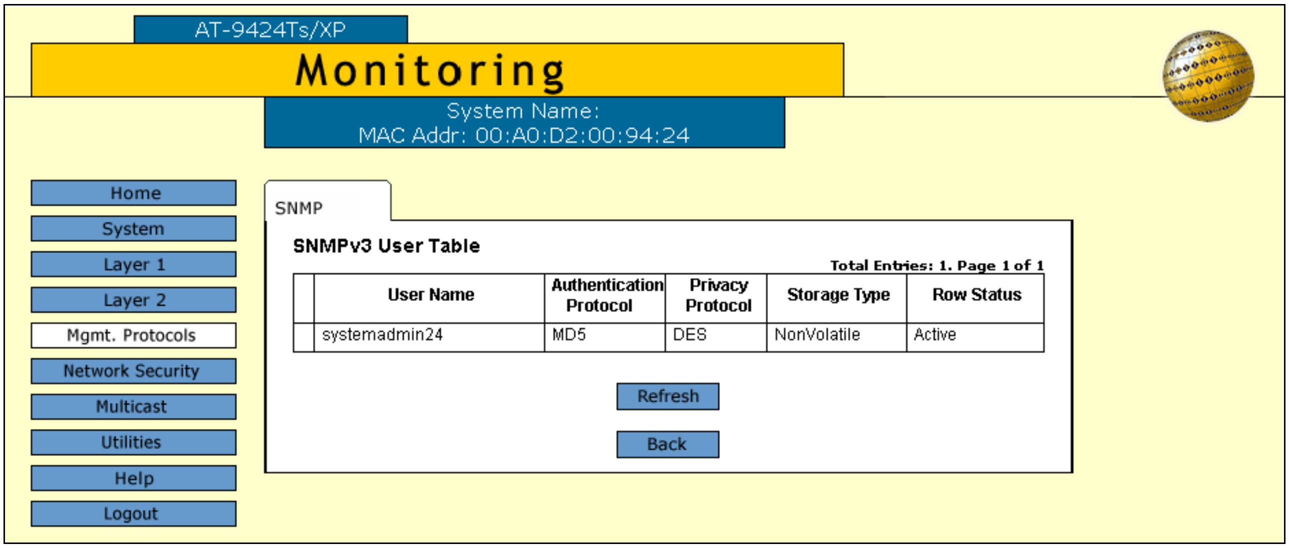
This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- "Displaying the User Table Entries," next
- "Displaying the View Table Entries" on page 173
- "Displaying the Access Table Entries" on page 174
- "Displaying the SecurityToGroup Table Entries" on page 175
- "Displaying the Notify Table Entries" on page 176
- "Displaying the Target Address Table Entries" on page 177
- "Displaying the Target Parameters Table Entries" on page 178
- "Displaying the SNMPv3 Community Table Entries" on page 179

Displaying the User Table Entries

To display the entries in the SNMPv3 User Table:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 14 on page 58.
3. In the SNMPv3 section, click the radio button for **View User Table** and the **View** button to display the SNMPv3 User Table tab in Figure 62. The parameters that define the user table entries are described in Table 22 on page 135.



System Name:
MAC Addr: 00:A0:D2:00:94:24

SNMPv3 User Table

Total Entries: 1. Page 1 of 1

	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status
	systemadmin24	MD5	DES	NonVolatile	Active

Figure 62. SNMPv3 User Table Tab (Monitoring)

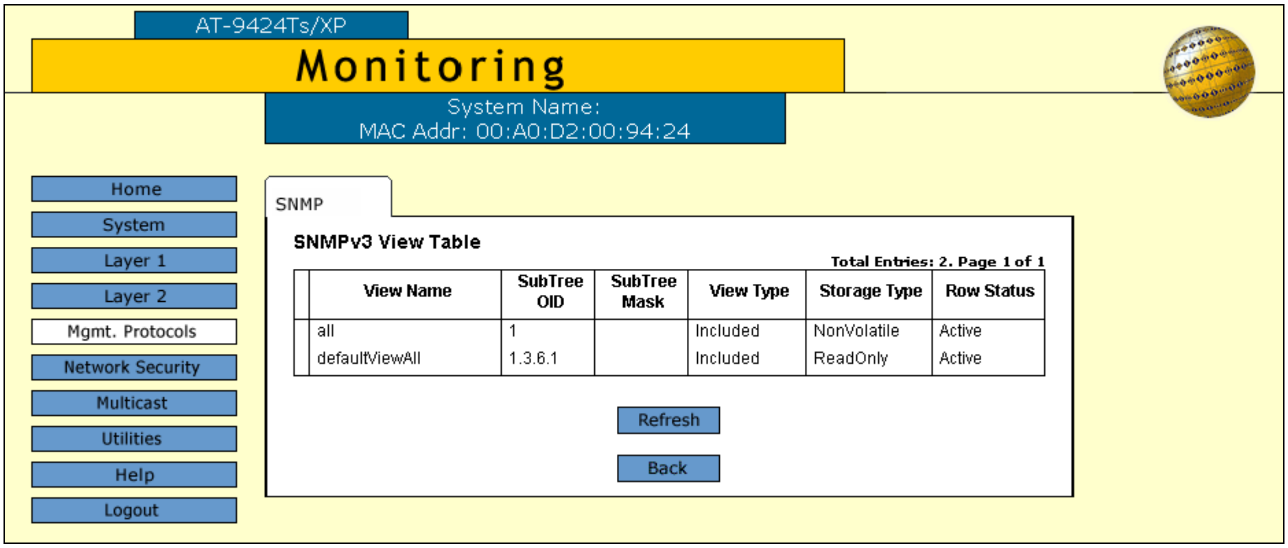
Displaying the View Table Entries

To display the entries in the SNMPv3 View Table:

1. From the Home page, select **Monitoring**.

2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **View View Table** and the **View** button to display the SNMPv3 View Table tab in Figure 63. The parameters that define the view table entries are described in Table 23 on page 140.



SNMPv3 View Table

Total Entries: 2. Page 1 of 1

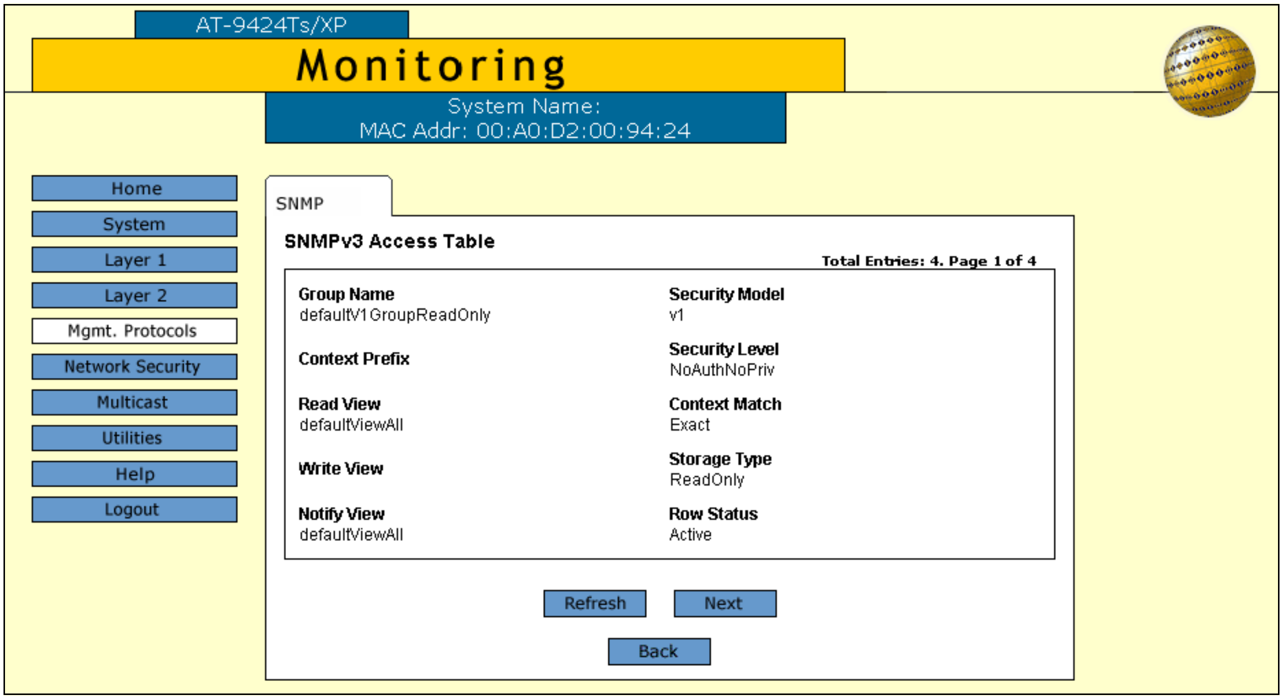
	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
	all	1		Included	NonVolatile	Active
	defaultViewAll	1.3.6.1		Included	ReadOnly	Active

Figure 63. SNMPv3 View Table Tab (Monitoring)

Displaying the Access Table Entries

To display the entries in the SNMPv3 Access Table:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **View Access Table** and the **View** button to display the SNMPv3 Access Table tab in Figure 64. The parameters that define the access table entries are described in Table 24 on page 145.



SNMPv3 Access Table

Total Entries: 4. Page 1 of 4

Group Name
defaultV1GroupReadOnly

Security Model
v1

Context Prefix

Security Level
NoAuthNoPriv

Read View
defaultViewAll

Context Match
Exact

Write View

Storage Type
ReadOnly

Notify View
defaultViewAll

Row Status
Active

Figure 64. SNMPv3 Access Table Tab (Monitoring)

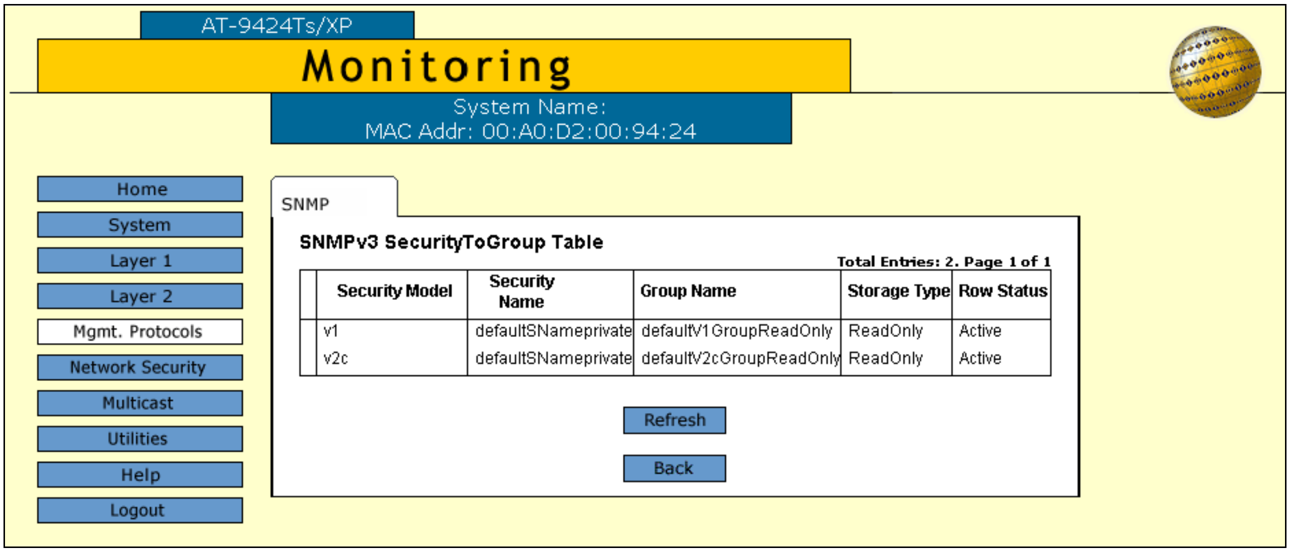
Displaying the SecurityToGroup Table Entries

To display the entries in the SNMPv3 SecurityToGroup Table:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **View SecurityToGroup Table** and the **View** button to display the SNMPv3 SecurityToGroup Table tab in Figure 65. The parameters that define security to group entries are described in Table 25 on page 151.



SNMPv3 SecurityToGroup Table

Total Entries: 2. Page 1 of 1

	Security Model	Security Name	Group Name	Storage Type	Row Status
	v1	defaultSNameprivate	defaultV1GroupReadOnly	ReadOnly	Active
	v2c	defaultSNameprivate	defaultV2cGroupReadOnly	ReadOnly	Active

Figure 65. SNMPv3 SecurityToGroup Table Tab (Monitoring)

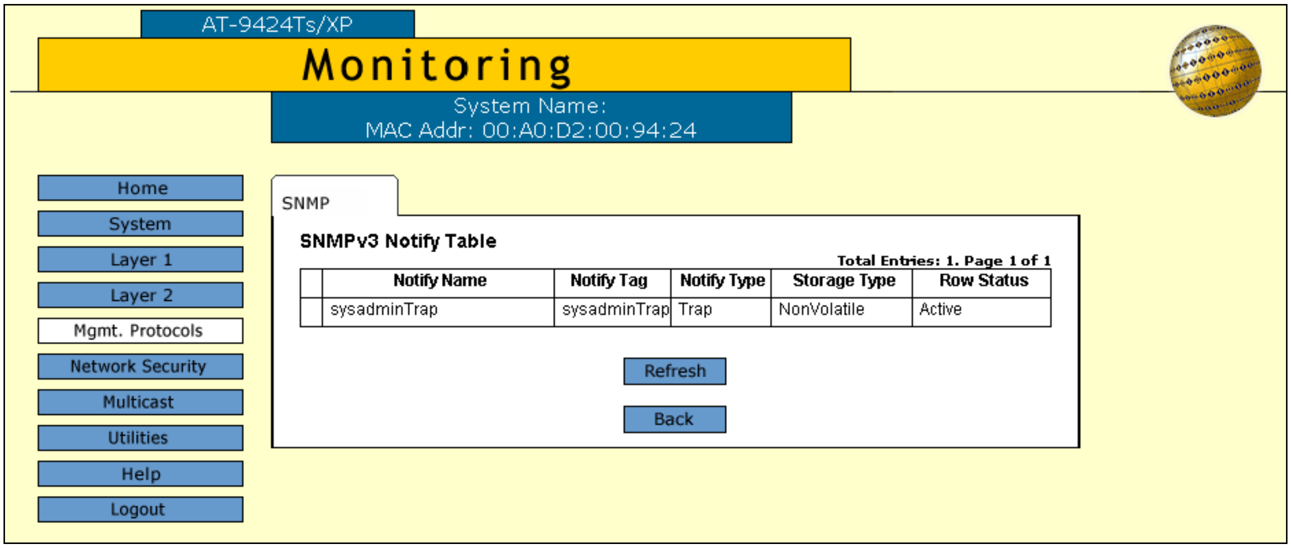
Displaying the Notify Table Entries

To display the entries in the SNMPv3 Notify Table:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **View Notify Table** and the **View** button to display the SNMPv3 Notify Table tab in Figure 66. The parameters that define notify table entries are described in Table 26 on page 155.



SNMPv3 Notify Table

Total Entries: 1. Page 1 of 1

	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
	sysadminTrap	sysadminTrap	Trap	NonVolatile	Active

Figure 66. SNMPv3 Notify Table Tab (Monitoring)

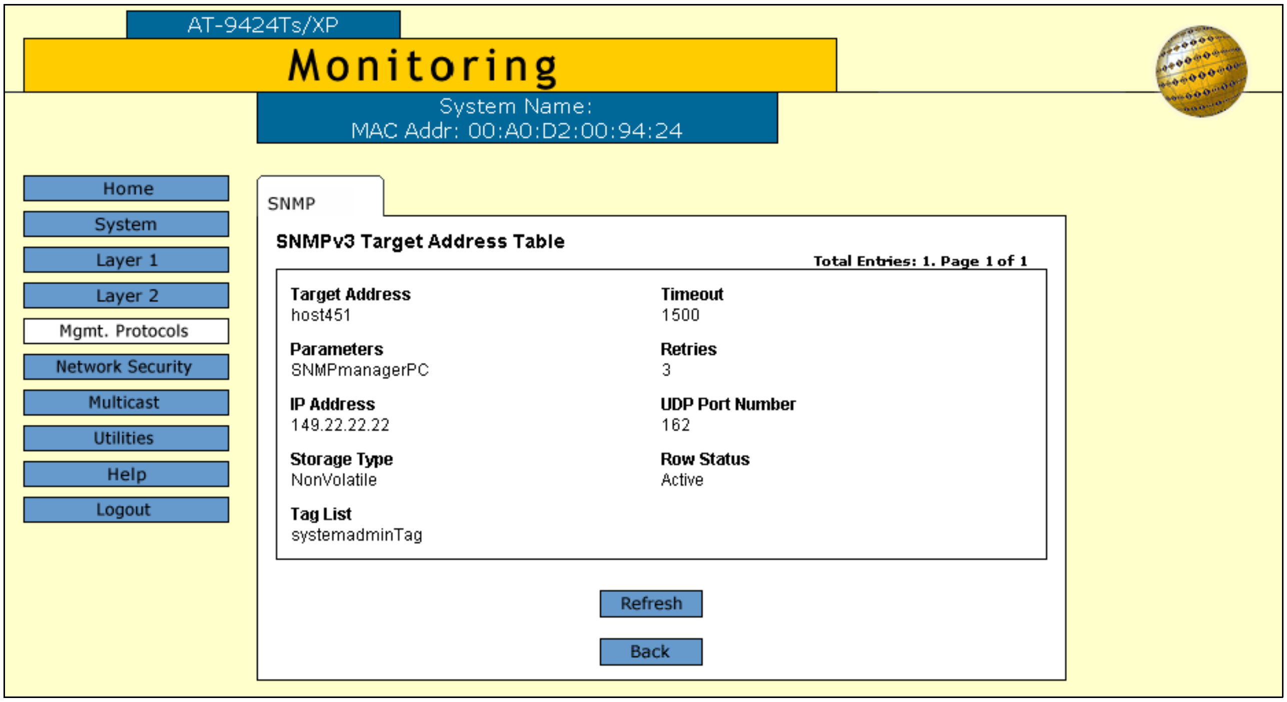
Displaying the Target Address Table Entries

To display the entries in the SNMPv3 Target Address Table:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **View Target Address Table** and the **View** button to display the SNMPv3 Target Address Table tab in Figure 67. The parameters that define target address table entries are described in Table 27 on page 159.



SNMPv3 Target Address Table

Total Entries: 1. Page 1 of 1

Target Address
host451

Timeout
1500

Parameters
SNMPmanagerPC

Retries
3

IP Address
149.22.22.22

UDP Port Number
162

Storage Type
NonVolatile

Row Status
Active

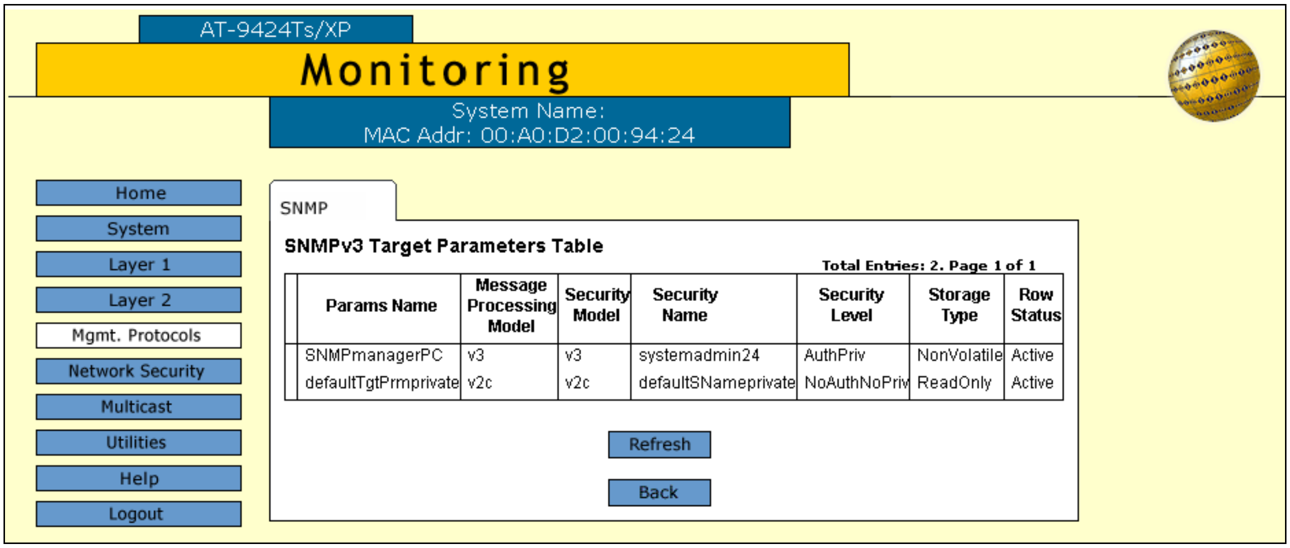
Tag List
systemadminTag

Figure 67. SNMPv3 Target Address Table Tab (Monitoring)

Displaying the Target Parameters Table Entries

To display the entries in the SNMPv3 Target Parameters Table:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.
3. In the SNMPv3 section, click the radio button for **View Target Parameters Table** and the **View** button to display the SNMPv3 Target Parameters Table tab in Figure 68. The parameters that define target parameters table entries are described in Table 28 on page 164.



SNMPv3 Target Parameters Table

Total Entries: 2. Page 1 of 1

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
	SNMPmanagerPC	v3	v3	systemadmin24	AuthPriv	NonVolatile	Active
	defaultTgtPrmprivate	v2c	v2c	defaultSNameprivate	NoAuthNoPriv	ReadOnly	Active

Figure 68. SNMPv3 Target Parameters Table Tab (Monitoring)

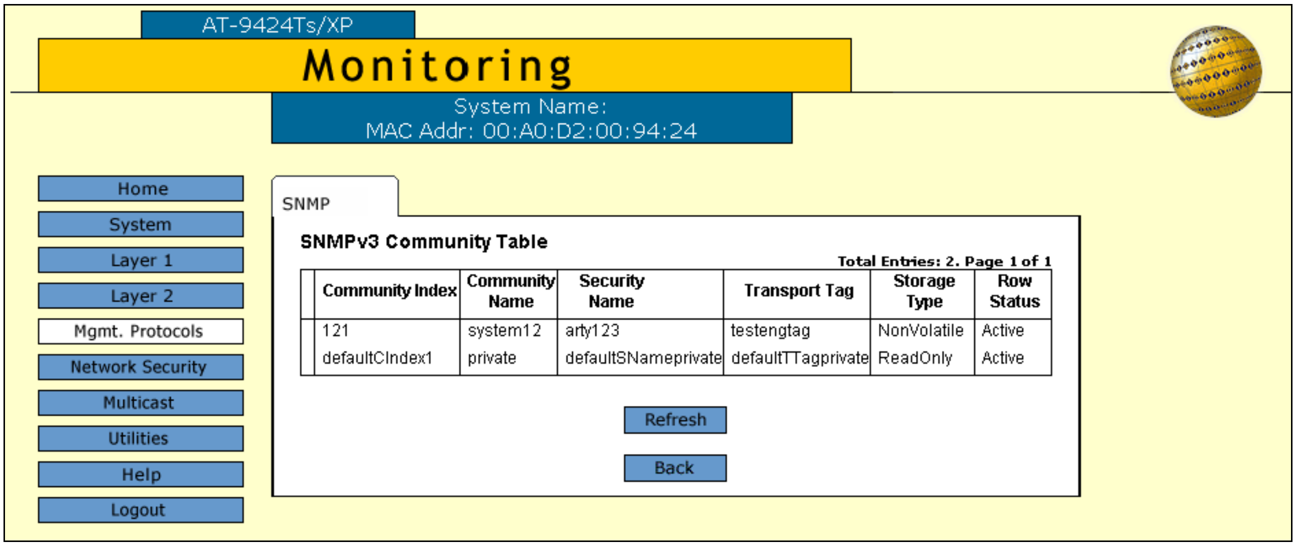
Displaying the SNMPv3 Community Table Entries

To display the entries in the SNMPv3 Community Table:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Mgmt. Protocols** button to display the SNMP tab, shown in Figure 11 on page 50.

3. In the SNMPv3 section, click the radio button for **View Community Table** and the **View** button to display the SNMPv3 Community Table tab in Figure 69. The parameters that define community table entries are described in Table 29 on page 169.



SNMPv3 Community Table

Total Entries: 2. Page 1 of 1

	Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
	121	system12	arty123	testengtag	NonVolatile	Active
	defaultCIndex1	private	defaultSNameprivate	defaultTTagprivate	ReadOnly	Active

Figure 69. SNMPv3 Community Table Tab (Monitoring)

Section IV

Spanning Tree Protocols

This section has the following chapter:

Chapter 12

Spanning Tree and Rapid Spanning Tree Protocols

This chapter explains how to configure STP and RSTP. The sections in the chapter include:

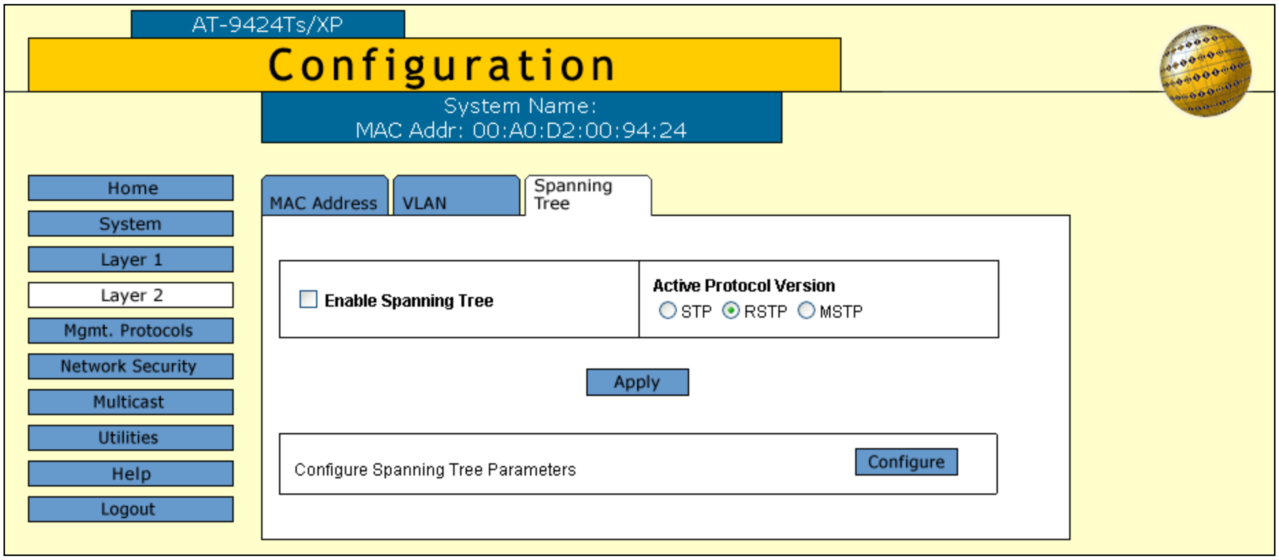
Enabling or Disabling a Spanning Tree Protocol

To enable or disable a spanning tree protocol on the switch or to select the active spanning tree protocol:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. Select the **Spanning Tree** tab, shown in Figure 70.



System Name:
MAC Addr: 00:A0:D2:00:94:24

□ Enable Spanning Tree

Active Protocol Version
○ STP ● RSTP ○ MSTP

Configure Spanning Tree Parameters

Figure 70. Spanning Tree Tab

4. To select a spanning tree protocol for the stack, click the **STP** or **RSTP** radio button for the Active Protocol Version parameter. The default is RSTP.

Caution
Do not select Multiple Spanning Tree Protocol (MSTP). MSTP is not supported in a stack.

Note
A stack can support only one spanning tree protocol at a time.

5. To enable or disable the spanning tree protocol on the stack, 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.

6. Click the **Apply** button. Your changes are immediately implemented on the stack.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

8. If you activated STP, go to “Configuring STP” on page 186. If you activated RSTP go to Step “Configuring RSTP” on page 196.

Configuring STP

This section contains the following procedures:

❐ ”Configuring the STP Bridge Settings”, next

❐ “Configuring the STP Port Settings” on page 190

❐ “Displaying the STP Settings” on page 192

❐ “Restoring the STP Default Settings” on page 194

⚠ **Caution**
The default settings for the STP parameters are adequate for most networks. Adjusting the parameters without prior knowledge or experience with STP might adversely impact your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

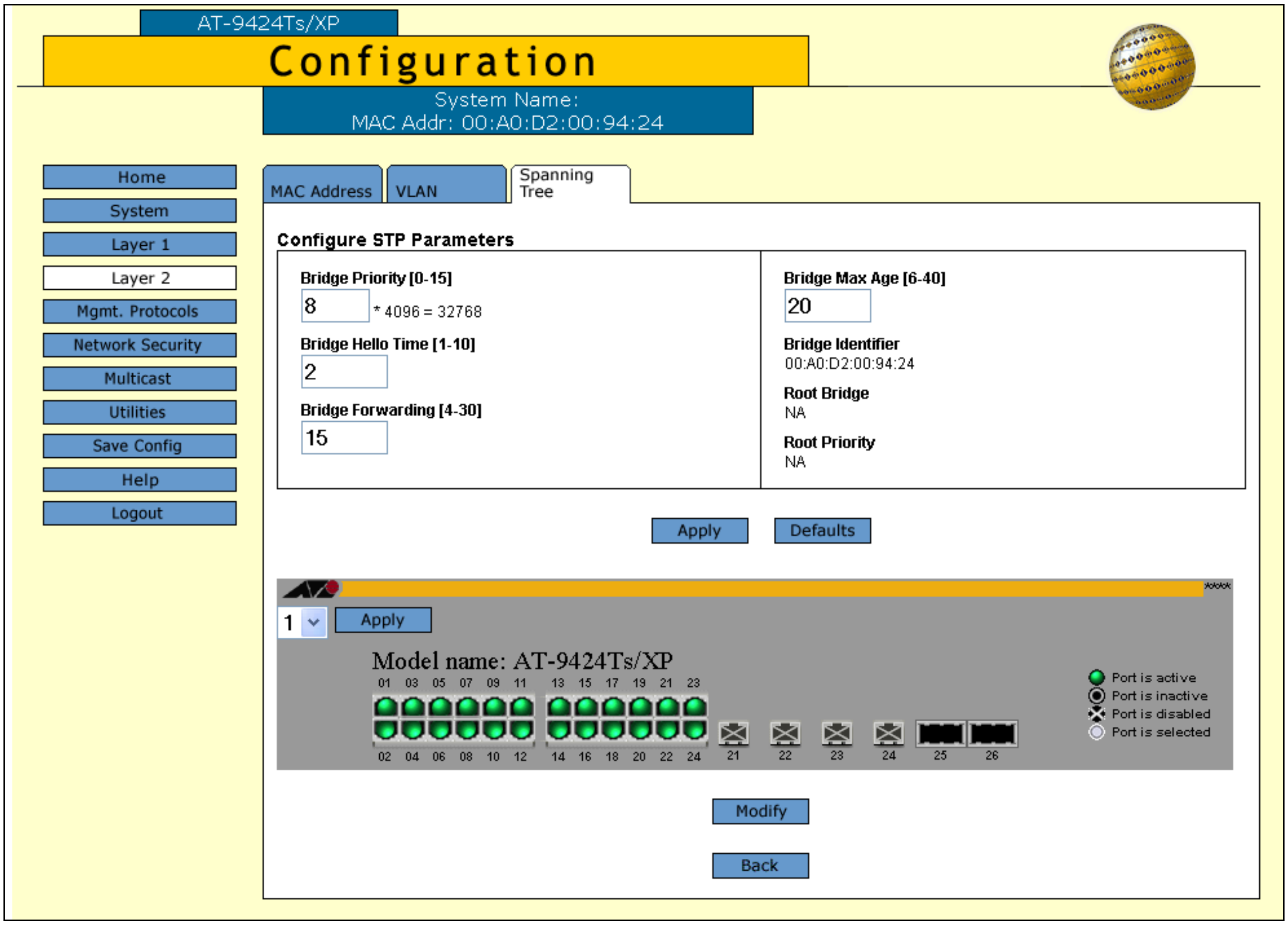
The following procedures assume that STP is the active spanning tree protocol on the stack. For directions on selecting the active spanning tree protocol, refer to “Enabling or Disabling a Spanning Tree Protocol” on page 184.

Configuring the STP Bridge Settings

To configure the STP bridge settings:

1. From the Home page, select the **Configuration** button.
2. From the Configuration menu, click the **Layer 2** button.
3. Select the **Spanning Tree** tab, shown in Figure 70 on page 184.

4. Click the **Configure** button to display the Configure STP Parameters tab shown in Figure 71.



System Name:
MAC Addr: 00:A0:D2:00:94:24

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:A0:D2:00:94:24

Root Bridge
NA

Root Priority
NA

Figure 71. Configure STP Parameters Tab

Note
The Defaults button restores the default values to all of the STP settings in the stack.

---

5. Configure the STP parameters, described in Table 30, as needed.

Table 30. STP Parameters

Parameter	Definition
Bridge Priority	Specifies the priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 31 on page 190.
Bridge Hello Time	Specifies 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	Specifies 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	Specifies 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.

Table 30. STP Parameters

Parameter	Definition
Bridge Max Age (continued)	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	Specifies the MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.
Root Bridge	Specifies the MAC address of the root bridge of the spanning tree domain. This value cannot be changed and is only displayed when STP is activated on the switch.
Root Priority	Specifies the priority value on the root bridge of the spanning tree domain. This parameter is only displayed when STP is enabled on the switch. To change the priority value on the root bridge, you must start a management session on the switch functioning as the root bridge and change its bridge priority value.

Table 31. 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

6. After you have changed the parameters, click the **Apply** button.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the STP Port Settings

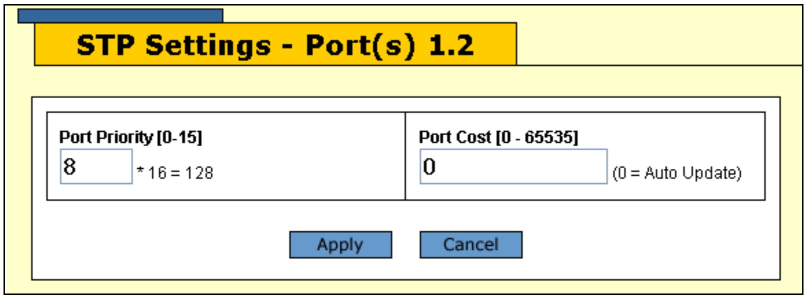
To configure STP port parameters:

1. Perform steps 1 to 4 in “Configuring the STP Bridge Settings” on page 186 to display the Spanning Tree tab.

2. Use the Stack ID pull-down menu in the switch image to select the ID number of switch you want to configure and click the **Apply** button. You can configure only one switch at a time.

3. In the switch image 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.

4. Click the **Modify** button to display the STP Settings popup window, shown in Figure 72.



STP Settings - Port(s) 1.2

Port Priority [0-15]
8 * 16 = 128

Port Cost [0 - 65535]
0 (0 = Auto Update)

Figure 72. STP Settings Window

5. Configure the STP port parameters, described in Table 32, as needed.

Table 32. STP Port Settings

Parameter	Definition
Port Priority	Specifies the port priority. This parameter is used as a tie breaker when two or more ports 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 33.
Port Cost	Specifies the 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. If you select Auto-Detect, the management software assigns a value of 100 to a port operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

Table 33. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge 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

6. After configuring the parameters, click the **Apply** button.

7. To configure the ports on another switch in the stack, repeat this procedure starting with step 3.

8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

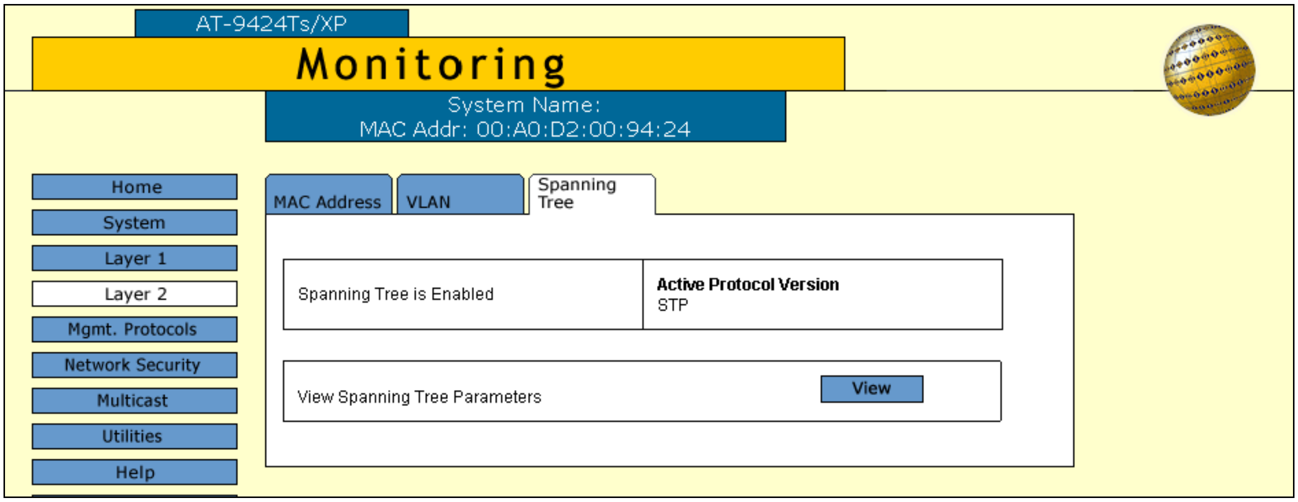
Displaying the STP Settings

To display the STP settings:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Layer 2** button.

3. Click the **Spanning Tree** tab to display the Spanning Tree tab in Figure 73.



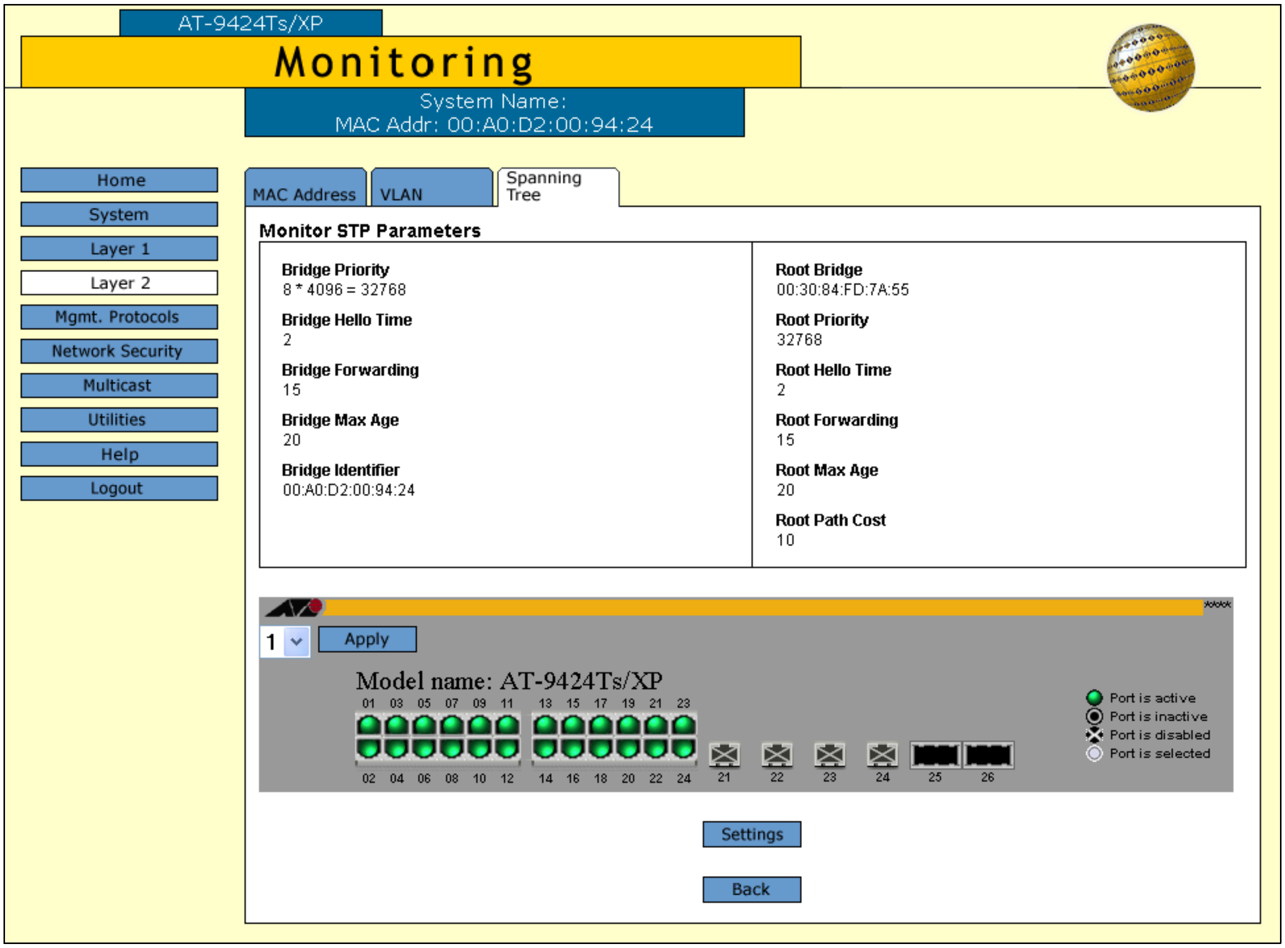
Spanning Tree is Enabled

Active Protocol Version
STP

View Spanning Tree Parameters

Figure 73. Spanning Tree Tab (Monitoring)

4. Click **View** button to display the Monitor STP Parameters tab in Figure 74.



Monitor STP Parameters

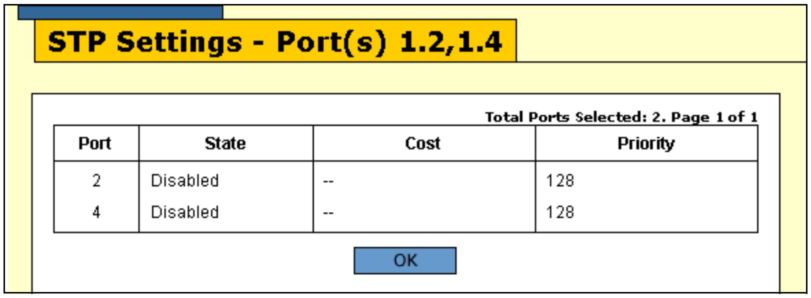
Bridge Priority 8 * 4096 = 32768	**Root Bridge** 00:30:84:FD:7A:55
Bridge Hello Time 2	**Root Priority** 32768
Bridge Forwarding 15	**Root Hello Time** 2
Bridge Max Age 20	**Root Forwarding** 15
Bridge Identifier 00:A0:D2:00:94:24	**Root Max Age** 20
	Root Path Cost 10

Figure 74. STP Parameters Tab (Monitoring)

5. To view the port settings, use the Stack ID pull-down menu in the switch image to select the ID number of switch you want to view and click the **Apply** button. You can view only one switch at a time.

6. In the switch image click the port you want to view. A selected port turns white. To deselect a port, click it again. You can view more than one port at a time.

7. Click the **Settings** button. The STP Settings window is shown in Figure 75.



STP Settings - Port(s) 1.2,1.4

Total Ports Selected: 2. Page 1 of 1

Port	State	Cost	Priority
2	Disabled	--	128
4	Disabled	--	128

Figure 75. STP Settings Window

The columns in the STP Settings window are described in this table:

Table 34. STP Port Settings

Column	Definition
Port	Displays the port number.
State	Displays the current state of a port. The possible states are Listening, Learning, Forwarding, or Blocking when spanning tree is enabled on the switch. When spanning tree is not enabled on the switch or if a port is not being used, its state will be disabled.
Cost	Displays the port cost of the port.
Priority	Displays the port's priority value. The number is used as a tie breaker when two or more ports have equal costs to the root bridge.

8. Click the **OK** button to close the window.

Restoring the STP Default Settings

To restore the default values to the STP parameters in the stack:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 2** button.
3. Select the **Spanning Tree** tab, shown in Figure 70 on page 184.
4. Verify there is no check in the **Enable Spanning Tree** check box. If there is a check, click the option to remove it. You have to disable spanning tree before you can restore its default settings.
5. Click the **Configure** button to display the Configure STP Parameters tab shown in Figure 71 on page 187.

6. Click the **Defaults** button to restore the default values to the STP settings in the stack.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring RSTP

This section contains the following procedures:

- ”Configuring the RSTP Bridge Settings”, next
- “Configuring the RSTP Port Settings” on page 200
- “Displaying RSTP Settings” on page 202
- “Restoring the RSTP Default Settings” on page 204

⚠ **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.

The following procedures assume that RSTP is the active spanning tree protocol on the stack. For directions on selecting the active spanning tree protocol, refer to “Enabling or Disabling a Spanning Tree Protocol” on page 184.

Configuring the RSTP Bridge Settings

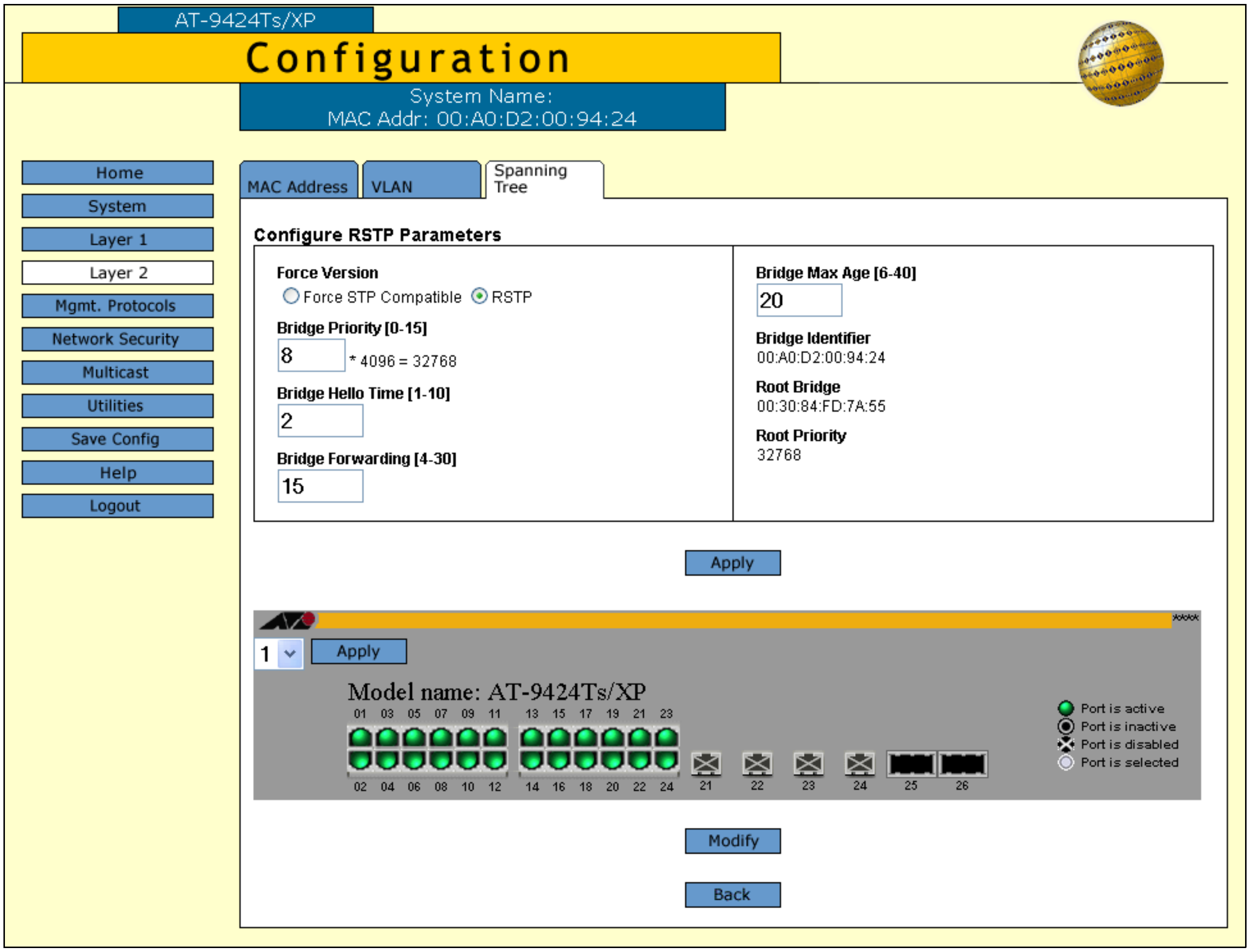
To configure RSTP bridge parameters:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. Select the **Spanning Tree** tab, shown in Figure 70 on page 184.

4. Click the **Configure** button to display the Configure RSTP Bridge Parameters tab shown in Figure 76.



System Name:
MAC Addr: 00:A0:D2:00:94:24

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:A0:D2:00:94:24

Root Bridge
00:30:84:FD:7A:55

Root Priority
32768

Model name: AT-9424Ts/XP

Figure 76. Configure RSTP Parameters Tab

5. Configure the parameters, described in Table 35, as needed.

Table 35. RSTP Parameters

Parameter	Definition
Force Version	Specifies whether the bridge operates 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.

Table 35. RSTP Parameters

Parameter	Definition
Bridge Priority	Specifies 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 31 on page 190.
Bridge Hello Time	Specifies 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	Specifies the waiting period before a bridge changes to a new state, for example, when it becomes the new root bridge after a topology change. 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.
Bridge Max Age	Specifies 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.

Table 35. RSTP Parameters

Parameter	Definition
Bridge Max Age (continued)	When selecting a value for maximum age, observe the following rules: MaxAge must be greater than (2 x (HelloTime + 1)). MaxAge must be less than (2 x (ForwardingDelay - 1))
Bridge Identifier	Specifies the MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.
Root Bridge	Specifies the MAC address of the root bridge of the spanning tree domain. This value cannot be changed and is only displayed when RSTP is activated on the switch.
Root Priority	Specifies the priority value on the root bridge of the spanning tree domain. This parameter is only displayed when RSTP is enabled on the switch. To change the priority value on the root bridge, you must start a management session on the switch functioning as the root bridge and change its bridge priority value.

6. After entering your changes, click the **Apply** button.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the RSTP Port Settings

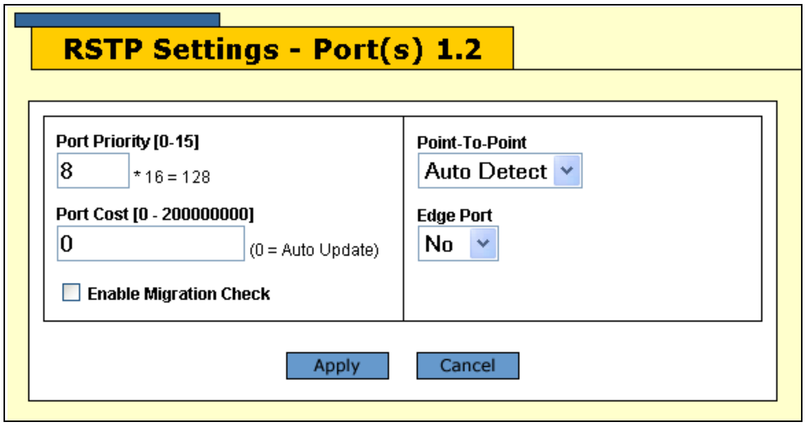
To configure the RSTP port parameters:

1. Perform steps 1 to 4 in “Configuring the RSTP Bridge Settings” on page 196 to display the Spanning Tree tab.

2. Use the Stack ID pull-down menu in the switch image to select the ID number of the switch you want to configure and click the **Apply** button. You can configure only one switch at a time.

3. In the switch image 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.

4. Click the **Modify** button to display the RSTP Port Settings window in Figure 77.



RSTP Settings - Port(s) 1.2

Port Priority [0-15]: 8 * 16 = 128

Port Cost [0 - 200000000]: 0 (0 = Auto Update)

□ Enable Migration Check

Point-To-Point: Auto Detect

Edge Port: No

Figure 77. RSTP Port Settings Window

5. Configure the parameters as needed.

Table 36. RSTP Port Parameters

Parameter	Definition
Port Priority	Specifies the 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 33 on page 191.

Table 36. RSTP Port Parameters

Parameter	Definition
Port Cost	Specifies the 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. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.
Enable Migration Check	Resets an RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely. Type C to reset the MSTP port to transmit RSTP BPDUs. This parameter is displayed only when RSTP is enabled.
Point-to-Point	Specifies whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 22, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Features Guide*.
Edge Port	Specifies whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 22, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Features Guide*.

6. After configuring the parameters, click the **Apply** button.

7. To save your changes in he master configuration file, click the **Save Config** button in the Configuration menu.

Displaying RSTP Settings

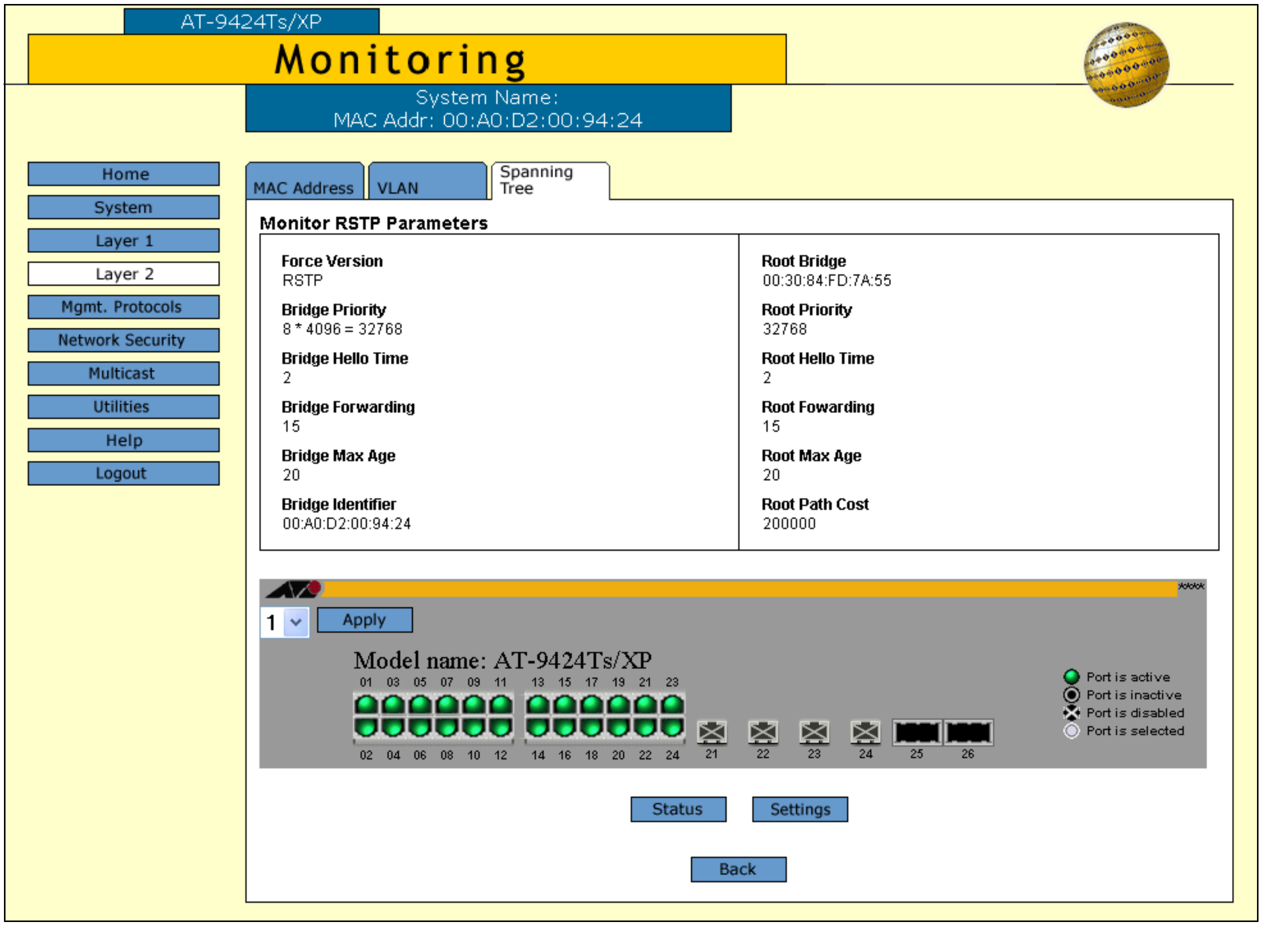
To display the RSTP parameter settings:

1. From the Home page, click the **Monitoring** button.

2. From the Monitoring menu, click the **Layer 2** button.

3. Select the **Spanning Tree** tab, shown in Figure 73 on page 192.

4. Click the **View** button to display the Monitor RSTP Parameters tab in Figure 78.



Monitor RSTP Parameters

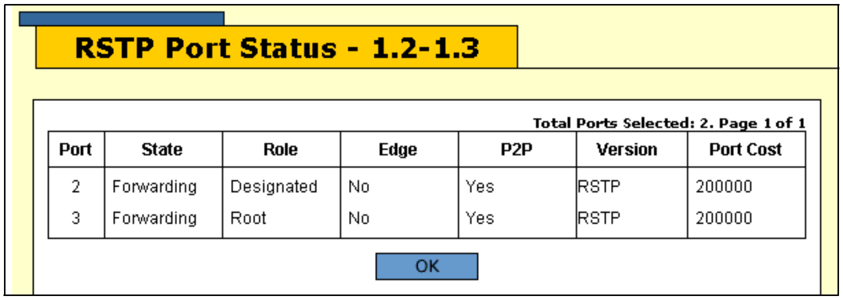
Force Version RSTP	**Root Bridge** 00:30:84:FD:7A:55
Bridge Priority 8 * 4096 = 32768	**Root Priority** 32768
Bridge Hello Time 2	**Root Hello Time** 2
Bridge Forwarding 15	**Root Fowarding** 15
Bridge Max Age 20	**Root Max Age** 20
Bridge Identifier 00:A0:D2:00:94:24	**Root Path Cost** 200000

Figure 78. Monitor RSTP Parameters Tab

5. Use the Stack ID pull-down menu in the switch image to select the ID number of the switch that you want to view and click the **Apply** button. You can view only one switch at a time.

6. In the switch image click the port you want to view. A selected port turns white. To deselect a port, click it again. You can view more than one port at a time.

7. Click the **Status** or **Settings** button. An example of the RSTP Status window is shown in Figure 80.



RSTP Port Status - 1.2-1.3

Total Ports Selected: 2. Page 1 of 1

Port	State	Role	Edge	P2P	Version	Port Cost
2	Forwarding	Designated	No	Yes	RSTP	200000
3	Forwarding	Root	No	Yes	RSTP	200000

Figure 79. RSTP Port Status Window

The columns in the RSTP Port Status window are described here.

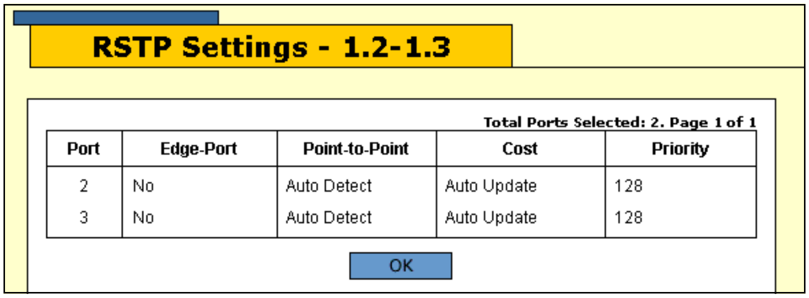
Table 37. RSTP Port Status Window

Column	Definition
Port	Displays the port number.
State	Displays the RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding. The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Blocking. The possible states for a port not being used or where spanning tree is not activated is Disabled.
Role	Displays the RSTP role of the port. Possible roles are: Root - The port that is connected to the root switch, directly or through other switches, with the least path cost. Alternate - The port offers an alternate path in the direction of the root switch. Backup - The port on a designated switch that provides a backup for the path provided by the designated port. Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Table 37. RSTP Port Status Window

Column	Definition
Edge-Port	Displays whether or not the port is operating as an edge port. The possible settings are Yes and No.
P2P	Displays whether or not the port is functioning as a point-to-point port. The possible settings are Yes and No.
Version	Displays whether the port is operating in the RSTP mode or the STP-compatible mode.
Port Cost	Displays the port cost of the port.

An example of the RSTP Settings page is shown in Figure 80.



RSTP Settings - 1.2-1.3

Total Ports Selected: 2. Page 1 of 1

Port	Edge-Port	Point-to-Point	Cost	Priority
2	No	Auto Detect	Auto Update	128
3	No	Auto Detect	Auto Update	128

Figure 80. RSTP Settings Window

For the descriptions of the parameters, refer to Table 36 on page 200.

8. Click the **OK** button to close the window.

Restoring the RSTP Default Settings

To restore the default values to the RSTP parameters in the stack:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 2** button.
3. Select the **Spanning Tree** tab, shown in Figure 70 on page 184.
4. Verify that there is no check in the **Enable Spanning Tree** check box. If there is a check, click the option to remove it. You have to disable RSTP to restore the default settings.
5. Click the **Configure** button to display the Configure RSTP Bridge Parameters tab shown in Figure 76 on page 197.
6. Click the **Defaults** button to restore the default settings to the RSTP parameters.

7. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Section V

Virtual LANs

This section has the following chapter:

Chapter 13

Port-based and Tagged VLANs

The procedures in this chapter are used to create, modify, and delete port-based and tagged VLANs. The sections in the chapter include:

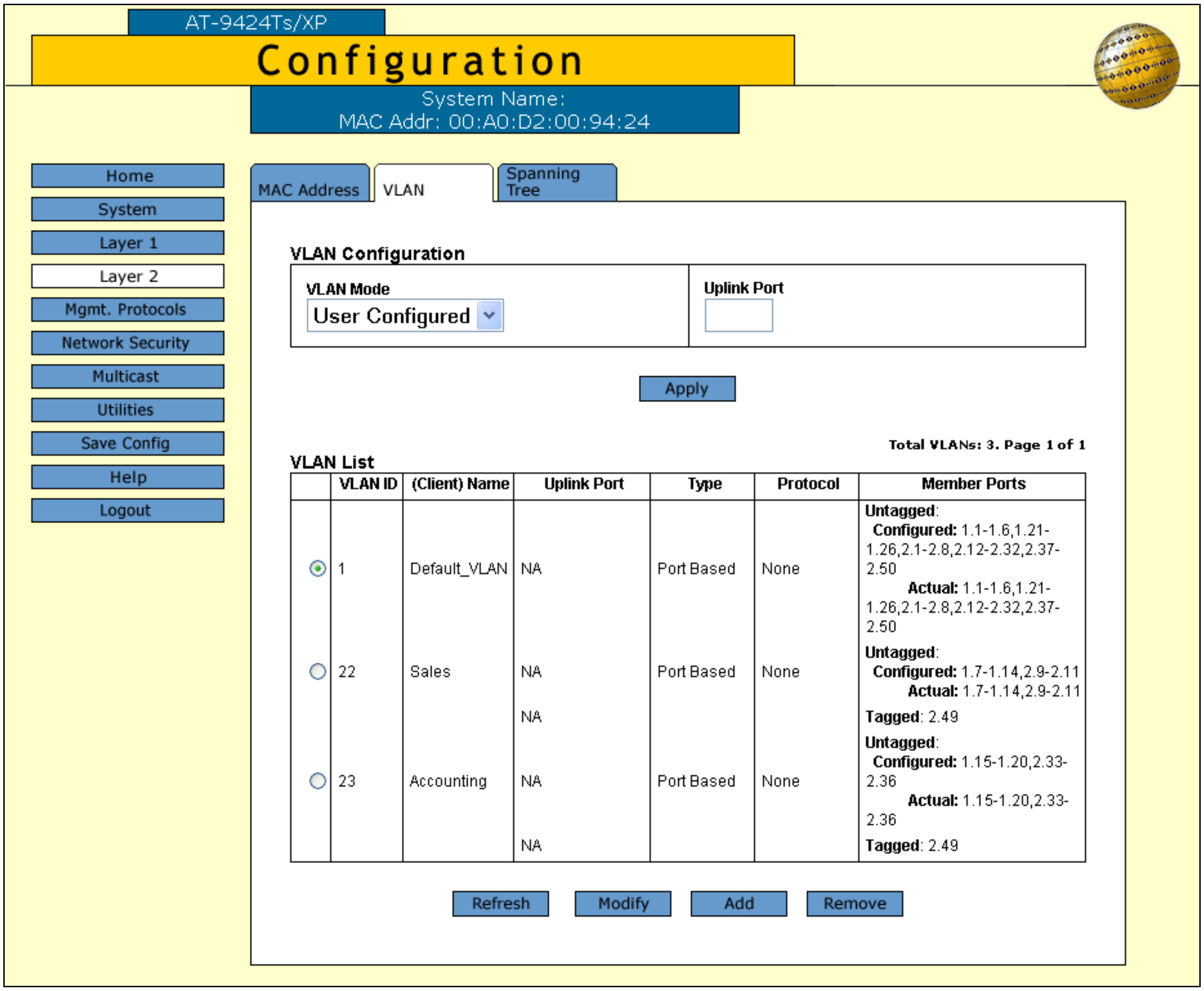
Creating New Port-Based or Tagged VLANs

To create a new port-based or tagged VLAN:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Layer 2** button.

3. Click the **VLAN** tab, shown in Figure 81.



System Name:
MAC Addr: 00:A0:D2:00:94:24

VLAN Configuration

VLAN Mode: User Configured

Uplink Port:

Total VLANs: 3. Page 1 of 1

VLAN List

	VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Member Ports
●	1	Default_VLAN	NA	Port Based	None	**Untagged**: **Configured:** 1.1-1.6,1.21-1.26,2.1-2.8,2.12-2.32,2.37-2.50 **Actual:** 1.1-1.6,1.21-1.26,2.1-2.8,2.12-2.32,2.37-2.50
○	22	Sales	NA NA	Port Based	None	**Untagged**: **Configured:** 1.7-1.14,2.9-2.11 **Actual:** 1.7-1.14,2.9-2.11 **Tagged**: 2.49
○	23	Accounting	NA NA	Port Based	None	**Untagged**: **Configured:** 1.15-1.20,2.33-2.36 **Actual:** 1.15-1.20,2.33-2.36 **Tagged**: 2.49

Figure 81. VLAN Tab

Note
Do not change the VLAN Mode parameter from User Configured. Although the AT-9400 Switches can support a variety of VLAN modes when they are used as stand-alone units, when assembled into a stack they only support just that mode. Furthermore, do not enter a value for the Uplink Port parameter because it is not used in the User Configured mode.

The VLAN List section of the tab lists the VLANs in the stack:

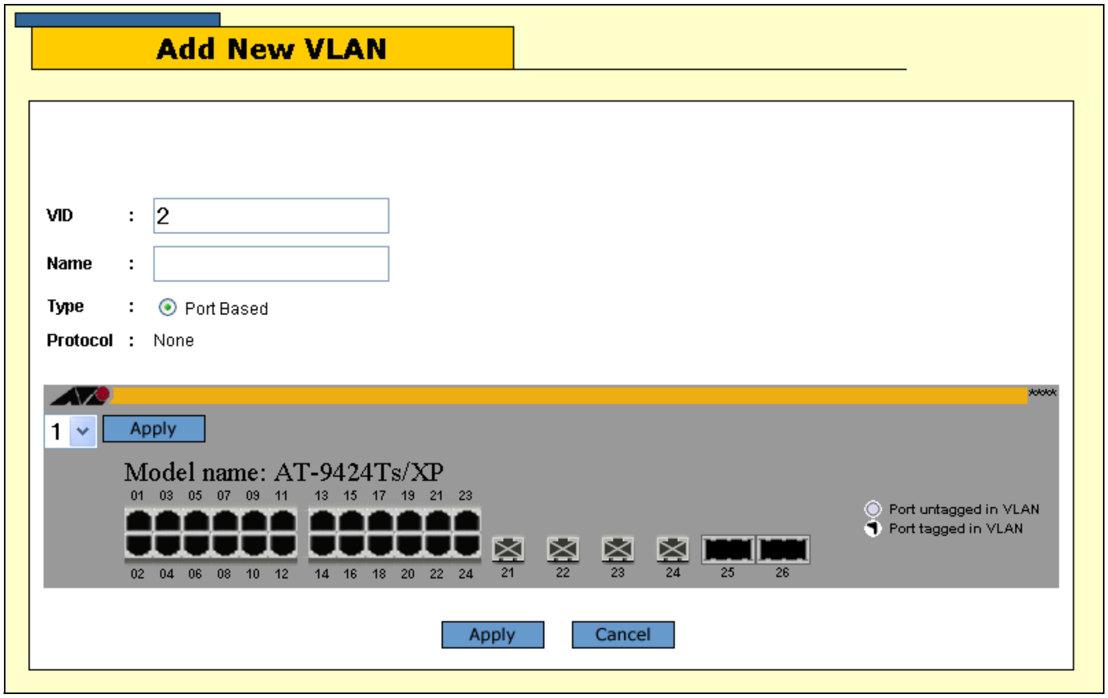
Table 38. VLAN Tab

Column	Definition
VID ID	Displays the ID numbers of the VLANs.
(Client) Name	Displays the names of the VLANs.
Uplink Port	Displays "NA," for Not Applicable, for port-based and tagged VLANs, which are the only type of VLANs supported by a stack.
Type	Displays "Port Based" for port-based and tagged VLANs.
Protocol	Displays "None" for port-based and tagged VLANs.
Member Ports	Displays the untagged and tagged ports of the VLANs. The untagged ports of a VLAN are listed as follows. Configured: The untagged ports that were assigned to the VLAN when it was created or last modified. Actual: The current untagged ports of the VLAN. If you are not using 802.1x Port-based Network Access Control, the Configured and Actual untagged ports of a VLAN will always be the same.

Table 38. VLAN Tab

Column	Definition
Member Ports (Continued)	If you are using 802.1x and assigned a Guest VLAN to an authenticator port or associated a VLAN to an 802.1x supplicant on the authentication server, an untagged port can be in different VLAN than the virtual LAN where it was originally assigned. In these situations, the Configured and Actual port lists can be different, with the Actual list detailing the ports that are currently functioning as untagged ports of the VLAN. For example, if a port is listed as a Configured member of a VLAN, but not as an Actual member, that would mean either the port is currently a part of a Guest VLAN or the supplicant who logged on the port was associated with a VLAN assignment on the authentication server.

4. To add a new VLAN to the stack, click the **Add** button to display the Add New VLAN page shown in Figure 82.



Add New VLAN

VID : 2

Name :

Type : ● Port Based

Protocol : None

Model name: AT-9424Ts/XP

Figure 82. Add New VLAN Page

Note
Stacks do not use the Type or Protocol parameter.

5. Click the **VID** field and enter an ID number for the VLAN. The range is 2 to 4096. The default is the next available VID number in the stack.

6. Click the **Name** field and enter a name of up to fifteen alphanumeric characters for the new VLAN. To make the VLAN easy to identify, select a name that reflects the function of the user’s of the VLAN (for example, Sales or Accounting). Spaces and special characters, such as asterisks (*), are not permitted.

7. Click the **Apply** button.

8. To add the ports of the VLAN, go to “Adding or Removing VLAN Ports” on page 214.

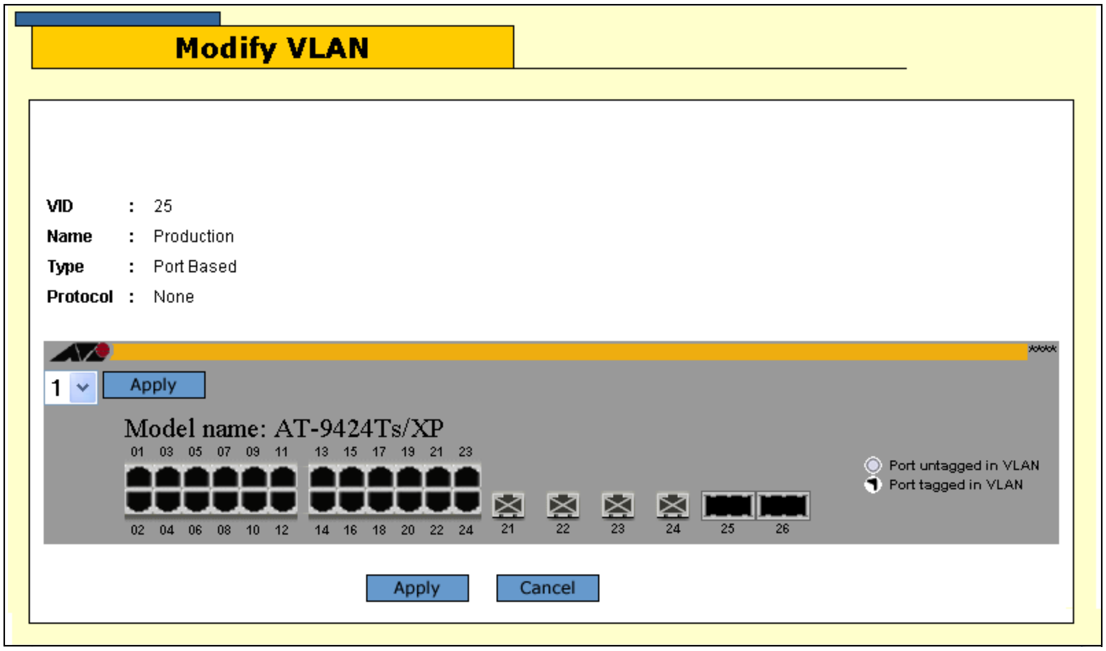
Adding or Removing VLAN Ports

This procedure is used to add or remove ports from tagged or untagged VLANs. Here are a few guidelines:

- You cannot change the VID of a VLAN. If you need to change a VLAN’s ID number, you have to delete and recreate the VLAN.
- To change the name of a VLAN, you have to use the command line commands.
- A port that is set to the supplicant or authenticator role in 802.1x Port-based Network Access Control cannot be moved to a different VLAN until you change its role to “None.” For instructions, refer to “Setting the Port Roles” on page 222.

To add or remove ports from a VLAN:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 2** button.
3. Click the **VLAN** tab, shown in Figure 81 on page 210.
4. Click the radio button of the VLAN you want to modify. You can modify only one VLAN at a time.
5. Click the **Modify** button to display the Modify VLAN popup window. An example of the window is shown in Figure 83.



VID : 25
Name : Production
Type : Port Based
Protocol : None

Figure 83. Modify VLAN Window

6. Use the stack ID pull-down menu in the switch image to select the ID number of a switch that has ports you want to add or remove from the VLAN, and click the **Apply** button. (If the switch is already displayed, skip this step.)

7. In the switch image click the ports you want to add or remove from the VLAN. Clicking a port toggles it through the settings in Table 39.

Table 39. Port Settings in a VLAN

Setting	Definition
□	The port is an untagged member of the VLAN.
⚑	The port is a tagged member of the VLAN.
■	The port is not a member of the VLAN.

8. Click the **Apply** button.

9. To add or remove ports from the VLAN from other switches in the stack, repeat this procedure starting with step 3.

10. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Deleting VLANs

This procedure is used to delete port-based and tagged VLANs from a stack. Here are a few guidelines:

- You cannot delete the Default_VLAN.
- To delete a VLAN that has one or more routing interfaces, you have to delete the routing interfaces first. Deleting a routing interface has to be performed from the command line commands.
- All of the untagged ports in a deleted VLAN are returned to the Default_VLAN as untagged ports.
- When you delete a VLAN, any static MAC addresses assigned to its ports become obsolete and should be deleted from the MAC address table. For instructions, refer to “Deleting Unicast or Multicast MAC Addresses” on page 67.

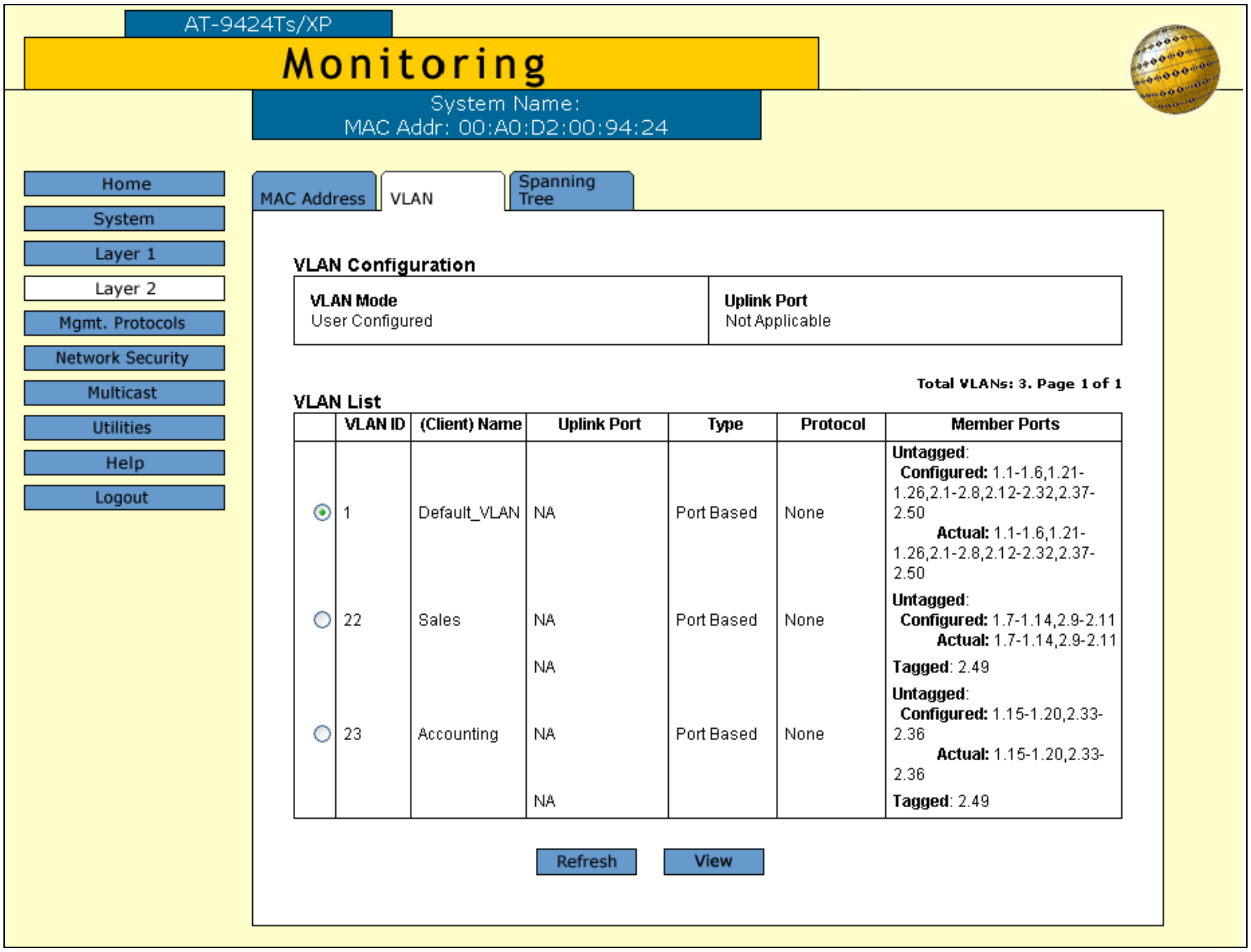
To delete a port-based or tagged VLAN from a stack:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Layer 2** button.
3. Select the **VLAN** tab, shown in Figure 81 on page 210.
4. Click the radio button of the VLAN you want to delete. You can delete only one VLAN at a time. (You cannot delete the Default_VLAN.)
5. Click the **Remove** button.
6. At the confirmation prompt click **OK** to delete the VLAN or **Cancel** to cancel the procedure. If you click OK, the VLAN is deleted from the stack and its untagged ports are returned to the Default_VLAN.
7. To save your changes in the master configuration file, click **Save Config** in the Configuration menu.

Displaying VLANs

To display the VLANs from an operator session:

1. From the Home page, click the **Monitoring** button.
2. From the Monitoring menu, click the **Layer 2** button.
3. Click the **VLAN** tab shown in Figure 84.



System Name:
MAC Addr: 00:A0:D2:00:94:24

VLAN Configuration

VLAN Mode User Configured	**Uplink Port** Not Applicable

Total VLANs: 3. Page 1 of 1

VLAN List

	VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Member Ports
●	1	Default_VLAN	NA	Port Based	None	**Untagged**: **Configured:** 1.1-1.6,1.21-1.26,2.1-2.8,2.12-2.32,2.37-2.50 **Actual:** 1.1-1.6,1.21-1.26,2.1-2.8,2.12-2.32,2.37-2.50
○	22	Sales	NA NA	Port Based	None	**Untagged**: **Configured:** 1.7-1.14,2.9-2.11 **Actual:** 1.7-1.14,2.9-2.11 **Tagged**: 2.49
○	23	Accounting	NA NA	Port Based	None	**Untagged**: **Configured:** 1.15-1.20,2.33-2.36 **Actual:** 1.15-1.20,2.33-2.36 **Tagged**: 2.49

Figure 84. VLAN Tab (Monitoring)

Refer to Table 38 on page 211 for information about this tab.

Section VI

Port Security

This section has this chapter:

Chapter 14

802.1x Port-based Network Access Control

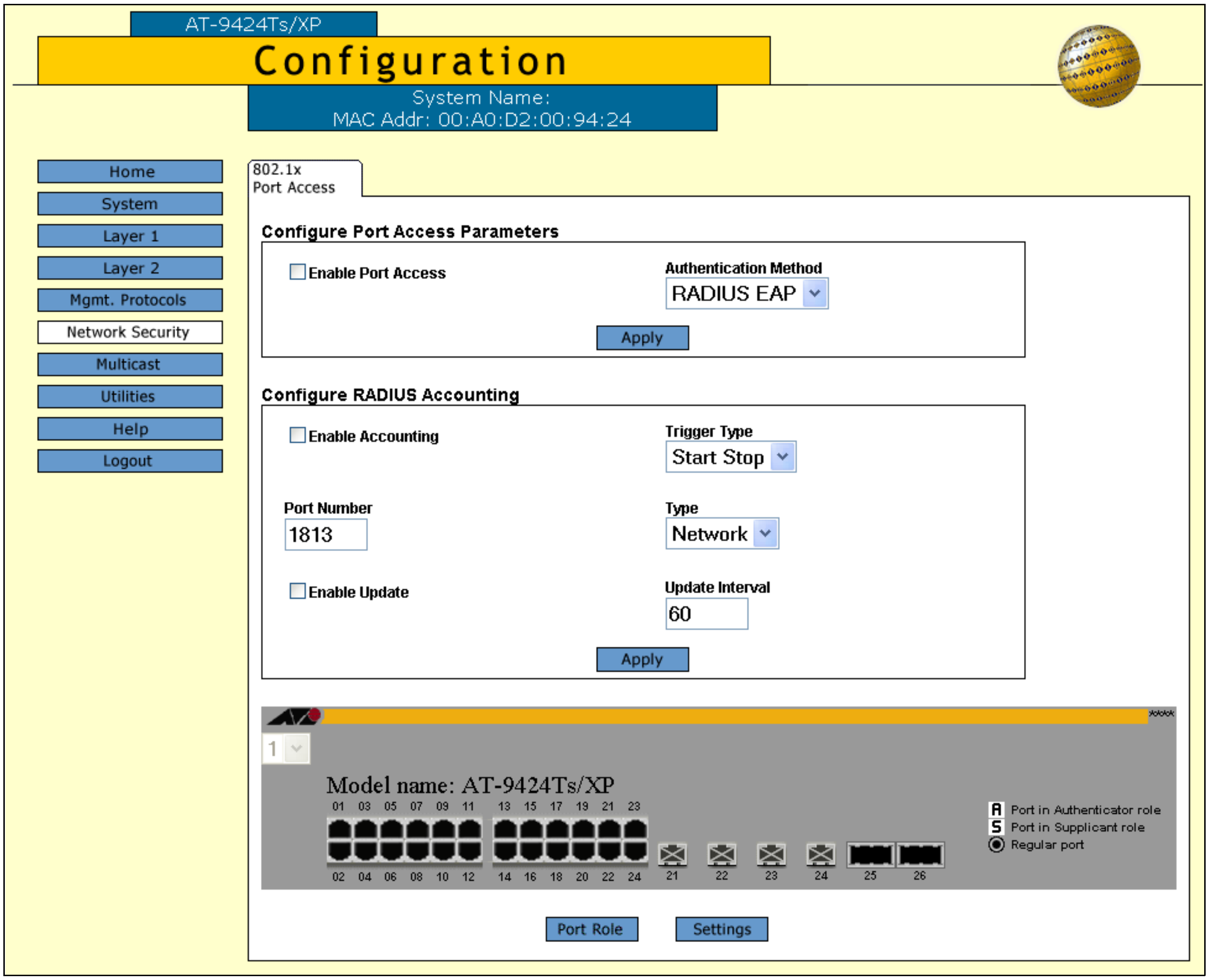
This chapter contains instructions on how to configure the 802.1x Port-based Network Access Control feature on the stack. The chapter contains the following sections:

Note
You cannot configure the RADIUS authentication client on the stack from the web browser windows. Rather, that management function has to be performed from the command line commands. For instructions, refer to the *AT-S63 Command Line User's Guide for AT-9400 Stacks*.

Setting the Port Roles

To set the authenticator or supplicant roles on the ports in the stack:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Network Security** button to display the **802.1x Port Access** tab shown in Figure 85.



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

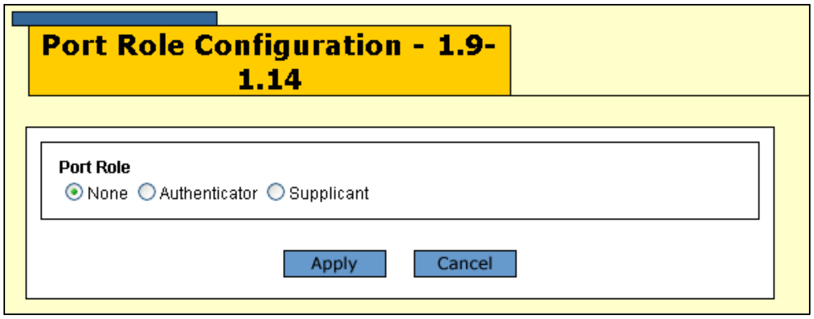
Figure 85. 802.1x Port Access Tab

The roles of the ports are displayed in the image of the switch. An “A” indicates an authenticator port and an “S” a supplicant port. 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.

3. In the switch image, use the Stack ID pull-down menu to choose the switch that has the authenticator ports you want to configure. If the switch is already displayed, skip this step.

4. Click the port that you want to configure. A selected port turns white. You can configure more than one port at a time.

5. Click the **Port Role** button to display the popup window in Figure 86.



Port Role Configuration - 1.9-1.14

Port Role

● None ○ Authenticator ○ Supplicant

Figure 86. Port Role Configuration Window

6. Select the new role for the port. A port can have only one port role at a time. The port role are described in this table.

Table 40. 802.1 Port Roles

Port Role	Definition
None	The port does not participate in 802.1x port-based access control. This is the default setting.
Authenticator	The port functions as an authenticator. This is the appropriate setting if the port is connected to a supplicant.
Supplicant	The port functions as an supplicant. This is the appropriate setting if the port is connected to an authenticator.

7. Click **Apply**.

   The new role is immediately implemented on the port.

8. To save your changes in the master configuration file, click **Save Config** in the Configuration menu.

   To enable or disable port-based access control, go to “Enabling or Disabling 802.1x Port-based Network Access Control” on page 224. To configure authenticator port settings, go to “Configuring the Authenticator Port Parameters” on page 225. To configure supplicant port settings, go to “Configuring the Supplicant Port Parameters” on page 232.

Enabling or Disabling 802.1x Port-based Network Access Control

To enable or disable 802.1x Port-based Network Access Control:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab shown in Figure 85 on page 222.

3. Click the **Enable Port Access** check box. A check in the box means the feature is activated on the switch and no check means the feature is disabled.

4. Click the **Apply** button. The new status of the 802.1x Port-based Network Access Control is immediately implemented on the stack.

5. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the Authenticator Port Parameters

> **Note**
> A port must be set to the authenticator role before you can configure its parameters. For instructions, refer to "Setting the Port Roles" on page 222.

To configure the 802.1x parameters on authenticator ports:

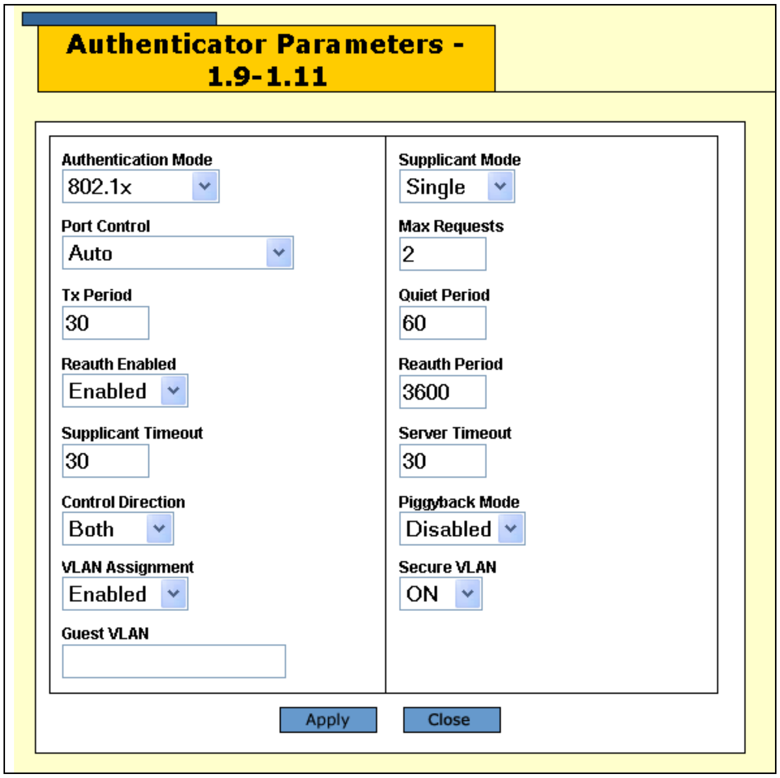
1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab in Figure 85 on page 222.

3. In the switch image, use the Stack ID pull-down menu to choose the switch that has the authenticator ports you want to configure. If the switch is already displayed, skip this step.

4. In the switch image, click the authenticator ports you want to configure. Selected ports turns white.

5. Click the **Settings** button to display the window in Figure 87.



Authenticator Parameters - 1.9-1.11

Authentication Mode: 802.1x
Port Control: Auto
Tx Period: 30
Reauth Enabled: Enabled
Supplicant Timeout: 30
Control Direction: Both
VLAN Assignment: Enabled
Guest VLAN:
Supplicant Mode: Single
Max Requests: 2
Quiet Period: 60
Reauth Period: 3600
Server Timeout: 30
Piggyback Mode: Disabled
Secure VLAN: ON

Figure 87. Authenticator Parameters Page

6. Configure the parameters and click the **Apply** button. The parameters are described in this table.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
Authenticator Mode	Sets the authenticator mode of an authenticator port. This parameter has the following values: 802.1x - Specifies 802.1x username and password authentication. With this authentication method the supplicant must provide, either manually or automatically, a username and password to the authenticator port. This authentication method requires 802.1x client software on the supplicant nodes. MAC Based - Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames received from a supplicant and automatically sends the address as both the username and password of the supplicant to the authentication server. Supplicant nodes do not need 802.1x client software for this authentication method.
Supplicant Mode	Sets the supplicant mode of an authenticator port. The possible settings are: Single - Configures the authenticator port to accept only one authentication. This mode should be used together with the piggy-back mode. When an authenticator port is set to the Single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
Supplicant Mode (continued)	Multiple - Configures the port to accept up to 20 authentications. Every client using an authenticator port in this mode must have a username and password.
Port Control	The possible settings are: Auto - Activates 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. 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. A supplicant connected to an authenticator port set to force-authorized must have 802.1x client software if the port's authenticator mode is 802.1x. Though the force-authorized setting prevents an authentication exchange, the supplicant must still have the client software to forward traffic through the port. Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
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 default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.
TX Period	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.
Quiet Period	Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.
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. The options are Enabled or Disabled. The default is Enabled.
Reauth Period	Specifies the time period in seconds between reauthentications of the client when the Reauth Enabled option is set to Enabled. The default value is 3600 seconds. The range is 1 to 65,535 seconds.
Supplicant Timeout	Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
Server Timeout	Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.
Control Direction	Specifies how the port handles 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 only accepts EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, are discarded until the supplicant has logged in. The options are: Ingress - A port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client, but forwards all egress broadcast and multicast traffic to the same client. Both - A port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the client logs in. This is the default.
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. The port forwards all packets, regardless of the client, after one client has been authenticated. If set to Disabled, the switch port forwards only those packets from the client who was authenticated and discards packets from all other users.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
VLAN Assignment	Controls whether an authenticator port uses the VLAN assignments returned by a RADIUS server. Options are: Enabled - Specifies that the authenticator port is to use the VLAN assignment returned by the RADIUS server when a supplicant logs on. This is the default setting. The port automatically moves to the designated VLAN after the supplicant successfully logs on. Disabled - Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even if the RADIUS server returns a VLAN assignment when a supplicant logs on. This is the default setting.
Secure VLAN	Controls the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode. Possible settings are: On - Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting. Off - Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

Table 41. 802.1 Authenticator Port Parameters

Parameter	Definition
Guest VLAN	Specifies the VID of a Guest VLAN. The authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN. You can specify a Guest VLAN by either its name or VID. To remove a Guest VLAN without assigning a new one, delete the name or VID of the assigned VLAN.

7. To configure the parameters of the authenticator ports on the other switches in the stack, repeat this procedure starting with step 3.

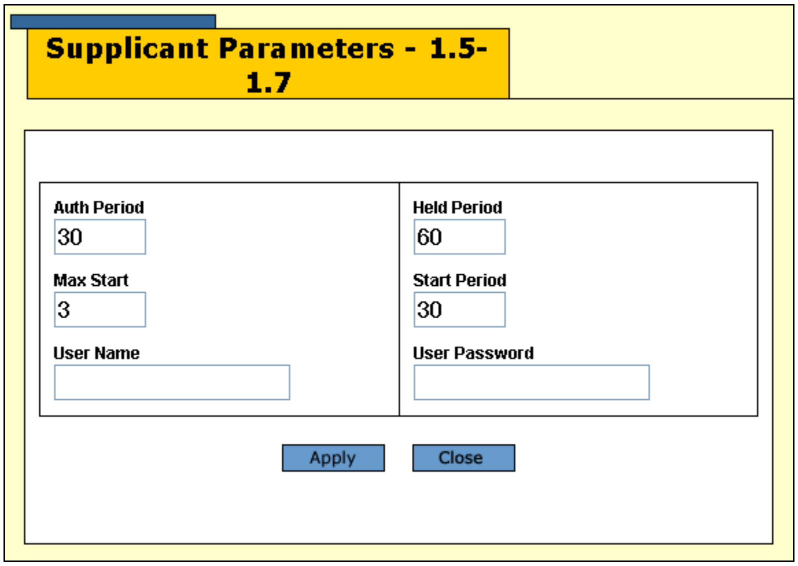
8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Configuring the Supplicant Port Parameters

Note
A port must be set to the supplicant role before you can configure its parameters. For instructions, refer to “Setting the Port Roles” on page 222.

To configure the 802.1x parameters on supplicant ports:

1. From the Home page, click the **Configuration** button.
2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab in Figure 85 on page 222.
3. In the switch image, use the Stack ID pull-down menu to choose the switch that has the supplicant ports you want to configure. If the switch is already displayed, skip this step.
4. In the switch image, click the supplicant ports you want to configure. You can configure more than one supplicant port at a time. Selected ports turn white.
5. Click the **Settings** button to display the window in Figure 88.



Supplicant Parameters - 1.5-1.7

Auth Period: 30

Held Period: 60

Max Start: 3

Start Period: 30

User Name:

User Password:

Figure 88. Supplicant Parameters Window

6. Configure the parameters and click the **Apply** button: The parameters are described in this table

Table 42. Supplicant Port Parameters

Parameter	Definition
Auth Period	Specifies the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 300 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. After 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 sends 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 from be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case sensitive.

Table 42. Supplicant Port Parameters

Parameter	Definition
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 from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case sensitive.

7. To configure the parameters of the supplicant ports on the other switches in the stack, repeat this procedure starting with step 3.

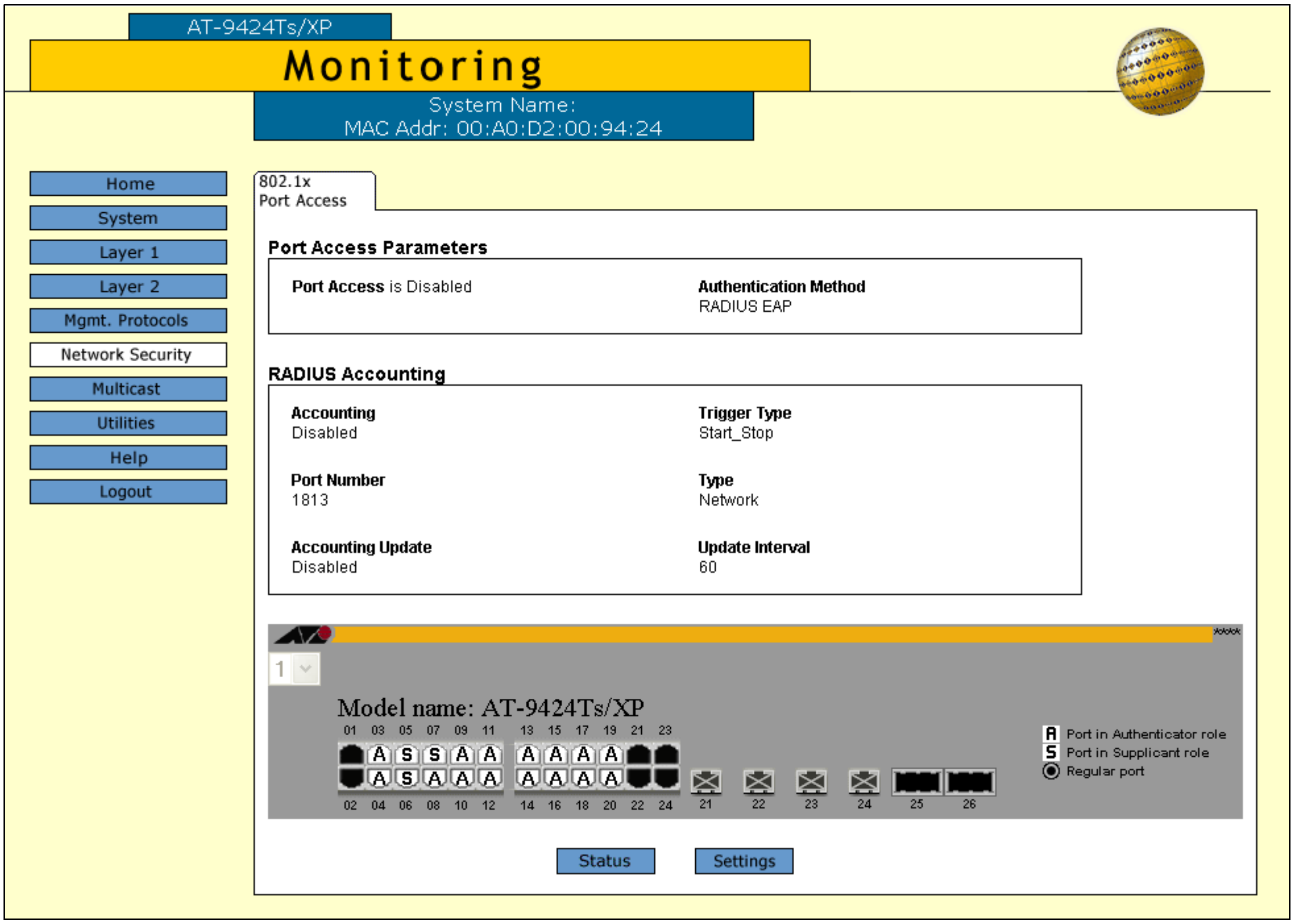
8. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying the Port Parameters and Port Status

To display the parameters or the status of authenticator and supplicant ports:

1. From the Home page, select the **Monitoring** button.

2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab shown in Figure 89.



Port Access Parameters

Port Access is Disabled

Authentication Method
RADIUS EAP

RADIUS Accounting

Accounting
Disabled

Trigger Type
Start_Stop

Port Number
1813

Type
Network

Accounting Update
Disabled

Update Interval
60

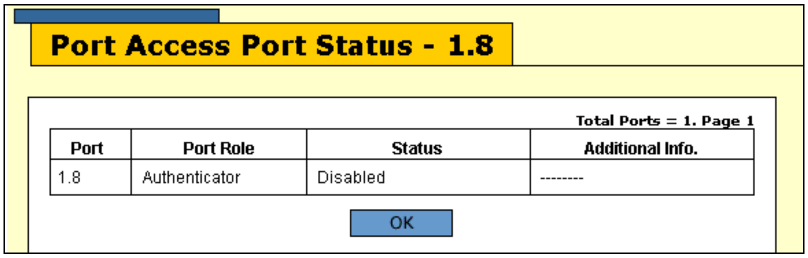
Figure 89. 802.1x Port Access Tab (Monitoring)

The port roles are display in the switch image. Ports with an “A” are authenticator ports and those with an “S” are supplicant ports. Ports that are black have not been assigned a port role and do not participate in port-based access control. This is the default setting for a port.

3. In the switch image, use the Stack ID pull-down menu to choose the switch that has the ports you want to view. If the switch is already displayed, skip this step.

4. To view the parameter settings of an authenticator or supplicant port, click the port and click the **Settings** button. You can view more than one port at a time. The authenticator parameters are described in Table 41 on page 226 and the supplicant parameters in Table 42 on page 233.

5. To view the status of an authenticator or supplicant port, click the port and the **Status** button. You can display the status of more than one port at a time. The Port Access Port Status page is shown in Figure 90.



Port Access Port Status - 1.8

Total Ports = 1. Page 1

Port	Port Role	Status	Additional Info.
1.8	Authenticator	Disabled	--------

Figure 90. Port Access Port Status Window

The columns of information in the window are described in this table.

Table 43. 802.1x Port Status Window

Column	Definition
Port	Displays the port number.
Port Role	Displays the port’s role of None, Authenticator, or Supplicant.
Status	Displays the status of the port. The possible states of authenticator ports are listed here: Aborting Authenticated Authenticating Connecting Disconnected Force_Auth Force_Unauth Held Initialize

Table 43. 802.1x Port Status Window

Column	Definition
Status (continued)	The possible states of supplicant ports are listed here: Acquired Authenticated Authenticating Connecting Disconnected Held Logoff
Additional Info	This field displays the MAC address of an authenticated node after the node has been authenticated by the RADIUS server.

Configuring RADIUS Accounting

To configure RADIUS accounting:

1. From the Home page, click the **Configuration** button.

2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab shown in Figure 85 on page 222.

3. Configure the parameters in the Configure RADIUS Accounting section of the tab and click the **Apply** button. The parameters are described in this table.

Table 44. Configure RADIUS Accounting Section

Parameter	Definition
Enable Accounting	Activates or deactivates RADIUS accounting on the switch. Select Enabled to activate the feature or Disabled to deactivate it. The default is Disabled.
Trigger Type	Specifies the action that prompts the switch to send accounting information to the RADIUS server. The possible settings are: Start_Stop - The switch sends accounting information when a client logs on or 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. You cannot change this value.
Enable Update	Controls whether the switch is to send interim accounting updates to the RADIUS server. A check in the box indicates that updating is enabled. No check in the box means that updating is disabled.

Table 44. Configure RADIUS Accounting Section

Parameter	Definition
Update Interval	Specifies the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

4. To save your changes in the master configuration file, click the **Save Config** button in the Configuration menu.

Displaying the RADIUS Accounting Settings

To display the RADIUS accounting settings:

1. From the Home page, click the **Monitoring** button.
2. From the Configuration menu, click the **Network Security** button to display the 802.1x Port Access tab shown in Figure 85 on page 222. The information in the RADIUS Accounting section of the tab is described in this table.

Table 45. 802.1x Port Access Tab (Monitoring)

Parameter	Definition
Accounting	The status of RADIUS accounting, either Enabled or Disabled.
Trigger Type	The action that causes the switch to send accounting information to the RADIUS server. The possible settings 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	The UDP port for RADIUS accounting.
Type	The type of RADIUS accounting. The default is Network.
Accounting Update	Whether or not the switch sends interim accounting updates to the RADIUS server. The options are Enabled or Disabled.
Update Interval	The intervals, in seconds, at which the switch sends interim accounting updates to the RADIUS server.

Index